O’ZBEKISTON RESPUBLIKASI
OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

GULISTON DAVLAT UNIVERSITETI

AXBOROT TEXNOLOGIYALARI KAFEDRASI

AXBOROT XAVFSIZLIGI

fanidan o’quv uslubiy majmua

Bilim sohasi: 100000 - Gumanitar

Ta’lim sohasi: 110000 - Pedagogika

Ta’lim yo’nalishi: 5110700 - Informatika o’qitish metodikasi

Guliston – 2018

O’quv - uslubiy majmua Oliy va o’rta maxsus ta’lim vazirligi tomonidan 2018 yil 24.08. dagi 603 – sonli buyrug’ining 2 - ilovasi bilan tasdiqlangan Axborot xafvsizligi fani dasturi (№ BD - 5110700 3.12 2018 - yil 18.08) talablari asosida tayyorlangan.

Tuzuvchilar: Qudratov A.N. – GulDU “Axborot texnologiyalari” кafedrasi katta o’qituvchisi
Mavlov SH.M. - GulDU “Axborot texnologiyalari” кafedrasi o’qituvchisi

Taqrizchilar: M.E. Mamarajabov - Toshkent davlat pedagogika universiteti dotsenti, pedagogika fanlari nomzodi

D.B. Abduraximov - GulDU “Axborot texnologiyalari” кafedrasi mudiri, pedagogika fanlari nomzodi

Ushbu o’quv–uslubiy majmua Guliston davlat universiteti O’quv – metodik Kengashi tomonidan (28.12.2018 y. dagi, № 6- sonli bayonnoma) nashrga tavsiya etilgan.

M U N D A R I J A

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 ormoqda. 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 «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». Darhaqiqat, 2002-yil 12-dekabrda qabul qilingan bu qonunda 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-mavze. AXBOROT XAVFSIZLIGINING ASOSIY TYSHUNHALARI.

Re;a:

1. Axborotlarga nisbatan mavjud xavf-xatarlari.

2. Axborotlarga nisbatan xavf-xatarlar tasnifi.

3. Axborot tizimlarida malumotlarga nisbatan xavflar.

Tayanch ibora va tushunchalar:

Xakerlar, krekerlar, tashkil qilingan ayg’oqchilik, terroristik guruxlar, iqtisodiy ayroqchilik, "mantiqiy bomba", axborotlar urushi, axborotlarni himoyalash, siyosiy dissident.

1. Axborotlarga nisbatan mavjud xavf-xatarlari.

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, albakilashtirish) ko‘riladigan zararning oldini olishni ta’minlashi lozim. Axborotni muhofaza ilish 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.

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida 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

Konfedensial axborot – hujjatlashtirilgan axborot, undan foydalanish qonun hujjatlariga muvofiq chegaralanadi 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-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».

2. Axborotlarga nisbatan xavf-xatarlar tasnifi.

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 axborot xavfsizligi axborot borasidagi xