O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI

A K A D E M I Y A

AXBOROT XAVFSIZLIGI ASOSLARI

(Ma’ruzalar kursi)

Toshkent – 2013

O‘zbekiston Respublikasi IIV Akademiyasining
Tahririyat-noshirlik ha’yatida ma’qullangan

Mualliflar jamoasi:

fizika-matematika fanlari nomzodi, katta ilmiy xodim **I. M. Karimov;**
fizika-matematika fanlari nomzodi, dotsent **N. A. Turgunov;**
texnika fanlari nomzodi, dotsent **F. Kadirov;**
texnika fanlari nomzodi, dotsent **X.K. Samarov;**
fizika-matematika fanlari nomzodi **A. A. Iminov;**
fizika-matematika fanlari nomzodi **M. X. Djamatov**

Taqrizchilar:

Toshkent Axborot texnologiyalari universiteti axborot xavfsizligi kafedrasi mudiri,
texnika fanlari nomzodi **S.Y. Yusupov;**

O‘zbekiston Respublikasi IIV Axborot markazi boshlig‘i **A.X.Xakimov**

A-95 **Axborot xavfsizligi asoslari:** Ma’ruzalar kursi / fizika-matematika fanlari nomzodi, katta ilmiy xodim I.M.Karimovning umumiy tahriri ostida. – T.: O‘zbekiston Respublikasi IIV Akademiyasi, 2013. – 123 b.

Ma’ruzalar kursi axborot xavfsizligini ta’minlashning nazariy asoslari, asosiy tushunchalari, tashkiliy va boshqaruv tamoyillari to‘g‘risidagi bilimlarni shakllantirish, O‘zbekiston Respublikasida axborotni muhofaza qilishning davlat tizimining tashkiliy asoslari va vazifalarini o‘rganish, tinglovchilarga axborot xavfsizligi va ma’lumotlarni muhofaza qilish sohasidagi xalqaro tajriba, axborot xavfsizligini ta’minlashning usul va vositalari hamda ma’lumotlarni muhofaza qilishning kompleks tizimlari bilan tanishtirish, shaxs, jamiyat va davlatning axborot xavfsizligi, davlat organlarining axborot xavfsizligini ta’minlash sohasidagi asosiy faoliyat yo‘nalishlari, axborot xavfsizligining obyektlari, tahdidlar va ularning manbalari, axborotlarni kriptografik va texnik himoyalash asoslari, axborotlarni muhofaza qilishning tashkiliy chora-tadbirlari, ma’lumotlarni muhofaza qilish va axborot xavfsizligini ta’minlashning usul va vositalari, ma’lumotlarning chiqib ketish kanallari va ularning oldini olish yo‘llari haqida nazariy bilimlarni chuqurlashtirish imkonini beradi.

IIV Akademiyasi tinglovchilariga, professor-o‘qituvchilarga, tadqiqotchilarga hamda huquqni muhofaza qilish idoralari va boshqa turdosh sohalarda faoliyat yuritayotgan mutaxassislarga mo‘ljallangan.

BBK 73ya73

«*Fuqarolarning axborot sohasidagi huquq va erkinliklarini ta’minlash masalasi insonning axborot olish, axborotni va o‘z shaxsiy fikrini tarqatish huquqi va erkinligini o‘zida mujassam etgan bo‘lib, bu O‘zbekistonda demokratik jamiyat asoslarini barpo etishning muhim sharti, ta’bir joiz bo‘lsa, tamal toshi hisoblanadi*»[1].

Islom Karimov

KIRISH

Ma’lumki, har qanday davlatning axborot resurslari uning iqtisodiy va harbiy salohiyatini belgilovchi omillaridan biri hisoblanadi. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirilishini ta’minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha ilg‘or axborot-kommunikatsiyalar texnologiyalarini qo‘llash keng ko‘lamda amalga oshiriladi.

Axborotlashgan jamiyat tezlik bilan shakllanib bormoqda. Axborot dunyosida davlat chegaralari degan tushuncha yo‘qolib bormoqda. Jahon kompyuter tarmog‘i davlat boshqaruvini tubdan o‘zgartirmoqda.

Hududiy joylashishidan qat’i nazar, kundalik hayotimizga turli xildagi axborotlar Internet xalqaro kompyuter tarmog‘i orqali kirib keldi. Shuning uchun ham mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi.

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[2].

---

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

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

«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»[1]. Darhaqiqat, 2002-yil 12-dekabrda qabul qilingan bu qonunda[2] axborot xavfsizligini ta’minlash sohasidagi davlat siyosati axborot sohasidagi ijtimoiy munosabatlarni tartibga solishga qaratilgan bo‘ladi hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlash sohasida davlat hokimiyati va boshqaruv organlarining asosiy vazifalari hamda faoliyat yo‘nalishlarini belgilaydi deb belgilangan.

Kompyuter tizimlari va tarmoqlarida axborotni muhofaza qilishi deganda, uzatilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta’minlash maqsadida turli vosita va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

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.

Ushbu ma’ruzalar kursi tinglovchilar va huquqni muhofaza qilish idoralari xodimlariga axborot xavfsizligini ta’minlashga oid nazariy bilimlarni, axborot tizimlarida axborotni muhofaza qilishni tashkil etishning tashkiliy, huquqiy, texnik, kriptografik, apparat-dasturiy usullarini qo‘llashga oid zarur bilimlarni egallash imkonini beradi.

---

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

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

I. AXBOROT XAVFSIZLIGI VA AXBOROTNI MUHOFAZA QILISH

1.1. Axborotni muhofaza qilish, axborot xavfsizligi va uning zamonaviy konsepsiyasi.

1.2. Axborot xavfsizligiga tahdid va uning turlari.

1.3. Axborot xavfsizligi va ma'lumotlarni himoyalash bo'yicha me'yoriy-huquqiy hujjatlar. Axborotni muhofaza qilish sohasida xalqaro standartlar.

Har qanday taraqqiy etgan jamiyat hayotida axborotning ahamiyati uzluksiz ortib bormoqda. Uzoq o'tmishdan davlatning harbiy-strategik ahamiyatiga molik bo'lgan ma'lumotlar qat'iy sir tutilgan va himoyalangan. Hozirgi vaqtda ishlab chiqarish texnologiyalariga va mahsulotlarni sotishga tegishli axborot tovar ko'rinishiga ega bo'lib, ichki va tashqi bozorda unga bo'lgan talab ortib bormoqda. Axborot texnologiyalari avtomatlashtirish va axborotni muhofaza qilish yo'nalishlarida muntazam mukammallashib bormoqda.

Zamonaviy axborot texnologiyalarining taraqqiyoti sanoat shpionaji, kompyuter jinoyatchiligi, konfedensial ma'lumotlarga ruxsatsiz kirish, o'zgartirish, yo'qotish kabi salbiy hodisalar bilan birgalikda kuzatilmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi hisoblanadi. O'zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimi yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o'z ifodasini topmoqda. «Axborotlashtirish to'g'risida», «Davlat sirlarini saqlash to'g'risida», «Elektron hisoblash mashinalari dasturlari va ma'lumotlar bazalarini huquqiy himoya qilish to'g'risida» va boshqa qonunlar hamda bir qator Hukumat qarorlari qabul qilindi va amalga tatbiq etildi.

Axborotni muhofaza qilish axborotni ixtiyoriy ko'rinishda yo'qotishda (o'g'irlash, buzish, qalbakilashtirish) ko'riladigan zararning oldini olishni ta'minlashi lozim. Axborotni muhofaza qilish choralari axborot xavfsizligiga oid amaldagi qonun va me'yoriy hujjatlar asosida va axborotdan foydalanuvchilarning manfaatlariga ko'ra tashkil etilishi zarur. Yuqori darajada axborotni muhofaza qilishni kafolatlash uchun muntazam ravishda murakkab ilmiy-texnik vazifalarni hal etish va himoya vositalarini takomillashtirish talab etiladi.

1.1. Axborotni muhofaza qilish, axborot xavfsizligi va uning zamonaviy konsepsiyasi

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida[1] axborot va uning turlari to‘g‘risida quyidagi ta’riflar keltirilgan:

axborot – manbalari va taqdim etilish shaklidan qat’i nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to‘g‘risidagi ma’lumotlar;

axborotni muhofaza etish – axborot borasidagi xavfsizlikka tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish chora-tadbirlari;

ommaviy axborot – cheklanmagan doiradagi shaxslar uchun mo‘ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar;

hujjatlashtirilgan axborot – identifikatsiya qilish imkonini beruvchi rekvizitlari qo‘yilgan holda moddiy jismda qayd etilgan axborot;

maxfiy axborot – foydalanilishi qonun hujjatlariga muvofiq cheklab qo‘yiladigan hujjatlashtirilgan axborot. Ushbu ta’rif O‘zbekiston Respublikasi Vazirlar Mahkamasining «O‘zbekiston Respublikasi Prezidentining «Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida» 2011-yil 8-iyuldagi PQ–1572-son qarorini amalga oshirish chora-tadbirlari haqida»gi 2011-yil 7-noyabr 296-sonli qarorida quyidagicha ifodalangan: *maxfiy axborot* – O‘zbekiston Respublikasi qonun hujjatlariga muvofiq foydalanish cheklangan, davlat sirlariga mansub axborot mavjud bo‘lmagan hujjatlashtirilgan axborot[2].

Konfedensial axborot – hujjatlashtirilgan axborot, undan foydalanish qonun hujjatlariga muvofiq chegaralanadi[3].

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,

---

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

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

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

ilmiy-texnik, ishlab chiqarishga yoki tijoratga oid hamda maxfiy, konfedensial yoki nomaxfiy bo‘lishi mumkin.

O‘zbekiston Respublikasining 1993-yil 7-maydagi 848-XII-sonli «Davlat sirlarini saqlash to‘g‘risida»gi qonunning[1] 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».

Mazkur qonunning 3-moddasida davlat sirlarining toifalari 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».

Axborot xavfsizligi tushunchasi, uning tashkil etuvchilari tavsifi. Axborot xavfsizligi deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan qilingan ta’sirlardan axborot va uni qo‘llab-quvvatlab turuvchi infrastukturaning himoyalanganligi tushuniladi. Bunday ta’sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo‘llab quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin.

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida[2] axborot xavfsizligi *axborot borasidagi xavfsizlik* deb belgilangan va u

---

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

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

axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

Axborot sohasida *shaxs manfaatlari* fuqarolarning axborotdan foydalanishga doir konstitutsiyaviy huquqlarini amalga oshishida, qonunda taqiqlanmagan faoliyat bilan shug‘ullanishida hamda jismoniy, ma’naviy va intellektual rivojlanishda axborotlardan foydalanishlarida, shaxsiy xavfsizlikni ta’minlovchi axborot himoyasida namoyon bo‘ladi.

Axborot sohasida *jamiyat manfaatlari* bu sohada shaxs manfaatlarini ta’minlashda, demokratiyani mustahkamlashda, ijtimoiy huquqiy davlatni qurishda, ijtimoiy hamjihatlikni qo‘llab-quvvatlashda o‘z aksini topadi.

Axborot sohasida *davlat manfaatlari* milliy axborot infrastrukturasining rivojlanishiga sharoitlar yaratishda, axborot olish sohasida shaxs va fuqarolarning konstitutsiyaviy huquq va erkinliklarini amalga oshishida, O‘zbekistonning hududiy birligini, suverenitetini va konstitutsiyaviy tuzumining mustahkamligini, siyosiy, iqtisodiy va ijtimoiy barqarorligini ta’minlash maqsadida axborotdan foydalanishda, qonuniylik va huquq tartibotni qat’iy amalga oshishida, o‘zaro tenglik va o‘zaro manfaatdorlikdagi xalqaro hamkorlikni rivojlantirishda ifodalanadi.

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

Bugungi kunda axborot xavfsizligini ta’minlaydigan uchta asosiy tamoyil mavjud:

– *ma’lumotlar butunligi* – axborotni yo‘qotilishiga olib keluvchi buzilishlardan, shuningdek ma’lumotlarni mualliflik huquqi bo‘lmagan holda hosil qilish yoki yo‘q qilishdan himoya qilish;

– axborotning *konfedensialligi*. Axborot va uning tashuvchisining holatini belgilaydi va unda axborot bilan ruxsatsiz tanishishning yoki uni ruxsatsiz hujjatlashtirishning (nusxa ko‘chirishning) oldini olish ta’minlangan bo‘ladi;

– foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan *foydalana olishliklari*.

Ta’kidlash joizki, ayrim faoliyat sohalari (bank va moliya institutlari, axborot tarmoqlari, davlat boshqaruv tizimlari, mudofaa va maxsus tuzulmalar) ularda ko‘riladigan masalalarning muhimligi va xarakteriga ko‘ra, ularning axborot tizimlari faoliyati ishonchliligiga nisbatan yuqori talablar va xavfsizlik bo‘yicha maxsus choralar ko‘rilishini talab etadi.

Axborot xavfsizligining milliy xavfsizlik tizimidagi o‘rni. XXI asrda shaxs, jamiyat va davlat taraqqiyotida axborot resurslari va texnologiyalarining rolini ortishi natijasida O‘zbekistonda 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, balki xavfsizlik sohasidagi barcha xavfsizlik obyektlarining asosiy elementlari hamdir;

– 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 erishishning 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 hamda 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 ruxsatsiz 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 himoyalanganligi;

– 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.

Axborotni muhofaza qilish – axborot xavfsizligining (ma’lumotlarning butunligi, foydalana olish va zarur bo‘lganda, ma’lumotlarni kiritish, saqlash, qayta ishlash va uzatishda foydalaniluvchi axborot va uning zaxiralari konfedensialligi) muhim jihatlarini ta’minlashga yo‘naltirilgan tadbirlar majmuidir.

Xavfsiz tizimda tegishli apparat va dasturiy vositalardan foydalanib, axborotni o‘qish, yozish, hosil qilish va o‘chirish huquqiga ega shaxslar yoki ular nomidan amalga oshiradigan jarayonlar orqali axborotdan foydalana olish boshqariladi.

Ma’lumki, absolut xavfsiz tizimlar mavjud emas, lekin «ishonish mumkin bo‘lgan tizim» ma’nosidagi ishonchli tizimlardan foydalaniladi. Yetarlicha apparat va dasturiy vositalardan foydalanib, bir vaqtning o‘zida turli maxfiylik darajasidagi ma’lumotlarni foydalanuvchilar guruhi tomonidan foydalanish huquqlarini buzmagan holda qayta ishlash imkonini beruvchi tizim ishonchli hisoblanadi.

Ishonchlilikni baholovchi asosiy mezonlar – bu xavfsizlik siyosati va kafolatlanganlik.

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.

Kafolatlanganlik himoyaning passiv qismi bo‘lib, tizimdan foydalanishda unga bo‘lgan ishonch darajasini ifodalaydi.

Ishonchli tizimda xavfsizlikka taalluqli barcha jarayonlar ro‘yxatga olib borilishi kerak.

---

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

Axborotni muhofaza qilish tushunchasi axborot xavfsizligi tushunchasi bilan chambarchas bog‘liq.

Tor ma’noda axborotni muhofaza qilish deganda axborotni yig‘ish, uzatish, qayta ishlash va saqlash jarayonida uning xavfsizligi (konfedensialligi va butunligi)ni ta’minlashga qaratilgan tadbirlar va harakatlar majmui tushuniladi. Bu ta’rif axborotni muhofaza qilish va axborot xavfsizligi tushunchalarining bir-biriga yaqin ekanligini bildiradi.

Axborot xavfsizligi – bu uzatiluvchi, yig‘iluvchi va saqlanuvchi axborotning xususiyati (holati) bo‘lib, uning tashqi muhit (inson va tabiat) va ichki tahdidlardan himoyalanganlik darajasini xarakterlaydi.

Axborotni muhofaza qilish keng ma’noda axborot xavfsizligiga tahdidni oldini olish va ularning asoratlarini yo‘q qilishga qaratilgan tashkiliy, huquqiy va texnik choralar kompleksini bildiradi.

Axborotni muhofaza qilish axborotga bo‘lgan salbiy ta’sir manbalarini hamda sabab va sharoitlarni aniqlash va bartaraf etish ma’nosini anglatadi. Bu manbalar axborot xavfsizligiga tahdidlarni tashkil etadi.

Axborotni muhofaza qilish quyidagilarga yo‘naltirilgan:

– axborot xavfsizligini ta’minlash bo‘yicha tahdidlarning oldini olish;

– tizimli tahlil va nazorat orqali real va ehtimoli katta bo‘lgan tahdidlarni aniqlash va ularni o‘z vaqtida oldini olish choralari;

– aniq tahdidlar va jinoiy harakatlarni aniqlash maqsadida tahdidlarni topish;

– jinoiy harakatlarni bartaraf etish, shuningdek aniq jinoiy harakatlarni hamda tahdidlarni yo‘q qilish bo‘yicha choralar ko‘rish;

– tahdid va jinoiy harakatlarning oqibatlarini yo‘q qilish va mavqeini saqlash.

Ushbu barcha usullarning maqsadi axborot resurslarini noqonuniy tahdidlardan himoya qilish va quyidagilarni ta’minlashdan iborat:

– konfedensial axborotlarning tarqab ketishini oldini olish;

– konfedensial axborot manbalariga noqonuniy kirishni taqiqlash;

– axborotning butunligi, to‘liqligi va undan foydalana olishni saqlash;

– axborot konfedensialligiga rioya qilish;

– mualliflik huquqlarini ta’minlash.

Yuqoridagilarni e’tiborga olib, axborotni muhofaza qilish deganda davlat, jamiyat va shaxslarning axborot xavfsizligini ta’minlashga yo‘naltirilgan usul, vosita va choralar majmuini tushunish mumkin.

1.2. Axborot xavfsizligiga tahdid va uning turlari

Axborotni muhofaza qilishning maqsadi va konseptual asoslari. Umuman olganda *axborotni muhofaza qilishning maqsadini* quyidagicha ifodalash mumkin:

– axborotni tarqab ketishi, o‘g‘irlanishi, buzilishi, qalbakilashtirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk obyekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfedensialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda subyektlarning huquqlarini ta’minlash.

Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan konsepsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

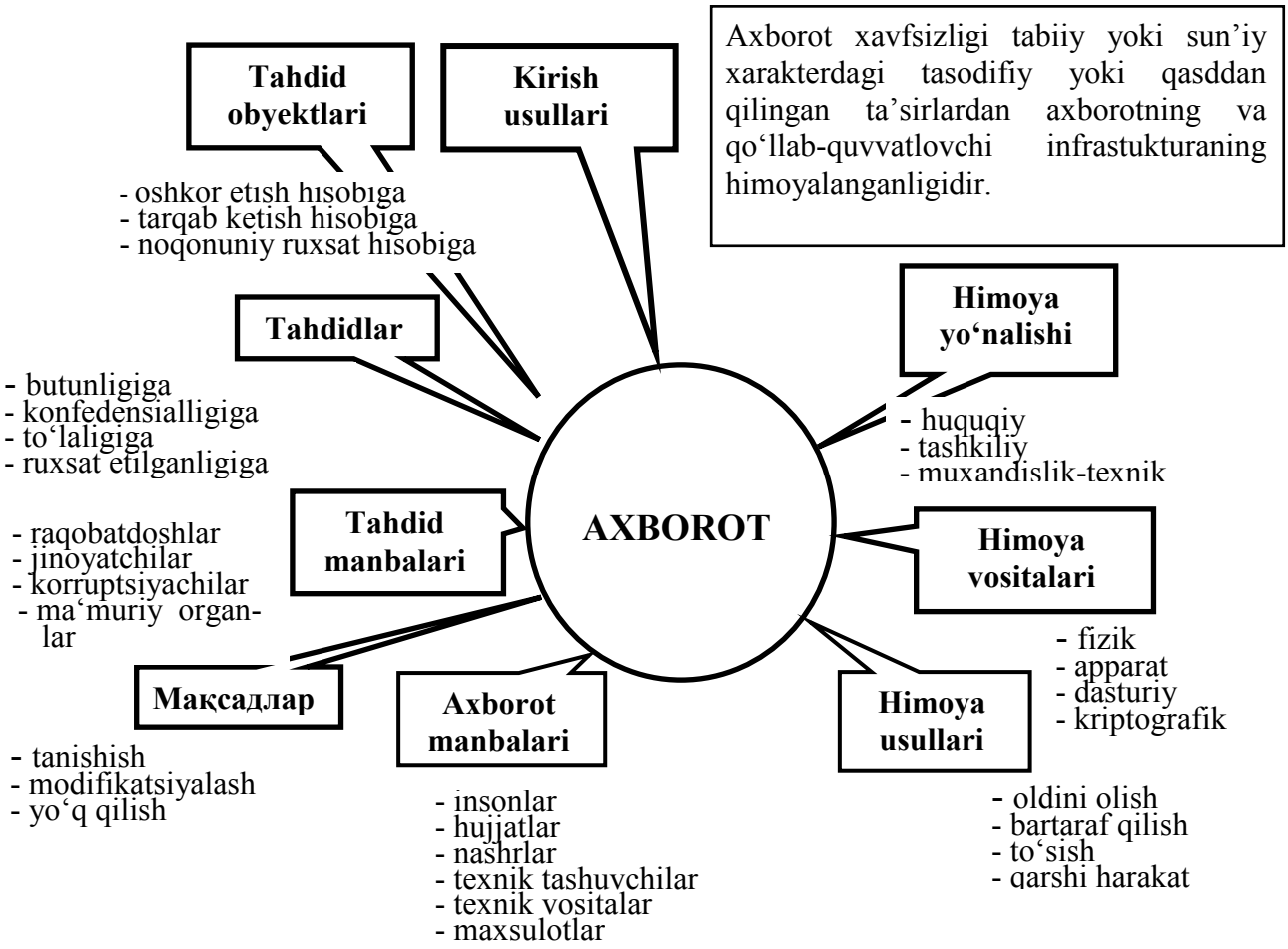
– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– axborotni muhofaza qilish masalalarini hal etishga ixtisoslashtirilgan tashkilotlarning mavjudligi;

– ushbu muammoga oid yetarlicha aniq ifodalangan qarashlar tizimi;

– yetarlicha amaliy tajriba va boshqalar.

Biroq, xorijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendensiyasiga ega bo‘lib bormoqda.



Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi. Umumiy yo'nalishga ko'ra axborot xavfsizligiga tahdidlar quyidagilarga bo'linadi:

– O'zbekistonning ma'naviy ravnaqi sohalarida, ma'naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

– mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig'ish, saqlash va samarali foydalanishni ta'minlashga nisbatan tahdidlar;

– Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining me'yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.

Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchini ko‘rib chiqish maqsadga muvofiq:

1) axborot;

2) texnik va dasturiy vositalar;

3) xizmat ko‘rsatuvchi personal va foydalanuvchilar.

Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida hal etilishi zarur.

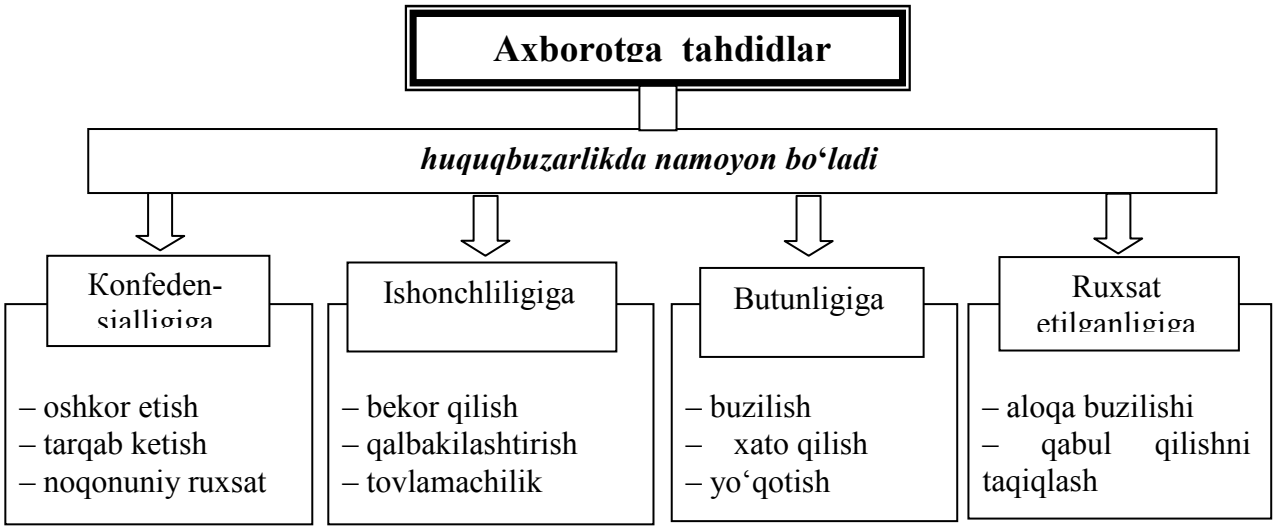
Axborot tarqab ketishiga konfedensial ma’lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi.

Tahdidning uchta ko‘rinishi mavjud.

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgartirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgartirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqonuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisoblanadi. Axborot butunligi – axborotning buzilmagan holatda mavjudligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik – axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.



Axborot xavfsizligiga tahdidlarning toifalanishi. Axborot xavfsizligiga tahdidlar darajasiga kora quyidagicha toifalanishi mumkin:

a) shaxs uchun:

– axborotlarni qidirish, olish, uzatish, ishlab chiqish va tarqatish bo‘yicha fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini buzilishi;

– fuqarolarni shaxsiy hayot daxlsizligi huquqidan mahrum qilish;

– g‘ayriixtiyoriy zararli axborotlardan fuqarolarning o‘z sog‘liqlarini himoya qilish huquqlari buzilishi;

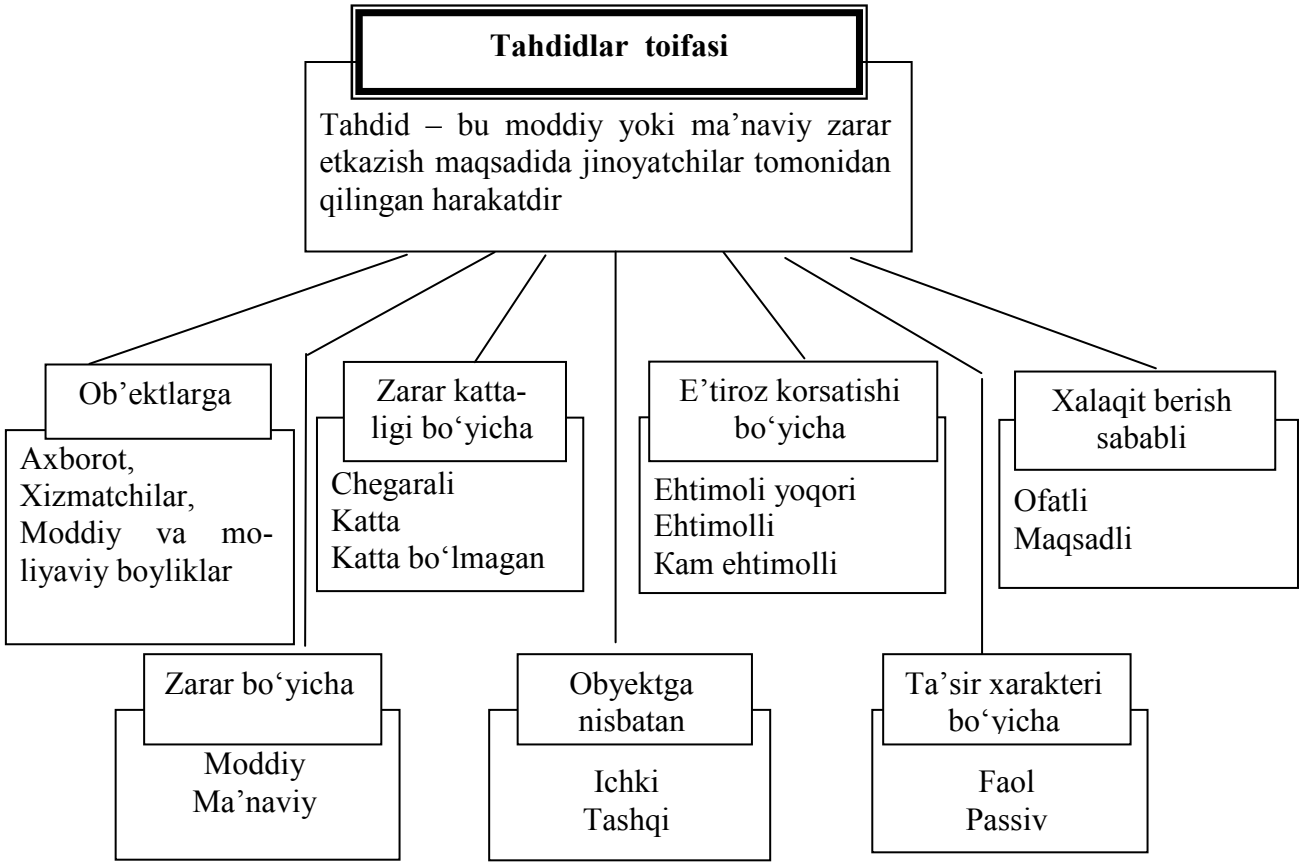
– intellektul mulk obyektlariga tahdid.

b) jamiyat uchun:

– axborotlashtirilgan jamiyatni qurishga to‘siqlar;

– jamiyatning ma’naviy yangilanish, uning ma’naviy boyliklarini saqlash, fidoyilik va xolislik, mamlakatning ko‘p asrlik ma’naviy an’analarini rivojlantirish, milliy, madaniy merosni targ‘ib qilish, axloq me’yorlari huquqlaridan mahrum qilish;

– zamonaviy telekommunikatsiya texnologiyalarini taraqqiy etishi, mamlakat ilmiy va ishlab chiqarish potensialini rivojlantirish va saqlab qolishga qarshilik qiluvchi muhitni yaratish.



v) davlat uchun:

– shaxs va jamiyat manfaatlari himoyasiga qarshi harakatlar;

– huquqiy davlat qurishga qarshilik;

– davlat boshqaruv organlari ustidan jamoat nazorati institutlarini shakllantirishga qarshi harakatlar;

– shaxs, jamiyat va davlat manfaatlarini ta'minlovchi davlat boshqaruv organlari tomonidan qarorlarni tayyorlash, qabul qilish va tatbiq etish tizimini shakllantirishga qarshilik;

– davlat axborot tizimlari va davlat axborot resurslari himoyasiga to'siqlar;

– mamlakat yagona axborot muhiti himoyasiga qarshi harakatlar.

Axborot himoyasiga metodologik yondashuv – bu konfedensial axborotlarni saqlash vazifasini turli bosqichlarda yechish bo'yicha asos bo'luvchi g'oyalar, muhim tavsiyalardir. Ular axborotni me'yoriy himoya qilish bazalarini yaratishda inobatga olinadi. Shuningdek, qonun va qonunosti aktlarini qabul qilishda me'yor sifatida tatbiq qilinadi hamda ularni bajarish majburiy xarakterga ega bo'ladi.

Axborotni muhofaza qilish tamoyillarini uchta guruhga bo'lish mumkin: huquqiy, tashkiliy hamda texnik razvedkadan himoyalanishda va hisoblash texnikasi vositalarida axborotga ishlov berishda axborotni muhofaza qilishdan foydalanish.

Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko‘rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo‘lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:

1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat’iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma’naviy-etik. Obyektda qat’iy belgilangan o‘zini tutish qoidalarining buzilishi ko‘pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo‘llab quvvatlash.

3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to‘siqlar yaratish.

4. Ma’muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo‘llash.

Fizik, apparatli, dasturli va hujjatli vositalarni o‘z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda *himoya obyekti* sifatida qaraladi.

Odatda, so‘nggi vaqtlarda axborotdan foydalanish, saqlash, uzatish va qayta ishlashda turli ko‘rinishdagi axborot tizimlarida amalga oshirilmoqda.

Axborot tizimi – bu odatda matnli yoki grafik axborotlarni yig‘ish, saqlash, qidirish va qayta ishlashga mo‘ljallangan amaliy dasturiy, ba’zan esa apparat-dasturiy nimtizimdir.

Ma’lumotlarning axborot tizimida mavjud bo‘lishining moddiy asosi bu elektron va elektron-mexanik qurilmalar, shuningdek axborot tashuvchilardir.

Axborot tashuvchilari sifatida qog‘oz, magnit va optik tashuvchilar, elektron sxemalar foydalanilishi mumkin.

Demak, qurilma va nimtizimlarni hamda axborot tashuvchilarini himoya qilish zarur.

Turli axborot tizimlarida foydalanuvchilar xizmat ko‘rsatuvchi personal hisoblanib, axborot manbai va tashuvchilari bo‘lishi mumkin.

Shuning uchun himoya obyekti tushunchasi keng ma’noda talqin

etiladi. Himoya obyekti deganda nafaqat axborot resurslari, apparat va dasturiy vositalar, xizmat ko‘rsatuvchi personal va foydalanuvchilar, balki bino hamda u joylashgan hudud ham tushuniladi.

Axborotni muhofaza qilishning asosiy *obyektlariga* quyidagilar kiradi:

– davlat sirlari bilan bog‘liq va konfedensial ma’lumotlarni o‘zida saqlovchi axborot resurslari;

– vositalar va axborot tizimlari (hisoblash texnikasi vositalari, tarmoqlar va tizimlar), dasturiy vositalar (operatsion tizimlar, ma’lumotlar bazalarini boshqarish tizimlari, amaliy dasturiy ta’minot), avtomatlashtirilgan boshqaruv tizimlari, aloqa va ma’lumotlarni uzatish tizimlari, ruxsati chegaralangan axborotni qabul qilish, uzatish va qayta ishlash texnik vositalari (ovoz yozish, ovoz kuchaytirish, ovoz eshitish, so‘zlashuv va televizion qurilmalar, hujjatlarni tayyorlash, ko‘paytirish vositalari hamda boshqa grafik, matn va harfli-raqamli ma’lumotlarni qayta ishlash vositalari), konfedensial va davlat sirlari toifasiga oid bevosita qayta ishlovchi tizim va vositalar. Bunday tizim va vositalarni ko‘pincha axborotlarni qabul qilish, qayta ishlash va saqlash texnik vositalari (AQITV) deb atashadi.

AQITV tarkibiga kirmaydigan, biroq konfedensial ma’lumotlar qayta ishlanuvchi hududga joylashgan texnik vosita va tizimlar ham mavjud. Bunday texnik vosita va tizimlar yordamchi texnik vosita va tizimlar (YOTVT) deb ataladi. Ularga quyidagilar kiradi: telefon, aloqa ovoz kuchaytirgich texnik vositalari, yong‘in va qo‘riqlash signalizatsiyasi tizimlari, radioaloqa tizimida ma’lumotlarni uzatish vositalari, nazorat-o‘lchov qurilmalari, xo‘jalik elektr asboblari va boshqalar, shuningdek ular joylashgan bino.

AQITVga statsionar jihozlar, periferiya qurilmalari, ulash liniyalari, taqsimlovchi va kommunikatsion qurilmalar, elektr manba tizimlarini o‘ziga biriktirgan tizim sifatida qarash mumkin. Konfedensial ma’lumotlarni qayta ishlashga mo‘ljallangan texnik vositalar, shuningdek ular joylashgan bino ham AQITV obyektini ifodalaydi.

Axborot xavfsizligini ta’minlashga yo‘naltirilgan himoya harakatlari qator kattaliklar bilan tavsiflanishi mumkin: tahdid xarakteri, harakat usullari, uning tarqalganligi, o‘rab olish masshtabi kabilar.

Tahdid xarakteriga ko‘ra himoya harakatlari ma’lumotlarni oshkor bo‘lishi, chiqib ketishi va noqonuniy kirishdan himoya qilishga yo‘naltiriladi. Harakat usullariga ko‘ra ularni kamomad yoki boshqa zararlarni: ogohlantirish, aniqlash, oldini olish va tiklash kabilarga taqsimlash mumkin. O‘rab olish bo‘yicha himoya harakatlari hududga,

binoga, inshoatga, qurilmalarga yoki ularning alohida elementlariga yo‘naltirilgan bo‘lishi mumkin. Himoya tadbirlarining masshtabi esa obyekt, guruh yoki individual himoya bo‘yicha tavsiflanadi.

Axborot himoyasi turlari ikki asosiy belgiga ko‘ra tasniflanadi:

birinchidan, axborot xususiyligi, aniqrog‘i qo‘riqlanadigan sirlar turiga ko‘ra;

ikkinchidan, axborot himoyasi uchun qo‘llaniluvchi kuchlar, vositalar va usullar guruhlari bo‘yicha.

Birinchi guruhga quyidagi asosiy yo‘nalishlar kiritilishi mumkin: davlat sirlarini himoya qilish, davlatlararo maxfiy ma’lumotlarni himoya qilish, tadbirkorlik sirlarini himoya qilish, xizmat sirlarini himoya qilish, mutaxassislik sirlarini himoya qilish va xususiy ma’lumotlarni himoya qilish.

Ikkinchi guruhga quyidagi asosiy yo‘nalishlar kiradi: axborotlarni huquqiy himoyalash, axborotlarni tashkiliy himoyalash, axborotlarni muhandislik-texnik himoyalash.

Huquqiy himoyalash – bu huquqiy asosda axborot himoyasini ta’minlovchi maxsus qonunlar, boshqa me’yoriy hujjatlar, qoidalar, jarayonlar va tadbirlar.

Tashkiliy himoya – bu bajaruvchilarga yetkazilishi mumkin bo‘lgan ixtiyoriy zararni bartaraf etuvchi yoki yengillashtiruvchi, bajaruvchilarning me’yoriy-huquqiy asosdagi o‘zaro muomalasi va ishlab chiqarish faoliyatini qat’iy belgilash.

Muhandislik-texnik himoya – bu faoliyatga yetkaziluvchi zararlarga qarshilik qiluvchi turli texnik vositalardan foydalanishdir.

Axborot himoyasi vositalarini va usullarini tasniflash. Axborotni muhofaza qilishda foydalaniluvchi asosiy usullar quyidagilar hisoblanadi: yashirish, ranjirlash, noto‘g‘ri ma’lumot berish, bo‘laklash, sug‘urta qilish, hisobga olish, kodlash va shifrlash.

Yashirish – axborotni muhofaza qilish usuli sifatida amaliyotda ma’lumotlarni himoyalashning asosiy tashkiliy usullaridan biri hisoblanadi, maxfiy ma’lumotlarga ruxsat etilgan shaxslar sonini chegaralaydi. Yashirish axborotlarni himoya qilishda juda keng qo‘llaniluvchi usullardan biri hisoblanadi.

Ranjirlash axborot himoya usuli sifatida, birinchidan, maxfiy ma’lumotlarni maxfiylik darajasi bo‘yicha taqsimlaydi, va ikkinchidan himoyalangan axborotga ruxsatni chegaralaydi.

Noto‘g‘ri ma’lumot berish – axborot himoya usullaridan biri bo‘lib, biror obyekt haqidagi haqiqiy ma’lumot o‘rniga atayin yolg‘on ma’lumot tarqatishni anglatadi.

Axborotni bo‘laklash usuli axborotni bo‘laklarga bo‘lib, uning biror qismi orqali to‘liq ma’lumot olib bo‘lmaslikni anglatadi. Bu usul harbiy texnika va qurollanish vositalarini ishlab chiqarishda, shuningdek yangi mahsulotlarni ishlab chiqarishda keng qo‘llaniladi.

Sug‘urta qilish – axborotni muhofaza qilish usuli sifatida endigina tan olinmoqda. Uning ma’nosi axborot egasi huquqlari va manfaatlarini yoki axborot vositalarini an’anaviy tahdidlar va axborot xavfsizligi tahdidlaridan himoya qilishni bildiradi. Ushbu usul tijorat sirlarini saqlashda ko‘proq qo‘llanilishi ehtimoli mavjud. Axborotni sug‘urta qilishda u dastlab, auditorlik tekshiruvidan o‘tishi va xulosaga ega bo‘lishi talab etiladi.

Axborotlarni ma’naviy-ma’rifiy himoyalash usuli axborotni muhofaza qilishda juda muhim rol o‘ynaydi. Aynan inson, u korxona yoki tashkilot xodimi, maxfiy ma’lumotlardan voqif bo‘lib, o‘z xotirasida ko‘plab ma’lumotlarni jamlaydi va ba’zi hollarda axborot chiqib ketishi manbaiga aylanishi mumkin hamda uning aybi bilan o‘zgalar ushbu axborotga noqonuniy ega bo‘ladilar. Axborotlarni ma’naviy-ma’rifiy himoyalash usuli quyidagilarni nazarda tutadi:

– xodimni tarbiyalash, u bilan ma’lum sifatlarni, qarashlarni shakllantirishga yo‘naltirilgan maxsus ishlarni olib borish (vatanparvarlik, axborotni muhofaza qilish uning shaxsan o‘zi uchun ham qanday ahamiyat kasb etishini tushuntirish);

– xodimni axborotni muhofaza qilish qoidalari va usullariga o‘rgatish, konfedensial axborot tashuvchilar bilan amaliy ishlash ko‘nikmalarini shakllantirish.

Hisobga olish axborotni muhofaza qilishning muhim usullaridan biri bo‘lib, konfedensial ma’lumotlar tashuvchilarning hamda undan foydalanuvchilarning ixtiyoriy vaqtda qayerda joylashganligi haqida ma’lumot olish imkonini beradi. Ushbu usulsiz himoya muammosini hal etish juda qiyin. Sir saqlanuvchi axborotlarni hisobga olish tamoyillari:

– himoyalanuvchi axborotlarni tashuvchilarning barchasini ro‘yxatga olish majburiyligi;

– muayyan axborot tashuvchini ro‘yxatga olish bir marta bo‘lishligini (takrorlanmasligini) ta’minlash;

– ro‘yxatda konfedensial ma’lumot tashuvchining ayni vaqtda qaysi manzildaligini ko‘rsatish;

– har bir himoyalangan axborot tashuvchining saqlanishiga yagona javobgarlik va hisobda ushbu axborotni ishlatgan foydalanuvchi haqida ma’lumotni aks ettirish.

Kodlash – himoyalanuvchi axborotni raqibdan yashirish maqsadida,

axborotni kanal orqali uzatish jarayonida o‘zgalar tomonidan tutib olinishi xavfi mavjud bo‘lganda, uni kodlash usuli yordamida ochiq matnni shartli axborotga aylantirish usulidir. Kodlash uchun odatda belgilar to‘plami (belgilar, raqamlar va boshqalar), shuningdek axborotni tushunarsiz belgilar to‘plami ko‘rinishiga aylantirish imkonini beruvchi ma’lum qoidalar tizimi foydalaniladi. Bu axborotni o‘qish uchun esa uni yana o‘z xoliga keltirish, ya’ni kodni ochish (kalit) kerak bo‘ladi. Axborotni kodlash texnik vositalar yordamida yoki qo‘lda amalga oshirilishi mumkin.

Shifrlash – axborotni muhofaza qilish usuli bo‘lib, ko‘pincha axborotlarni radioqurilmalar vositasida uzatishda, raqib tomonidan tutib olish xavfi bo‘lganda qo‘llaniladi. Axborotni shifrlash, uni o‘zgalar tomonidan tutib olinganda ham kalitsiz ma’nosini tushunib bo‘lmaydigan holatga o‘tkazishni anglatadi.

Axborotni muhofaza qilish vositalari – bu axborotni muhofaza qilish masalalarini hal etish uchun foydalaniluvchi muhandislik-texnik, elektr, elektron, optik va boshqa qurilma vositalar to‘plamidir.

Axborotni muhofaza qilishning kadr va resurs ta’minoti. Davlat sirlarini tashkil etuvchi axborotni muhofaza qilishni tashkil etuvchi kadrlar tayyorlash tizimiga quyidagilar kiradi:

1. Tashkilot va bo‘linma rahbarlari.
2. Axborotni muhofaza qilish bo‘yicha maxsus komissiyalar.
3. Yagona xavfsizlik xizmati tarkibiga kiruvchi ixtisoslashgan bo‘linmalar.

Boshqa sohalar kabi axborotni muhofaza qilish sohasi ham kadrlar tayyorlashdan tashqari moddiy, iqtisodiy va axborot resurslari bilan ta’minlanishi kerak.

Moddiy resurslar axborotni muhofaza qilishda maxsus ahamiyatga ega. Unga maxsus ajratilgan bino, maxsus qurilmalar, qabul qilingan me’yorlar asosida attestatsiya qilingan kompyuter va orgtexnika, apparat vositalari, dastur vositalari, axborotni muhofaza qilish vositalari va boshqalar.

Axborot resurslari – bu tashkilot miqyosida axborotni muhofaza qilish bo‘yicha optimal boshqaruv yechimlari qabul qilinadigan axborot. Unga quyidagilar kiradi:

– huquqiy axborot (xavfsizlik muammolari bo‘yicha me’yoriy baza);

– tijorat axborotlari (ishlab chiqariladigan mahsulot va unda axborotni muhofaza qilish bo‘yicha ko‘rsatiladigan xizmatlar haqida axborot);

– ilmiy-texnik axborot (xavfsizlik bo‘yicha mamlakat va chet el davlatlari siyosati haqida axborot);

– ishlab chiqarish texnologiyasi jarayonlari bo‘yicha axborot;

– tashkilotning axborot xavfsizligi holati, unga tahdidlar bo‘yicha axborot-tahliliy faoliyat natijasida olingan tahliliy axborot.

Moddiy resurslar. Axborotni muhofaza qilishni loyihalashtirishni, uni ishga tushirishni moddiy ta’minotsiz amalga oshirib bo‘lmaydi. Bu ish murakkab sharoitlarda amalga oshiriladi: xavfsizlik sohasida raqobatchilik, xizmat ko‘rsatuvchining kam xarajat qilib ko‘p foyda olish istagi, xavfsizlik bo‘yicha sifatsiz ishlarni amalga oshirishi va hokazo.

Axborot xavfsizligi uning egalari tomonidan himoyalanuvchi axborotning tarqab ketish, buzilish, yo‘q qilish va modifikatsiya qilishni oldini olish maqsadiga yo‘naltirilgan kompleks chora-tadbirlarni ifodalaydi.

Axborotni muhofaza qilish tizimi deganda davlat axborotni muhofaza qilish tizimini hamda muayyan obyektlardagi himoya tizimlarini tushunish kerak.

Davlat axborotni muhofaza qilish tizimiga quyidagilar kiradi:

– davlat me’yoriy hujjatlari, standartlar, boshqaruv hujjatlari va talablari;

– axborotni muhofaza qilish bo‘yicha konsepsiya, talablar, me’yoriy-texnik hujjatlar va ilmiy-uslubiy tavsiyalarni ishlab chiqish;

– davlat mulki bo‘lgan axborotni muhofaza qilishga yo‘naltirilgan chora-tadbirlarning tashkil etilishi, bajarilishi va amal qilinishi tartibi, shuningdek jismoniy va yuridik shaxslar ixtiyorida bo‘lgan axborotni muhofaza qilish bo‘yicha tavsiyalar;

– axborotni muhofaza qilish vositalarini sinash va sertifikatsiyalashni tashkillashtirish;

– axborotni muhofaza qilish uchun tashkilot va sohaviy koordinatsion tuzilmalarni tashkil etish;

– axborotni muhofaza qilishni tashkil etish bo‘yicha ishlarni nazorat qilish;

– chet el fuqarolari bo‘lgan yuridik va jismoniy shaxslarning davlat mulki bo‘lgan axborotdan yoki davlat tomonidan axborotni tarqatishga chegara qo‘yilgan yuridik va jismoniy shaxslar ma’lumotlaridan foydalana olish tartibini aniqlash.

Axborotlashtirishning muayyan obyektlarida axborotni muhofaza qilishning maqsadlari ehtimoli bo‘lgan tahdidlarning ro‘yxati bilan belgilanadi.

Har qanday axborotni muhofaza qilish tizimi o‘zining xususiyatiga ega bo‘lish bilan birga umumiy talablarga javob berishi kerak. Axborotni muhofaza qilishga ko‘proq qo‘yiladigan umumiy talablar quyidagilardir:

Axborotni muhofaza qilish tizimi

– bir butunlikda bo‘lishi;

– axborotning, axborot vositalarining xavfsizligini va axborot munosabatidagilar manfaatlarining himoyasini ta’minlashi;

– tizimning ichida uning elementlari orasida axborot aloqasini ta’minlashi;

– axborot faoliyatining texnologik kompleksini o‘ziga qamrab olishi;

– foydalanish vositalari bo‘yicha turli, axborotdan foydalana olishlilik bo‘yicha ko‘p darajali iyerarxik ko‘rinishda bo‘lishi;

– axborot xavfsizligi choralarini o‘zgartirish va to‘ldirishga ochiq bo‘lishi;

– nostandart bo‘lishi (himoya vositalarini tanlashda buzg‘unchining himoya imkoniyatlari bilan tanish emasligiga ishonishmaslik);

– texnik xizmat ko‘rsatishga oddiy va foydalanish uchun qulay bo‘lishi;

– ishonchli bo‘lishi kerak (texnik vositalardagi ixtiyoriy buzilish axborotning tarqab ketish kanali bo‘lib qolishi mumkin).

Boshqa tizimlar kabi axborotni muhofaza qilish tizimi o‘z ta’minotining ma’lum turlariga ega bo‘lishi kerak. Shu sababli bu tizim quyidagilarga ega bo‘lishi mumkin:

– *huquqiy ta’minot* (bunga bajarilishi majburiy bo‘lgan me’yoriy hujjatlar, ko‘rsatmalar, yo‘riqnomalar, talablar kiradi);

– *tashkiliy ta’minot* (bunda axborotni muhofaza qilish ma’lum bir tuzilmaviy birliklar orqali qo‘llanilishi nazarda tutiladi: hujjatlar himoyasi xizmati; qo‘riqlash, kirishga ruxsat berish xizmati; texnik vositalar yordamida axborotni muhofaza qilish xizmati; axborot-tahliliy faoliyat va boshqalar);

– *apparat ta’minoti* (bunda axborotni muhofaza qilish hamda muhofaza qilish tizimi faoliyatini ta’minlash uchun texnik vositalardan keng miqyosda foydalanish nazarda tutiladi);

– *axborot ta’minoti* (ushbu ta’minot tarkibiga tizimning faoliyatini ta’minlovchi vazifalarni hal yotuvchi ma’lumotlar, axborotlar, ko‘rsatkichlar, kattaliklar kiradi. Shuningdek, unga xavfsizlik ta’minoti xizmati faoliyati bilan bog‘liq bo‘lgan turli xarakterdagi ko‘rsatkichlar: ruxsat berish, ro‘yxatga olish, saqlash kabilar ham kiradi);

– *dasturiy ta’minot* (bunga konfedensial axborot manbalariga noqonuniy kirish yo‘llari hamda axborotni chiqib ketish kanallari mavjudligiga baho beruvchi turli axborot, hisobga olish, statistik va hisoblash dasturlari kiradi);

– *matematik ta’minot* (bu himoya uchun zarur bo‘lgan har xil hisoblarni amalga oshirishda, buzg‘unchilar texnik vositalarining xavfi tomonidan me’yorlar, hududlarga baho beruvchi matematik usullarni qo‘llashni nazarda tutadi);

– *lingvistik ta’minot* (axborotni muhofaza qilish sohasida mutaxassislar va foydalanuvchilar tomonidan qo‘llaniluvchi maxsus til vositalarining to‘plami);

– *me’yoriy-uslubiy ta’minot* (bunga axborotni muhofaza qilishni ta’minlovchi organlar, xizmatlar, vositalar faoliyati me’yorlari va reglamentlari, axborotni muhofaza qilish qattiq talab etiladigan sharoitlarda foydalanuvchilar tomonidan o‘z vazifalarini bajarishda faoliyatni ta’minlovchi turli uslublar kiradi).

1.3. Axborot xavfsizligi va ma’lumotlarni himoyalash bo‘yicha me’yoriy huquqiy hujjatlar. Axborotni muhofaza qilish sohasida xalqaro standartlar

Me’yoriy-huquqiy hujjat tushunchasi. 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 tahriri)»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».

Me’yoriy 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.

Me’yoriy huquqiy hujjat huquqning asosiy manbai hisoblanadi. Me’yoriy 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. Me’yoriy huquqiy hujjatlar mamlakat bo‘yicha amal qiladi va yagona tizimni hosil qiladi.

Me’yoriy huquqiy hujjatlar belgilari:

– me’yoriy xarakter

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

– huquqiy akt
– huquq ijodkorligi natijasi hisoblanadi
– umummajburiylik
– rasmiy hujjat ko‘rinishida tuziladi
– huquq me’yorlarini guruhlashda ma’lum bir tartibga rioya qilinadi.

Me’yoriy huquqiy hujjatlar turlari. O‘zbekiston Respublikasining 2012-yil 24-dekabrdagi «*Normativ-huquqiy hujjatlar to‘g‘risida* (yangi tahriri)»gi qonunining 5-moddasi me’yoriy huquqiy hujjatlarning turlarini aniqlaydi:

Quyidagilar me’yoriy huquqiy hujjat hisoblanadi:
– O‘zbekiston Respublikasi Konstitutsiyasi;
– O‘zbekiston Respublikasi qonunlari;
– O‘zbekiston Respublikasi Oliy Majlisi palatalari qarorlari;
– O‘zbekiston Respublikasi Prezidenti farmonlari;
– O‘zbekiston Respublikasi Vazirlar Mahkamasi qarorlari;
– Vazirliklar, davlat komitetlari va tashkilotlari hujjatlari;
– Davlat hokimiyatining joylardagi organlari qarorlari.

Me’yoriy huquqiy hujjatlar qonunchilik hujjatlari hisoblanadi va O‘zbekiston Respublikasi qonunchiligini tashkil etadi.

O‘zbekiston Respublikasi Konstitutsiyasi, O‘zbekiston Respublikasi Qonunlari, O‘zbekiston Respublikasi Oliy Majlisi palatalari qarorlari qonunchilik hujjatlari hisoblanadi.

O‘zbekiston Respublikasi Prezidenti Farmonlari, O‘zbekiston Respublikasi Vazirlar Mahkamasi qarorlari, Vazirliklar, davlat komitetlari va tashkilotlari aktlari, davlat hokimiyatining joylardagi organlari qarorlari qonunosti hujjatlari hisoblanadi (ushbu qonunning 6-moddasi).

Axborot xavfsizligini ta’minlashda me’yoriy-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.

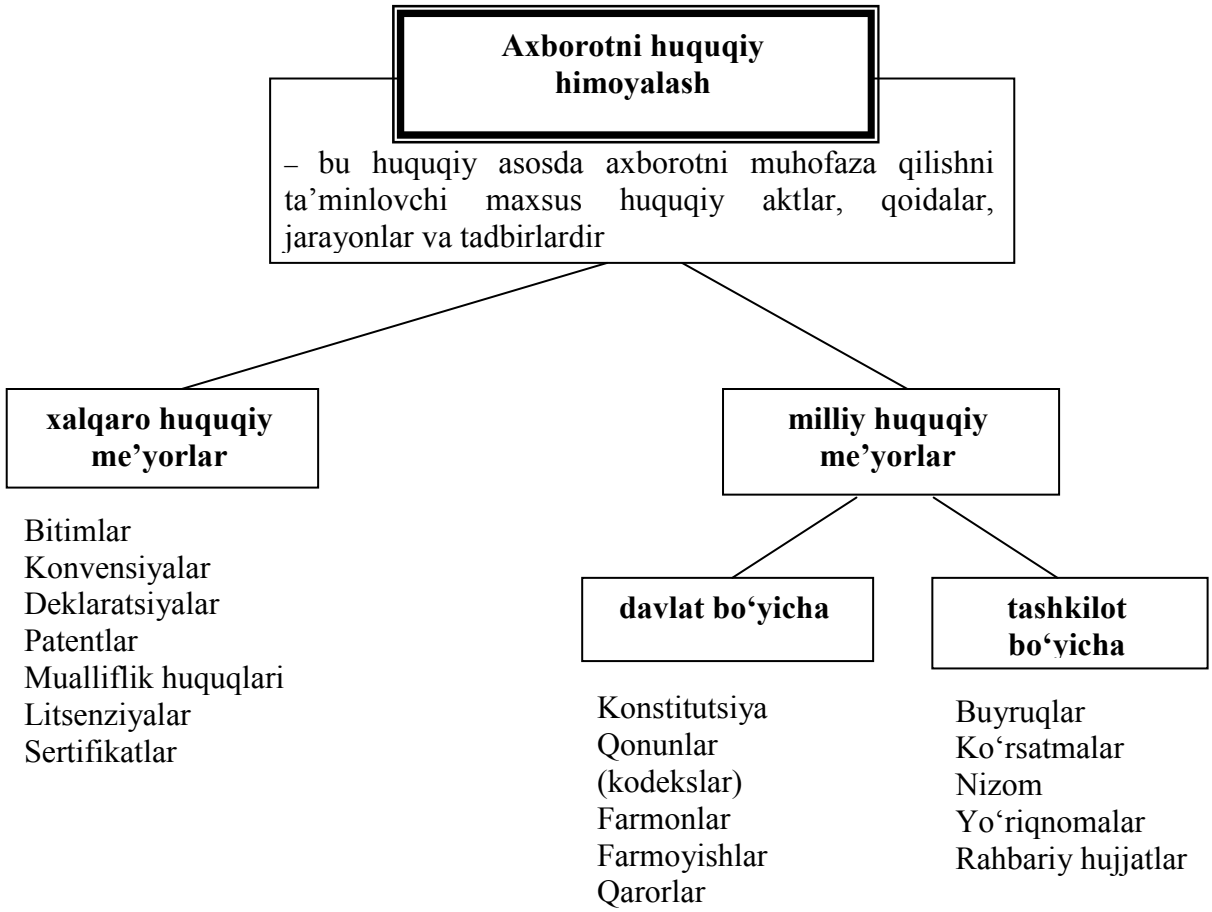
Axborotni muhofaza qilish sohasiga oid me’yoriy-huquqiy hujjatlarda:

– 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.

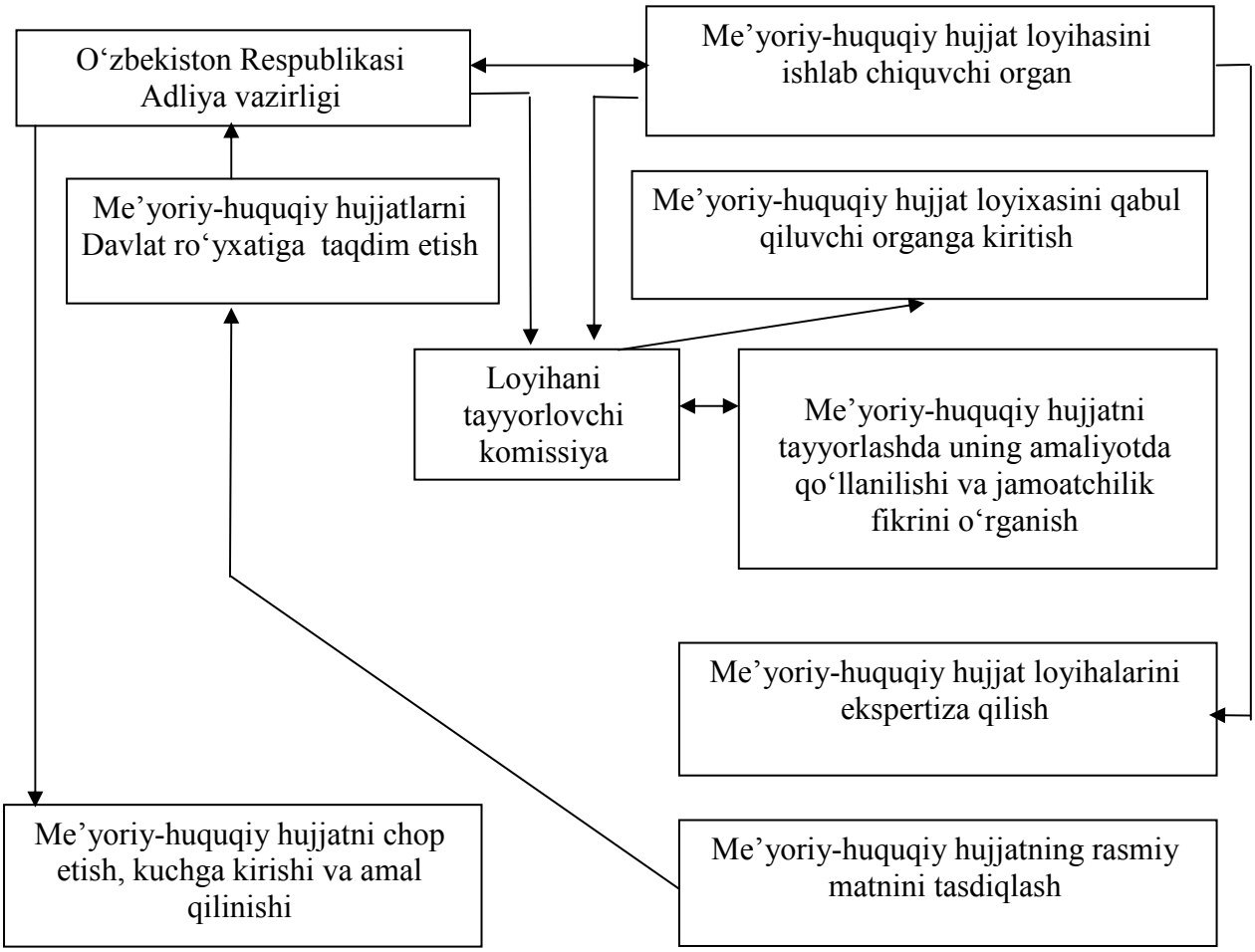
O‘zbekiston Respublikasida axborot xavfsizligi va ma’lumotlarni himoyalash bo‘yicha me’yoriy huquqiy hujjatlar. Axborotni huquqiy himoyalash zaxira sifatida davlat va xalqaro miqyosda tan olingan hamda xalqaro shartnoma, konvensiya va deklaratsiyalarda aniqlanadi. Davlat miqyosida axborotni huquqiy himoyalash davlat va tashkilot hujjatlari orqali nazorat qilinadi.

Bizning mamlakatimizda bunday me’yoriy hujjatlarga Konstitutsiya, O‘zbekiston Respublikasi Qonunlari, Hukumat qarorlari, fuqarolik, ma’muriy va jinoyat kodekslarida keltirilgan tegishli moddalar kiradi. Tashkilot me’yoriy hujjatlariga esa ushbu tashkilot doirasida amal qilinuvchi buyruq, yo‘riqnoma, ko‘rsatma kabilar kiradi.



Axborot xavfsizligi va ma’lumotlarni himoyalash sohasida me’yoriy huquqiy hujjatlarni qabul qilish va amal qilishda tizimli ketma-ketlik. Xavfsizlikni 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).

Me’yoriy-huquqiy hujjatlarni qabul qilish
va qo‘lla shning tizimli ketma-ketligi



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

Bunga javob tariqasida GFR 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* GFR, 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.

ITSEC Oq kitobda xavfsizlik kriteriyalarining quyidagi asosiy qismlari keltirilgan:

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.

ITSEC Yevropa kriteriyalariga ko‘ra axborot xavfsizligi olti asosiy element va uning qismlarini o‘z ichiga oladi:

1. Axborot konfedensialligi (axborotni noqonuniy olishdan himoyalash).
2. Axborot butunligi (axborotni noqonuniy o‘zgartirishdan himoyalash).
3. Axborotdan foydalana olishlilik (axborot va tizim resurslarini noqonuniy yoki tasodifiy ushlab qolishlardan himoyalash).
4. Xavfsizlik maqsadlari (axborot xavfsizligi funksiyalari nima uchun kerak).
5. Axborot xavfsizligi funksiyalarining tasnifi:

– identifikatsiya va autentifikatsiya (foydalanuvchining haqiqiyligini an'anaviy tekshirishgina emas, yangi foydalanuvchilarni ro‘yxat ga 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, umumfoydala-niluvchi 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.

Oq kitobda «tizim» va «mahsulot» o‘rtasida farq ifodalanadi.

«Tizim» deganda ma’lum bir maqsadda va ma’lum bir doirada qo‘lla niluvchi aniq apparat-dasturiy konfiguratsiya tushuniladi. «Mahsulot» deganda esa, o‘z xohishiga ko‘ra sotib olib ixtiyoriy «tizim»ga o‘rnatilishi mumkin bo‘lgan apparat-dasturiy paket tushuniladi. «Tizim» va «Mahsulot»ning kriteriyalarini umumlashtirish maqsadida **ITSECda** yagona – «obyekt» atamasi kiritilgan. «Obyekt»ni ishonchli deb qabul qilish uchun, xavfsizlikni kafolatlovchi ma’lum bir darajadagi ishonch kerak bo‘ladi. U esa samaradorlik va aniqlikni o‘z ichiga oladi. Ba’zi manbalarda kafolatlanganlikni himoya vositalarining adekvatligi deb ham nomlanadi.

Himoyaning samaradorligini tekshirishda konfedensiallik, butunlik, axborotga ruxsat etilganlik bo‘yicha xavfsizlik vazifalarining o‘zaro mosligi tahlil qilinadi. Shuningdek, huquqbuzarlar tomonidan himoyaning qaltis joylaridan foydalanish oqibatlari o‘rganib chiqiladi. Bundan tashqari, «samaradorlik» tushunchasiga himoya mexanizmlarining quvvati deb nomlanuvchi to‘g‘ridan-to‘g‘ri hujumlar bo‘lgandagi qobiliyatlari ham kiradi. **ITSECda** himoya mexanizmlari quvvatining uchta darajasi (bazaviy, o‘rta, yuqori) keltirilgan.

ITSEC bo‘yicha tizim xavfsizligini umumiy baholash ikki qismdan iborat – kafolatlangan xavfsizlik mexanizmlarining darajasini baholash va ularning kafolatlangan aniqligi darajasini baholash.

Tizimning xavfsizligi umuman olganda «tizim» va «mahsulot»ni alohida baholash bilan amalga oshiriladi. Uning himoyalanganligi xavfsizlik mexanizmlarining muhim bo‘laklaridan yuqori bo‘la olmaydi.

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 larga 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 butunligina 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.

Kanada o‘zining **STSRES** nomli kriteriyalarini, AQSh esa yangi Federal Kriteriyalar (Federal Criteria)ni ishlab chiqdi. Ushbu kriteriyalar o‘zaro moslasha olmasligi sababli, ularni o‘zaro muvofiqlashtirib (birlashtirib), ular himoyalanganlikni baholovchi **CommonCriteria** (CC) nomli to‘plam yaratishga qaror qabul qilindi. Kriteteriyalarning umumiy to‘plami himoyalanganlikni baholash bo‘yicha quyidagilarni aniqlaydi:

– funksional imkoniyatlar va kafolatlarga talablar;

– foydalanuvchi so‘rashi mumkin bo‘lgan ishonchning 7 darajasi (baholashda kafolat darajalari). Bunda EAL1 daraja tizimning konkretliligа uncha yuqori bo‘lmagan ishonchni ta’minlasa, EAL7 daraja juda yuqori kafolatlarni beradi;

– ikki tushuncha: Himoya profili (RR) va xavfsizlik maqsadi (ST).

Yuqorida qayd etilgan standartlarning analogi sifatida Rossiyada «Avtomatlashtirilgan tizimlar. Axborotni noqonuniy kirishdan himoyalash. Avtomatlashtirilgan tizimlarni tasniflash va axborot himoyasiga talablar» nomli Davlat texnika komissiyasining Boshqaruv hujjati ishlab chiqilgan.

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

Har qanday tashkilot faoliyati axborot texnologiyalaridan foydalanish oqibatida ko‘plab tahdidlardan holi bo‘lmaganligi sababli tahdidlarni boshqarish nomli yangi funksiya paydo bo‘ldi. U o‘z ichiga ikki faoliyatni oladi: tahdidlarni baholash (o‘lchash) va samarali va tejamkor himoya boshqaruvchisini tashlash.

Tahdidlarni boshqarish jarayonini quyidagi bosqichlarga bo‘lish mumkin:

1. Tahlil qilinuvchi obyektlarni tanlash va ularni ko‘rib chiqishda batafsillik darajasi.

2. Tahdidlarni baholash metodologiyasini tanlash.
3. Aktivlarni identifikatsiyalash.
4. Tahdid va uning oqibatlari tahlili, himoyaning zaifliklarini aniqlash.
5. Tahdidlarni baholash.
6. Himoya choralarini tanlash.
7. Tanlangan choralarni qo‘llash va tekshirish.
8. Qoldiq tahdidni baholash.

Ushbu munosabatlarni huquqiy boshqarish avvalo, axborot tahdidlaridan sug‘urta qilish orqali amalga oshirilishi mumkin va zarur.

Mustaqil tayyorgarlik uchun savollar

1. *Axborot xavfsizligi tushunchasi nimani anglatadi?*
2. *Axborot xavfsizligining qanday tashkil etuvchilari mavjud?*
3. *Axborot xavfsizligi milliy xavfsizlik tizimida qanday o‘rin tutadi?*
4. *Axborot xavfsizligining zamonaviy konsepsiyasi nima?*
5. *Axborot xavfsizligiga tahdid deganda nima tushuniladi?*
6. *Axborotni muhofaza qilishning qanday usullari va turlari mavjud?*
7. *Axborotni muhofaza qilish qanday obyektlarga ega?*
8. *Axborotni muhofaza qilish vositalariga nimalar kiradi?*
9. *Axborotni muhofaza qilish tizimlari qanday vazifani bajaradi?*
10. *Axborot xavfsizligi va ma’lumotlarni himoyalash bo‘yicha qanday me’yoriy-huquqiy hujjatlar mavjud?*
11. *Axborotni muhofaza qilish sohasida qanday xalqaro standartlar mavjud?*

II. AXBOROTLARNI TEXNIK HIMOYALASH

2.1. Texnik vositalar bilan himoyalanadigan axborotlarning turlari.
2.2. Axborot chiqib ketish texnik kanallarining tasnifi va tarkibi.
2.3. Obyektlarni kuzatish, signallarni eshitish va tutib olishning asosiy usul va tamoyillari.
2.4. Axborotlarni injener-texnik himoyalash.

Hozirgi kunda ma'lumotlarni texnik himoyalash masalasi dolzarb vazifalardan biriga aylangan.

Ma'lumotlarni himoyalashning texnik vositalariga mexanik, elektro-mexanik, elektron-mexanik, optik, akustik, lazer, radio, radiolokatsion va boshqa qurilmalar hamda himoyalanadigan obyektga borish yo‘lini to‘sishga mo‘ljallangan tizim va binolar kiradi.

Ma'lumotlar va obyektlarni himoyalash uchun murakkab va takomillashgan usullaridan foydalaniladi.

Tashkilotlardagi ma'lumotlarni elektron qayta ishlash markazlari kuchli elektromagnit nur manbai bo‘lgan obyektlardan uzoqda joylashgan bo‘lishi va atrofi devor bilan o‘ralishi kerak. Nazorat zonasini kuzatish televizion, radiolokatsiyali, lazerli, optik, akustik va boshqa umumiy pultga ulangan tizim orqali amalga oshirilishi mumkin.

Axborot xavfsizligi muammosi tashkiliy chora-tadbirlar va talablar, axborot tizimlaridan foydalanish va loyihalash bosqichlarida hal qilinadi. Ular orasida himoyalanayotgan axborot tizimi joylashgan obyektni qo‘riqlash muhim o‘rinni egallaydi. Bunda hisoblash texnika vositalaridagi ma'lumotlarni o‘g‘irlashni oldini oladigan va qiyinlashtiradigan, axborot tashuvchilar, shuningdek aloqa liniyalaridan va axborot tizimidan ruxsat berilmagan foydalanishni man etadigan tegishli qo‘riqlash postlari, texnik vositalar o‘rnatiladi.

2.1. Texnik vositalar bilan himoyalanadigan axborotlarning turlari

Axborotlarni muhofaza qilishning texnik vositalari – obyektning niqoblovchi (maskirovkalovchi) belgilari ochilishini bartaraf etish yoki kamaytirish, yolg‘on alomatlarni yaratish hamda texnik vositalar orqali

axborotga ruxsatsiz kirishga to‘sqinlik qilishga mo‘ljallangan texnik vositalardir.

Ma’lumotlarni ruxsatsiz olishning obyektlari, usullari va vositalari quyidagilar bo‘lishi mumkin:

– bino, inshoat va qurilish konstruksiyalari (devorlar, tomlar, pollar, deraza va eshiklar, deraza oynalari, isitish va suv bilan ta’minlash tizimlari, havo tozalash quvurlari); konfedensial muzokara va majlislarni o‘tkazishda akustik tebranish kanallari bo‘yicha ma’lumotlarni ruxsatsiz olish;

– harakatlanuvchi obyektlar (avtomobil, temir yo‘l, suv va havo yo‘llari transportlari); konfedensial suhbatlar olib borishda – akustik tebranish kanallari bo‘yicha;

– kuchsiz tok texnika vositalari (aloqa qurilmalari, ovoz kuchaytirgichlar, audio- va telequrilmalar, elektr soatlar, radio eshittirishlar, yong‘in va qo‘riqlash signalizatsiya qurilmalari, elektr yozuv mashinkalari, konditsionerlar va ulardan foydalanilganda hamda bu vositalar yopiq tasnifli tadbirlarni o‘tkazishga mo‘ljallangan binoga joylashganda – elektroakustik o‘zgarishlar bo‘yicha va yondosh elektromagnit nurlanishlar va navodkalar (YOEMNN-PEMIN) hisobiga;

– hisoblash texnikasi vositalari (monitordagi tasvir efir orqali ma’lum bir masofaga uzatiladi) – YOEMNN hisobiga;

– elektr manbasi va yerga ulangan o‘tkazgichlar tizimi (bu zanjir orqali ovoz kuchaytirish, kompyuterda kotiba bilan aloqa va shu kabilarni amalga oshiruvchi qurilmalarda qayta ishlanadigan ma’lumotlarni tutib olish mumkin) – YOEMNN hisobiga;

– bino, avtomashina va boshqalardagi akustika (so‘z, tovushlar) – radiokanal va simlarda akustik radiomikrofonlar («juchoklar») bo‘yicha hamda lazer qurilmalari orqali qo‘lga kiritish hisobiga;

– telefonda so‘zlashuvlar – radiokanal va simlar orqali telefon «juchoklar» hisobiga;

– faks orqali ma’lumotlar – yondosh nurlanishlar va navodkalar hamda aloqa liniyasi orqali qo‘lga kiritish hisobiga;

– «juchoklar» o‘rnatilgan «sovg‘a» va «suvenirlar», mebellar;

– yo‘naltirilgan mikrofonlar yordamida masofadagi shaxs akustikasi (so‘zi);

– uyali aloqa tarmog‘i orqali radioso‘zlashuvlar.

Himoyaning texnik 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.

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.

Obyektni topishda texnik razvedka vositalarining faoliyat ko'rsatish jarayonida obyektning texnik demaskirovka belgilari aniqlanadi va uning mavjudligi haqida xulosa qilinadi.

Demaskirovka belgilari quyidagilar bilan farq qiladi:

– joylashuvi – boshqa obyektlar va atrofdagi predmetlar orasida obyekt joylashuvini aniqlab beradigan belgi;

– tarkibiy ko'rinish – obyektning tuzilishi va to'laligicha ko'rinishini aks ettiradigan kattaliklarini (tarkibi, soni va alohida obyektlarning joylashuvi, shakli va geometrik o'lchamlari) aniqlovchi belgilar;

– faoliyati – obyektning fizik faoliyat yuritishi orqali uni ochib beruvchi belgilar.

Texnik demaskirovka belgilarini ikki toifaga bo'lish mumkin:

– to'g'ridan-to'g'ri demaskirovka belgilari – himoya obyektining faoliyati va uning fizik maydonlari (elektromagnit, akustik, radiatsion va boshqalar) bilan bog'liq bo'lgan, himoya qilinadigan axborotga bog'liq bo'lmagan atrof-muhitning fizik maydoni fonidan farq qiladigan belgilar;

– bilvosita demaskirovka belgilari – obyektning faoliyat ko'rsatishi natijasida atrof-muhitdagi o'zgarishlar natijasida yuzaga keladigan belgilar (faoliyatning optik-vizual belgilari, geometrik o'lchamlar, yoritilganlikning keskin farq qilinishi, ishlab chiqarish faoliyatidan qolgan izlar va hokazo).

Axborotni muhofaza qilishning samaradorlik ko'rsatkichi himoya obyektining texnik demaskirovka belgilari kattaligi bo'lib, unga nisbatan axborotni muhofaza qilish samaradorligining me'yorlari belgilanadi.

Xavfli signal, obyekt belgisining ko‘rsatkichi bo‘lib, undan konfedensial ma’lumotlarni olish uchun texnik razvedkada (TR) foydalaniladi. Obyektni aniqlash – TR vositalarining faoliyati bo‘lib, natijada obyekt demaskirovka belgilarining kattaliklari aniqlanadi va uning tavsifi haqida xulosa qilinadi (klassifikatsiyalash amalga oshiriladi). Aniqlangan obyektga ma’lum bir toifa beriladi. Ixtiyoriy obyektda bir qancha belgilar bo‘lishi mumkin, biroq obyektni aniqlashda bu belgilarning ma’lum to‘plamidan foydalaniladi.

Himoya obyektlarining demaskirovka belgilari. Obyektlarning demaskirovka belgilariga quyidagilar kiradi:

– faoliyat belgilari: transport mashinalarining harakati, ovozlar, olovlar, chaqnashlar, tutun, chang;

– maxsus qurilmalarda qayd qilinadigan turli nurlanishlarni (elektromagnit, infraqizil, issiqlik) qaytarish va chiqarish qobiliyati;

– faoliyat izlari: so‘qmoq va qatnov yo‘llari, ishlab chiqarish materiallarining qoldiqlari, maishiy chiqindilar va hokazo;

– tavsiflovchi ko‘rinishi (shakli), obyektni o‘lchami va joylashuvining muhim tomonlari;

– obyekt sirtining rangi, ayrim hollarda uning yaltirashi (oynaning yaltirashi, metalning tovlanishi);

– obyektning o‘zidan tushadigan va uning sirtiga tushadigan soya.

Texnik vositalar bilan himoyalanadigan ma’lumotlarning manbasi va tashuvchilari:

– obyekt tarkibining fizik xususiyatlarini tavsiflovchi belgilar (issiqlik va elektr o‘tkazuvchanligi, tarkibi, qattiqligi va hokazo);

– obyekt tomonidan hosil bo‘ladigan fizik maydonni tavsiflovchi belgilar (eletromagnit, radiatsion, akustik, gravitatsion va hokazo);

– obyektning shakli, rangi, o‘lchami va elementlarini tavsiflovchi belgilar;

– obyektning fazoviy koordinatalarini (harakatlanadigan obyektlarning tezligini) tavsiflovchi belgilar;

– obyektlar va ularning elementlari o‘rtasidagi ma’lum bir aloqalar mavjudligini tavsiflovchi belgilar;

– obyekt faoliyati natijasini (tutun chiqarish, changitish, obyektning tuproqdagi izi, suv va havoni ifloslantirish va shu kabi) tavsiflovchi belgilar.

Obyektni aniqlash uning demaskirovka belgilari bo‘yicha amalga oshiriladi. Bu belgilar *ko‘rinishi, faoliyat belgisi va joylashuvi* bo‘yicha uchta guruhga bo‘linadi.

Ko‘rinishi bo‘yicha demaskirovka belgilarga obyektning fizik (optik va radiolakatsion diapazonli nurlanish to‘lqinlarini qaytarish qobiliyati, issiqlik diapazonida energiyaga ega bo‘lgan nurlanish chiqarishi) va geometrik (obyekt shakli va uning alohida tashkil etuvchilarining o‘lchamlari) xususiyatlari kiradi.

Faoliyatning demaskirovka belgilari obyekt ta’siri (harakatlanish, atrof-muhitning o‘zgarishi va shu kabilar) natijasida namoyon bo‘ladi.

Joylashuv belgilari obyektning atrofdagi predmetlarga nisbatan joylashuv holati bilan aniqlanadi.

Obyektning ko‘rinadigan elektromagnit spektr diapazonidagi demaskirovka belgilari. Obyekt va atrof-muhitning optik kattaliklari razvedkada hamda razvedkaning texnik vositalaridan samarali himoya qilishda muhim rol o‘ynaydi. Obyektlarning optik tasviri va ularning alohida tashkil etuvchilari fonga nisbatan yorqinligi, o‘lchami, shakli va rangi bilan farq qiladi. Ko‘rinadigan to‘lqin diapazonida obyektning tasviri uning yorqinligi bilan aniqlanadi. Obyekt bilan fon orasidagi rang yorqinligining farqi qo‘shimcha ma’lumot hisoblanadi. Obyekt bilan fon orasidagi yorqinlik farqi, ularning yorug‘lik qaytarish qobiliyatining turlichaligi natijasida paydo bo‘ladi.

Obyektning elektromagnit infraqizil spektr diapazonidagi demaskirovka belgilari. Bu belgilarga qizigan jismning o‘zidan chiqargan nuri (tabiiy) va obyektlardan qaytgan (sun’iy) infraqizil nurlar kiradi. Tabiiy infraqizil nurlar manbasi yer ustidagi (tuproq, o‘rmon va hokazo), atmosferadagi (bulut, gazlar) va kosmosdagidan (quyosh, oy, yulduzlar) iborat bo‘ladi. Tabiiy infraqizil nurlar obyektni aniqlashni qiyinlashtiruvchi fon nurlari hisoblanadi. Obyekt va fonning issiqlikni nurlash qobiliyatidagi farq hisobiga obyektni aniqlash mumkin.

Radioelektron vositalarni demaskirovka belgilari. Radioelektron qurilmalarni demaskirovka belgilari radiodiapazondagi elektromagnit to‘lqin nurlanishlari bilan bog‘liq. Elektromagnit to‘lqinlar texnik vosita va tizimlarning vazifasi hamda tavsiflari haqidagi ma’lumotlarni tashishi mumkin. Nurlanish asosiy va yordamchi vositalardan, nazorat-o‘lchash qurilmalaridan, trenajyorlardan, imitatordan va boshqalardan chiqishi mumkin.

Radionurlanish bilan bog‘liq bo‘lgan barcha demaskirovka belgilari radiosignalning texnik tavsiflari bilan aniqlanadi. Ularni *chastotali, vaqtli, energetik, spektrli, fazo-energetik, fazoli, polyarizatsiyali* guruhlarga ajratish mumkin.

Radionurlanishning texnik alomatini *guruhli, individual va tezkorga* ajratish mumkin.

Guruhli texnik belgilar radioelektron tizim (RET)ni biror sinfga taalluqli ekanligini aniqlash imkonini beradi. Ular aniq RET turiga mos keluvchi tavsif yoki tavsiflar majmui bilan aniqlanadi. Unga quyidagilar kiradi: fazoviy ko‘rish sohasining tavsifi; antennaning aylanish tezligi; nurlanish turi; chastotani qayta sozlash tartibi va chegarasi; modulyatsiya qilinuvchi signalning turi va o‘zgarish qonuniyati; signal kattaliklarining qiymatlari (tashuvchi chastotalar, impuls davomiyligi, impulsning chiqish chastotasi va boshqalar).

Individual demaskirovka belgilari RET to‘plamidagi biror turga oid va aniq namuna haqidagi ma’lumotlardan iborat bo‘ladi. RETda o‘ziga xos demaskirovka belgilari signal kattaliklarining texnologik va ishlatishdagi tarqoqligi natijasida namoyon bo‘ladi.

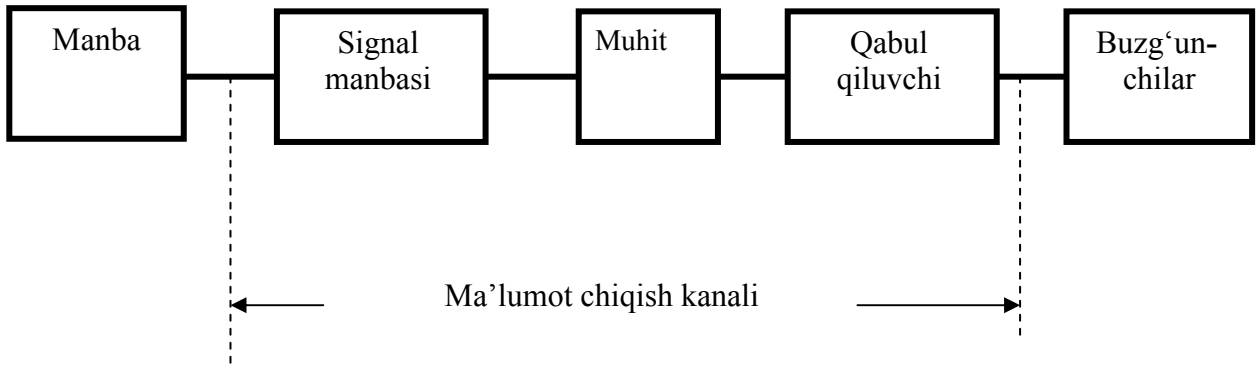
2.2. Axborot chiqib ketish texnik kanallarining tasnifi va tarkibi

Ma’lumot maydon yoki modda orqali uzatiladi. Bu yo akustik to‘lqin (tovush), yo elektromagnit nurlanish yo matn yozilgan bir varaq qog‘ozdir. Biroq, na uzatilgan energiya, na foydalanilgan modda o‘z-o‘zicha hech qanday qiymatga ega emas, ular faqat ma’lumot tashuvchi hisoblanadi, xolos.

Fizik tabiatiga ko‘ra quyidagilar ma’lumot tashuvchi vositalar hisoblanadi: yorug‘lik nuri; tovush to‘lqinlari; elektromagnit to‘lqinlar; material va moddalar.

Tabiatda ma’lumotlarni tashish uchun bulardan boshqalari mavjud emas. O‘z manfaatlariga qarab insonlar u yoki bu fizik maydondan foydalanib o‘zaro ma’lumot uzatishning biror tizimini yaratadilar. Bunday tizimlarni *aloqa tizimi* deb nomlash qabul qilingan. Ixtiyoriy *aloqa tizimi (ma’lumot uzatish tizimi)* ma’lumotlar manbai, uzatgich, ma’lumot uzatish kanali, qabul qilgich va qabul qilib oluvchi haqidagi ma’lumotdan tashkil topadi. Bu tizimlar kundalik hayotda biror maqsad uchun foydalaniladi va ma’lumot uzatishning rasmiy vositasi hisoblanadi. Uning faoliyati ishonchlilikni, aniqlilikni va ma’lumot uzatish xavfsizligini ta’minlash maqsadida nazorat qilinadi. Bu esa raqobatchilarning tizimga ruxsatsiz kirishni oldini oladi. Biroq, ma’lum sharoitlar mavjudki, unda bir joydan boshqasiga ma’lumot uzatish tizimi obyekt va manbaning xohishiga bog‘liq bo‘lmaydi. Bunday hollarda, albatta, bunday kanal o‘zini ochiqcha namoyon qilmasligi kerak. Ma’lumotlar uzatish kanali singari bunday kanal *ma’lumot chiqib ketish kanali* deb ataladi. U ham signal manbai, uni tarqatuvchi fizik muhit va yovuz niyatli shaxslar (buzg‘unchilar)

tomonidagi qabul qiluvchi qurilmalardan tashkil topadi. Quyidagi rasmda ma’lumot chiqib ketish kanalining tuzilishi keltirilgan.



Ma’lumotlar chiqib ketish kanali deb konfedensial ma’lumotlar manbasidan yovuz niyatli shaxsgacha bo‘lgan fizik yo‘l tushuniladi. Bu yo‘l orqali ma’lumot chiqib ketishi yoki saqlanayotgan ma’lumotga ruxsatsiz kirish mumkin. Ma’lumotlar chiqib ketish kanalining vujudga kelishi (paydo bo‘lishi, o‘rnatish) uchun ma’lum fazoviy, energetik va vaqtdagi sharoit hamda yovuz niyatli shaxsda ularga mos ma’lumotlarni qabul qilish va qayd qilish vositalari mavjud bo‘lishi kerak.

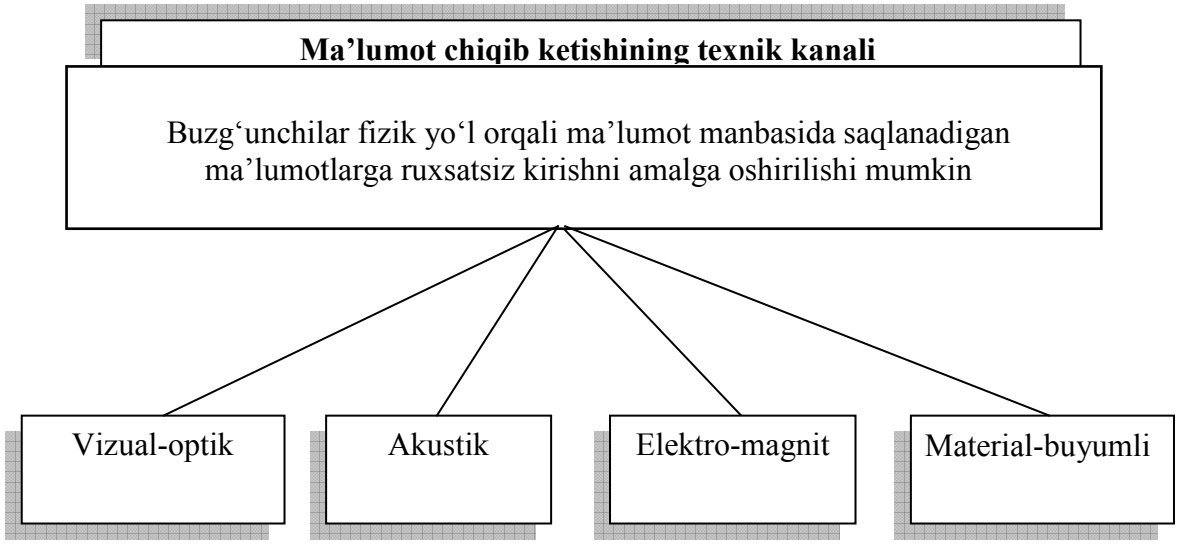
Fizik xususiyatlarini inobatga olgan holda ma’lumotlar chiqib ketish kanalining paydo bo‘lishini quyidagi guruhlarga ajratish mumkin:

– vizual-optik;

– akustik;

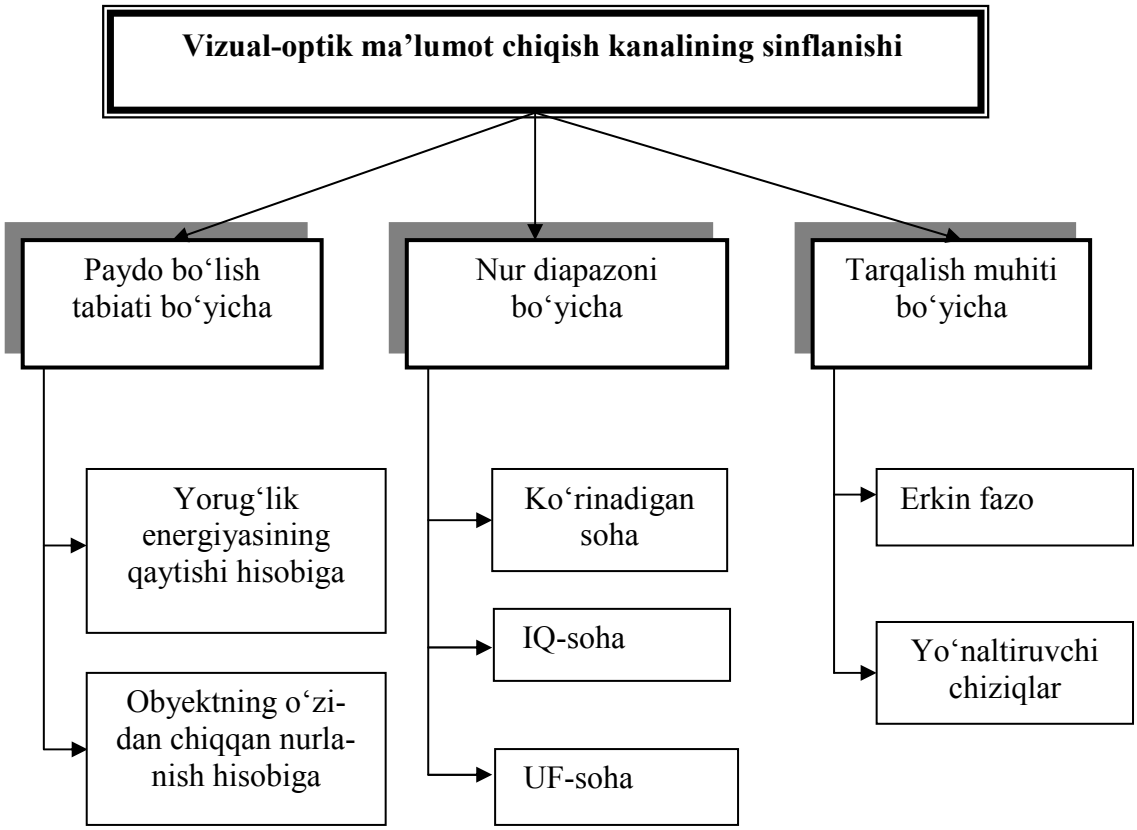
– elektromagnit (magnit va elektrik maydonni o‘z ichiga oladi);

– material-buyumli (qog‘oz, foto, magnitli tashuvchilar, turli ko‘rinishdagi qattiq, suyuq, gaz holatidagi sanoat chiqindilari).



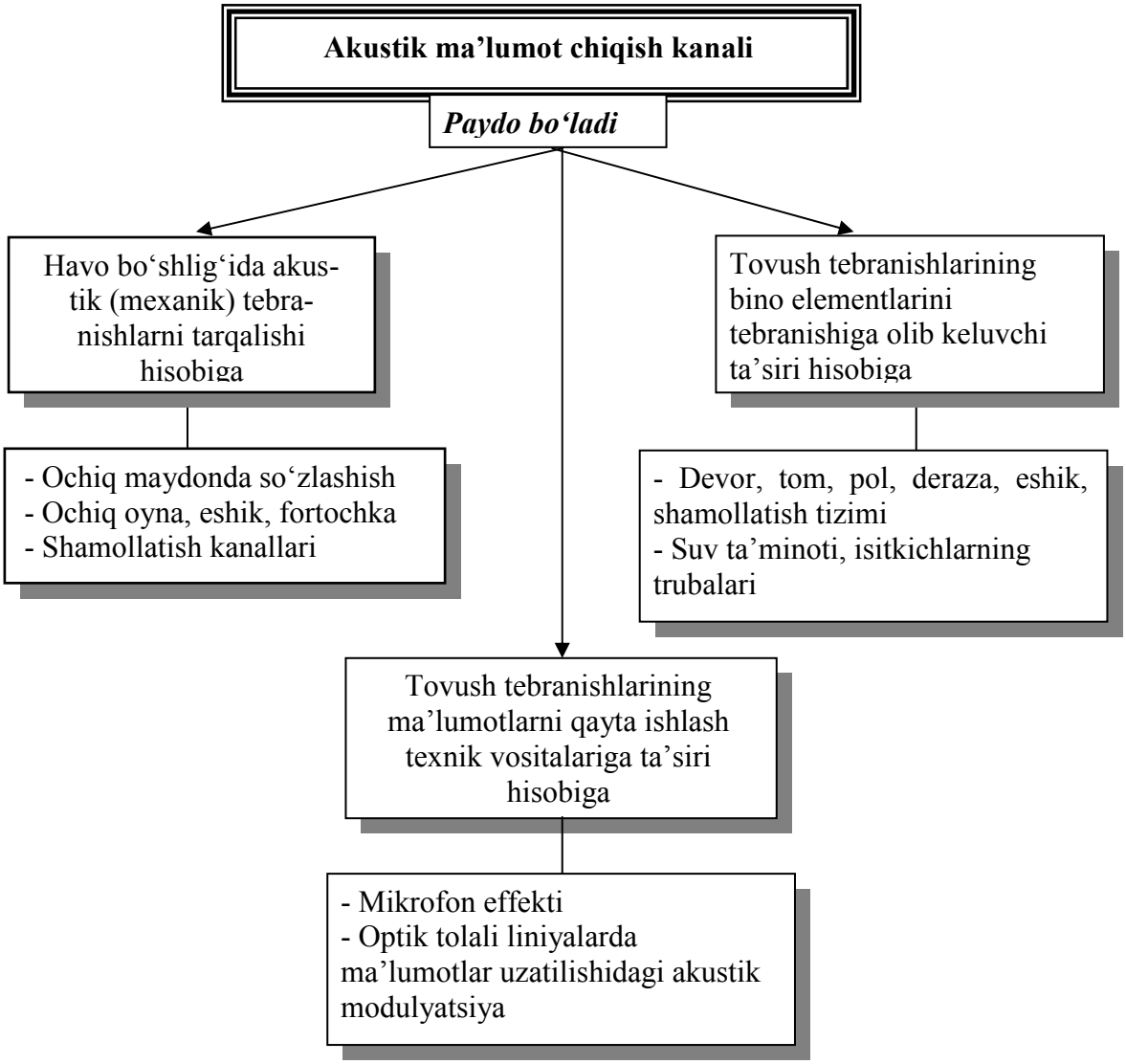
Vizual-optik kanallar – bu bevosita yoki uzoqdan (jumladan televizion) kuzatishdir. Ma’lumot tashuvchi bo‘lib, konfedensial ma’lumot manbasi chiqaradigan yoki undan qaytuvchi Ko‘rinadigan, infraqizil va ultrafiolet diapazondagi yorug‘lik xizmat qiladi.

Akustik kanallar. Inson uchun ma’lumotlarni eshitish qobiliyati ko‘rishdan keyin ikkinchi o‘rinda turadi. Shu sababli ma’lumot chiqib ketishi kanalining eng ko‘p tarqalgani akustik kanal hisoblanadi. Akustik kanalda ma’lumot tashuvchilarga ultra (20000 Gs dan yuqori), eshitish va infratovush diapazondagi to‘lqinlar kiradi. Inson eshitadigan tovush chastotasi 16 dan 20000 Gs gacha va inson gapirgandagi 100 dan 6000 Gs gacha bo‘ladi.

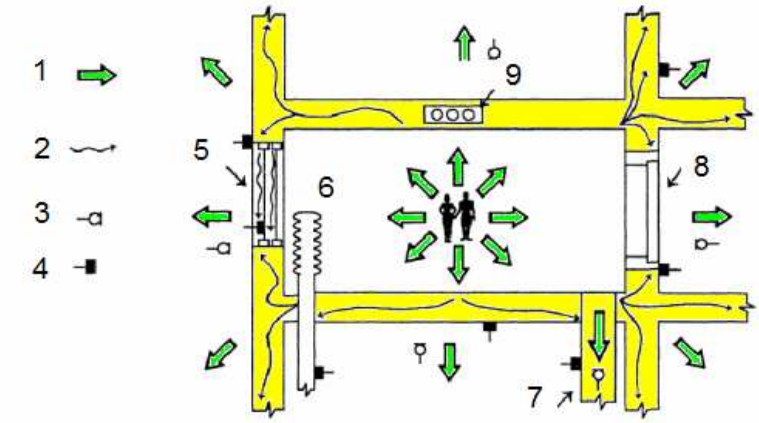


Havoda akustik to‘lqin tarqalganda havo zarralari tebranadi va buning natijasida biridan-biriga energiya uzatiladi. Agar tovush yo‘lida to‘siq bo‘lmasa, u hamma tomonga birday tarqaladi. Agar tovush to‘lqinlari yo‘lida devor, oyna, eshik, tom va kabi boshqa to‘siqlar bo‘lsa, tovush to‘lqini ularga ma’lum darajada bosim beradi hamda ularni ham tebrantiradi. Tovush to‘lqinlarining bunday ta’siri akustik ma’lumot chiqib ketishi kanalining paydo bo‘lishiga asosiy sabab bo‘ladi.

Muhitga qarab tovush to‘lqinlarining tarqalishi farq qiladi. Bu tovushning havo bo‘shlig‘ida to‘g‘ri tarqalishi, qattiq muhitda (tarkibiy tovush) tarqalishidir. Bundan tashqari, tovushning bino va imoratlarga bosim bilan ta’siri qilishi ularning tebranishiga sabab bo‘ladi.

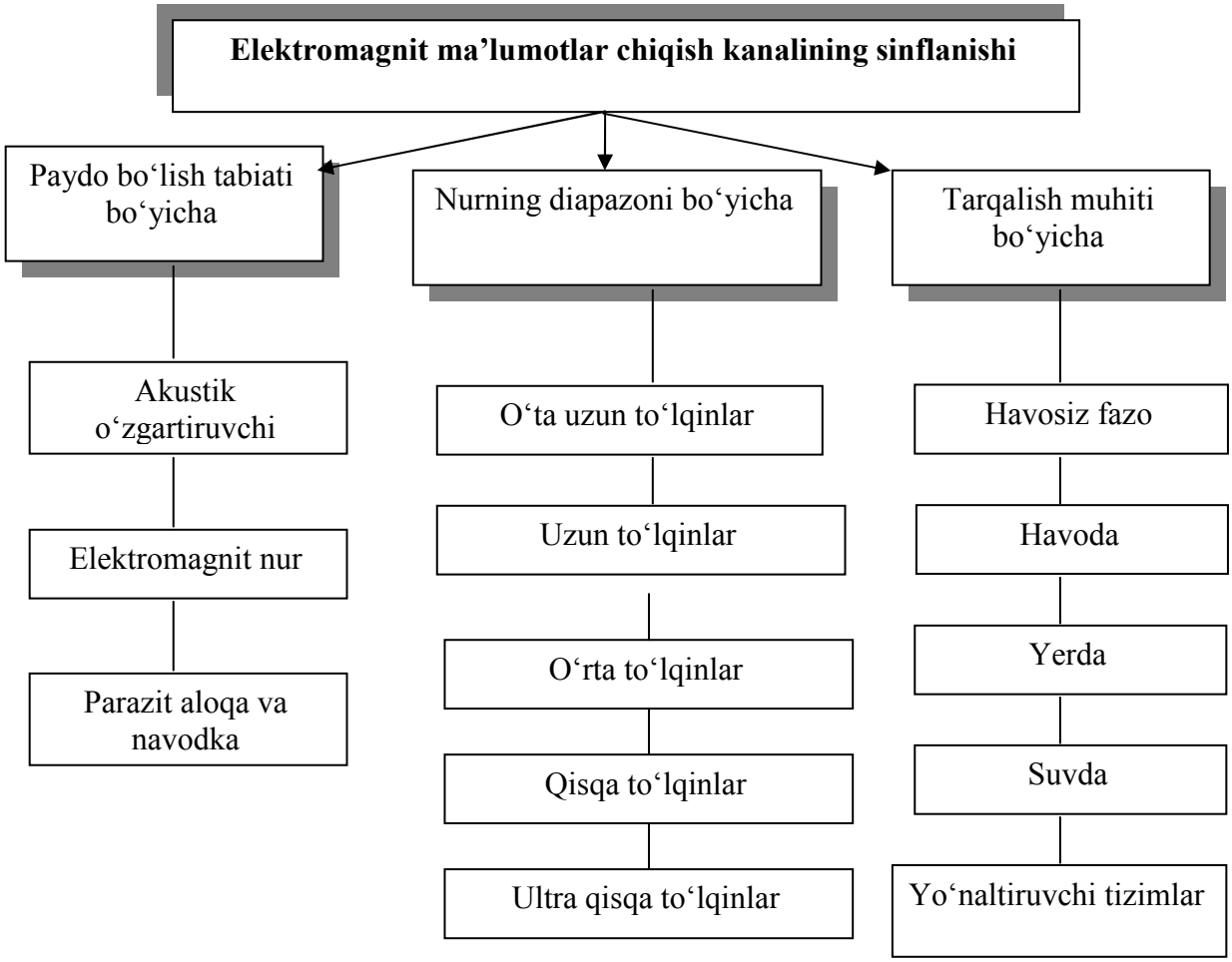


Quyidagi rasmda akustik va vibratsion tebranishlar orqali ma’lumotlar chiqib ketish kanallarining chizmasi keltirilgan bo‘lib, unda akustik tebranish va tovushlarning qattiq muhitda, metal buyumlarda va binoning boshqa elementlarida tarqalishi tasvirlangan.

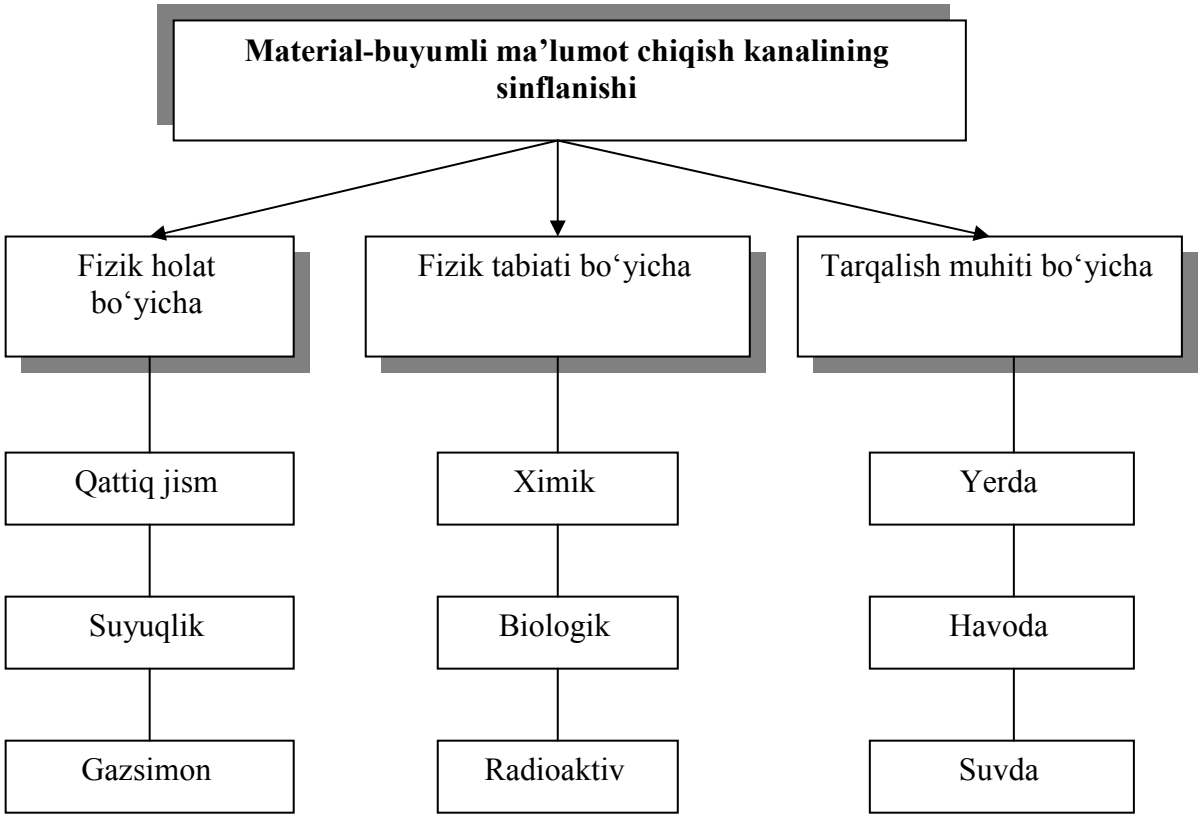


1. Akustik tebranishlarning tarqalishi
2. Vibratsion tebranishlarning tarqalishi
3. Eshitish mikrofoni
4. Eshitish vibrodatchigi
5. Deraza
6. Isitgich batareyalari
7. Havo tozalagich
8. Eshik
9. Kabellar uchun joy

Elektromagnit kanallar. Bunday hollarda ma’lumot tashuvchi, o‘ta uzun to‘lqin uzunligidan (10000 m – chastotasi 30 Gs dan kichik) submillimetrligacha (1-0,1 mm – chastotasi 300dan 3000 GGs gacha) bo‘lgan diapazondagi elektromagnit to‘lqinlar hisoblanadi. Bu ko‘rinishdagi har bir elektromagnit to‘lqin tarqalishning fazo va uzoqligi bo‘yicha o‘ziga xos xususiyatiga ega. Masalan, uzun to‘lqinlar juda uzoq masofalarga, millimetrlilar esa aksincha, faqat to‘g‘ri yo‘nalishda bir va bir necha o‘n kilometrga tarqaladi. Bundan tashqari, turli telefon va aloqa simlari hamda kabellari o‘z atrofida magnit va elektr maydonini hosil qiladi. Yaqin masofada bular ham ma’lumotlarning chiqib ketishi elementlariga kiradi.



Material-buyumli ma’lumot chiqib ketishi kanaliga qattiq, suyuq va gazsimon yoki korpuskulyar (radioaktiv elementlar) ko‘rinishdagi moddalar kiradi. Bular, juda ko‘p hollarda, sanoatning turli chiqindilari, sifatsiz mollar, xomaki materiallar va boshqalar bo‘lishi mumkin. Shunday ekan har bir konfedensial ma’lumot manbai u yoki bu darajadagi ma’lumot chiqib ketishi kanaliga ega bo‘lishi mumkin.



Ishlab chiqarishda, ilmiy faoliyatlarda va axborotlarni avtomatik qayta ishlashda turli texnik ta’minot vositalaridan keng foydalanish deb nom olgan ma’lumotlar chiqib ketishi *texnik* kanallari guruhining paydo bo‘lishiga olib keldi. Ularda ma’lumotlarni tashuvchi bo‘lib, turli xil toifadagi yondosh elektromagnit nurlanishlar va navodkalar (YOEMNN): akustik-o‘zgartiriladigan, nurlanuvchan hamda zararli aloqa va navodkalar hisoblanadi. YOEMNN ixtiyoriy elektron qurilmaga, tizimlarga, tabiiy xususiyatlarga ega bo‘lgan mahsulotlarga xosdir.

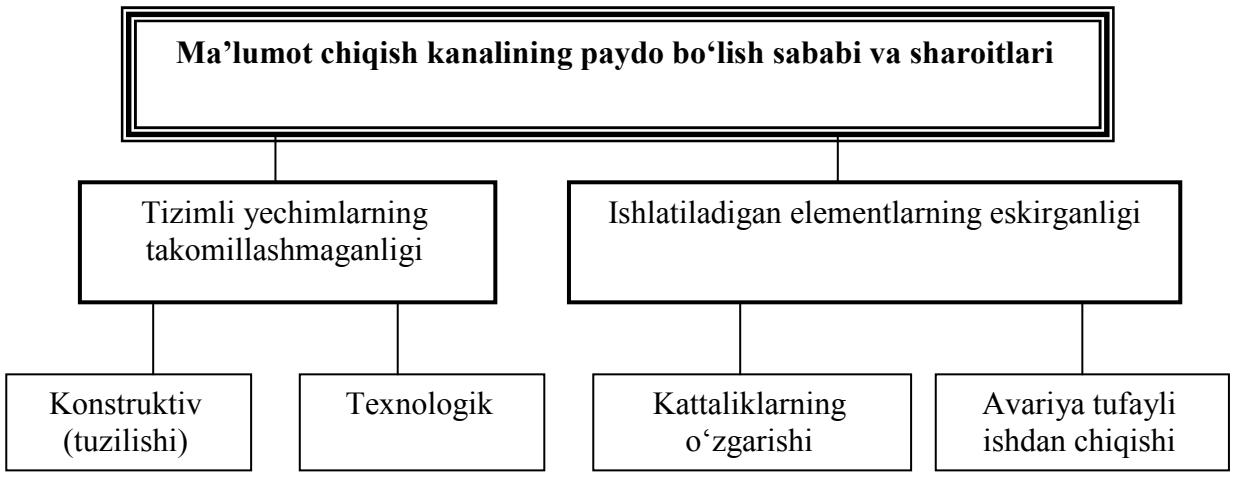
Xavfli nurlanishga asos bo‘luvchi fizik hodisalar turli xil tavsiflarga ega. Shuning bilan birga, bunday nurlanish hisobiga bo‘ladigan umumiy ko‘rinishidagi ma’lumotlar chiqib ketishini, himoyalanadigan ma’lumotlarning biror «qo‘shimcha» aloqa tizimi orqali uzatilishi deb qarash mumkin.

Shuni ta’kidlash joizki, texnik vosita va tizimlar nafaqat qayta ishlanadigan axborotlardan iborat bo‘lgan signallarni fazoga tarqatadi, balki o‘zining mikrofon yoki antennasi yordamida akustik yoki magnit (elektromagnit) nurlanishlarni qabul ham qiladi, ularni elektr signaliga aylantiradi va o‘z aloqa liniyasi orqali, odatda nazoratsiz, jo‘natadi. Bu esa ma’lumot chiqib ketishi xavfini yanada orttiradi.

Alohida texnik vositalar o‘z tarkibida «mikrofon» va «antenna» kabi

qurilmalardan tashqari yuqori chastotali yoki impulsli generatorlarga ham ega bo‘ladi. Ularning nurlanishi konfedensial ma’lumotlarga ega bo‘lgan turli signallarga moslashtirilgan bo‘lishi mumkin.

Xavfli «mikrofon effekt»i (zararli elektr signallarining paydo bo‘lishi) ayrim telefon qurilmalarida, hatto telefon trubkasi qo‘yilgan holda bo‘lishiga qaramasdan ham paydo bo‘ladi. Elektromagnit nurlanishlar tovush chiqaruvchi va tovush kuchaytiruvchi qurilmalarning radiochastotalarida o‘z-o‘zidan paydo bo‘lishida ham hosil bo‘lishi mumkin.



YOEMNNning paydo bo‘lish manbasining sharoiti va sababining tahlili shuni ko‘rsatadiki, uning paydo bo‘lishiga ma’lum toifadagi texnik vositalarning ishlash sxemasini takomillashmaganligini, elementlarning ishlatilishi natijasida eskirganligini va shu kabilar asos bo‘ladi.

Texnik kanal bo‘yicha ma’lumotlar chiqib ketishidan himoyalashda, odatda quyidagi amallarning bajarilishi talab etiladi**:**

1. Mumkin bo‘lgan ma’lumotlar chiqib ketishi kanallarini o‘z vaqtida aniqlash.
2. Nazorat zonasi (hududi, kabineti) chegarasida ma’lumot chiqib ketishi kanalining energetik tavsiflarini aniqlash.
3. Yovuz niyatli shaxslar tomonidan kanalni nazorat qilish vositalarining imkoniyatlarini baholash.
4. Tashkiliy, tashkiliy-texnik yoki texnik chora va vositalar yordamida ma’lumot chiqib ketishi kanallarining energetikasini yo‘q qilish yoki zaiflashtirish.

2.3. Obyektni kuzatish, eshitish va signalni tutib olishning asosiy usullari va tamoyillari

Ma'lumotlarni vizual-optik kanal bo'yicha chiqib ketishidan himoyalash – konfedensial ma'lumotlarning yorug'lik energiyasi hisobiga nazorat zonasidan chiqib ketishini bartaraf etish yoki kamaytirish bo'yicha kompleks tadbirlardir.

Ma'lumotlarni vizual-optik kanal bo'yicha chiqib ketishidan himoyalash maqsadida quyidagilar tavsiya etiladi:

– himoya obyekti shunday joylashtiriladiki, undan qaytadigan yorug'lik yovuz niyatli shaxslar joylashgan tomonga tushmasligi kerak (fazoviy to'siq);

– himoya obyektining yorug'lik qaytarish xususiyatini kamaytirish;

– himoya obyektining yorug'ligini kamaytirish (energetik chegaralash);

– atrofini o'rash vositalari (ekranlar, pardalar, qoraytirilgan oyna, niqob, to'siqlar va turli chegaralovchi vositalar)dan foydalanish yoki qaytgan yorug'likni iloji boricha susaytirish;

– himoya qilish va yovuz niyatlilarni chalg'itish maqsadida yashirish (maskirovka), imitatsiya va boshqa vositalarni qo'lla sh;

– himoya obyektini yorug'lik qaytarish xususiyati va fon yorqinligini o'zgartirish orqali maskirovkani amalga oshirish;

– nazoratsiz tarqalayotgan chiquvchi yoki qaytuvchi nurlardan manbani himoyalashda faol va passiv himoya vositalaridan foydalanish;

– obyektni maskirovka qilishda aerozol parda, maskirovkalovchi setka, bo'yoq kabilarni qo'lla sh.

Yashirishning tezkor vositalari sifatida aerozol pardalari keng qo'lla niladi. Ular turli moddalarning gazda suzib yuruvchi mayda zarralari bo'lib, o'lchami va agregat holatiga qarab tutun, tuman, qurum hosil qiladi va himoya obyektidan qaytgan yorug'likni to'sadi. Tutunsimon moddalar yorug'likni yaxshi yutish xususiyatiga ega.

Kuzatuv va foto suratga olishdan himoyalanishda quyidagilar tavsiya etiladi:

– hujjatlashtirish, ko'paytirish va ma'lumotlarni tasvirlash vositalari (kompyuter monitori, umumfoydalanishga mo'ljallangan ekran va boshqalar)ni to'g'ridan-to'g'ri yoki masofadan kuzatishning oldini olish uchun ularni optimal joylashtirish;

– yorug‘lik o‘tkazmaydigan oynalardan, pardalardan, plyonkalardan va boshqa himoyalash ashyolaridan (reshetka, deraza eshiklari va hokazo) foydalanish;

– derazalari xavfsiz zonaga (yo‘nalishga) qaratilgan xonalarni tanlash;

– ma’lum bir vaqtdan keyin kompyuter monitori va umumfoydalanish ekranlarini o‘chiruvchi vositalardan foydalanish (vaqt bo‘yicha ishlash rejimi).

Kuzatuvdan va joylarda foto suratga olishdan himoyalashda maskirovka choralarini ko‘rish, joylashish relyefidan foydalanib obyektni yashirish va obyekt faoliyatini yashirishni ta’minlovchi qo‘riqlash rejimini tashkil etish kerak.

Qiyinroq sharoitlarda faol yashirish vositalari (maskirovkalovchi tutun, aerozollar va boshqa vositalar)ni qo‘lla sh mumkin.

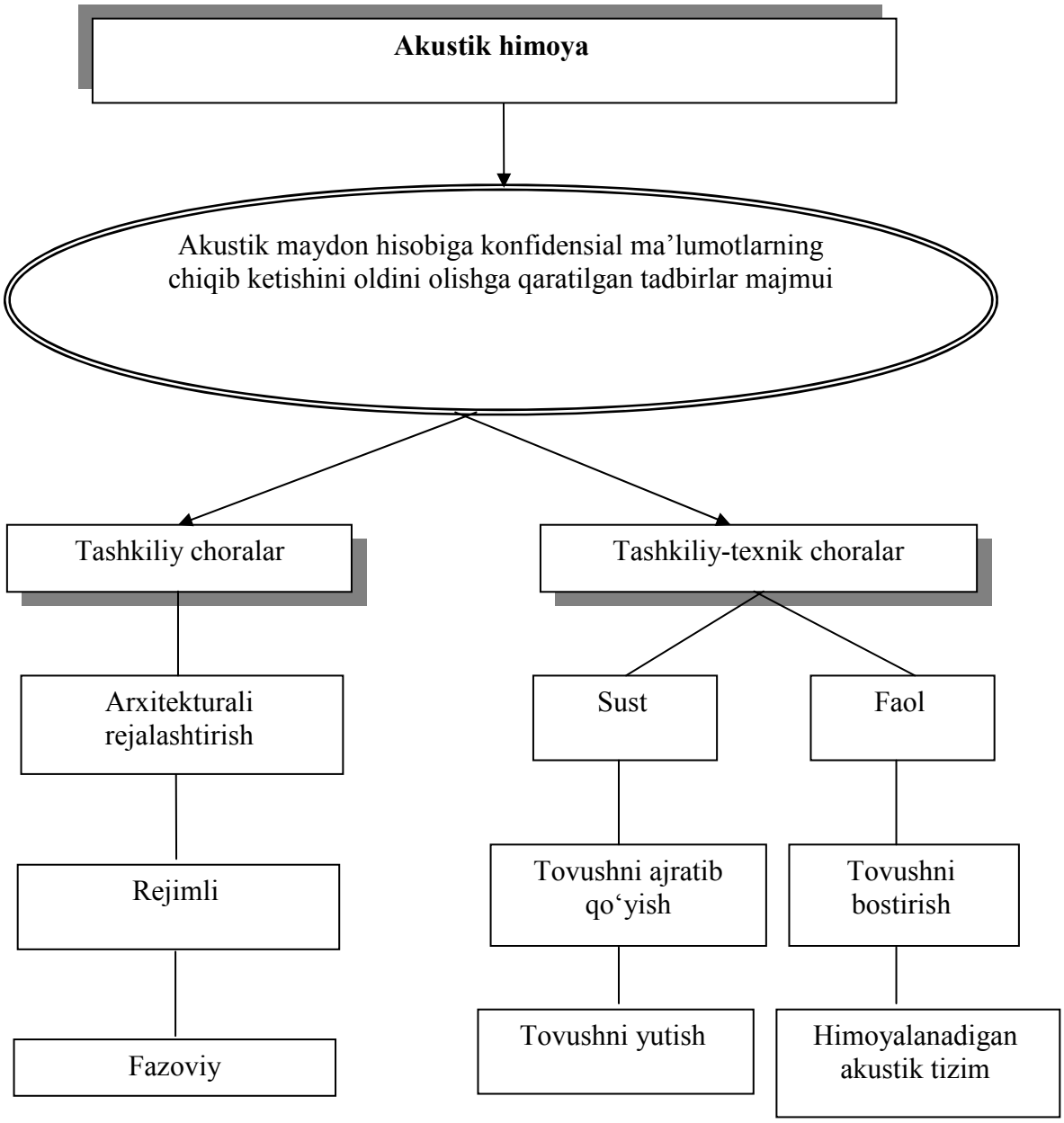
Ma’lumotni akustik kanal orqali chiqib ketishidan himoyalash – bu konfedensial ma’lumotlarni akustik maydon hisobiga nazorat zonasidan chiqib ketishini bartaraf etish yoki kamaytirish bo‘yicha kompleks tadbirlardir.

Himoyaning bu turidagi asosiy tadbirlarga tashkiliy va tashkiliy-texnik choralar kiradi.

Tashkiliy choralar arxitekturali rejalashtirish, fazoviy va rejimli tadbirlarni o‘tkazishni ko‘zda tutsa, *tashkiliy-texnik choralar* – sust (tovushni o‘tkazmaydigan qilish, tovushni yutish) va faol (tovushni bostirish) tadbirlardan tashkil topadi. Texnik tadbirlarni konfedensial so‘zlashuvlarni maxsus himoyalangan vositalardan foydalanish hisobiga o‘tkazish mumkin.

Tovushni o‘tkazmaydigan qilish bilan himoyalashning samaradorligini aniqlash uchun shovqin o‘lchagichlar ishlatiladi. *Shovqin o‘lchagich* – tovush bosimi tebranishlarini tovush bosimi darajasiga mos ko‘rsatkichlarga aylantiruvchi o‘lchov asbobidir. Odam tovushini akustik himoya qilish sohasida analogli shovqin o‘lchagichlardan foydalaniladi.

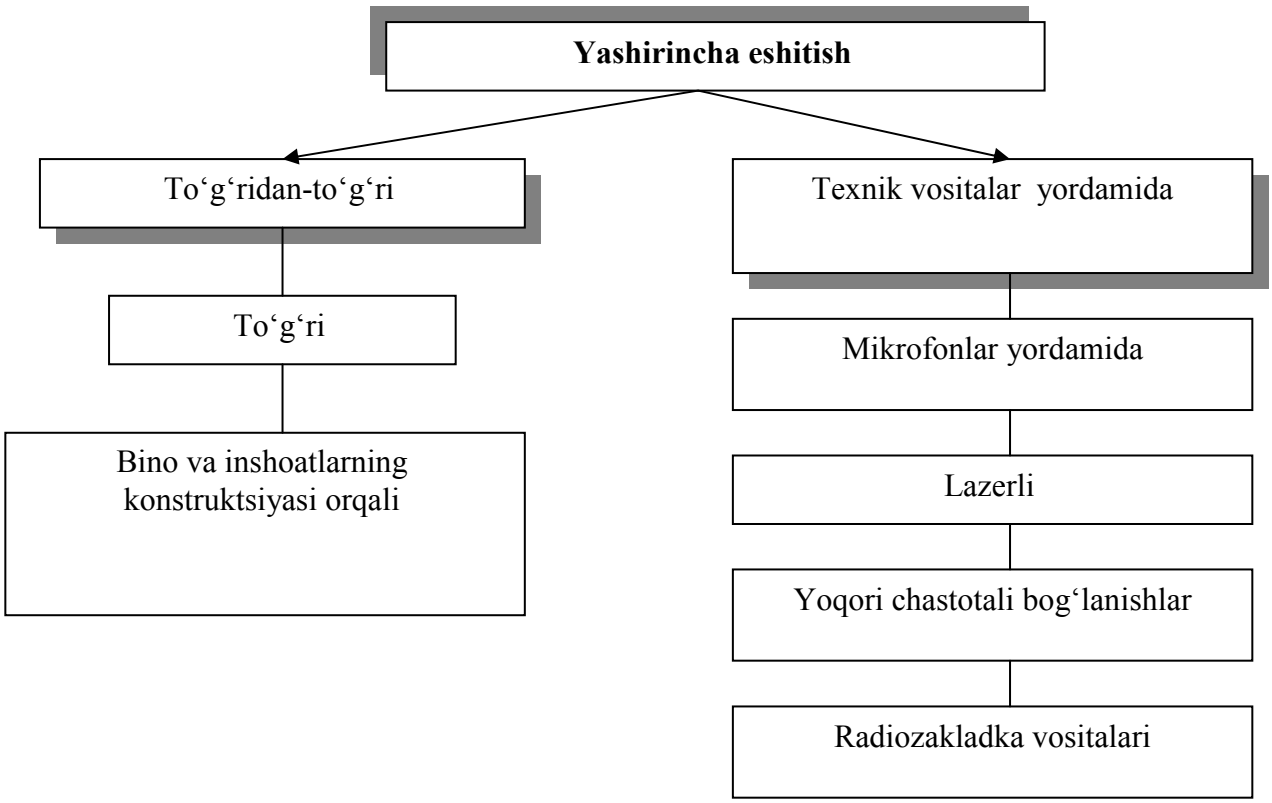
Aniqlik darajasi bo‘yicha shovqin o‘lchagichlar to‘rt sinfga ajratiladi. Nolinchi sinfdagi shovqin o‘lchagichlar laboratoriyadagi o‘lchashlarda, birinchisi – tabiiy sharoitdagi o‘lchashlarda, ikkinchisi – umumiy maqsadlardagi o‘lchashlarda, uchinchisi – yo‘naltirilgan o‘lchashlarda ishlatiladi. Amaliyotda akustik kanalning himoyalanganlik darajasini baholash uchun shovqin o‘lchagichlarning ikkinchi sinfi, kam hollarda birinchi sinfidan foydalaniladi.



Yashirincha eshitish – razvedka va sanoat ayg‘oqchiligini olib borish usuli bo‘lib, ayg‘oqchilar, kuzatuvchilar, pinhona eshitishning maxsus postlari, barcha razvedka bo‘linmalari tomonidan qo‘lla niladi. Aloqaning texnik vositalari orqali uzatiladigan so‘zlashuvlar va xabarlarni ham yashirincha eshitish amalga oshirilishi mumkin.

Ma’lumki, eshitish bevosita bo‘lishi mumkin, ya’ni gapiruvchining akustik tebranishlari to‘g‘ridan-to‘g‘ri yoki bino va inshoatlarning elementlari orqali eshituvchiga yetib boradi.

Ammo turli texnik vositalar: mikrofonlar, lazerlar, radiozakladka, yuqori chastotali tebranishlardan foydalanib so‘zlashuvlarni eshitish keng tarqalgan.



Ma’lumotlarni *elektromagnit kanal orqali chiqishdan himoyalash* – bu konfedensial ma’lumotlarni yondosh tasnifga ega elektromagnit maydon va navodkalar hisobiga nazorat zonasidan chiqib ketishini bartaraf etish yoki kamaytirish bo‘yicha kompleks tadbirlardir.

Ma’lumot chiqishining quyidagi elektromagnit kanallari mavjud:

– elektron sxemalar elementlarining mikrofon effekti;

– yuqori va past chastotali elektromagnit nurlanishlar;

– parazit kuchaytirgichlarning yuzaga kelishi;

– elektron sxemalarning manba zanjirlari va yerga ulanish zanjirlari;

– aloqa liniyasi va simlarning o‘zaro ta’siri;

– yuqori chastotali bog‘lanishlar;

– optik-tolali tizimlar.

Elektromagnit kanallardan ma’lumotlar chiqib ketishini himoyalash uchun umumiy himoyalash usullari va aynan shu turdagi kanalga mo‘ljallangan maxsus himoyalash usullari qo‘lla niladi. Bundan tashqari, himoya choralarini konstruktor-texnologik yechimlar va ekspluatatsion (foydalanish) sinflariga ajratish mumkin. Konstruktor-texnologik yechimlarda ma’lumotlarning chiqib ketishi ehtimoli mavjud bo‘lgan kanallarning paydo bo‘lishi bartaraf etiladi. Ekspluatatsion himoyada ishlab chiqarish va mehnat faoliyati sharoitida turli xil texnik vositalarni qo‘lla sh orqali chiqib ketish kanallari to‘siladi.

Ma’lumotlarga ishlov beruvchi va uzatuvchi texnik vositalardagi

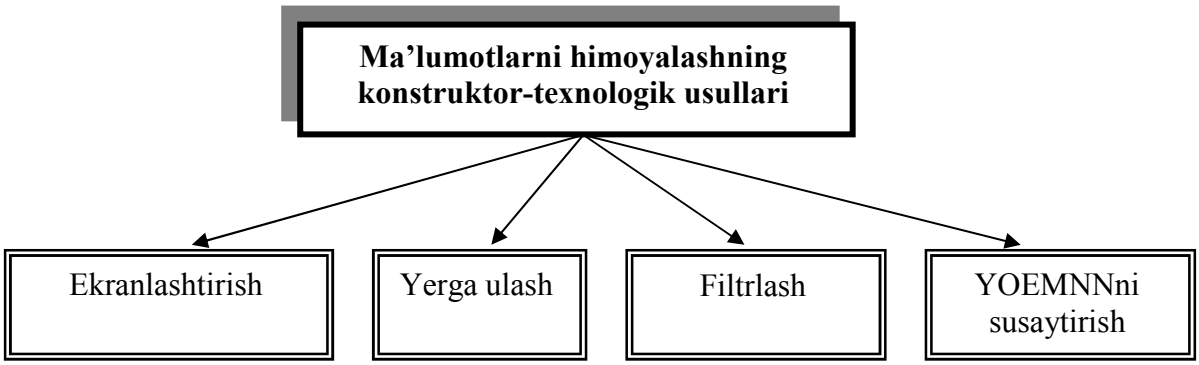
YOEMNN hisobidan paydo bo‘lishi mumkin bo‘lgan ma’lumotlar chiqib ketish kanalini oldini olish bo‘yicha konstruktor-texnologik tadbirlar maqbul konstruktor-texnologik yechimlarni qabul qilishga olib keladi. Unga quyidagilar kiradi:

– qurilma element va uzellarini ekranlashtirish;

– elementlar va tok o‘tkazuvchi simlar orasidagi elektromagnit, hajmli, induktiv aloqalarni susaytirish;

– manba va yerga ulanish zanjirlaridagi signallarni filtrlash va YOEMNNni susaytirish yoki bartaraf etish kabi tadbirlar.

Ekranlashtirish elementlarni keraksiz akustik va elektromagnit signallardan va o‘zining elektromagnit maydon nurlanishidan himoyalash imkonini beradi hamda tashqi nurlanishlarning zararli ta’sirini susaytiradi (yoki bartaraf etadi).



Qurilma va uning elementlarini yerga ulash hamda sirtlarini metall purkab qoplash yo‘naltirilgan signallarni yerga o‘tkazib yuborish, alohida zanjirlar orasidagi zararli aloqalarni susaytirishning ishonchli vositasidir.

Turli maqsadlarga mo‘ljallangan filtrlar paydo bo‘lgan yoki tarqaladigan signallarni kamaytirish yoki susaytirishga hamda axborotlarni qayta ishlash qurilmalarining manba tizimini himoya qilish uchun xizmat qiladi.

Tutib olish – bu radiodiapazondagi elektromagnit signallarni qabul qilish hisobiga konfedensial ma’lumotlarni ruxsatsiz olishdir.

Konfedensial ma’lumotlarni ruxsatsiz olish shaklidan biri bo‘lgan radio tutib olish jihatlariga ega:

– kriminal qiziqishli obyekt bilan bevosita bog‘lanmasdan amalga oshiriladi;

– turli diapazondagi radioto‘lqinlarning tarqalish chegarasi bilan aniqlanadigan katta masofa va fazoda o‘rinli;

– yil va kunning ixtiyoriy vaqtida va turli ob-havoda uzluksiz ta’minlanadi;

– ma’lumot aynan manbadan chiqqani uchun ishonchli ma’lumotlar bilan ta’minlaydi;

– turli statistik va tezkor tasnifdagi ma’lumotlarni olish imkonini beradi;

– qiziqtirgan ma’lumotlarni aniq vaqtda, amalga oshiriladigan voqealarni (u yoki bu amallarni bajarish haqidagi buyruqlarni tutish orqali) olish imkonini beradi;

– yashirincha amalga oshiriladi, chunki ma’lumot manbasi, odatda, ruxsatsiz kirilganlikni aniqlay olmaydi.

Turli diapazondagi radioto‘lqin nurlanish manbalari:

– mobil va statsionar tizimlar, jumladan yo‘ldoshlar, radioreleli va boshqalar uchun mo‘ljallangan radioaloqa vositalari;

– uyali radioaloqa vositalari;

– peydjingli aloqa vositalari;

– tezkor xizmat radioaloqa vositalari;

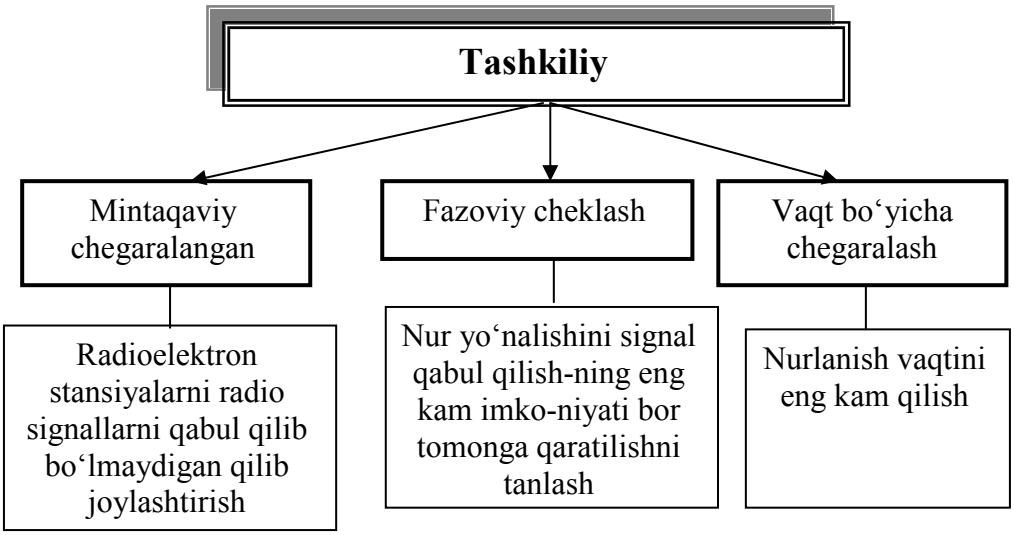
– radiotelefon uzaytirgich signallari;

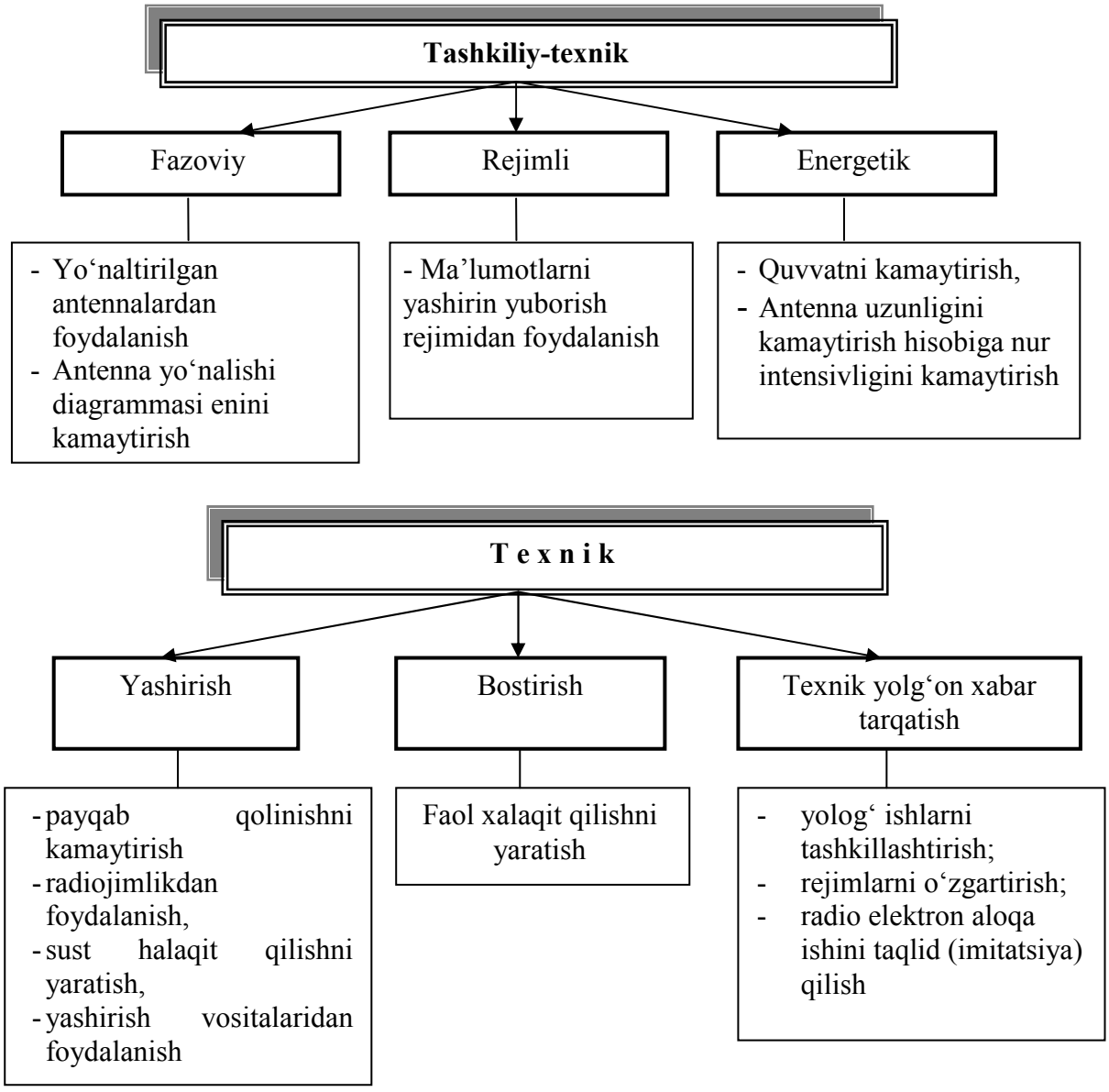
– radiomikrofon signallari;

– texnik vosita va tizimlarning signallari (radiolokatsion, radionavigatsiya tizimlar, elektron-hisoblash mashinalari vositalarining signallari);

– aloqa va texnologik tasnifdagi radiosignallar ochiq nurlanishining boshqa tizimlari (masalan, samolyotlar uchishini ta’minlovchi vositalar, suvda qutqarish vositalari va boshqalar).

Tutib olishdan himoyalash usullari: tashkiliy, tashkiliy-texnik, texnik.





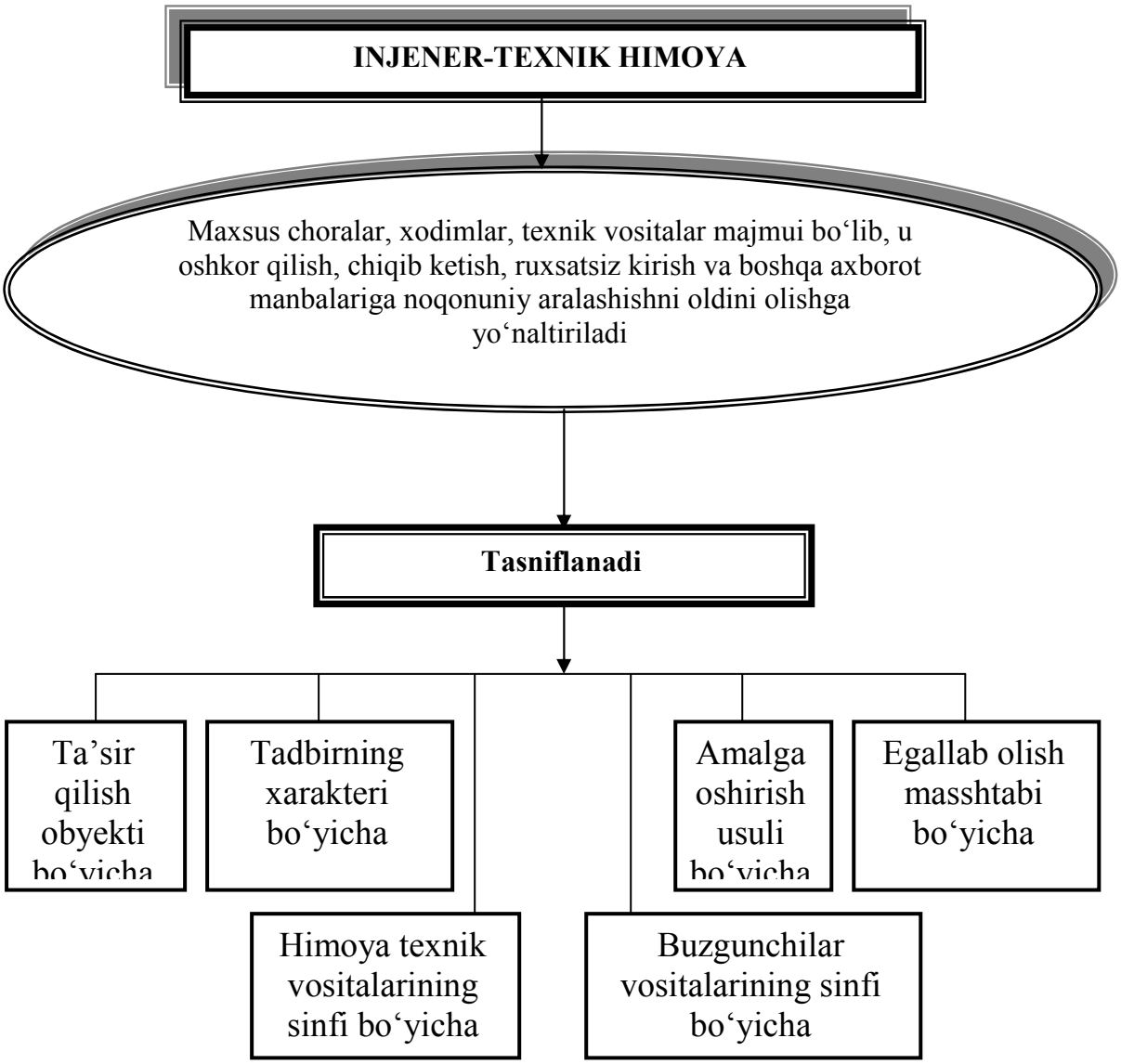
2.4. Axborotlarni injener-texnik himoyalash

Injener-texnik himoyaning tasnifi – bu konfedensial ma’lumotlarni himoyalashga qaratilgan maxsus idoralar, texnik vositalar va tadbirlar majmuidir.

Maqsad, vazifa, himoya obyektlari va o‘tkaziladigan tadbirlarning turlichaligi ko‘rinish, yo‘nalganlik va boshqa tavsiflar bo‘yicha vositalarning sinflanish tizimini qarab chiqishni taqozo etadi.

Masalan, himoyaning injener-texnik vositalarini ta’sir qilish obyektlari bo‘yicha qarash mumkin. Shu ma’noda ular insonlarni, moddiy boyliklarni, moliyani, ma’lumotlarni himoyalash uchun qo‘lla nilishi mumkin.

Quyidagi rasmda injener-texnik himoyaning taxminiy sinflanish tuzilishi keltirilgan:



Klassifikatsiya tavsiflarining turlichaligi injener-texnik vositalarni ta’sir obyekti, tadbir tavsifi, amalga oshirish usuli, egallash masshtabi, yovuz niyatlilar vositalarining sinfi bo‘yicha qarash imkonini beradi. Ularga qarshi faoliyatni xavfsizlik xizmati ko‘rsatadi.

Funksional vazifasi bo‘yicha injener-texnik himoya vositalarini guruhlarga ajratish mumkin:

– *fizik vositalar*. Ular himoya obyektlariga va konfedensial ma’lumotli moddiy tashuvchilarga yovuz niyatlilarni kirishiga (yoki foydalanishiga) to‘sqinlik qiladigan turli vosita va inshoatlardan tashkil topadi va xodimlarga, moddiy boyliklarga, moliya hamda axborotlarga noqonuniy ta’sir qilishdan himoyalashni amalga oshiradi;

– *apparat vositalari.* Bunga axborotlarni himoya qilish uchun ishlatiladigan asboblar, jihozlar, uskunalar va boshqa texnik vositalar kiradi. Tashkilotlarning ish faoliyatida juda ko‘p qurilmalar, telefon

apparatlaridan tortib avtomatlashtirilgan tizimlargacha ishlatiladi. Apparat vositalarining asosiy vazifasi – ishlab chiqarish faoliyatidagi texnik vositalar orqali ma’lumotlarning oshkora bo‘lishi, chiqib ketishi va ularga ruxsatsiz kirishdan qat’iy himoya qilishdir;

– *dasturiy vositalar*. Ular maxsus dasturlardan, dasturiy komplekslardan va turli maqsadlarga yo‘naltirilgan axborot tizimlaridagi va ma’lumotlarni qayta ishlash vositalaridagi himoya tizimlaridan iborat;

– *kriptografik vositalar* – bu ma’lumotlarni himoyalashning maxsus matematik va algoritmik vositalaridir. Ma’lumotlar tizim va aloqa tarmog‘i orqali uzatilishida, kompyuterda saqlanishida va qayta ishlanishida turli shifrlash usullardan foydalaniladi.

Himoyaning apparat vositalari va usullari keng tarqalgan. Biroq, ular yetarlicha o‘zgaruvchanlikka ega bo‘lmaganligi sababli himoyalangan ishlash prinsiplarining oshkora bo‘lishi ulardan ko‘pincha kelajakda foydalanishni yo‘qqa chiqaradi.

Himoyaning dasturiy vositalari va usullari ishonchli bo‘lib, ularning kafolatli ishlatilishi apparat vositalarga nisbatan ancha keng.

Kriptografik usul muhim ahamiyatga ega bo‘lib, ma’lumotlar himoyasini uzoq vaqtga saqlashni ta’minlaydigan vosita hisoblanadi.

Ma’lumotlarni himoyalash vositalarining bunday taqsimlash shartli hisoblanib, amaliyotda ular ko‘pincha: bir-birini to‘ldiradi, kompleks (ma’lumotlarni berkitish algoritmlaridan keng foydalanuvchi apparat-dasturiy modul) shaklda namoyon bo‘ladi.

Himoya tizimini ishlab chiqish bosqichlari.

Birinchi bosqichda (himoya obyektini tahlili) nimani himoya qilish aniqlanadi: himoyalash kerak bo‘lgan ma’lumotni aniqlash; himoyalanadigan ma’lumotning muhim elementlarni ajratish; himoyalanadigan ma’lumot muhim elementining yashash muddatini aniqlash (raqobatchi tomonidan qo‘lga kiritilgan ma’lumotni ochish uchun vaqt); himoyalanayotgan ma’lumotlarni tavsifini aks ettiruvchi kalit elementlarni (indikatorlarni) aniqlash; korxonaning faoliyat zonasi (ishlab chiqarish – texnologik jarayonlari, ishlab chiqarishning moddiy-texnik ta’minoti tizimi, boshqaruv bo‘linmalari) bo‘yicha indikatorlarini klassifikatsiyalash.

Ikkinchi bosqich xavfni aniqlashdan iborat: himoyalanadigan ma’lumot bilan kim qiziqishi mumkinligi aniqlanadi; raqobatdoshlarning ma’lumotni olish uchun foydalanadigan usullari baholanadi; ma’lumot chiqishi mumkin bo‘lgan kanallar aniqlanadi; raqobatdosh yoki ixtiyoriy buzg‘unchilarning

harakatini chegaralash bo‘yicha tadbirlar tizimi ishlab chiqiladi.

Uchinchi bosqichda qabul qilingan va doimiy ishlatiladigan xavfsizlikni ta’minlash tizimining samaradorligini tahlil qilish (hujjatlarning fizik xavfsizligi, xodimlarning ishonchliligi, konfedensial ma’lumot yuboriladigan aloqa kanalining xavfsizligi va boshqalar) amalga oshiriladi.

Himoya obyekti va ma’lumot chiqib ketish texnik kanalini modellashtirish asoslari. Zarar keltiruvchi ko‘p sonli manbalarni, obyektlarni va ta’sirlarni tahlil qilish uchun modellashtirish usullaridan foydalanish maqsadga muvofiqdir. Chunki bunda real holatlarni «o‘rnini bosuvchi» modellardan foydalaniladi. Model originalga nisbatan sodda hisoblanadi. Shu bilan birga, real holatni, uning murakkab tomonlarini hisobga olgan holda tasvirlash uchun yetarlicha umumiy bo‘lishi kerak.

Axborot xavfsizligi konseptual modelining tashkil etuvchilari quyidagilar bo‘lishi mumkin: xavf-xatar obyektlari; xavf-xatarlar; xavf-xatarlar manbai; yovuz niyatlilar tomonidan bo‘ladigan xavf-xatarlarning maqsadi; ma’lumotlar manbai; konfedensial ma’lumotlarni qonunga xilof ravishda egallash usullari (kirish usullari); ma’lumotlarni himoyalash yo‘llari; ma’lumotlarni himoyalash usullari; ma’lumotlarni himoyalash vositalari.

Hozirgi kunda barcha tashkilotlarda ma’lumotlarni himoyalash dolzarb vazifalardan biriga aylangan. Bu esa o‘z navbatida ma’lumotlar xavfsizligini fizik sathda ham ta’minlash zaruratini keltirib chiqaradi.

Ma’lumotlarni himoyalashning texnik vositalariga, himoya obyektiga borish yo‘liga to‘siqlarni hosil qilishga mo‘ljallangan, ma’lumotlarni himoyalashni mustaqil yoki boshqa vositalar bilan kompleksda amalga oshiruvchi mexanik, elektromexanik, elektron-mexanik, optik, akustik, lazer, radio, radiolokatsion va boshqa qurilmalar hamda tizim va binolar kiradi.

Ma’lumotlarni himoyalash muammosi paydo bo‘lganga qadar himoyaning fizik vositalari mavjud edi. Ular bank, do‘kon, muzey va shu kabilarni anchadan beri ma’lum bo‘lgan qo‘riqlash vositalaridan deyarli farq qilmaydi. Ma’lumotlar saqlanadigan va ularga ishlov beriladigan obyektlarni va ma’lumotlarning o‘zini himoyalash uchun murakkab va takomillashgan usullaridan foydalaniladi.

Fizik vositalar ma’lumotlar va hisoblash tizimi elementlari himoyasining birinchi chizig‘i hisoblanadi. Shuning uchun ham bunday tizim va qurilmalarning fizik butligini ta’minlash ma’lumotlar himoyasining

zaruriy sharti hisoblanadi. Rivojlangan xorijiy davlatlarda himoyaning fizik vositalari qo‘lla nishiga va takomillashuviga katta e’tibor qaratilmoqda.

Fizik himoya vositalarining asosiy vazifalari: 1.Hududni qo‘riqlash. 2. Asbob-uskunalar va ma’lumot tashuvchilarni qo‘riqlash. 3. Ichki xonalarni qo‘riqlash va ularni kuzatish. 4. Nazorat zonalariga nazoratli o‘tishni joriy qilish. 5. Navodka va nurlanishlarning ta’sirini yo‘qotish. 6. Vizual kuzatuvlarga to‘sqinlik qilish. 7.Yong‘inga qarshi himoya. 8. Buzg‘unchi shaxslarning harakatini blokirovka qilish.

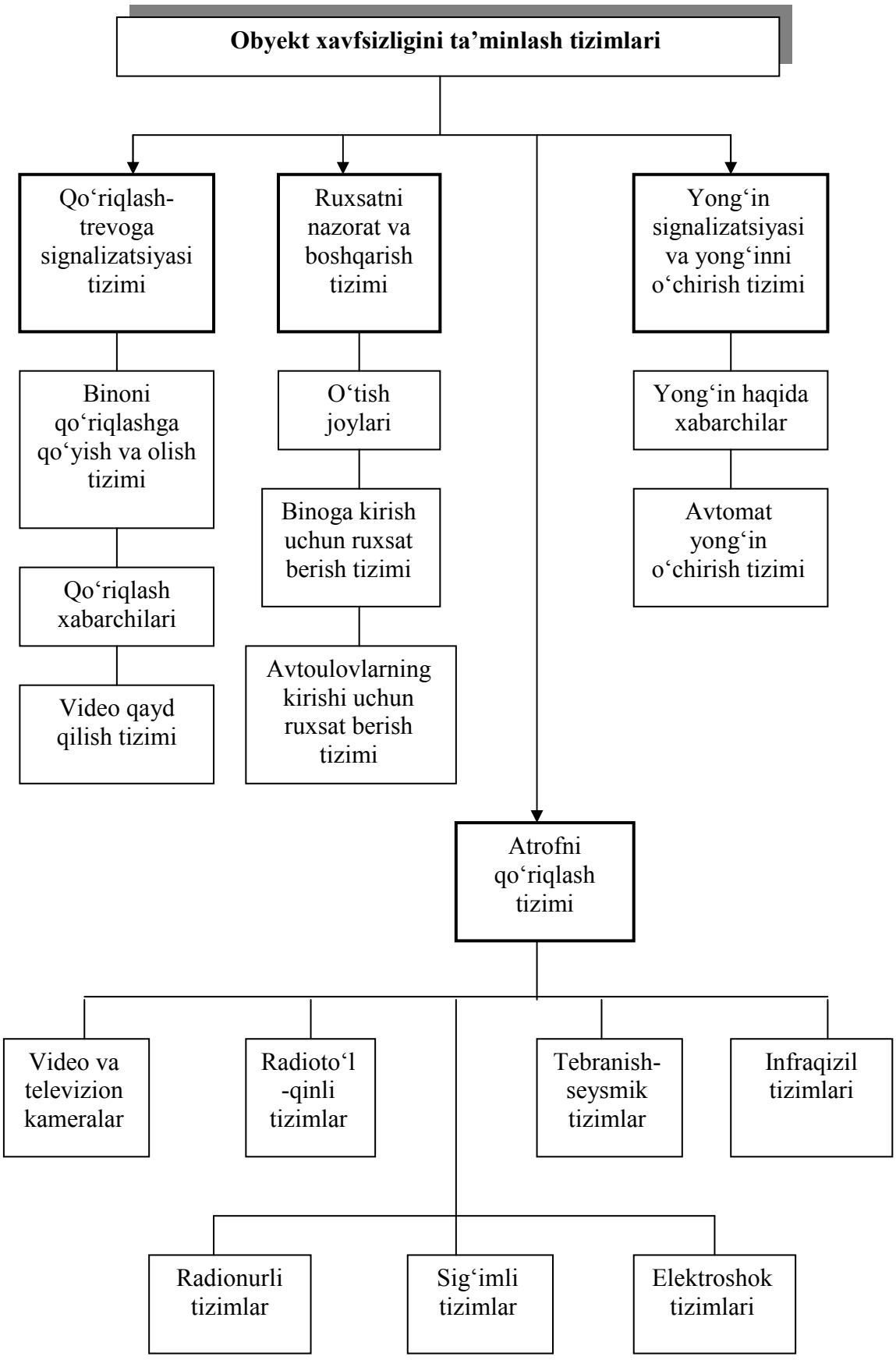
Tashkilotlardagi ma’lumotlarni elektron qayta ishlash markazlari kuchli elektromagnit nur manbai bo‘lgan obyektlardan uzoqda joylashgan bo‘lishi va atrofi devor bilan o‘ralishi kerak. Nazorat zonasini kuzatish televizion, radiolokatsion, lazerli, optik, akustik va boshqa umumiy pultga ulangan tizim orqali amalga oshirilishi mumkin.

Obyektlar xavfsizligini ta’minlash tizimlarining umumiy tuzilishi quyidagi rasmda keltirilgan. Aniq holatlar uchun sxemaning ayrim elementlari bo‘lmasligi yoki ayrim elementlar qo‘shilishi mumkin.

Odatda, obyektning xavfsizligini ta’minlash quyidagi tamoyillarga asoslanadi: obyektga bo‘lgan xavf-xatarni aniqlash va baholash; adekvat (mos) himoya choralarini ishlab chiqish va ularni qo‘lla sh.

Adekvat himoyalashda quyidagi va choralari choralar ko‘zda tutiladi: obyekt hududi, bino va xonalariga ruxsatsiz kirishni umumiy nazorat qilish; «yopiq» bino va xonalarga kiruvchi odamlarni cheklash va nazorat qilish hamda nazorat natijalarini hujjatlashtirish; yovuz niyatli shaxslarni oldiga qo‘ygan maqsadi tomon harakatining boshlang‘ich bosqichida aniqlash; vaziyatni baholash; tartibbuzarni ushlash uchun qo‘riqlovchilar tomonidan uning yo‘nalishini fizik to‘siqlar orqali to‘sish; yovuz niyatli shaxslar harakatini to‘xtatish uchun tezkor choralarni qo‘lla sh; obyektning o‘ta muhim uchastkalaridagi xodimlar harakatini videohujjatlashtirish.

Qo‘riqlash-ogohlantirish signalizatsiya tizimi (QOS): binolarni qo‘riqlashni qabul qiladi va topshiradi; yopilgan va qo‘riqlashga topshirilgan binoga begona shaxslarning ruxsatsiz kirishlarida yoki kirishga harakat qilishlarida trevoga signalini beradi; integrallashgan xavfsizlik tizimining avtomatlashtirilgan ish joyida qo‘riqlanayotgan binoning holatini bu bino plani bo‘yicha grafik rejimda kuzatadi hamda planda trevoga signalini yoki nosozliklarni grafik, matn va tovush shaklida akslantiradi; kompyuter xotirasida QOS tizimining holati haqida bayonnoma yuritadi hamda uni ko‘rish va chop etish imkonini beradi; standart va nostandart holatlarda operator faoliyatini qayd etuvchi elektron jurnalni yuritadi.



Kirishni nazorat qilish va boshqarish tizimi (KNBT) ruxsat etilgan xodimlarga tashkilot hududiga, kirish cheklangan xona va zonalarga kirishiga hamda ruxsati yo‘qlarga to‘siq bo‘lishga yo‘naltirilgan kompleks

tadbirlarni bajarish uchun mo‘ljallangan.

Yong‘in haqida signal berish tizimi:

– binoda aniqlangan yong‘in manbasi joyidagi datchiklardan kelayotgan xabarlarni qo‘riqlash posti xonasiga yuborish (har bir datchik «diqqat» va «yong‘in» degan xabarlarni berishi uchun alohida sezgirlik bo‘yicha sozlanishi hamda bu sozlashlar kunduzgi va kechki rejimlar uchun har xil bo‘lishi kerak);

– nosoz datchik manzilini ko‘rsatuvchi xabar qo‘riqlash postiga yuborish;

– odamlarga yong‘in haqida xabar berish va ventilatsiya tizimlari orqali havo oqimi kelishini to‘sib qo‘yishi

– avtomat ravishda yong‘in o‘chirish qurilmalarini boshqarish;

– yuqoridagi talablarni bajarishda avtonom rejimda ishlashi;

– yong‘in sodir bo‘lganligi holati va vaqtini qayd etish hamda hodisa haqidagi xabarning operatorlar ish joyidagi monitorlarda aks ettirish;

– integrallashgan xavfsizlik tizimining avtomatlashtirilgan ish joyida qo‘riqlanayotgan binoning holatini bu bino plani bo‘yicha grafik rejimda kuzatish hamda planda «yong‘in» signalini yoki nosozliklarni grafik, matn va tovush shaklida tasvirlash;

– kompyuter xotirasida yong‘in tizimining holati haqida bayonnoma yuritilish hamda uni ko‘rish va chop etish imkonini berish;

– standart va nostandart holatlarda operator faoliyatini qayd etuvchi elektron jurnalni yuritish uchun mo‘ljallanadi.

Obyektni perimetri bo‘yicha qo‘riqlashni tashkil etishda uning ichki hududi (qo‘riqlanadigan maydon) shartli ravishda: aniqlash, kuzatish, to‘xtatib qolish, nishonga olish kabi bir necha funksional zonalarga bo‘lib, har bir zonada o‘ziga xos texnik vositalar joylashishi kerak.

Mustaqil tayyorgarlik uchun savollar

1. Axborotlarni muhofaza qilishning texnik vositalari tushunchasi nimani anglatadi?

2. Ma’lumotlarni ruxsatsiz olishning obyektlari, usullari va vositalari nimalardan iborat?

3. Maskirovkalovchi belgilarning ochilishi tushunchasini nimani bildiradi?

4. Demaskirovka belgilari nimalar bilan farq qiladi?

5. Himoya obyektlarining demaskirovka belgilariga nimalar kiradi?

6. Texnik vositalar bilan himoyalanadigan ma’lumotlarning manbalari

va tashuvchilari nimalardan iborat?

7. Obyektning demaskirovka belgilari qanday guruhlarga bo‘linadi?

8. Obyektning ko‘rinadigan va infraqizil elektromagnit spektr diapazonlaridagi demaskirovka belgilari nimalardan iborat?

9. Radioelektron vositalarning qanday demaskirovka belgilari mavjud?

10. Nimalar ma’lumot tashuvchi vositalar hisoblanadi?

11. Ma’lumotlar chiqish kanali deb nimaga aytiladi?

12. Ma’lumotlar chiqib ketish kanali qanday guruhlarga ajratiladi?

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

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

15. Ma’lumotlarni vizual-optik kanal bo‘yicha chiqib ketishidan himoyalash qanday amalga oshiriladi?

16. Akustik kanal orqali ma’lumot chiqishidan himoyalashda qanday choralar Ko‘riladi?

17. Ma’lumot chiqishining qanday elektromagnit kanallari mavjud?

18. Ma’lumotlarni himoyalashning qanday konstruktor-texnologik usullari bor?

19. Tutib olishdan himoyalashning qanday usullar mavjud?

20. Injener-texnik himoya tushunchasi nimani bildiradi?

21. Funksional vazifasi bo‘yicha injener-texnik himoya vositalari qanday guruhlarga ajratiladi?

22. Himoya tizimini ishlab chiqish bosqichlari nimalardan iborat?

23. Fizik himoya vositalarining asosiy vazifalariga nimalar kiradi?

24. Obyekt xavfsizligini ta’minlash tizimlari nimalardan iborat?

III. AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH USULLARI

3.1. Kriptografiya: uning asosiy tushunchalari va qisqacha tarixi.
3.2. Sodda shifrlar va ularning xossalari.
3.3. Ochiq va yopiq kalitlar bilan shifrlash tizimi.

Kriptografiya axborotni muhofaza qilish usullaridan biri hisoblanadi. Kriptografiya axborot (ma'lumotlar)ni o'zgartirish tamoyillari, vositalari va usullarini tadqiq etadi. Bundan maqsad axborot mazmunidan ruxsat etilmagan foydalanishdan muhofazalash va uni buzishni bartaraf qilish. Kriptografiya ma'lumotlarni aloqa kanallari orqali uzatishda yoki saqlashda konfedensiallikni yoki haqiqiylikni ta'minlash usullari bilan shug'ullanadi.

Shu bilan birga kriptografiya ma'lumotlarni xabardor bo'lmagan shaxslar uchun tushuna olmaydigan qilish maqsadida o'zgartirish usuli hamdir. Ma'lumotlar xavfsizligi tizimining muhim tarkibiy bo'lagi. Uning mohiyati ma'lumotlarni uzatishdan oldin ma'nosiz belgilar yoki signallar yig'masiga aylantirish va ma'lumotlarni oluvchi qabul qilib olgandan so'ng, ularni dastlabki shakliga qayta tiklashdir.

3.1. Kriptografiya: asosiy tushunchalari va qisqacha tarixi

Insoniyat axborotni himoya qilish muammosi bilan yozuv paydo bo'lgandan beri shug'ullanadi. Bu muammo harbiy va diplomatik ma'lumotlarni yashirincha uzatish zaruratidan kelib chiqqan. Masalan, antik spartalilar harbiy ma'lumotlarni shifrlashgan. Xitoyliklar tomonidan oddiy yozuvni iyerogriflar ko'rinishida tasvirlashlari uni xorijiylardan yashirish imkonini bergan.

«Kriptografiya» atamasi grek tilidan tarjima qilinganda «yashirish, yozuvni berkitib qo'ymoq» ma'nosini bildiradi. Atamaning ma'nosi kriptografiya kerakli ma'lumotni yashirin saqlash va himoyalash maqsadida qo'llanishini anglatadi.

Kriptografiya axborotni himoyalash vositasi, shuning uchun u axborot xavfsizligini ta'minlashning bir tarmog'i hisoblanadi.

Kriptologiyaning (kripto – yashirin, logiya – fan, bilim) rivojlanishini

uchta bosqichga ajratish mumkin. *Birinchi bosqich* – kriptologiyani fan sifatidan e'tirof etilmagan davri, tor doiradagi qiziquvchilarga xos faoliyat turi bo‘lgan. *Ikkinchi bosqich* 1949-yildan boshlanib, K.Shenonning «*Maxfiy tizimlarda aloqa nazariyasi*» nomli risolaning chop etilishi bilan bog‘lanadi. Bu risolada shifrlashning fundamental ilmiy tadqiqoti va uning mustahkamligi yoritib berilgan. Bu kitobning chop etilishi kriptologiya amaliy matematikaning tarkibiy qismi sifatida shakllanishiga asos bo‘ldi. Va, nihoyat *3-bosqich* 1976-yilda U.Diffi va M.Xellman tomonidan «*Kriptografiyaning yangi yo‘nalishlari*» nomli asarning chop etilishi bilan belgilanadi. Unda maxfiy aloqa, yopiq kalitni avvaldan bermasdan ham, amalga oshirish mumkinligi bayon etilgan. Ushbu sanadan boshlab to hozirgi kungacha an'anaviy klassik kriptografiya bilan bir qatorda ochiq kalitli kriptografiyaning intensiv rivojlanishi davom etmoqda.

Bir necha asrlar davomida yozuvning paydo bo‘lishini o‘zi axborotni himoyalash sifatida e'tirof etilar edi, chunki yozuvni hamma ham tushunmas edi.

Eramizdan oldingi XX asr. Mesopatamiyada o‘tkazilgan qazilmalar vaqtida eng qadimiy shifrlangan matnlar topilgan. Loydan yasalgan taxtachaga qoziqchalar bilan yozilgan matn hunarmandlarning sopol buyumlarini qoplash uchun tayyorlanadigan bo‘yoqning retsepti bo‘lib, u tijorat siri hisoblangan. Qadimgi misrliklarning diniy yozuvlari va tibbiyot retseptlari ham ma'lum.

Eramizdan oldingi IX asrning o‘rtalari. Plutarx bergan ma'lumotlariga ko‘ra, ana shu davrda shifrlovchi qurilma – skital, qo‘lla nilgan bo‘lib, u o‘rin almashtirishlar orqali matnni shifrlash imkonini bergan. Matnni shifrlashda so‘zlar biror diametrli silindrga (skitalga) o‘ralgan ensiz lentaga yozilgan. Lenta yoyilganda unda ochiq matn harflarining o‘rinlari almashtirilgan holati hosil bo‘lgan. Bunda kalit sifatida silindrning diametri xizmat qilgan. Bunday matnni shifrdan yechish usulini Aristotel taklif etgan. U lentani konusga o‘ragan va o‘qilishi mumkin bo‘lgan so‘z yoki so‘zning bir qismini ko‘rsatuvchi joy silindrning diametri deb hisoblagan.

Eramizning 56-yili. Y.Sezar gallar bilan urush vaqtida shirflashning almashtirish turini qo‘llagan. Ochiq matn alfaviti ostiga sikl bo‘yicha (Sezarda uchta pozitsiyaga) siljitish orqali shu alfavit yozilgan. Shifrlashda ochiq matndagi alfavitlar, ya'ni yuqori qismda joylashgan harflar quyi qismdagi mos harflar bilan almashtirilgan. Bu turdagi shifrlash Y.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. Alfavit kvadrat jadval koʻrinishida tasvirlanadi. Shifrlashda ochiq matn harfi jadvaldagi ikkita songa almashtirilgan – mos tushuvchi harfning joylashgan ustun va qator raqamlariga. Alfavitni jadvalda ixtiyoriy tarzda joylashtirish va u orqali qisqa xabarni shifrlash zamonaviy qarashlar nuqtai nazari boʻyicha ham mustahkam shifrlash hisoblanadi. Bu gʻoya birinchi jahon urushida murakkab shifrlashlarda amalga oshirilgan.

V asrda Rim imperiyasining yemirilishi fan va san'at, shular qatorida kriptografiya rivojlanishining toʻxtashiga sabab boʻldi. U paytlarda cherkov maxfiy belgilar bilan yozilgan xatni ta'qib qilgan va uni afsungarlik va jodugarlik deb hisoblagan. Chunki ma'lumotlarni shifrlash cherkov tomonidan ularni nazorat qilish imkonini bermas edi.

Fransuz rohibi va faylasufi R.Bekon (1214–1294) maxfiy yozuvning yettita tizimini bayon etgan. U davrlarda koʻpgina shifrlar ilmiy axborotlarni yashirish uchun qoʻlla nilgan.

XV asrning ikkinchi yarmi. Vatikanda ishlagan, arxitektor va matematik, shifrlar toʻgʻrisidagi kitob muallifi Leon Batista Alberta ikkita konsentrik aylana asosida almashtirish shifrini bayon qilgan. Birinchi aylanaga ochiq matnning alfaviti joylashtirgan boʻlsa, ikkinchisiga shifrlovchi alfavit yozilgan. Bu shifrlovchi alfavitdagi harflar ketma-ket joylashtirilmagan. Matnda harflarning turli darajada qaytarilish xususiyatini Alberta birinchi boʻlib shifrni yechish uchun qoʻllagan. Shuningdek, shifrlashning mustahkamligini oshirish uchun boshqa shifrlash tizimlari yordamida qayta shifrlashni taklif etgan.

Tarixdan ma'lumki, 1546-yilda Fransiya qiroli Fransisk I fuqarolariga shifrlashni taqiqlovchi farmon e'lon qilgan. Vaholanki, u davrdagi shifrlar oddiy boʻlishiga qaramay, ularni ochib boʻlmas edi.

Germaniyalik Iogann Tritemiy (1462–1516) kriptografiya boʻyicha birinchi darsliklardan birini yozgan. «Ave Maria» deb nomlangan koʻp qiymatli almashtirishli original shifrlashni taklif etgan. Ochiq matnning har bir harfi shifrlovchining tanlovi boʻyicha bir emas, bir nechta harflarga almashtirilishi mumkin boʻlgan. Bunda harflar harf yoki soʻzlar bilan shunday almashtirilganki, natijada psevdomatn hosil boʻlgan. koʻp qiymatli almashtirish usulidan hozirgi kunda ham foydalaniladi (masalan, ARJ arxivatorida).

Italiyalik matematik, mexanik, vrach Djirolamo Kardano (1506–1576) Kardano panjarasi deb nomlangan shifrlash tizimini ixtiro qilgan. Ikkinchi jahon urushi vaqtida Buyuk Britaniya harbiy-dengiz qoʻshinlarining

mustahkam shifrlaridan biri shu tizim asosida yaratilgan. Panjaralar chizilgan karton bo‘lagida ixtiyoriy tartibda nomerlangan teshikchalar qilingan. Shifrlangan matnni hosil qilish uchun, karton bo‘lagini qog‘ozni ustiga qo‘yib, kartonning teshiklari bo‘lgan joylariga tanlangan tartibda harflar yozib chiqilgan. Karton olib tashlangandan so‘ng, yozilgan harflarning oralari psevdomazmunli jumlalar bilan to‘ldirilgan, shu orqali shifrlangan xabar yaratilgan. Agar harflar orasidagi masofalar katta bo‘lib, so‘zlar uzunligi kichik bo‘lsa (masalan ingliz tilidagi so‘zlar), yashirish oson amalga oshirilgan.

XVI asr. 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‘lla nilmoqda.

XVII asr. Fransiya qiroli Lyudovik XIII huzuridagi vazir kardinal Rishelye dunyoda birinchi bo‘lib shifrlash xizmatini tashkil etgan.

Lord Frensis Bekon (1562–1626) 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.

XVII asrda lug‘atli shifrlar ixtiro etilgan. Shifrlashda ochiq matn harflari ikkita son bilan belgilangan. Bunda keng tarqalgan kitoblardan biri olinib, shifrlanuvchi harf kitobning ma’lum betidagi qator nomeri va harf nomeriga almashtirilgan. Bu tizim mustahkam shifrlash usuli hisoblanadi, lekin undan foydalanish qulay emas. Shu bilan birga, kitob raqib qo‘liga tushib qolishi ehtimolidan holi emas.

Ma’lumki, kriptografik vositalar hozirgi vaqtgacha asosan davlat sirlarini himoya qilishga qaratilgan edi, shuning uchun bu vositalar maxsus organlar tomonidan yaratilgan. Bunda yuqori kriptomustahkamlikka ega bo‘lgan kriptotizimlar qo‘lla nilgan, bu esa katta xarajatlarni talab qilgan. Oxirgi yillarda ma’lumotlarni kriptografik o‘zgartirishning yangi usullari intensiv ishlab chiqilmoqda, ular an’anaviy qo‘lla nishiga qaraganda kengroq sohalarga tatbiq etilmoqda.

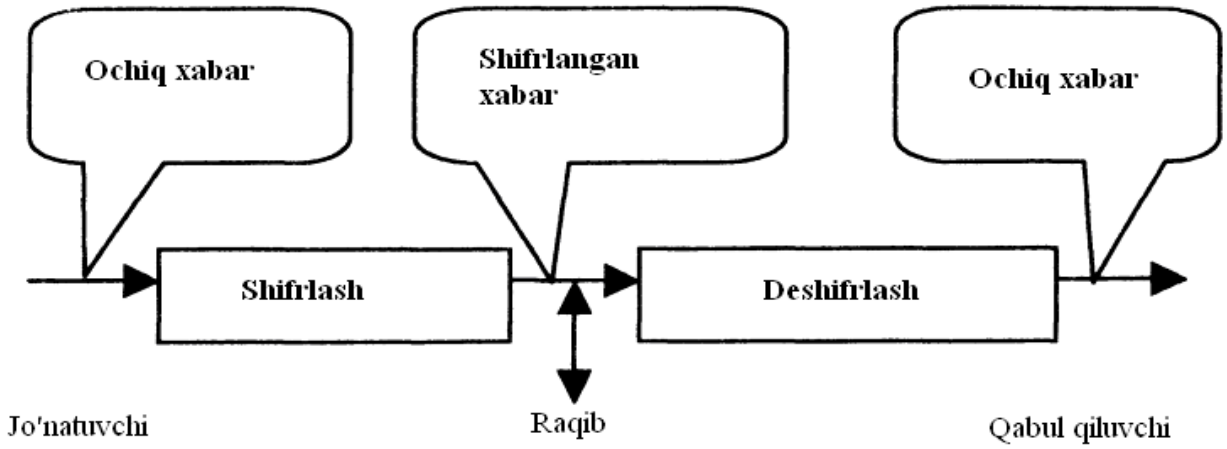
Avtomatlashtirilgan tizimlarda ma’lumotlar himoyasining kriptografik usullari hisoblash texnikasi vositalarida qayta ishlanayotgan yoki har xil turdagi saqlash qurilmalarida saqlanayotgan ma’lumotlarni himoyalashda, shuningdek aloqa liniyalari orqali tizim elementlariga uzatilayotgan ma’lumotlarni himoyalashda qo‘lla niladi. Hozirgi vaqtda ko‘plab har xil

shifrlash usullari ishlab chiqilgan va ularni qo‘lla shning nazariy va amaliy asoslari yaratilgan.

Axborot tizimlarida kriptografik usullar keng qo‘lla nilmoqda. Chunki kompyuter tarmoqlari, jumladan Internet jadal rivojlanmoqda. Tarmoq orqali davlat, harbiy, tijorat va xususiy tasnifga ega katta hajmdagi ma’lumotlar uzatilmoqda. Bu ma’lumotlarga begona shaxslarning kirishi mumkin emas. Shu bilan birga, yuqori quvvatli kompyuterlarning, tarmoq va neyron hisoblash texnologiyalarining paydo bo‘lishi avval o‘ta mustahkam, amalda yechimi yo‘q deb hisoblangan kriptografik tizimlarni obro‘sizlantirdi. Bu esa zamonaviy kriptografik usullardan foydalanish o‘ta dolzarb ekanligini anglatadi.

Zamonaviy kriptografiya axborot xavfsizligining *konfedensiallik*, *butunlik*, *autentifikatsiya* va *tomonlarning mualliflikni inkor etolmasliklari* muammolarini hal etuvchi bilim sohasi hisoblanadi.

Konfedensiallikni ta’minlash deganda axborot bilan tanishish huquqi bo‘lmagan shaxslardan bu axborotni himoyalash tushuniladi.



Raqib tomonidan nazoratda bo‘lgan aloqa kanali orqali uzatiladigan xabarning konfedensialligini ta’minlash muammosi kriptografiyaning an’anaviy masalalaridan hisoblanadi. Oddiy holda bu muammo uchta subyekt (tomonlar)ning o‘zaro munosabati sifatida bayon etiladi. Axborot egasi (jo‘natuvchi), raqibdan himoya qilish maqsadida, ochiq kanal orqali qabul qiluvchiga yuborilayotgan ochiq ma’lumotni o‘zgartiradi, ya’ni shifrlaydi.

Uzatilayotgan xabar ma’nosi bilan tanishish huquqi yo‘q subyekt raqibni anglatadi. Deshifrlash bilan shug‘ullanuvchi kriptotahlilchi ham raqib sifatida qaralishi mumkin. Olingan xabarni haqiqiy qabul qiluvchi *deshifrlaydi*. Raqib esa himoyalangan xabarga egalik qilmoqchi bo‘ladi, uning harakati *hujum* hisoblanadi. Hujum *faol* yoki *sust* bo‘lishi mumkin. *Sust* hujum yashirin eshitish, trafikni tahlil qilish, shifrlangan xabarni qo‘lga kiritish, *deshifrovka qilish*, ya’ni himoyani «sindirish»ga qaratilgan

harakatlar hisoblanadi. *Faol* hujumda raqib xabarni uzatish jarayonini to‘xtatib qo‘yishi, qalbaki xabarlar yuborishi yoki shifrlab uzatilayotgan xabarni modifikatsiya qilishi mumkin. Bu faol harakatlar mos ravishda imitatsiya qilishga va almashtirib qo‘yishga urinish hisoblanadi.

Kalit shifrlashning asosiy elementi bo‘lib, berilgan xabarni shifrlashdagi almashtirishlar u orqali amalga oshiriladi. Odatda, kalit harf va sonlarning biror-bir ketma-ketligidan iborat bo‘ladi.

Har bir almashtirish kalit bilan bir qiymatli aniqlanadi va biror kriptografik algoritm orqali amalga oshiriladi. Shifrlashda bir kriptografik algoritm har xil rejimlarda qo‘lla nishi mumkin. Shu tarzda har xil shifrlash usullari (oddiy almashtirish, gammalash va boshqalar) amalga oshiriladi. Har bir rejimning afzallik va kamchilik tomonlari mavjud. Shuning uchun rejimni tanlash konkret holatga bog‘liq. Deshifrlashdagi kriptografik algoritm, umumiy holda, shifrlashdagi algoritmdan farq qilishi mumkin. Bu holatda shifrlashdagi va deshifrovka qilishdagi kalitlar ham mos tushmasligi mumkin. Shifrlovchi va deshifrovka qiluvchi algoritmlar juftligini kriptotizim, bu algoritmlarni amalga oshiruvchi qurilmani shifrovchi texnika deyiladi.

Barcha holatlarga mos yagona shifr yo‘q. Shifrlash usulini, ya’ni kriptografik algoritm va undan foydalanish rejimini tanlash uzatilayotgan axborotning xususiyatiga (qiymatiga, hajmiga, tasvirlash usuliga, zaruriy uzatish tezligiga va boshqalar) hamda axborot egasining axborotni himoya qilish imkoniyatiga (qo‘llanilayotgan texnik vositalarining narxiga, qo‘lla shining qulayligiga, ishlashining ishonchligiga va boshqalar) bog‘liq. Himoyalanadigan axborot turli-tuman shakllarga (matnli, tovushli, rasmli va boshqalar) ega bo‘lishi mumkin. Har bir shaklning o‘ziga xos xususiyatlari mavjud bo‘lib, shifrlash usulini tanlashda uni inobatga olish kerak. Shifrlangan axborotning hajmi, uni talab etilgan tezlikda uzatish hamda aloqa kanalining har xil xalaqit beruvchi shovqinlardan himoyalanganligi katta ahamiyatga ega. Bularning barchasi kriptografik algoritmni tanlashda va himoyalangan aloqani tashkil etishda muhim rol o‘ynaydi.

Butunlikni ta’minlash deganda axborotni ruxsatsiz o‘zgartirib bo‘lmasligining kafolati tushuniladi. Butunlikni kafolatlash uchun ma’lumotlar bo‘yicha biron-bir o‘zgartirishlarni amalga oshirishni aniqlaydigan sodda va ishonchli mezon bo‘lishi kerak. Bu o‘zgartirishlar matnni o‘chirish, almashtirish, yangisini qo‘yish orqali amalga oshirilishi mumkin.

Autentifikatsiyalashni ta’minlash axborotli o‘zaro munosabat jarayonida axborotning o‘zini va tomonlarning haqiqiyligini tasdiqlash

usullarini ishlab chiqishni anglatadi. Aloqa kanali orqali uzatilayotgan axborot manbasi, yaratilgan sanasi, tashkil etuvchi ma’lumotlari, uzatish sanasi va shu kabilar bilan auditenfikatsiya qilinishi kerak.

Mualliflikni inkor etolmaslikni ta’minlash bu subyektlar tomonidan amalga oshirilgan harakatlarni tan olmaslik holati mumkinligini oldini oladi.

*Kriptografik faoliyatning tasnifi. ko‘p*gina kriptografik himoya usullarini qo‘lla shda biror-bir axborot almashish zaruriyati vujudga keladi. Masalan, axborot-telekommunikatsiya tizimi obyektlarini auditentifikatsiya qilish identifikatsiyalovchi va autentifikatsiyalovchi axborotlar almashinuvi orqali amalga oshadi. Umumiy holda, bunday tizimlar obyektlari (subyektlari)ning o‘zaro munosabati ma’lum bir kelishuvlar (*protokollar*)ga rioya etilgan holda bo‘ladi. Obyekt (subyekt)larning ma’lum bir maqsadga erishish uchun ketma-ket bajaradigan amalini formal jihatdan protokol deyish mumkin. qo‘yilgan maqsad protokolning tuzilishini va qo‘lla sh xususiyatini belgilaydi.

Kriptologiya ikki yo‘nalishdan: kriptografiya va kriptotahlildan iborat. Kriptotahlil kriptografiyaga teskari bo‘lib, unda kalitni bilmasdan turib axborotni deshifrlash amalga oshiriladi.

3.2. Sodda shifrlar va ularning xossalari

An’anaviy (klassik) shifrlash usullariga o‘rinlarini almashtirish shifrlari, oddiy va murakkab almashtirish shifrlari va ularning kombinatsiyalari va modifikatsiyalari kiradi. Ta’kidlash joizki, o‘rinlarini almashtirish shifrlari va almashtirish shifrlarining kombinatsiyalari amaliyotda qo‘lla nilayotgan har xil turdagi simmetrik shifrlarni tashkil etadi.

O‘rinlarini almashtirish shifrlarida shifrlanadigan matnning harflari shu matn bloki ichida ma’lum qoidalar bo‘yicha o‘rin almashtiriladi. O‘rinlarini almashtirish shifrlari eng sodda va eng qadimiy hisoblanadi.

Shifrlovchi jadvallar. Tiklanish (XIV asr oxirlari) davrining boshlarida o‘rinlarini almashtirish shifrlarida shifrlovchi jadvallardan foydalanilgan. Shifrlovchi jadvallarning kaliti sifatida: jadvalning o‘lchami; o‘rin almashtirishni belgilovchi so‘z yoki jumla; jadval tuzilishining xususiyati bo‘lgan.

Kalit sifatida jadvalning o‘lchami berilishi eng sodda jadvalli shifrlash hisoblanadi. Quyidagi matn berilgan bo‘lsin:

OBYEKT BELGILANGAN JOYGA BORADI

Ushbu axborot ustun bo‘yicha ketma – ket jadvalga kiritiladi:

O	K	L	A	N	G	R
B	T	G	N	J	A	A
Y	B	I	G	O	B	D
E	E	L	A	Y	O	I

Natijada, 4x7 o‘lchovli jadval tashkil qilinadi.

Endi shifrlangan matn qatorlar bo‘yicha aniqlanadi, ya’ni o‘zimiz uchun 4 tadan belgilarni ajratib yozamiz.

OKLA NGRB TGNJ AAYB IGOB DEEL AYOI

Bu yerda kalit sifatida jadval o‘lchovlari xizmat qiladi.

Tabiiyki, uzatuvchi va qabul qiluvchi kalit jadval o‘lchami bo‘lishligini o‘zaro kelishib olishlari kerak. Deshifrlashda teskari amal bajariladi.

Endi, kalit bo‘yicha oddiy o‘rnini almashtirish shifrini Ko‘rib chiqaylik. Bu usul oldingisiga nisbatan deshifrovka qilish uchun ancha murakkabdir. Bu usulda jadval ustunlari kalit bo‘luvchi so‘z, ibora, jumla orqali o‘rin almashtiriladi.

Misol tariqasida **UCHRASHUV INDINGA XIVA KINOTEATRIDA** matnini TEGIRMON so‘zini kalit sifatida qabul qilib, O‘rnini almashtirish shifrini qo‘lla b shifrlaylik. Matnda 32 ta va kalitda 8 ta harflar borligi uchun 8x4 jadval tuzamiz.

U	A	V	I	X	K	T	R
C	S	I	N	I	I	E	I
H	H	N	G	V	N	A	D
R	U	D	A	A	O	T	A

Endi kalit orqali 8x6 jadval tuzib kalitdagi harflarni alfavit bo‘yicha raqamlab chiqamiz.

T	e	g	i	r	m	o	n
8	2	1	3	7	4	6	5

U	A	V	I	X	K	T	R
C	S	I	N	I	I	E	I
H	H	N	G	V	N	A	D
R	U	D	A	A	O	T	A

Raqam bo‘yicha ustunlar o‘zgartiriladi.

g	e	i	m	n	o	r	T
1	2	3	4	5	6	7	8
V	A	I	K	R	T	X	U
I	S	N	I	I	E	I	C
N	H	G	N	D	A	V	H
D	U	A	O	A	T	A	R

Qator bo‘yicha 4 tadan bloklarga bo‘lib, simvollar ketma-ketligidagi shifrlangan matnni olamiz. Shuni e’tiborga olish kerakki, agar qatorda ketma-ket ikkita bir xil harf kelsa, chap tarafdan kelayotgan harf birinchi raqamlanadi, keyin esa ikkinchisi raqamlanadi va shifrlangan matn hosil qilinadi. Natijada quyidagi shifrlangan matn hosil bo‘ladi:

VAIK RTXU ISNI IEIC NHGN DAVN DUAO ATAR

Shifrni ochishda teskari jarayon amalga oshiriladi.

Shifrlangan matnning ochilishini yanada murakkablashtirish uchun u qaytadan shifrlanishi mumkin. Bu usul *ikki tomonlama o‘rin almashtirish* shifri deyiladi. Bu usulda kalit sifatida ustun va qatordagi harflar tartibidagi sonlardan foydalaniladi. Avvalam bor kalit simvollariga qarab jadval tuziladi va ochiq matn joylashtirilib chiqiladi. so‘ngra raqamlar navbatma-navbat tartiblanib, avval ustun, keyin qatorlar o‘rni almashtiriladi va jadvaldagi ma’lumot qator bo‘yicha o‘qilib, shifrlangan matnga ega bo‘linadi. Masalan: «**OBYEKT BUGUN KASAL**» ochiq matni shifrlash talab etilsin. Bu yerda kalit bo‘lib **1342** va **2341** xizmat qiladi.

4x4 jadval yaratib, ochiq matn qator bo‘yicha yoziladi:

	2	3	4	1
1	O	B	Y	E
3	K	T	B	U
4	G	U	N	K
2	A	S	A	L

K_1

Endi qator va ustunlar tartib bo‘yicha o‘rinlari almashtiriladi.

	2	3	4	1
1	O	B	Y	E
2	A	S	A	L
3	K	T	B	U
4	G	U	N	K

	1	2	3	4
1	E	O	B	Y
2	L	A	S	A
3	U	K	T	B
4	K	G	U	N

Oxirgi jadvalga asosan shifrlangan matnni yozamiz va bloklarga bo‘lib chiqamiz.

EOBY LASA UKTB KGUN

Ikki tomonlama almashtirishda jadval kattaligiga qarab variantlar ham ortib boradi. Jadval o‘lchamining kattaligi shifr chidamliligini oshiradi: 3x3 jadvalda 36 ta variant, 4x4 jadvalda 576 ta variant, 5x5 jadvalda 14400 variant.

Sehrli kvadrat deb, katakchalariga 1 dan boshlab natural sonlar yozilgan, undagi har bir ustun, satr va diagonal bo‘yicha sonlar yig‘indisi

bitta songa teng bo‘lgan kvadrat shaklidagi jadvalga aytiladi.

Sehrli kvadratga sonlar tartibi bo‘yicha belgilar kiritiladi va bu belgilar satrlar bo‘yicha o‘qilganda matn hosil bo‘ladi.

Misol tariqasida 4x4 o‘lchovli sehrli kvadratni olamiz, bunda sonlarning 880 ta har xil kombinatsiyasi mavjud. Kvadratni quyidagicha to‘ldiramiz:

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

Boshlang‘ich matn sifatida quyidagi **TOVAR OLTIDA KELDI** matnini olamiz va jadvalga joylashtiramiz:

I	**V**	**O**	**E**
R	**D**	**A**	**T**
I	**O**	**L**	**K**
A	**D**	**L**	**T**

Shifrlangan matn jadval elementlarini satrlar bo‘yicha o‘qish natijasida tashkil topadi:

IVOE RDAT IOLK ADLT

O‘rta va katta o‘lchamdagi sehrli kvadratlar yordamida, u davrlarda mustahkam shifrlashni amalga oshirish mumkin bo‘lgan. Chunki deshifrovka qilishda barcha variantlarni qo‘lda amalga oshirib bo‘lmas edi.

Oddiy almashtirish orqali shifrlash

Shifrlanadigan matnning harflari berilgan qoida bo‘yicha shu yoki boshqa alfavitdagi harflarga almashtiriladi. Oddiy almashtirish shifrida berilgan matnning har bir harfi shu alfavitdagi unga mos qo‘yilgan boshqa harfga almashtiriladi. Odatda, bu shifrlash usuli bir alfavitli almashtirish shifri deb ataladi.

Sezarning shifrlash tizimi. Sezarning shifrlash usuli oddiy almashtirish shifrining xususiy holidir. Bu usulda alfavitning har bir harfi K songa surilgan harfga almashtirilgan. Surilish alfavit oxiriga yetganda, uning boshidan boshlangan. Sezar K=3 bo‘lgan siljitishni qo‘llagan. Quyidagi jadvalda bu siljitishdagi lotin grafikasidagi harflarining mosligi keltirilgan:

A	D	J	M	S	V
B	E	K	N	T	W

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

Sezarning «keldim, ko‘rdim, yutdim» mazmundagi xabari VENI VIDI VICI, u taklif etgan usulda shifrlanganda YHQL YLGL YLFL ko‘rinishni oladi.

Sezar usulining kamchiligi bu bir xil harflarning o‘z navbatida, bir xil harflarga almashishidir. Kriptotahlilda harflarning takrorlanish chastotasi yordamida bu usulda shifrlangan matn tezgina rasshifrovka qilinishi mumkin.

Kalit so‘zli Sezar tizimi. Sezarning kalit so‘zli shifrlash tizimi bitta alfavitli almashtirish tizimi hisoblanadi. Bu usulda kalit so‘zi orqali harflarning surishda va tartibini o‘zgartirishda foydalanadi.

Misol tariqasida kalit so‘zi sifatida DIPLOMAT so‘zi va surish 5 ga teng qilib olingan bo‘lsin. Kalit so‘zi alfavit ostiga 5 ta harfga surilgan holda yoziladi:

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

Alfavitning qolgan alfavit ketma-ketligida kalit so‘zdan keyin yoziladi.

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

Natijada, berilgan matnning harflariga mos almashtiruvchi harflar aniqlanadi. Agar ochiq matn TOVAR KELDI bo‘lsa, shifrlashdan so‘ng JCNVG MZAYL matniga aylanadi.

*Vijinerning shifrlash tizimi***.** XVI asrda fransuz diplomati Vijiner tomonidan yaratilgan shifrlash tizimi 1586-yilda chop etilgan. U mashhur ko‘p alfavitli tizim hisoblanadi. Vijiner tizimi Sezar shifrlash tizimiga qaraganda mukammalroq hisoblanib, unda kalit harfdan harfga almashtiriladi. Bunday ko‘p alfavitli almashtirish shifrini shifrlash jadvali orqali ifodalash mumkin. Quyidagi jadvallarda rus va lotin alfavitlari uchun mos keluvchi jadvallar ko‘rsatilgan. Bu jadvallardan matnni

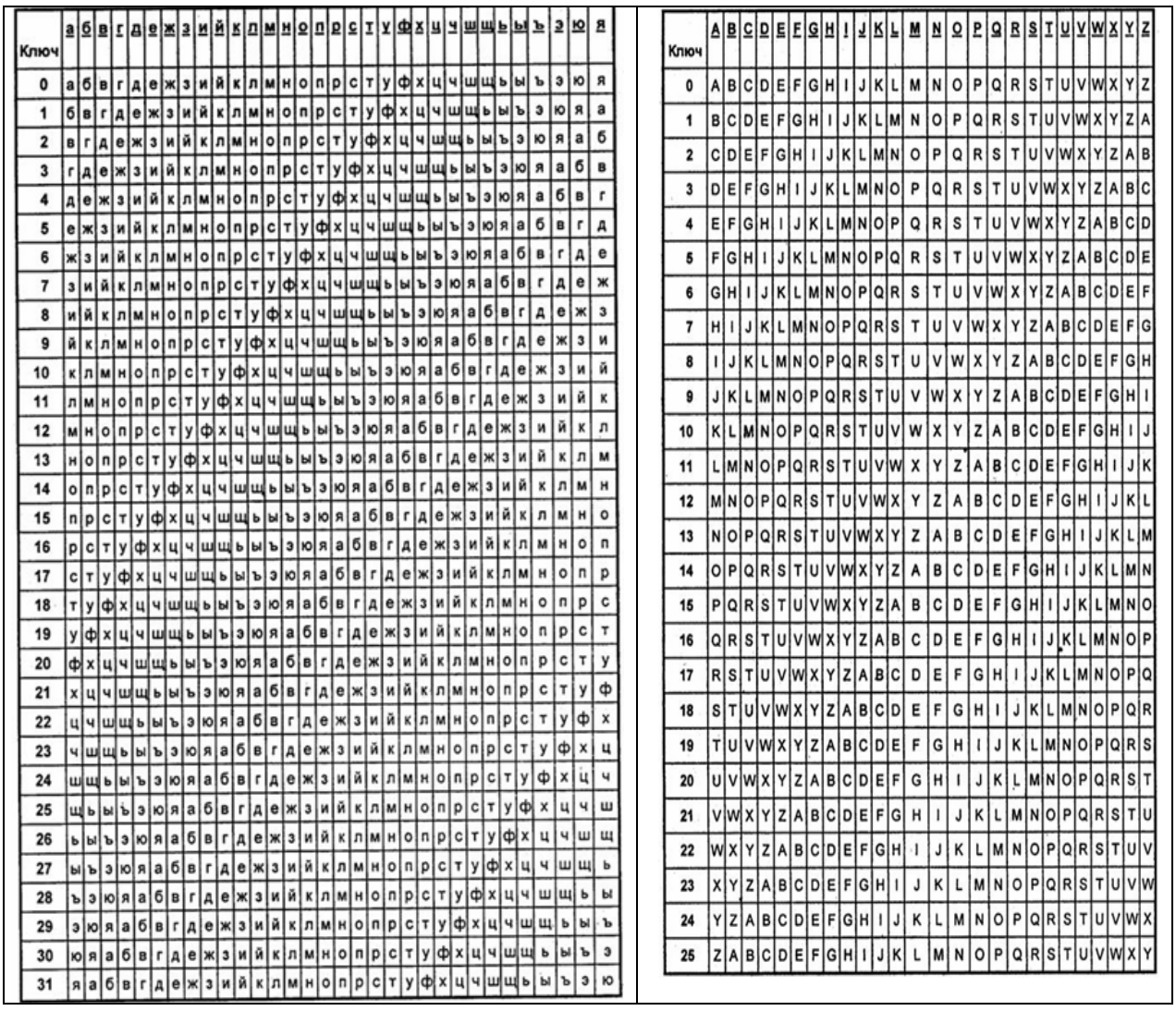
shifrlash va uni ochish uchun foydalaniladi. Jadvalning ikkita kirishi bo‘lib:

– yuqori qatordagi harflardan kiruvchi ochiq yozuv uchun foydalaniladi.

– chap ustunda esa kalit so‘zi joylashadi.

Ochiq matnni shifrlashda bu matn bir satrga yoziladi. Uning ostidagi satrga kalit so‘z joylashtiriladi. Agar kalit so‘zning uzunligi qisqa bo‘lsa, bu so‘z ochiq matnning oxirgi harfigacha takrorlab yoziladi. Shifrlash jarayonida jadvalning yuqori qismida joylashgan ochiq matnning harfi topiladi va chap qismdan kalit so‘zning harfi tanlanadi. Satr va ustun kesishgan katakdagi harf berilgan harfni almashtiradi.

Xabar	B	A	Y	R	A	M	K	U	N	I
Kalit	V	A	Z	A	V	A	Z	A	V	A
Shifrmatn	G	A	R	R	V	M	S	U	P	I



3.3. Ochiq va yopiq kalitlar bilan shifrlash tizimi

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

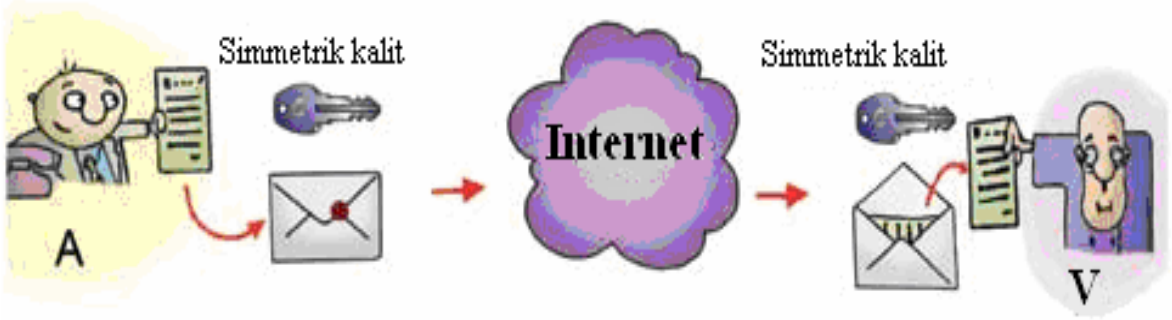
Xabarlarni shifrlash uchun foydalanilgan kalit shifrni ochish kalitidan olingan va aksi o‘rinli bo‘lsa, bunday kriptografik algoritmlar simmetrik deb nomlanadi. Ko‘pgina simmetrik algoritmlarda yagona kalitdan foydalaniladi. Bunday algoritmlar *bir kalitli* yoki maxfiy kalitli algoritmlar deb ataladi hamda xabarni yuboruvchi va uni qabul qiluvchi qanday kalitdan foydalanishni kelishib olishlarini talab etadi. Bir kalitli algoritmlarning ishonchliligi kalitni tanlash bilan aniqlanadi. Agar jinoyatchiga kalit ma’lum bo‘lsa, hech qanday qarshiliksiz barcha tutib olingan ma’lumotlar shifrini ochish imkoni yaratiladi. Demak tanlangan kalitni begonalardan sir saqlash zarur.

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 algoritmlar* yoki *blokli shifrlar* deb nomlanadi. Blokli shifrlashning zamonaviy kompyuter algoritmlarida, odatda, blok uzunligi 64 bitni tashkil etadi. Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

1) Axborot almashuvida ishtirok etuvchilar qanday yo‘l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?

2) Jo‘natilgan xabarning haqiqiyligini qanday aniqlasa bo‘ladi?

Simmetrik kalit bilan shifrlash sxemasini quyidagi misolda ko‘rib chiqamiz. Ali (A) va Vali (V) nomli korrespondentlar bir-biri bilan xabar almashishmoqchi. Korrespondentlarning har biri o‘zining maxfiy kalitiga ega, bu kalitdan xabarni tarmoq orqali yuborishdan avval ma’lumotlarni shifrlashda foydalanishi mumkin. Shifrlash sxemasini ko‘rimliroq tasvirlash uchun, kalitni oddiy kalit, shifrlangan xabarni esa konvertga solingan hujjat ko‘rinishida tasvirlaymiz. Shifrlash va qayta shifrlash jarayoni quyidagi rasmda tasvirlangan.



Simmetrik kalit yordamida shifrlash tizimi

Foydalanuvchi A o‘zining maxfiy kaliti bilan xabarni shifrlaydi va xabarni tarmoq orqali jo‘natadi, qabul qiluvchi V (xuddi shunday maxfiy kalitdan foydalanib) xabarni qayta tiklaydi. Rasmda sxemaning simmetrik ekanligi ko‘rinib turibdi. Chap va o‘ng tomondagi foydalanuvchilar bir xil (simmetrik) kalitlardan foydalanishmoqda, shuning uchun bunday turdagi shifrlash simmetrik kalit yordamida shifrlash deb yuritiladi.

Maxfiy kalit yordamida shifrlash usuli ma’lum kamchiliklardan holi emas. Birinchi navbatda, simmetrik shifrlash autentifikatsiyalash muammosini hal qilib bermaydi. Masalan, Ali (A) Soli (S)ga xat yozib yuborishi, lekin bu xatni Vali (V) yozgan deb tan olmasligi mumkin. Bundan tashqari, simmetrik kalit xabar yuborilishidan oldin xabar jo‘natuvchi va qabul qiluvchi kompyuterlarda o‘rnatilgan bo‘lishi kerak. Tabiiyki, Internetda xavfsiz muloqot qilish uchun shifrlash, korrespondentlarning shaxsan uchrashishlari shart bo‘lmagan holatda ma’noga ega. Muammo maxfiy kalitni uzatishda yuzaga keladi. Haqiqatda, agar jo‘natuvchi Ali qabul qiluvchi Valiga kalitni shifrlamasdan uzatsa, kalitni tutib olishlari mumkin. Agar kalit shifrlangan ko‘rinishda jo‘natilsa, unda qabul qiluvchi Vali uni ocha olmaydi. Bir nechta korrespondentlar bilan yozishmalar olib borish uchun, har bir qabul qiluvchi uchun alohida kalitlar bo‘lishi lozim, bu esa noqulaylikni tug‘diradi. Bu muammoni yechimini topish uchun asimmetrik shifrlash (ochiq (ommaviy) kalit yordamida shifrlash) sxemasi taklif etilgan.

Ochiq kalitli shifrlash yoki shifrlashning asimmetrik algoritmlari deb ataluvchi algoritmlarda shifrlash uchun ishlatiladigan kalit shifrni ochish uchun ishlatiladigan kalitdan farq qiladi. Bundan tashqari, shifrlash kalitini bilgan holda, shifrni ochish uchun zarur kalitni juda katta muddat ichida hisoblab topish imkoni bo‘lmaydi. Ixtiyoriy foydalanuvchi shifrlash kaliti yordamida xabarni shifrlashi mumkin, lekin bu kalitga mos shifrni ochish kalitiga ega shaxsgina bu xabarni o‘qiy oladi. Shifrlash kalitini ochiq (ommaviy) kalit, shifrni ochish kalitini esa yopiq (maxfiy, xususiy) kalit deyiladi. Xabarni yopiq yoki ochiq kalit yordamida shifrlash mumkin, qayta tiklash esa ikkinchi kalit yordamida amalga oshiriladi. Ya’ni, yopiq kalit yordamida shifrlangan matn faqat ochiq kalit yordamida qayta tiklanishi mumkin va aksincha. Yopiq kalit faqat egasiga ma’lum, va u hech kimga berilmaydi, ochiq kalit esa ochiq tarqatiladi va u hammaga ma’lum bo‘lishi mumkin. Ikkita kalitni autentifikatsiyalash masalasining yechimini topish uchun hamda konfedensiallikni ta’minlashda qo‘llash mumkin.

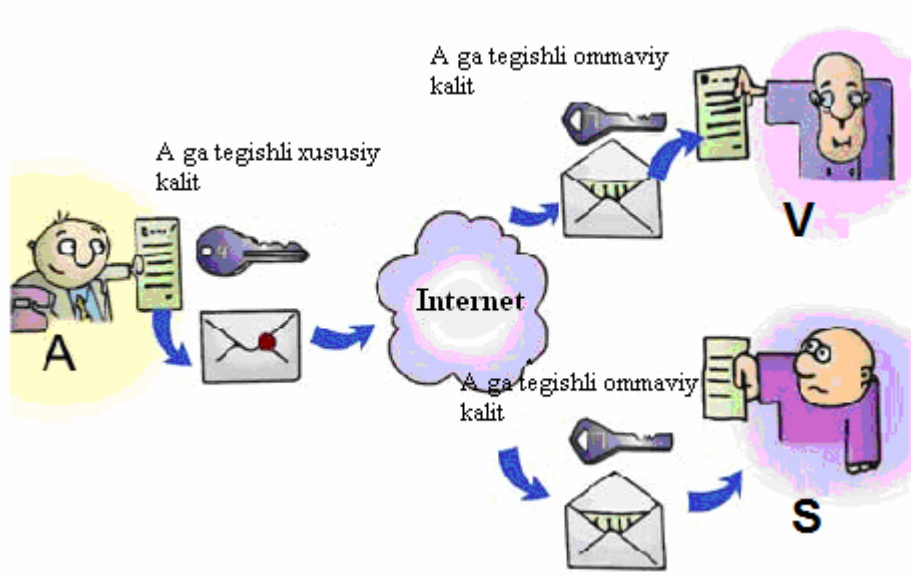
Agar birinchi kalit yopiq bo‘lsa, u holda u elektron imzo sifatida ishlatiladi va bu usul bilan axborotni autentifikatsiyalash, ya’ni axborotning butunligini ta’minlash imkoni paydo bo‘ladi.

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

– foydalanuvchini autentifikatsiyalash, ya’ni kompyuter tizimi resurslariga kirmoqchi bo‘lgan foydalanuvchini aniqlash;

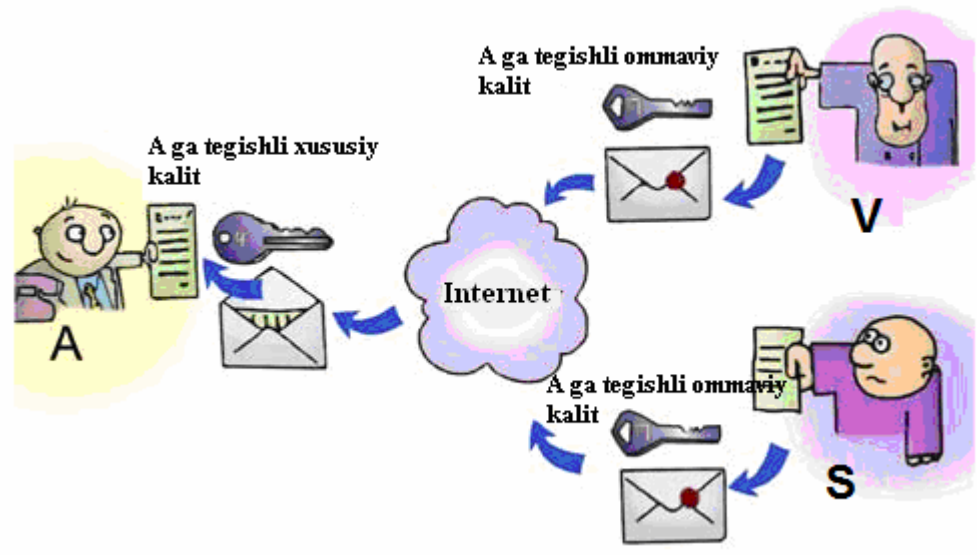
– tarmoq abonentlari aloqasini o‘rnatish jarayonida ularni o‘zaro autentifikatsiyalash.

Quyidagi sxemaga muvofiq, foydalanuvchi Ali (A) oldindan ochiq kalitni Vali (V) va Soli (S) nomli korrespondentlarga jo‘natadi, keyin esa yopiq kalit bilan shifrlangan matnni yuboradi.



Xabarni faqat Ali (A) jo‘natishi mumkin (yopiq kalit unga tegishli), bunda autentifikatsiya muammosi yechilgan. Lekin, masalan Vali (V)ning unga yo‘llangan xatni Soli (S) o‘qimaganligiga aniq ishonchi yo‘q. Demak, konfedensiallik ta’minlanmagan.

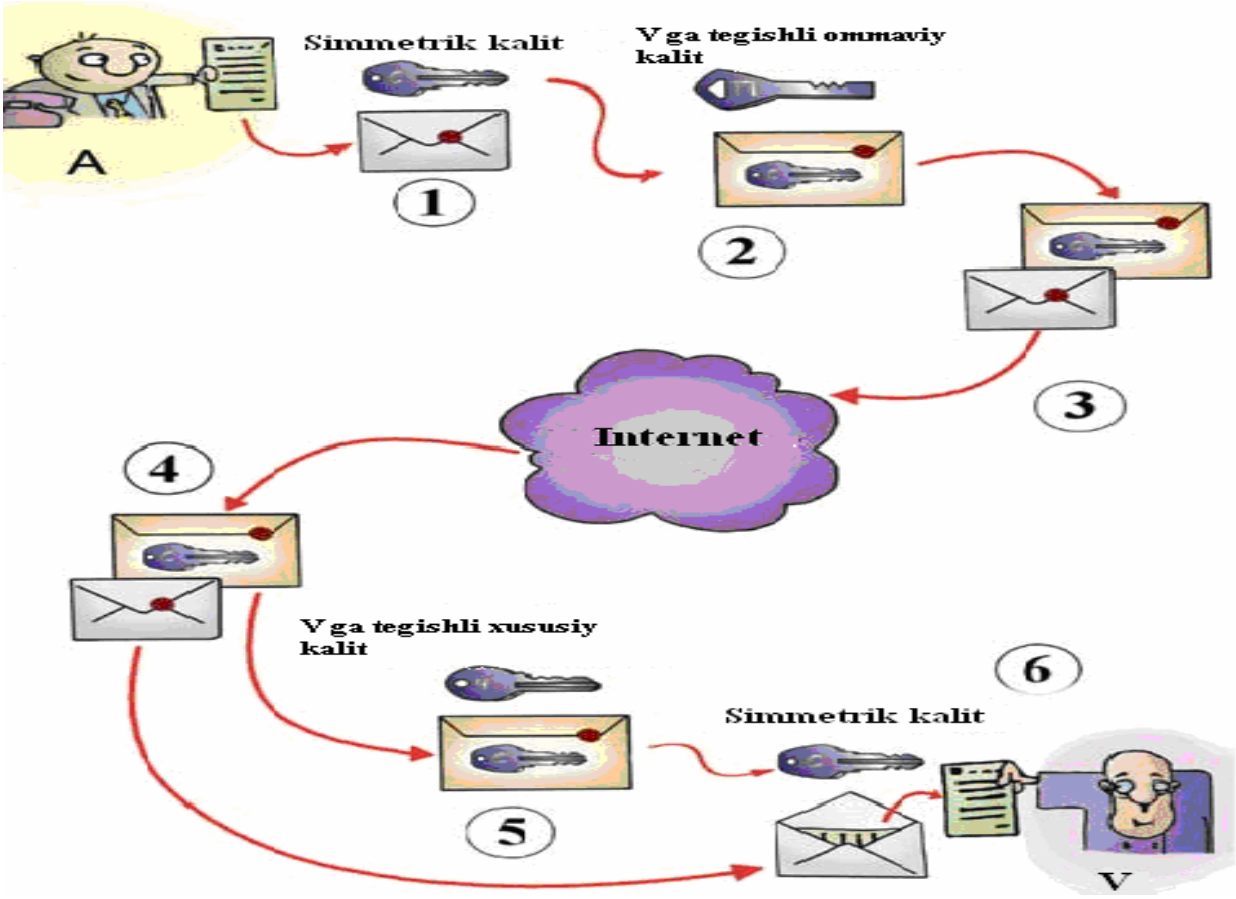
Konfedensiallikni ta’minlash sxemasi quyidagi rasmda tasvirlangan.



Xabarni faqat Ali (A) o‘qishi mumkin, chunki u xabarni qayta tiklash imkonini beruvchi yopiq kalitga ega, xabarni konfedensialligi ta’minlangan. Lekin, Ali (A) xabarni Soli (S) yubormaganiga aniq ishonchi yo‘q, chunki u Vali (V) nomidan xabarni yuborishi ham mumkin. Demak, autentifikatsiyalash ta’minlanmagan. Ikkita shaxs orasida xabar almashishda konfedensiallikni ta’minlash uchun ikkita kalit bo‘lishi shart.

Juft kalit bilan shifrlashda Ali (A) tomonidan hammaga ochiq kalit jo‘natilishi shart emas. Ochiq kalit tarmoqdagi ochiq foydalanishni imkonini beruvchi serverga joylashtirilishi mumkin.

Simmetrik va asimmetrik kalit yordamida shifrlash. Shuni ta’kidlash lozimki, asimmetrik shifrlash algoritmida ma’lumotlarni shifrlash va qayta tiklash uchun simmetrik shifrlashga qaraganda ko‘p vaqt talab qilinadi, shuning uchun zamonaviy shifrlash tizimlarida asimmetrik shifrlash va an’anaviy simmetrik shifrlashning kombinatsiyalari qo‘llaniladi. Ochiq kalit yordamida shifrlash simmetrik kalitni uzatishda foydalaniladi, bu kalit yordamida uzatiladigan axborot shifrlanadi. Bu sxemani ishlash qoidasi quyidagi rasmda keltirilgan.



Avval Ali (A) boshlang‘ich faylni simmetrik kalit yordamida shifrlaydi (1-punkt). Keyin (2-punkt) Ali ochiq manbalardan Vali (V)ga tegishli

bo‘lgan ochiq kalitni oladi va bu kalit yordamida o‘zining simmetrik kalitini shifrlaydi. So‘ngra (3-punkt) ikkala obyekt (shifrlangan fayl va shifrlangan simmetrik kalit) Internet orqali Vali (V)ning manziliga jo‘natiladi. Vali ikkala obyektni qabul qilib oladi (4-punkt). Simmetrik kalit Valiga tegishli bo‘lgan yopiq kalit yordamida qayta tiklanadi (5-punkt) va qayta tiklangan simmetrik kalit yordamida boshlang‘ich fayl shifrdan yechiladi (6-punkt).

Kimdir, sizning yopiq kalitingiz yordamida shifrlangan xabarni olsa, u sizdan xabar kelganiga ishonch hosil qiladi. Ya’ni, bu holatda, shifrlash imzo qo‘yganga ekvivalent bo‘ladi. Demak, raqamli (elektron) imzo – bu jo‘natuvchi yoki imzo muallifini autentifikatsiyalash usuli bo‘lib, hujjat mazmuni o‘zgartirilmaganligini tasdiqlaydi[1]. Raqamli imzo shifrlangan holda yoki ochiq shifrlanmagan holda yuborilishi mumkin.

Raqamli sertifikatlar. Ochiq kalitli shirflash sxemasidan foydalanganda ochiq kalitni mijozlarga tarqatish yoki tarmoqdagi serverga o‘rnatmoq kerak. Lekin raqib sizning nomingiz bilan o‘zini tanitishi va ochiq kalitni sizning nomingizdan tarqatishi mumkin. Ommaviy kalitni haqiqiy egasi kimligini aniqlash uchun, hamma korrespondentlar ishonch bildiradigan uchinchi tomonga ehtiyoj paydo bo‘ladi. Bu masala sertifikatlashtirish markazlari (Certification Authority) orqali hal etiladi. Ular tomonidan sertifikatlar – egasini identifikatsiyalaydigan ochiq kalit va axborotning mosligini tasdiqlaydigan raqamli ma’lumotlar, kafolatchi imzolagan raqamli imzo beriladi. Sertifikatda ommaviy kalit, kalitning egasi haqidagi ma’lumot, sertifikatlashtirish markazining nomi, sertifikatni amal qilish muddati kabi ma’lumotlar bo‘ladi. Sertifikatning har bir nusxasiga sertifikat bergan tashkilotning raqamli imzosi biriktiriladi, shuning uchun kim sertifikat olgan bo‘lsa, uning haqiqiyligiga ishonch hosil qilishi mumkin. Sertifikat shaxsni kimligini tasdiqlovchi hujjatning analogidir. Shaxsni identifikatsiya qilish muammosi (pasport, haydovchilik guvohnomasi va hokazo) uchrashuv paytida yuzaga keladi. Tarmoqda sherikni ko‘rmasdan turib muloqot qilishda, shaxsning kimligini bilish yanada muhimroqdir.

Shifrlashning kriptografik mustahkamligi. Himoyalangan axborotning xavfsizligi birinchi navbatda kalit bilan aniqlanadi. Shifrga hujum

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

(kriptotahlil) kalit va shifrlash algoritmi noma’lum bo‘lgan holatda shifrlangan axborotning shifrini yechish jarayonini bildiradi. Odatda, shifrlash algoritmi raqibga ma’lum va avvaldan tahlil etilishi mumkin deb hisoblanadi. Faqat shifrlashni amalga oshiruvchi kalit yashirin saqlanadi. Raqibning asosiy maqsadi bu kalitni qo‘lga kiritishdir.

Kriptomustahkamlik shifrning tasnifi bo‘lib, u kalitni bilmasdan turib shifrni yechishga bo‘lgan mustahkamlikni bildiradi. Shifrlash orqali axborotni himoyalashning samaradorligi kalitning yashirin saqlanishiga va shifrning kriptomustahkamligiga bog‘liq.

Shifrlashga qo‘yiladigan asosiy talablar. Zamonaviy shifrlash usullari quyidagi asosiy talablarga javob berishi kerak:

– shifrning mustahkamligi shifrlash algoritmining maxfiyligi bilan emas, kalitning sir saqlanishi bilan ta’minlanadi;

– faqat barcha mumkin bo‘lgan kalitlarni birma-bir to‘liq ko‘rib chiqish orqaligina shifrni yechish mumkinligi;

– kalitlarni birma-bir to‘liq ko‘rib chiqishdagi chekli amallar soniga zamonaviy kompyuterlarda erishib bo‘lmaslik;

– shifrlangan matn hajm jihatdan berilgan matndan juda ham katta bo‘lmasligi;

– shifrlash jarayonida ketma-ket ishlatilayotgan kalitlar oddiy va tezkor aniqlanadigan bog‘liqlikda bo‘lmasligi;

– shifrlash jarayonidagi xatolik axborotning buzilishi va yo‘qolishiga olib kelmasligi kerak;

– shifrlash juda ham ko‘p mehnat talab qilmasligi va uning qiymati himoyalanuvchi axborotning qiymati bilan mos kelishi kerak.

Ushbu talablarga shifrlash usullaridan: o‘rinlarini almashtirish; almashtirish; gammalashtirish; analitik o‘zgartirish kabilari javob beradi.

Keng tarqalgan shifrlash algoritmlari. Axborotni kriptografik himoyalash standartlari, xesh funksiya.

AES [advanced encryption standard (AES)] – AQShda ma’lumotlarni shifrlash standarti bo‘lib, simmetrik shifrtizimlarda foydalanish uchun qo‘llanadi. Blok o‘lchami 128 bit, kalit uzunligi 128, 192 yoki 256 bitdan iborat bo‘lgan bazaviy blokli shifrlash algoritmiga asoslagan. 2002-yildan beri amalda qo‘llanilmoqda.

DES [data encryption standard] shifrlash standarti Amerika standart shifrlash tizimi bo‘lib, simmetrik shifrtizimlarda foydalanish uchun mo‘ljallangan. Dunyoda shifrlashning birinchi ochiq rasmiy standarti

sifatida 1977-yildan 1997-yilgacha amal qilgan. Blok kattaligi 64 bit, kalit uzunligi 56 bitga teng bo‘lgan bazaviy blokli shifrlash algoritmi asosida qo‘llanilgan. Shifrlashning 4 rejimi va xabarni haqiqiyligini aniqlashtiruvchi kodni shakllantirishning 2 rejimiga ega.

DES-algoritmi qo‘llashining asosiy sohalari:

1) kompyuterda ma’lumotlarni saqlash (parol va fayllarni shifrlash);

2) xabarlarni autentifikatsiyalash (xabar va nazorat guruhiga ega bo‘lib, xabarni haqiqiyligiga ishonch hosil qilish qiyinchilik tug‘dirmaydi);

3) elektron to‘lov tizimlarida (ko‘p sonli mijozlar va banklar o‘rtasidagi operatsiyalarda);

4) tijorat xabarlarni elektron almashinuvida (xaridor, sotuvchi va bank xodimi o‘rtasida ma’lumotlar almashinuvida o‘zgartirishlar kiritish va ushlab qolishlardan himoyalangan).

GOST 28147-89 shifrlash standarti – Rossiya shifrlash standarti bo‘lib, simmetrik shifrtizimlarda foydalanish uchun mo‘ljallangan. Blok kattaligi 56 bit, kalit uzunligi 256, 512 bitga teng bo‘lgan bazaviy blokli shifrlash algoritmiga asoslangan. Shifrlashning 4 rejimiga ega.

Ko‘p sonli turli ochiq kalitli kriptotizimlar ichida keng tarqalgani 1977-yilda ixtiro qilingan va uning mualliflari Ron Rivest, Ada Shamir va Leonard Eydelman nomiga qo‘yilgan **RSA** kriptotizimidir. Ular, katta tub sonlarni aniqlash, hisoblash jihatdan oddiy ekanligidan hamda shunday ikkita katta sonlarning ko‘paytmasi bo‘lgan sonni ko‘paytuvchilarga ajratish judayam qiyin, amalda mumkin emasligidan foydalanishgan. **RSA** shifrini ochish shunday ko‘paytuvchilarga ajratishga tengligi isbotlangan (Rabin teoremasi). Shuning uchun kalit uzunligi qanday bo‘lishidan qat’i nazar shifrni ochish uchun talab qilinadigan amallarning quyi chegarasini baholash, zamonaviy kompyuterlarning tezligini bilgan holda shifrni ochish uchun kerak bo‘ladigan vaqtni ham aniqlash mumkin. RSA algoritmining himoyalanganlik kafolatini aniqlash imkoniyati, uning boshqa ochiq kalitli algoritmlar orasida mashhur bo‘lishining sababi hisoblanadi. Shuning uchun RSA algoritmidan bank kompyuter tizimlarida foydalanilmoqda, ayniqsa uzoq masofadagi mijozlar bilan ishlashda (kredit kartochkalarga xizmat ko‘rsatishda) qo‘llanilmoqda.

Xabar xesh-funksiyasi – qiymati kirish ketma-ketligining, ya’ni ikkilik sanoq tizimida berilgan xeshlovchi sonning har bir bitiga yoki xeshlovchi dastlabki matnning har bir ramziga bog‘liq bo‘lgan funksiya[1]. Xeshlash

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

algoritmi kirish matnidan bir xil uzunlikda natija chiqaradi. Bunda uzunlik deganda, ikkilik sanoq tizimida berilgan ifodadagi bitlar soni nazarda tutiladi. Masalan, kirish matni «AKT lug‘ati» bo‘lsa va xesh-funksiya qiymati «1011011101010100101»ga teng chiqsa, xesh-funksiya qiymati uzunligi 17 bitga teng bo‘ladi. Chiqish uzunligi 128, 192, 256 bit bo‘lgan xesh-funksiyalar ham mavjud. Xesh-funksiya samarali bo‘lishi uchun kirish xabari uchun natija noyob bo‘lishi lozim. Odatda, xesh-funksiyalar bir tomonli funksiyalardir. Chunki, chiqish qiymati asosida dastlabki matnni hisoblab topish juda qiyin. Xesh-funksiyalar axborot uzatish va saqlashda uning xavfsizligini muhofaza qilish uchun qo‘llaniladi.

Elektron raqamli imzo va ochiq kalitlar strukturasi. Elektron raqamli imzoni qo‘llashdan maqsad, birinchidan elektron hujjatdagi axborot asl nusxa ekanligini tasdiqlash, ikkinchidan uchinchi tarafga (arbitr, sudga va boshqalarga) hujjatni 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 paytda raqamli imzo keng qo‘llanilmoqda (uzatiladigan yoki saqlanadigan shifrlangan matnga biriktirilgan raqam, bu axborotning butunligini va muallifni haqiqiyligini tekshirish imkoniyatini kafolatlaydi). Simmetrik shifrlash algoritmlariga asoslangan raqamli imzo modellari ham mavjud.

Mustaqil tayyorgarlik uchun savollar

1. Kriptografiya nima?

2. Kriptografiya rivojlanishining qanday bosqichlari mavjud?

3. Zamonaviy kriptografiya qanaqa muammolarni hal etuvchi bilim sohasi hisoblanadi?

4. Axborotlarni sodda shifrlashni qanday usullari bor?

5. Sezarning shifrlash usuli qanday amalga oshiriladi?

6. Vijinerning shifrlash tizimi nima?

7. Kalit deganda nima tushuniladi?

8. Simmetrik shifrlash qanday amalga oshiriladi?

9. Asimmetrik shifrlash nima?

10. Simmetrik va asimmetrik kalit yordamida shifrlash qanday amalga oshiriladi?

11. Raqamli sertifikatlar nima?

12. Kriptotomustahkamlik nimani bildiradi?

13. Shifrlashga qanaqa talablar qo‘yiladi?

14. Qaysi shifrlash algoritmlari keng tarqalgan?

15. Elektron raqamli imzo nima maqsadda ishlatiladi?

IV. AXBOROT XAVFSIZLIGINI TA’MINLASHNING APPARAT-DASTURIY VOSITALARI

4.1. Asosiy tushunchalar. Foydalanish huquqini cheklashning usul va vositalari.

4.2. Dasturlarni o‘zgartirishlardan himoyalash va butunlikning nazorati.

4.3. Ma’lumotlarni uzatish tarmog‘ida axborot xavfsizligining apparat-dasturiy vositalari.

Axborotni muhofaza qilishning apparat-dasturiy vositalari – axborotni muhofaza qilish funksiyalarini (foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish, resurslardan foydalana olishni cheklash, voqealarni qayd qilish, axborotni kriptografik himoyalash va shu kabilar) bajaradigan (mustaqil yoki boshqa vositalar bilan birgalikda) turli elektron qurilmalar va maxsus dasturlardir.

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

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

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

Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlanadi. Buzg‘unchi tarmoqning biror-bir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin.

Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun «tarmoqlararo ekran» (**Firewall**) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

4.1. Asosiy tushunchalar. Foydalanish huquqini cheklashning usullari va vositalari

Axborotlarni himoyalashning apparat vositalariga, kompyuterning texnik vositalariga taalluqli bo‘lgan, axborot xavfsizligini ta’minlashning ayrim funksiyalarini mustaqil ravishda yoki dasturiy vositalar bilan bir majmua tarkibida bajaradigan elektron va elektron-mexanik moslamalari kiritiladi. Bunday qurilmalarni ma’lumotlarni himoyalashning injener-texnik vositalariga emas, balki apparat vositalariga kiritishning asosiy sharti, ularni kompyuterning texnik vositalari tarkibida kiritilishi bilan belgilanadi.

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 xalaqit 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 deganda, faqatgina axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlar tushuniladi.

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 hokazo) noqonuniy o‘zgartirishlardan, foydalanishlardan va ko‘paytirishlardan himoyalovchi dasturlar.

Kompyuter tizimlarida axborot xavfsizligini ta’minlashga taalluqli

ma’noda identifikatsiyalash atamasi kompyuter tizimlari subyektining unikal nomini bir qiymatli tanib olishni bildiradi. Autentifikatsiyalash esa taqdim etilgan nomni ushbu subyektga mosligini tasdiqlashni anglatadi (subyektning aslligini tasdiqlash).

Axborotlarni muhofaza qilishning yordamchi dasturiy vositalariga misol qilib quyidagilarni keltirish mumkin:

– qoldiq axborotlarni (tezkor xotira blokidagi, vaqtinchalik fayllardagi va hokazo) yo‘q qiluvchi dasturlar;

– kompyuter tizimlarining xavfsizligi tizimiga bog‘liq bo‘lgan turli voqea va hodisalarni tiklash hamda shunday voqea va hodisalar ro‘y berganini isbotlash uchun foydalaniladigan audit dasturlari (qayd qilish jurnallarini yuritish);

– qoidabuzar bilan ishlashni imitatsiyalovchi dasturlar (qoidabuzarni go‘yoki yopiq axborotlarni olgan deb chalg‘itish);

– kompyuter tizimlarining himoyalanganligini sinovdan o‘tkazuvchi nazorat dasturlar va boshqalar.

Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklariga quyidagilar kiradi:

– ko‘paytirishning osonligi;

– moslanuvchanlik (turli sharoitlarda qo‘llaniladigan muayyan kompyuter tizimlarini, axborot xavfsizligiga tahdidning o‘ziga xosligini hisobga olib, sozlash imkoniyati);

– qo‘llashning qulayligi – bir xil dasturlar, masalan shifrlovchi dasturlar «shaffof» (foydalanuvchiga ko‘rinmaydigan) rejimda ishlaydi, boshqalari foydalanuvchidan hech qanday qo‘shimcha yangi (boshqa dasturlari bilan taqqoslaganda) ko‘nikmalar talab qilmaydi;

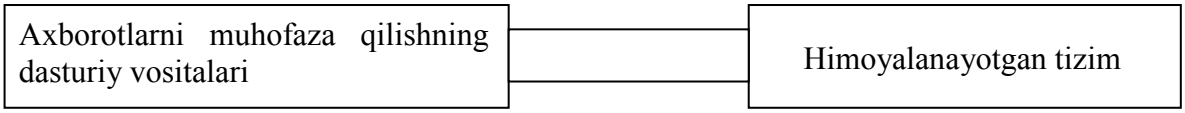
– ularni axborot xavfsizligiga yangi tahdidlar hisobini yuritish uchun o‘zgartirishlar kiritish yo‘li bilan takomillashuvining amaldagi chek-chegarasiz imkoniyatlari mavjudligi.

Axborotlarni muhofaza qilishning dasturiy vositalarining kamchiliklariga quyidagilar kiradi:

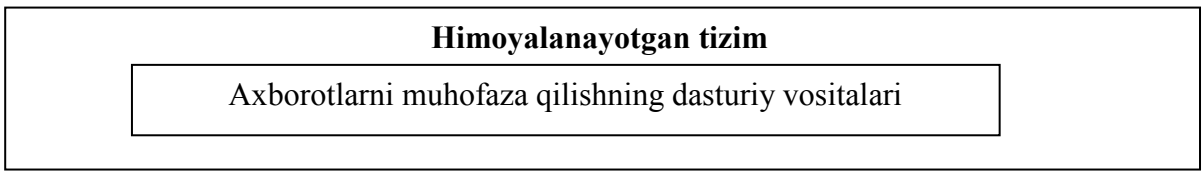
– himoyalovchi dasturlarning faoliyati kompyuter tizimlari resurslaridan foydalanish hisobiga bo‘lgani uchun bu tizimlar samaradorligining susayishi;

– juda past unumdorlik (xuddi shunday vazifani bajarayotgan apparat vositalar bilan taqqoslaganda, masalan shifrlovchi qurilma);

– axborotlarni himoyalovchi ko‘pgina dasturiy vositalarning kompyuter dasturiy ta’minotiga bevosita o‘rnatilmagani (quyidagi rasmlar), bu holat qoidabuzarning ushbu dasturlarni chetlab o‘tishiga prinsipial imkoniyatlar yaratadi;



Axborotlarni muhofaza qilish dasturining dasturiy ta’minotga ulanish chizmasi



– kompyuter tizimlaridan foydalanish jarayonida axborotlarni himoyalashning dasturiy vositalarini qasddan o‘zgartirish imkoniyati.

Kompyuter tizimlaridan foydalanish huquqini cheklashning usul va vositalari. Axborot xavfsizligini ta’minlashning asosiy konsepsiyasini turli aloqa va xavfsizlikni ta’minlash nimtizimlari, umumiy texnik vositalar, aloqa kanallari, dasturiy ta’minot va ma’lumotlar bazalariga ega yagona tizimga integrasiyasiga asoslangan kompleks yondashuv tashkil etadi.

Kompleks xavfsizlik – vujudga kelishi mumkin bo‘lgan barcha turdagi tahdidlar (noqonuniy foydalanish, ma’lumotlarni tutib olish, terrorizm, yong‘in, tabiiy ofatlar va hokazolar)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.

Obyektning axborot xavfsizligini ta’minlash tizimining samaradorligi muhim ahamiyat kasb etadi. Kompyuter tizimlari uchun ushbu samaradorlikni, hisoblash tizimida qo‘llanilayotgan apparat-dasturiy vositalarni tanlanganligi bilan baholash mumkin. Bunday samaradorlikni baholash, xavfsizlikni ta’minlash darajasi foydalanish huquqiga bo‘lgan nazoratni kuchaytirilishiga bog‘liqlikni ko‘rsatuvchi o‘suvchi egri chiziq orqali amalga oshirilishi mumkin.

Qurilmadan, jumladan kompyuterdan foydalana olish deganda, subyektga ushbu qurilmadan foydalanib, unga muayyan ruxsat etilgan harakatlarni bajara olish imkonini berish tushuniladi. Masalan, kompyuter foydalanuvchisiga kompyuterni ishga tushirish va o‘chirish, dasturlar bilan ishlash, ma’lumotlarni kiritish va chiqarishga ruxsat etiladi. Xizmat ko‘rsatuvchi shaxs esa o‘rnatilgan tartibda kompyuterni tekshiradi, ishdan chiqqan bloklarni almashtiradi va tiklaydi.

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

– ruxsat olayotgan subyektni identifikatsiyalash va autentifikatsiyalash;

– 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.

Konfedensial 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 xeshlangan holatda kompyuterning qattiq diskida saqlanadi. Parollarni taqqoslash operatsion tizim (OT) tomonidan foydalanuvchi huquqiga mos imkoniyatlar yuklangunga qadar amalga oshiriladi. Lekin, kompyuterning OTdan foydalanishda 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 identifikatsiyalash 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 kalkulatorga 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 imkoni bo‘lmaydi. Jetondan foylanishdan avval unga foydalanuvchi o‘zining shaxsiy parolini kiritishi lozim.

Atrubutivli identifikatorlardan (parollardan tashqari) ruxsat berilish va qayd qilish chog‘ida foydalanilish mumkin yoki ular ish vaqti tugagunga qadar ishlatilayotgan qurilmaga doimiy ulangan holda bo‘lishi shart. Qisqa vaqtga biror joyga chiqilganda ham identifikator olib qo‘yiladi va qurilmadan foydalanish blokirovka qilinadi. Bunday apparat-dasturiy vositalar nafaqat qurilmalardan foydalanishni cheklash masalalarini hal qila oladi, shu bilan birga axborotlardan noqonuniy foydalanishdan himoyalashni ta’minlaydi. Bunday qurilmalarning ishlash prinsipi qurilmaga o‘rnatilgan OT funksiyalarini kengaytirishga asoslangan.

Autentifikatsiyalash jarayoni kompyuter tizimlari bilan ruxsat etilgan subyekt orasida amalga oshiriladigan dialogni 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.

Ko‘pincha sodda identifikator sifatida mexanik kalitlardan foydalaniladi. Mexanik qulf qurilmaga tok yetkazib beruvchi qurilmaga o‘rnatilgan bo‘lishi mumkin. Qurilmaning asosiy boshqaruv organlari joylashgan joyni berkituvchi qopqog‘i qulflangan holda bo‘lishi mumkin. Qopqoqni ochmasdan qurilmani ishlatishning imkoni yo‘q. Bunday

qulfning mavjudligi, buzg‘unchining qurilmadan noqonuniy foydalanishni amalga oshirishi yo‘lida qo‘shimcha to‘siq bo‘lib xizmat qiladi.

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 konfedensial 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.

Himoyalovchi apparat-dasturiy komplekslarning ko‘pchiligi maksimal sondagi himoyalash mexanizmlaridan foydalaniladi. Bu mexanizmlarga quyidagilar kiradi:

– foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;
– fayllar, papkalar, disklardan foydalanishga ruxsatni cheklash;
– dasturiy vositalar va axborotlar butunligini nazorat qilish;
– foydalanuvchi uchun funksional yopiq muhitni yaratish imkoniyati;
– OTni yuklanish jarayonini himoyalash;
– foydalanuvchi yo‘qligida kompyuterni blokirovka qilish;
– ma’lumotlarni kriptografik o‘zgartirish;
– hodisalarni qayd qilish;
– xotirani tozalash.

Foydalanishni cheklash vositalari yordamida noqonuniy foydalanishdan himoyalash (NFH)ning usul va vositalaridan tashqari kompyuterni himoyalash uchun quyidagi uslub va vositalar qo‘llaniladi:

– qurilmalarni noqonuniy ulab olishga qarshi harakatlar;
– boshqaruv va ulanishlarni, ichki montajni noqonuniy aralashuvlardan himoyalash;
– foydalanish jarayonida dastur tuzilishining butunligini va himoyasini nazorat qilish.

Kompyuter tizimlariga (KT) qurilmalarni noqonuniy ulab olishga qarshi harakatlarni tashkil etishda, bu ulanish KTning texnik tuzilishini

noqonuniy o‘zgartirish imkonini beruvchi yo‘llardan bir ekanligini nazarda tutish lozim. Ushbu o‘zgartirishlar ro‘yxatdan o‘tkazilmagan qurilmalarni ulash yoki kompyuter tizimlarining tarkibiy vositalarini almashtirish orqali amalga oshiriladi.

Bunda tahdidlarni oldini olish uchun quyidagi usullardan foydalaniladi:

– qurilmaning o‘ziga xos xususiyatlarini tekshirish;

– qurilmalarni identifikatsiyalashdan foydalanish.

Kompyuter tizimlarining xotira qurilmalarida, odatda tizim konfiguratsiyasi haqidagi ma’lumotlar saqlanadi. Bunday ma’lumotlarga: qurilmaning (bloklarning) turi va ularning tavsiflari, tashqi qurilmalarning soni va ulanish sabablarini o‘ziga xos xususiyatlari, ish rejimlari va boshqalarni kiritish mumkin. Konfigursiyaning muayyan tuzilishi kompyuter tizimlarining va OTning turiga qarab aniqlanadi. Har qanday holatda ham dasturiy vositalar yordamida KT konfiguratsiyasi haqidagi ma’lumotlarni yig‘ish va taqqoslashni tashkil etish mumkin. Agar kompyuter tarmoqda ishlayotgan bo‘lsa, hech bo‘lmaganda uni tarmoqqa ulash paytida kompyuterning konfiguratsiyasi nazoratdan o‘tkaziladi.

Nazoratning yanada ishonchli va tezkor usuli, qurilmaning maxsus kod – identifikatoridan foydalanish hisoblanadi. Bu kod qurilma vositalarida hosil qilinadi va xotira qurilmasida saqlanishi mumkin. Generator nazorat qiluvchi qurilmaga qurilmaning unikal raqamlarini uzatishni amalga oshiradi. Xotira qurilmasidagi kod, KT administratorining vositalari yordamida davriy ravishda o‘qib va tahlil qilib boriladi. Konfiguratsiyaning o‘ziga xos xususiyatlarini tahlil qilish usullaridan kompleks foydalanish va qurilmalarni identifikatsiyalashdan foydalanish, noqonuniy ulanish yoki almashtirib qo‘yish uchun amalga oshirilgan urinishlarni payqash ehtimolligini oshiradi.

4.2. Dasturlarni o‘zgartirishlardan himoyalash va butunlikning nazorati

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga yetarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Viruslarning ta’sir mexanizmlarini, ularga qarshi kurash usullari va vositalarini bilish viruslanishga qarshi harakatlarni samarali tashkil etish, ularning ta’siridan

zararlanish ehtimolligini va talafatlarni minimumga keltirish imkonini beradi.

Kompyuter viruslari – bu KTda tarqalish va o‘zini o‘zi ishlab chiqish xususiyatiga ega bo‘lgan kichik hajmdagi bajariluvchi dasturlar. Viruslar KTda saqlanayotgan dasturiy vositalar yoki ma’lumotlarni yo‘q qilishi yoki o‘chirib yuborishi mumkin. Tarqalish jarayonida viruslar o‘zini modifikatsiyalashi mumkin.

Viruslarning ommaviy tarqalib ketishi va ularning KT resurslariga ta’siri oqibatlarining jiddiyligi, maxsus antivirus vositalarini va ularni qo‘llash usullarini yaratish va foydalanish zaruriyatini keltirib chiqardi. Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:

– KTda viruslarni topish;

– virus – dasturlar ishini blokirovka qilish;

– viruslar ta’sirining oqibatlarini bartaraf qilish.

Viruslarni topishni, ularni joylashib olish bosqichida yoki hech bo‘lmaganda virusning buzg‘unchilik funksiyalarini boshlagunga qadar amalga oshirgan maqsadga muvofiq. Shuni ta’kidlash joizki, barcha turdagi viruslarni topishni kafolatlovchi antivirus vositalar mavjud emas.

Virus topilgan holatda, uning tizimga keltirishi mumkin bo‘lgan zararli ta’sirini minimallashtirish maqsadida darhol virus-dasturning ishini to‘xtatilish lozim.

Virusning ta’sir oqibatlarini bartaraf qilish ikki yo‘nalishda olib boriladi:

– virusni o‘chirish;

– fayllarni, xotira sohalarini tiklash.

Tizimni qayta tiklash virus turiga, uni aniqlangan hamda zararlovchi ta’sirini boshlagan vaqtiga bog‘liq. Viruslar tizimga kirish jarayonida, o‘zini saqlaydigan joydagi ma’lumotlarni o‘chirib yuborsa hamda zararlovchi ta’siri natijasida ma’lumotlarni o‘zgartirish nazarda tutilgan bo‘lsa, zaxiraga olingan ma’lumotlarsiz yo‘qolgan ma’lumotlarni tiklab bo‘lmaydi.

Viruslarga qarshi kurashda aniq bir ketma-ketlik va kombinatsiyada qo‘llaniluvchi, viruslarga qarshi kurashish usullarini hosil qiluvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

KTning xavfsiz ishlashining asosiy shartlaridan biri, amalda sinovdan o‘tkazilgan va o‘zining yuqori samara berishini ko‘rsatgan bir qator qoidalarga[1] rioya qilish hisoblanadi.

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

Birinchi qoida – qonuniy rasmiy yo‘l bilan olingan dasturiy mahsulotlardan foydalanish. Dasturiy ta’minotning qaroqchilik yo‘li bilan ko‘paytirilgan nusxalarida, rasmiy yo‘l bilan olinganlariga nisbatan viruslarning mavjudlik ehtimoli juda yuqori.

Ikkinchi qoida – axborotlar zaxirasini hosil qilish. Avvalo dasturiy ta’minotning distributivlari yozilgan tashuvchilarni saqlash zarur. Bunda tashuvchilarga ma’lumotlarni yozish imkoni berilgan bo‘lsa, imkon qadar uni blokirovka qilish zarur. Ishga taalluqli ma’lumotlarni saqlanishiga jiddiy yondashishi zarur. Muntazam ishga taalluqli fayllarning zaxira nusxalarini yaratib borish va ularni yozishdan himoyalangan yechib olinuvchi tashuvchilarda saqlash kerak. Agar bunday nusxalar yechib olinmaydigan tashuvchilarda yaratilayotgan bo‘lsa, ularni butunlay boshqa kompyuterning doimiy xotirasida yaratish maqsadga muvofiq. Bunda yoki faylning to‘liq nusxasi yoki kiritilayotgan o‘zgarishlarning nusxalari saqlanadi.

Uchinchi qoida – antivirus vositalaridan muntazam foydalanish. Antivirus vositalari muntazam yangilanib turilishi lozim.

To‘rtinchi qoida – yangi yechib olinadigan axborot tashuvchilardan va yangi fayllardan foydalanilganda ehtiyotkorlikka rioya qilish. Yangi yechib olinadigan tashuvchilar olinganda, albatta, yuklanuvchi va fayl viruslari mavjudligiga, olingan fayllar esa fayl viruslari mavjudligiga tekshirilishi lozim. Tekshiruv, skanerlovchi – dasturlar va evristik tahlilni amalga oshiruvchi dasturlar yordamida amalga oshirilishi kerak. Olingan hujjatlar va jadvallar bilan ishlashda, ushbu fayllar to‘liq tekshirilgunga qadar, matn va jadval muharrirlariga o‘rnatilgan makrokomandalarning bajarilishini taqiqlash zarur.

Beshinchi qoida – tizimga, ayniqsa taqsimlangan tizimlarga yoki jamoa bo‘lib foydalaniladigan tizimlarga, kiritilayotgan fayllarni va yechiladigan axborot tashuvchilarni maxsus ajratilgan kompyuterlarda tekshirish. Uni tizim administratori yoki ma’lumotlar xavfsizligiga mas’ul bo‘lgan shaxsning avtomatlashtirilgan ish joyidan amalga oshirilishi maqsadga muvofiq. Disk va fayllarni har tomonlama antivirus tekshiruvidan o‘tkaziluvidan so‘ng ularni tizimdan foydalanuvchilarga taqdim etish mumkin.

Oltinchi qoida – agar axborotlarni tashuvchilarga yozish nazarda tutilmagan bo‘lsa, bunday amallarni bajarilishini blokirovka qilish.

Yuqorida keltirilgan tavsiyalarga doimiy rioya qilinishi virus dasturlar bilan zararlanish ehtimolini ancha kamaytiradi va foydalanuvchini axborotlarni qaytib tiklab bo‘lmaydigan yo‘qotishlardan saqlaydi.

KTdan foydalanish bosqichlarida tizimdagi axborotlarning butunligi va ulardan foydalanish huquqi quyidagilar orqali ta’minlanadi:

– KTda mavjud axborotlarning butunligi;

– KTning rad etishga barqarorligini oshirish;

– tizimning qayta yuklanishi va «osilib qolishi»ni bartaraf etish;

– axborot zaxiralarini yaratish;

– qat’iy belgilangan dasturlar majmuidan foydalanish;

– texnik xizmat ko‘rsatish va kam-ko‘stini to‘ldirish jarayonlarining o‘ziga xos tartibiga rioya qilish;

– antivirus tadbirlari kompleksini o‘tkazish.

Axborotning butunligi va foydalanishga qulayligi apparat vositalar zaxirasini yaratish, foydalanuvchilarning xato harakatlarini blokirovka qilish, kompyuter tizimlarining ishonchli elementlaridan va barqaror ishlovchi tizimlardan foydalanish yo‘li bilan amalga oshiriladi. Tizim elementlarini qasddan ortiqcha ishlatish tahdidlari bartaraf etiladi. Buning uchun bajariladigan dasturlarga buyurtmalarni kelib tushish intensivligini o‘lchash mexanizmlaridan va bunday buyurtmalarni berishni cheklash yoki blokirovka qilish mexanizmlaridan foydalaniladi. Bunday hollarda ma’lumotlarni uzatish yoki dasturlarni bajartirishga bo‘lgan buyurtmalar oqimining birdaniga keskin oshib ketishini aniqlash imkoni ham oldindan nazarda tutilgan bo‘lishi kerak.

KTda axborotlarning butunligi va foydalanishga qulayligini ta’minlashning asosiy shartlaridan biri ularning zaxiralarini hosil qilishdan iborat. Axborotlar zaxirasini yaratish strategiyasi axborotning muhimligini, KTning uzluksiz ishlashiga bo‘lgan talablarni, ma’lumotlarni tiklashdagi qiyinchiliklarni hisobga olgan holda tanlanadi.

Himoyalangan KTda faqatgina ruxsat etilgan dasturiy ta’minotdan foydalanilishi lozim. Foydalanishiga rasman ruxsat etilgan dasturlarning ro‘yxati, ularning butunligini nazorat qilishning usullari va davriyligi KTni ekspluatatsiya qilinishidan oldin aniqlanishi kerak.

Dasturlar butunligini nazorat qilishning sodda usullaridan biri nazorat yig‘indilari usuli hisoblanadi. Nazorat yig‘indisi – ma’lumotlar blokining oxiriga yoziladigan bitlar ketma-ketligi. Nazoratdagi faylga kiritilgan o‘zgartirishni, nazorat yig‘indini tuzatib qo‘yish bilan, berkitishni istisno qilish maqsadida nazorat yig‘indini shifrlangan holda saqlash yoki nazorat yig‘indini hisoblashning maxfiy algoritmidan foydalanish zarur.

Axborot butunligini nazorat qilishning ko‘proq maqbul bo‘lgan metodlarida bir xesh-funksiyadan foydalanish hisoblanadi. Xesh-funksiyaning qiymatini uning kalitini bilmasdan turib qalbakilashtirib

bo‘lmaydi, shu sababli xeshlash kalitini shifrlangan ko‘rinishda yoki jinoyatchining «qo‘li yetmaydigan» joydagi xotirada saqlash kerak.

Axborot xavfsizligini ta’minlashning dasturiy va apparat-dasturiy vositalardan foydalanishga qo‘yiladigan asosiy talablar. Xavfsizlik modelini to‘g‘ri tanlash OT mutaxassislarinigina emas, xavfsizlik bo‘yicha mutaxassislarning asosiy vazifasi hisoblanadi. Hozirda mavjud standartlar modellarning majburiy ro‘yxatini faqat ikki model, ya’ni foydanish huquqini boshqarishning *diskret* va *mandatli* turlari bilan cheklaydi. Ko‘p hollarda ushbu ikki modelning qo‘llanilishi yetarli hisoblanadi.

OTda axborot xavfsizligini samarali ta’minlash uchun quyidagi tavsiyalarni[1] bajarish lozim:

1. Xavfsizlik modelini to‘g‘ri joriy etish.

2. Obyektlar va subyektlarning ishonchli identifikatsiyalash va autentifikatsiyalashdan o‘tkazish. Ushbu muammo texnik xarakterga ega. Hozirda, ishonchli identifikatsiyalashni va berilgan aniqlikda autentifiksiyalashni ta’minlashlaydigan tizimlar mavjud. Identifikatsiyalashning ishonchliligi foydalanilayotgan belgilarning noyobligi (unikalligi) bilan, autentifikatsiyalashniki esa – qalbakilashtirishning qiyinligi bilan ta’minlanadi. Foydalanuvchilarni identifikatsiyalash va autentifikatsiyalashni ishonchli algoritmlarini qo‘llash uchun maxsus apparat vositalar – magnit kartalar, foydalanuvchining fiziologik kattaliklari (barmoq izlari, ko‘z to‘r pardasi va hokazo)ni o‘quvchi qurilmalar zurur. Ushbu usullarni dasturiy jihatdan ixtiyoriy mavjud tizimlarga joriy etish mumkin. Subyektlar va obyektlarning dasturiy (inson ishtirokisiz) identifikatsiyalash va autenfikatsiyalash uchun keyingi paytlar keng qo‘llanilayotgan elektron imzodan foydalanilmoqda. Identifikatsiyalash va autenfikatsiyalashning muayyan bir mexanizmi, qurilmasi va vositasini tanlash muayyan tizimga qo‘yiladigan talablardan kelib chiqadi va axborot xavfsizligini ta’minlashda qo‘llanilayotgan boshqa qarorlarga bog‘liq bo‘lmagan holda amalga oshirilishi mumkin.

3. Xavfsizlikni ta’minlash tizimini dasturiy amalga oshirishdagi xatoliklarni kamaytirish yoki to‘liq bartaraf etilishiga erishish. Boshqa dasturiy ta’minotlar singari himoyalashning usul va vositalari ham joriy etish xatoliklaridan holi emas. Himoya tizimining ixtiyoriy tashkil etuvchisidagi biror xatolik butun tizimning xavfsizligini shubha ostida qoldirishi tabiiydir. Shu sababli xavfsizlikka javobgar bo‘lgan dasturiy

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

ta’minotdagi xatoliklar nafaqat o‘z vazifani bajara olmay qoladi, balki butun tizimni izdan chiqaradi. Ushbu muammoni hal etilishiga qaratilgan chora-tadbirlar dasturlash texnologiyasi va OTning ishonchlik sohasiga taalluqli bo‘ladi.

4. Xavfsizlikni ta’minlash vositalarining butunligini tegishli nazoratini tashkil etish. Ushbu muammo sof texnologik xarakterga ega bo‘lib, hozirda butunlikni nazorat qilish usullari yetarlicha rivojlangan va ushbu masalaning ishonchli yechimlari topilgan (masalan, elektron raqamli imzo orqali). Ammo, amaliyotda, odatda ushbu metodlar faqatgina ma’lumotlar butunligini nazorat qilish uchungina (masalan, aloqa kanali orqali ma’lumotlarni uzatishda) qo‘llaniladi. Ushbu muammoni hal etish uchun birinchi navbatda, xavfsizlikni ta’minlovchi mexanizmlar butunligini nazorat qilish lozim.

5. Dasturiy va qurilmaviy mahsulotlarni ishlab chiqishning yakuniy bosqichida sozlash va testdan o‘tkazish vositalarini mavjudligini ta’minlash. Ushbu muammoni hal etilishi uchun tashkiliy tadbirlardan foydalanish mumkin. Xavfsizlik hal qiluvchi ahamiyatga ega bo‘lgan barcha tizimlar, o‘zida shunga o‘xshash imkoniyatlar mavjud emasligini tasdiqlovchi sertifikatlarga ega bo‘lishi lozim. Tabiiyki, ushbu talabni bajarilishi uchun to‘liq javobgarlikni ishlab chiqaruvchi o‘z zimmasiga oladi.

6. Administratsiyalashdagi xatoliklarni minimumga keltirish. Ushbu muammo inson faktori bilan bog‘liqligi sababli sof texnik vositalar yordamida hal etila olmaydi. Shu kabi xatoliklarni vujudga kelish ehtimolligini kamaytirish uchun xavfsizlikni boshqarish va foydalanishga ruxsat berishni nazorat qilish vositalarini qulay va ishlashga oson bo‘lgan interfeys bilan ta’minlash lozim hamda imkoniyatga qarab boshqaruvning avtomatlashtirilgan tizimidan foydalangan ma’qul. Bundan tashqari, hisoblash tizimi konfiguratsiyasini administrasiyalashning adekvat emasligini tekshiradigan verifikatsiyalovchi vositalarning qo‘llanilishi ham nazarda tutilishi mumkin.

Ma’lumotlarni bazasini boshqarish tizimi (MBBT)da ma’lumotlarni qayta ishlash jarayonini himoyalash. Ma’lumotlar bazasida axborotlarni qayta ishlash jarayonini himoyalash, fayldagi ma’lumotlarni himoyalashdan farq qiladi va quyidagi o‘ziga xos xususiyatlarga ega:

– tanlangan himoya mexanizmida ma’lumotlar bazasini boshqarish tizimini ishlay olishini hisobga olish zaruriyati;

– bazadagi ma’lumotlardan foydalanishga ruxsat berishni cheklashni fayl sathida emas, ma’lumotlar bazasining qismlari sathida amalga oshirish lozimligi.

Ma’lumotlar bazasida ma’lumotlarni qayta ishlash jarayonini himoyalash vositalarini yaratishda, ushbu vositalarning nafaqat OT bilan, balki MBBT bilan birgalikda ishlay olishini hisobga olish kerak.

Zamonaviy ma’lumotlar bazasida ma’lumotlardan foydalanishga ruxsat berishni cheklash, ma’lumotlarning fizik butunligini va mantiqiy saqlanganlik masalasi yetarli darajada muvaffaqiyatli hal etilgan. Hozirda foydalanuvchi tomonidan ma’lumotlar bazasi yozuvlaridan va yozuv maydonlaridan foydalanishga ruxsatni cheklash algoritmlaridan unumli foydalanilmoqda, ushbu himoyani jinoyatchi zararlovchi dasturlarni joriy etish yoki foydalanuvchi huquqlarini qalbakilashtirish yordamida yengib o‘tishi mumkin. Ma’lumotlar bazasi faylidan va bazaning qismlaridan foydalanishga ruxsat berish MBBT tomonidan, foydalanuvchining huquqlarini belgilab berish va ruxsat berilishi kerak bo‘lgan obyektlardan foydalanishga ruxsat berish huquqlarini nazorat qilish yo‘li bilan amalga oshiriladi.

Foydalanuvchi huquqlari MBBT administratori tomonidan belgilanadi. Odatda, foydalanuvchining standart identifikatori bo‘lib, shifrlangan ko‘rinishda uzatiladigan parol hisoblanadi. Taqsimlangan KTda foydalanuvchining haqiqiyligini tasdiqlash jarayoni, masofaviy jarayonlarni o‘zaro autentifikatsiyalash kabi maxsus protsedura bilan to‘ldiriladi.

4.3. Ma’lumotlarni uzatish tarmog‘ida axborot xavfsizligining apparat-dasturiy vositalari

Tarmoq texnologiyasining keng ko‘lamda qo‘llanishi natijasida umumiy resurslardan foydalanish imkonini beruvchi lokal tarmoqqa kompyuterlar birlashtirildi. Kliyent-server texnologiyasining tatbiq etilishi esa bu tarmoqni taqsimlangan hisoblash muhitiga aylantirdi. Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlanadi. Buzg‘unchi tarmoqning biror-bir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin.

Zamonaviy telekommunikatsiya texnologiyalari lokal tarmoqlarni global tarmoqqa – Internetga ulash imkonini berdi. Internetning rivojlanishi xavfsizlikni ta’minlashni dolzarb masalaga aylantirdi va Internetga ulangan tarmoq va tizimlarda, qanday ma’lumotlarga ishlov berilishidan qat’iy nazar, xavfsizlik vositalari bo‘lishini taqozo etadi. Chunki, Internetning imkoniyatlaridan foydalanib, buzg‘unchi xavfsizlikni

buzishni global masshtabda olib borishi mumkin. Internetga ulangan kompyuter tajovuz obyekti bo‘lsa, hujumni amalga oshirayotgan shaxsga uning qayerda (qo‘shni xonada yoki boshqa kontinentda) joylashgani katta ahamiyatga ega emas.

Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun «tarmoqlararo ekran» (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi. Odatda, alohida ajratilgan va himoyalangan KT «tarmoqlararo ekran» orqali hamma foydalanadigan tarmoqqa ulanadi.

Tarmoqlararo ekran himoyalangan KTga kelib tushayotgan va undan chiqib ketayotgan axborotlarni nazorat qilish uchun qo‘llaniladi.

Tarmoqlararo ekran quyidagi to‘rtta funksiyani bajaradi:

– ma’lumotlarni filtrlash;

– ekranlovchi agentlardan foydalanish;

– manzillarni translatsiyalash;

– hodisalarni qayd qilish.

Tarmoqlararo ekranning asosiy vazifasi (kirayotgan yoki chiqayotgan) trafikni filtrlashdan iborat. Korporativ tarmoqning himoyalanganlik darajasiga qarab filtrlashning turli qoidalari o‘rnatilishi mumkin. Filtrlash qoidalari filtrlar ketma-ketligini tanlash orqali amalga oshiriladi. Ushbu filtrlar o‘zidan keyingi filtrga yoki protokol sathiga ma’lumotlarni uzatilishiga ruxsat beradi yoki taqiqlaydi.

Tarmoqlararo ekran filtrlashni kanallar, tarmoqlar, transport va amaliy sathlarda amalga oshiradi. Ekran qancha ko‘p sathni o‘z ichiga olsa, shuncha takomillashgan hisoblanadi.

Tarmoqlararo ekranda, dasturiy vositachi vazifani bajaruvchi va subyekt va obyekt orasida ulanishni ta’minlovchi, so‘ngra axborotni qayd qilish va nazoratini amalga oshirib jo‘natuvchi, *ekranlovchi agentlardan* (proxy-serverlar) foydalaniladi. Ekranlovchi agentlarning qo‘shimcha vazifasi foydalanishga ruxsat berilgan subyektdan haqiqiy obyektni yashirishdan iborat. Ekranlovchi agentlarning o‘zaro aloqa ishtirokchilariga ta’siri yo‘q.

Tarmoqlararo ekranning manzillarni *translatsiyalash* funksiyasi haqiqiy ichki manzillarni tashqi abonentlardan yashirish uchun mo‘ljallangan. Bu tarmoq topologiyasini yashirish va agar himoyalangan tarmoq uchun yetarli miqdorda manzillar ajratilmagan bo‘lsa, yanada ko‘proq sondagi manzillardan foydalanishga imkon yaratadi.

Tarmoqlararo ekran maxsus jurnallarda *hodisalarni qayd* qilib boradi. Biror aniq talab bo‘yicha ekranni sozlash orqali jurnallarni yuritish

imkoniyati nazarda tutilgan. Yozuvlar tahlili o‘rnatilgan qoidalarni buzishga bo‘lgan buzg‘unchilarning urinishlarini qayd qilish va ularni aniqlash imkonini beradi.

Ekran simmetrik emas. U «tashqi» va «ichki» tushunchalarini farqlay oladi. Ekran ichki sohani nazoratsiz va adovatli bo‘lgan tashqi muhitdan himoyasini ta’minlab beradi. Shu bilan birga ekran himoyalangan tarmoq subyektlari tomonidan ommaviy tarmoq obyektlaridan foydalanishni cheklashni ham ta’minlaydi. Foydalanishga ruxsat berilgan subyektning vakolatlari buzilgan holatda uning ish faoliyati blokirovka qilinadi va barcha kerakli ma’lumotlar jurnalga yozib qo‘yiladi.

Tarmoqlararo ekranlarga quyidagi zamonaviy talablar qo‘yiladi:

1. Asosiy talablar – bu ichki tarmoqning xavfsizlikni ta’minlash va tashqaridan ulanishlar va aloqa seanslarini to‘liq nazorat qilish.

2. Ekranlovchi tizim tashkilotning xavfsizlik siyosatini oddiy va to‘liq yuritish uchun quvvatli va moslanuvchan boshqarish vositalariga ega bo‘lmog‘i darkor.

3. Tarmoqlararo ekran lokal tarmoq foydalanuvchilariga sezdirmasdan ishlashi va ular tomonidan ruxsat etilgan amallarni bajarishlariga xalaqit bermasligi lozim.

4. Tarmoqlararo ekran ko‘p miqdordagi murojaatlar bilan blokirovka qilib qo‘yishni va ishdan chiqishining oldini olish uchun, uning protsessori tez ishlay olish, pik rejimlarida kiruvchi va chiquvchi oqimlarni yetarli darajada samarali qayta ishlay olishga ulgurishi lozim.

5. Xavfsizlikni ta’minlash tizimi har qanday tashqi noqonuniy ta’sirlardan himoyalangan bo‘lishi lozim, chunki bu ta’sirlar tashkilotning konfedensial ma’lumotlarini ochish kaliti bo‘lishi mumkin.

6. Ekranni boshqaruv tizimi olisdagi filiallar uchun ham yagona xavfsizlik siyosatini yuritishni markazlashgan holda ta’minlash imkoniyatiga ega bo‘lmog‘i lozim.

7. Tarmoqlararo ekran foydalanuvchilarning tashqi ulanishlari orqali foydalanishga ruxsat berishning mualliflashtirish vositalariga ega bo‘lmog‘i kerak. Bu tashkilot xodimlarini xizmat safarida ham tarmoqdan foydalanishlariga imkon yaratadi.

Mustaqil tayyorgarlik uchun savollar

1. Axborotlarni muhofaza qilishning asosiy va yordamchi apparat vositalariga nimalar kiradi?

2. Axborotlarni muhofaza qilishning dasturiy vositalari qanday dasturlardan iborat?

3. Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklari va kamchiliklari nimalardan iborat?

4. Kompyuter tizimlaridan foydalanish huquqini cheklashning qanday usul va vositalari mavjud?

5. Qanday atributivli indentifikatorlarni bilasiz va ular qanday tartibda ishlaydi?

6. Himoyalovchi apparat-dasturiy komplekslarda himoyalash mexanizmlari nimalardan iborat?

7. Kompyuter viruslari nima?

8. Kompyuter tizimlarining xavfsiz ishlashi uchun qanday qoidalarga rioya etilishi talab etiladi?

9. Tizimdagi axborotlarning butunligi qanday ta'minlanadi?

10. Axborot xavfsizligini ta'minlashning dasturiy va apparat-dasturiy vositalardan foydalanishga qanday talablar qo'yiladi?

11. Ma'lumotlarni bazasini boshqarish tizimida ma'lumotlar qanday muhofaza qilinadi?

12. Tarmoqda axborot xavfsizligini ta'minlovchi qanday apparat-dasturiy vositalar mavjud?

13. Tarmoqlararo ekran qanday funksiyalarni bajaradi?

14. Tarmoqlararo ekranlarga qanday talablar qo'yiladi?

V. O‘ZBEKISTON RESPUBLIKASIDA AXBOROTNI MUHOFAZA QILISHNING DAVLAT TIZIMI

5.1. Axborotni muhofaza qilishning davlat tizimi.
5.2. Axborotni muhofaza qilish sohasida litsenziyalash va sertifikatsiyalash.
5.3. Yetakchi chet el mamlakatlarida axborotni muhofaza qilish tizimlari.

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 me’yoriy 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.

5.1. Axborotni muhofaza qilishning davlat tizimi

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, kadrlarni tayyorlash, maxsus aloqa tizimlari, ilmiy-tadqiqot va tajriba-konstruktorlik ishlarini tashkillashtirish tizimlarini o‘z ichiga oluvchi murakkab tizimdir.

Axborotni muhofaza qilishning davlat tizimi ish yuritishi quyidagi qonun, me’yoriy 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;
– «Faoliyat 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;
– 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 taraqqiyotiga ko‘maklashish, axborotni muhofaza qilish usul va vositalarini qo‘llab, O‘zbekiston milliy xavfsizligiga bo‘lgan zararni jiddiy kamaytirish – 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 idoralari 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 me’yoriy-metodik va axboriy ta’minlash.

5.2. Axborot muhofaza qilish sohasida litsenziyalash va sertifikatsiyalash

O‘zbekiston Respublikasining 2000-yil 25-maydagi «Faoliyatning ayrim turlarini litsenziyalash to‘g‘risida»gi 71-II-sonli Qonuni[1] turli

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

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.

O‘zbekiston Respublikasi Vazirlar Mahkamasi vakolatlari jumlasiga quyidagilar kiradi (5-modda):

– litsenziyalovchi organlarni va faoliyatning ayrim turlarini litsenziyalash tartibini belgilash, qonunda nazarda tutilgan hollar bundan mustasno;

– O‘zbekiston Respublikasi hududida litsenziyalar reyestrini yuritish tartibini belgilash;

– faoliyatning ayrim turlarini litsenziyalash sohasidagi qonun hujjatlariga litsenziyalovchi organlarning rioya etishlarini nazorat qilish;

– litsenziyalashning ayrim turlarini amalga oshirish.

Litsenziyalovchi organlarning vakolatlari jumlasiga quyidagilar kiradi (6-modda):

– faoliyatning ayrim turlarini qonun hujjatlariga muvofiq litsenziyalash;

– qonunda nazarda tutilgan hollarda faoliyatning tegishli turlarini litsenziyalash tartibi to‘g‘risidagi nizomlarni tasdiqlash;

– litsenziya talablari va shartlariga litsenziatlar rioya etishini nazorat qilish;

– litsenziyalarni qayta rasmiylashtirish;

– litsenziyalarning amal qilishini to‘xtatib turish, qayta tiklash;

– litsenziyalarning amal qilishini tugatish;

– litsenziyalarni bekor qilish;

– litsenziyalar reyestrini yuritish.

Faoliyatning litsenziyalanadigan turlari jumlasiga (7-modda) amalga oshirilishi fuqarolarning huquqlari va qonuniy manfaatlariga, sog‘lig‘iga, jamoat xavfsizligiga zarar yetkazishi mumkin bo‘lgan hamda tartibga solib turilishi litsenziyalashdan tashqari usullar bilan amalga oshirilishi mumkin bo‘lmagan faoliyat turlari kiradi.

Amalga oshirilishi uchun litsenziya talab qilinadigan faoliyat turlari qonunlar bilan belgilanadi.

Litsenziya olish uchun litsenziya da’vogari tegishli litsenziyalovchi organga quyidagilarni taqdim etadi (14-modda):

– litsenziya berish to‘g‘risidagi ariza – unda: yuridik shaxs uchun – yuridik shaxsning nomi va tashkiliy-huquqiy shakli, joylashgan yeri (pochta manzili), bank muassasasining nomi va bank muassasasidagi hisob raqami; jismoniy shaxs uchun – familiyasi, ismi va otasining ismi, fuqaroning shaxsini tasdiqlovchi hujjatning ma’lumotlari; yuridik yoki jismoniy shaxs amalga oshirishni mo‘ljallagan faoliyatning litsenziyalanayotgan turi (uning bir qismi), shuningdek qonun hujjatlarida nazarda tutilgan hollarda faoliyatning mazkur turi;

– yuridik shaxslar uchun – yuridik shaxs davlat ro‘yxatidan o‘tkazilganligi to‘g‘risidagi guvohnomaning notarial tasdiqlangan nusxasi; jismoniy shaxslar uchun – yakka tartibdagi tadbirkor davlat ro‘yxatidan o‘tkazilganligi to‘g‘risidagi guvohnomaning nusxasi;

– litsenziyalovchi organ litsenziya da’vogarining arizasini ko‘rib chiqishi uchun litsenziya da’vogari yig‘im to‘laganligini tasdiqlovchi hujjat;

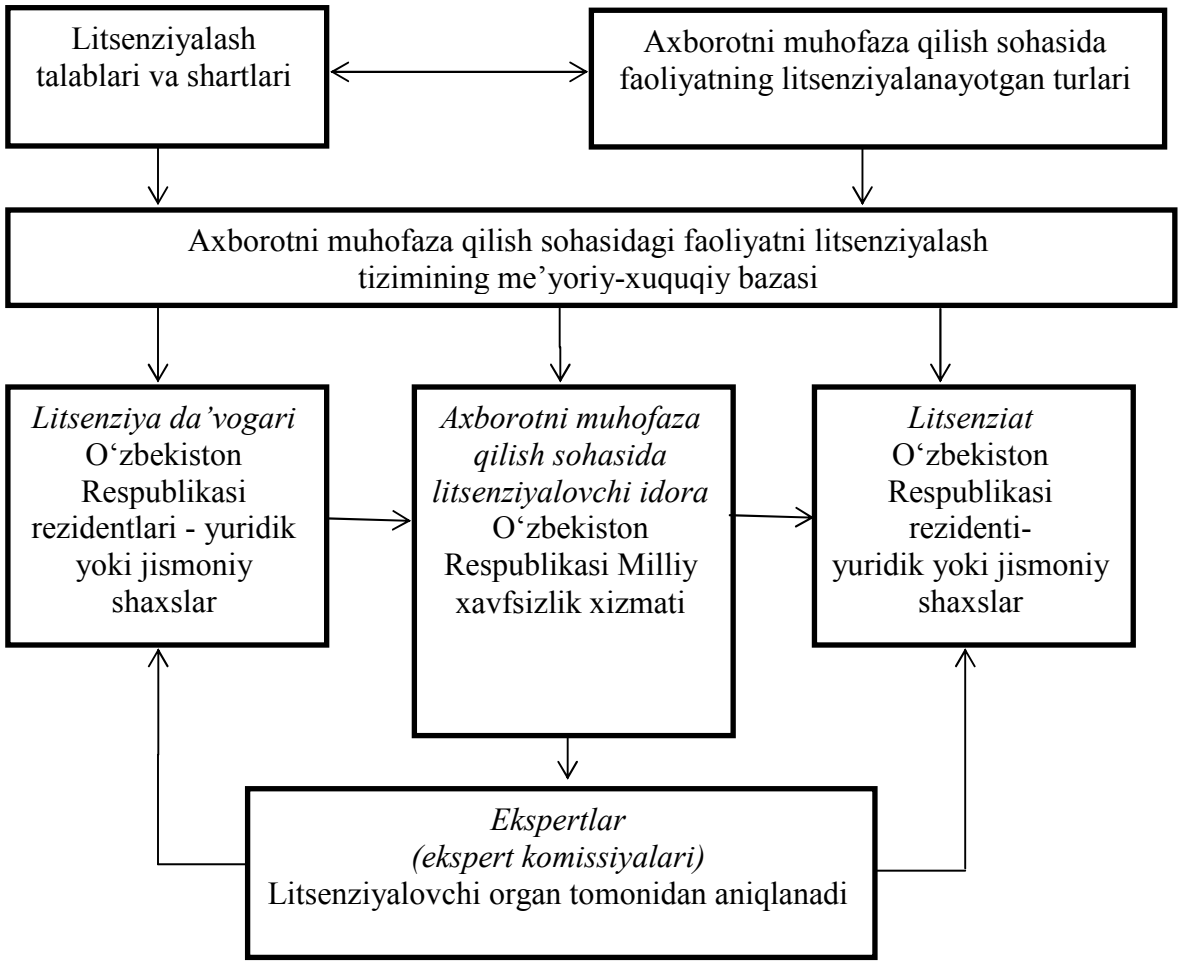
– faoliyatning ayrim turiga litsenziya olish uchun qo‘yiladigan talablar va shartlarni litsenziya da’vogari bajarishi mumkinligini tasdiqlovchi hamda qonun hujjatlarida belgilab qo‘yiladigan boshqa hujjatlar.

Litsenziya da’vogarining arizasini barcha zarur hujjatlar bilan birga olgan kundan e’tiboran o‘ttiz kundan oshmagan muddat ichida litsenziyalovchi organ namunaviy (oddiy) litsenziya berish haqida yoki berishni rad etish to‘g‘risida qaror qabul qiladi va litsenziyalovchi organ litsenziya da’vogarini qabul qilingan qaror to‘g‘risida uch kun ichida xabardor qilishi shart (16-modda).

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 loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta’mirlash va kriptografik himoya vositalarini qo‘llash kiradi.



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

Axborotni muhofaza qilishsh sohasidagi faoliyatni litsenziyalash tizimining me'yoriy-xuquqiy bazasini quyidagilar tashkil qiladi:

– O‘zbekiston Respublikasining 2007-yil-17 iyuldagi 102-sonli qonuni[1] «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[2] 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[3] bilan tasdiqlangan «Axborotning kriptografik himoya vositalarini loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta'mirlash va ulardan foydalanish faoliyatini litsenziyalash to‘g‘risidagi Nizom».

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2005-yil 25-noyabr kunidagi «Axborotlashtirish sohasida normativ-huquqiy bazani takomillashtirish to‘g‘risida»gi 256-sonli qarori[4] bilan tasdiqlangan «Davlat organlarining axborot tizimini yaratish tartibi to‘g‘risidagi Nizom»ning IV bo‘lim 24 bandiga muvofiq davlat idoralarining axborot tizimida qo‘llaniladigan axborotni himoyalash dasturiy-texnik vositalari litsenziyalangan va sertifikatlashtirilgan bo‘lishi kerak.

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

SMT faoliyatini reglamentatsiya qiluvchi asosiy me'yoriy-huquqiy akt bo‘lib O‘zbekiston Respublikasining 1993-yil 28-dekabr kunidagi «Mahsulotlar va xizmatlarni sertifikatlashtirish to‘g‘risida»gi 1006-XII

---

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

[2] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 2007. – №14. – 140-м.

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

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

sonli qonuni[1] 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;

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 akkreditasiya qilingan idoralar;

---

[1] Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – 1994. – №2. – 50-м.; Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – Т., 2000. – №7-8. – 217-м.; 2003. –№5. – 67-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 2006. – №14. – 113-м.; 2006. – №41. – 405-м.

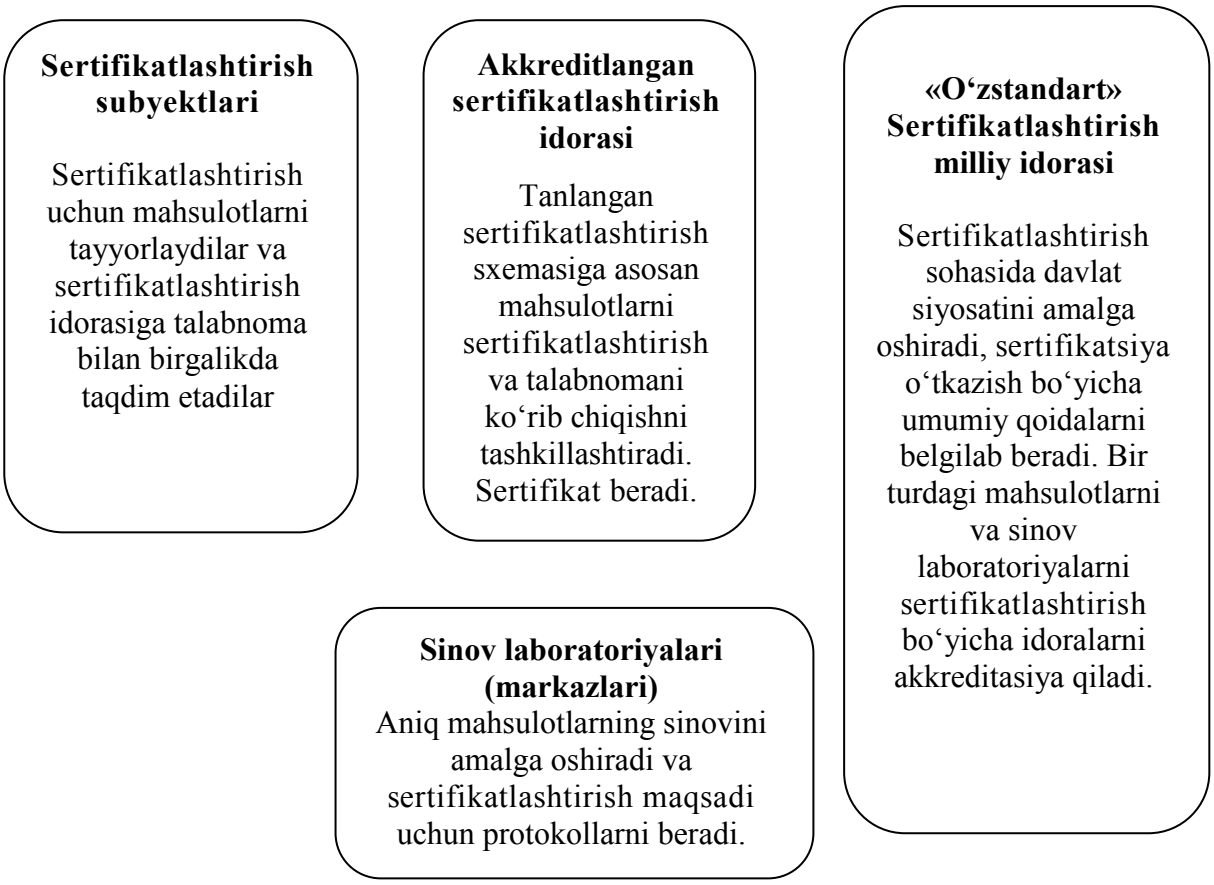
– sinov laboratoriyalari (markazlari).

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.

SMTda mahsulotlar (xizmatlar)ni sertifikatlashtirishning umumiy tartibi:



O‘zbekiston Respublikasi hududida majburiy sertifikatlashtirilishi lozim bo‘lgan mahsulotlar nomlari «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[1]

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

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 nashrlar erkin tarqatiladi (misol uchun yoshlar orasida ommalashgan «Xaker» va «Spetsxaker» jurnallarini keltirish mumkin). Hozirgi kunda ixtiyoriy o‘spirin arzimagan pulga axborot tizimlariga hujum qilishning elementar usullarini o‘rgatuvchi kitobni sotib 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 (ochiq) 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.

Kompyuter jinoyatchiligini sodir etishga qarshi immunitetni hosil qiluvchi yuqori axloq-odobni 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

---

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

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 huquqni muhofaza qiluvchi idoralarda va sudlarda kompyuter sohasidagi jinoyatchilikka qarshi kurashish bo‘yicha mutaxassislarni tayyorlash lozim.

O‘zbekiston Respublikasi Vazirlar Mahkamasining «Toshkent axborot texnologiyalari universiteti faoliyatini tashkil etish to‘g‘risida»gi 2002-yil 7-noyabr 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 «Milliy axborot-kommunikatsiya tizimlarining kompyuter xavfsizligini ta’minlash borasidagi qo‘shimcha chora-tadbirlar to‘g‘risida»gi 2005-yil 5-sentabr 167-sonli qaroriga muvofiq kompyuter va axborot texnologiyalarini rivojlantirish hamda joriy etish markazi «O‘zinfokom» huzurida «Kompyuter hodisalariga chora ko‘rish xizmati» tashkil etilgan.

Ushbu Xizmatning asosiy vazifalariga quyidagilar kiradi:

– kompyuter xavfsizligini ta’minlashda xalqaro tajribani o‘rganish va umumlashtirish asosida axborot tizimlariga noqonuniy kirish harakatlarini oldini olishni ta’minlovchi effektiv dasturiy-apparatli vositalarni qo‘llash bo‘yicha milliy foydalanuvchilarga tavsiyalar ishlab chiqish, ularga konsultativ xizmatlar va texnik yordam berish;

– ehtimoliy xavfni baholash, axborot tizimlarida va davlat korxona hamda tashkilotlarda kompyuter xavfsizligi holati bo‘yicha milliy foydalanuvchilarga konsultativ xizmatlar va texnik yordam berish, insident oqibati va sabablarini tahlil qilishda ko‘maklashish, kompyuter tizimlarini himoyalash uchun mexanizmlarni qidirish;

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

– kompyuter tizimini xavfsizligini ta’minlash masalalari bo‘yicha milliy axborot tizimlariga xizmat ko‘rsatuvchi davlat korxonalari, operatorlar va provayderlar mutaxassislari uchun o‘qitish va trening mashg‘ulotlarini o‘tkazishni tashkil etish.

5.3. Yetakchi chet el 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 ehtiyojini 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 holda milliy va korporativ tarmoqlarni jahon ochiq tarmog‘lariga ulanishini ta’minlovchi axborot texnologiyalarni takomillashtiruvchi davlat dasturini ishlab chiqish.

3. Jahon axborot tarmoqlarida ishlash uchun ommaviy foydalanuvchilarni va axborot xavfsizligi bo‘yicha mutaxassislarni tayyorlash va malakasini oshirish kompleks tizimini tashkil qilish.

4. Ochiq jahon tarmoqlari foydalanuvchilarining mas’uliyatlari va majburiyatlari, reglament huquqi va axborot resurslari bilan foydalanish qoidalarining milliy qonunchilik qismini ishlab chiqish. Jahon ochiq tarmoqlari ishlashining me’yoriy-huquqiy ta’minotini va xalqaro qonunchiligini ishlab chiqishda faol ishtirok etish.

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

AQSh ning 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. AQSh da kompyuter jinoyatchiligiga qarshi kurashish maqsadida 1996-yili «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.

AQSh ning 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 parlament komiteti Britaniya maxsus xizmatlari ustidan nazorat idorasi sifatida 1994-yilda tashkil etilgan. Bu komitet «Razvedka xizmatlari to‘g‘risida»gi qonunga muvofiq uchta maxsus xizmat: Maxfiy xizmat (MI5), SIS razvedkasi va Hukumat aloqa markazi tomonidan budjet mablag‘larining sarflanishini, bu xizmatlarning boshqarilishini va ularning olib borayotgan siyosatini nazorat qilish uchun tuzilgan.

Secret Intelligence Service/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 – Military Intelligence-5 (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 idorasi bo‘lib 1991-yilda tashkil etilgan Federal xavfsizlik xizmati (BSI) hisoblanadi. 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 mezonlar, 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 idoralari, politsiya va boshqa idoralarda axborot almashinishda maxsus xavfsizlik choralarini amalga oshirish;

– sanoat vakillariga maslahatlar berish.

Xavfsizlikni ta’minlovchi boshqa davlat idoralari:

– 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‘ysunadi. Barcha federal yerlarda mahalliy ichki ishlar vazirligiga bo‘ysunadigan 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‘ysunuvchi xizmatlarda ishlaydigan 12779 ga 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 har 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 idoralari strukturasi. Axborot xavfsizligining davlat siyosatini ishlab chiqish, qonunlar, normativ-me’yoriy hujjatlar tayyorlash,

axborotni muhofaza qilishni ta’minlash bo‘yicha o‘rnatilgan me’yorlarni bajarilishi ustidan nazoratni davlat idoralari amalga oshiradilar.

RF Prezidenti axborot xavfsizligini ta’minlovchi davlat idoralariga 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 idorasi 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 idorasi bo‘lib RF Prezidenti huzuridagi Davlat texnik komissiyasi hisoblanadi. Bu komissiya qonun loyihalarini tayyorlashni amalga oshiradi, normativ me’yoriy 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.

RF vazirlik va idoralarida axborot xavfsizligi siyosatining mos darajalarini boshqarishni ta’minlovchi iyerarxiyaga asoslangan tuzilmalar mavjud. Bu tuzilmalar, turli-xil nomlangani bilan o‘xshash funksiyalarni bajaradilar.

Mustaqil tayyorgarlik uchun savollar

1. *Axborotni muhofaza qilishning davlat tizimi nima?*
2. *Axborotni muhofaza qilishning davlat tizimi ish yuritishi qanday qonun, normativ-me’yoriy hujjatlar asosida amalga oshiriladi?*

3. Axborotni muhofaza qilishning davlat tizimida ko‘zlangan maqsad nima?

4. Axborotni muhofaza qilishning davlat tizimida ko‘zlangan maqsadni amalga oshirishda qanday vazifalarni bajarish kerak?

5. «Litsenziya» va «litsenziyalash» tushunchalari nimani anglatadi va ularning ta’rifi qaysi qonunda berilgan?

6. Axborotni kriptografik muhofaza qilish sohasidagi faoliyat qanday litsenziyalanadi?

7. Sertifikatsiyalashning milliy tizimi nima?

8. Sertifikatsiyalash nima maqsadda amalga oshiriladi?

9. Axborotni muhofaza qilish vositalarini sertifikatlashtirish qanday amalga oshiriladi?

10. Axborot xavfsizligi sohasida mutaxassislarni tayyorlash bo‘yicha qanday ishlar olib borilmoqda?

11. Axborot quroli qanday amallarni bajarishga yo‘naltirilgan?

12. Axborot qurolidan himoyalovchi amaliy tadbirlarga nimalar kiradi?

13. AQSh va Buyuk Britaniyadagi axborotni himoyalash tizimi haqida nimalarni bilasiz?

14. Germaniya, Fransiya va Rossiyada axborotni himoyalash qanday tashkil qilingan?

XULOSA

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.

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 dolzarb masalalardan biridir.

Amaliyot shuni ko‘rsatadiki, axborotni muhofaza qilishda yetarli darajadagi yutuqlarga erishish uchun huquqiy, tashkiliy va texnik choralarni birgalikda amalga oshirish zarur. Bu himoyalanadigan axborotning konfedensialligi, tahdidning tasnifi va himoya vositalarining mavjudligi bilan belgilanadi. Umumiy holda xavfsizlikni ta’minlashning kompleks choralariga:

- ruxsatsiz foydalanishdan kompleks himoya qilish vositalari;
- apparat-dasturiy vositalar;
- kriptografik muhofaza qilishning kompleks vositalari;
- injener-texnik tadbirlar;
- texnik kanallarni blokirovkalash kompleks vositalari;
- obyektlarni jismoniy qo‘riqlashni kiritish mumkin.

Bu choralarning har biri boshqasini to‘ldiradi, bironta usulning yo‘qligi yoki yetishmasligi yetarli darajadagi himoyaning buzilishiga sabab bo‘lishi mumkin.

FOYDALANILGAN ADABIYOTLAR

Ўзбекистон Республикасининг Конституцияси. – Т., 2012.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ўзбекистон Республикасининг «Маҳсулотлар ва хизматларни сертификатлаштириш тўғрисида»ги 1993 йил 28 декабрь 1006-XII сон қонуни // Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – 1994. – №2. – 50-м.; Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2000. – №7-8. – 217-м.; 2003. – №5. – 67-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – №14. – 113-м.; 2006. – №41. – 405-м.

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

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

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

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

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

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

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

Ўзбекистон Республикасининг «Ўзбекистон Республикаси Олий Мажлисининг 2001 йил 12 майда қабул қилинган «Амалга оширилиши учун лицензиялар талаб қилинадиган фаолият турларининг рўйхати тўғрисида»ги 222-II-сонли қарорининг 1-иловасига ўзгартиш ва қўшимчалар киритиш ҳақида»ги 2007 йил 17 июль ЎРҚ-102-сон қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №29-30. – 295-м.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

M U N D A R I J A

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

TURGUNOV Nozimjon Abdumannopovich
fizika-matematika fanlari nomzodi, dotsent;

KADIROV Faxriddin
texnika fanlari nomzodi, dotsent;

SAMAROV Xusniddin Kamariddinovich
texnika fanlari nomzodi, dotsent;

IMINOV Abdurasul Abdulatipovich
fizika-matematika fanlari nomzodi;

DJAMATOV Mustafa Xatamovich
fizika-matematika fanlari nomzodi

AXBOROT XAVFSIZLIGI ASOSLARI

Ma’ruzalar kursi

Muharrir **S. S. Qosimov**
Texnik muharrir **D. X. Hamidullayev**

Bosishga ruxsat etildi 01.01. 2013. Nashriyot hisob tabog‘i 8,0.
Adadi 100 nusxa. Buyurtma . Bahosi shartnoma asosida.

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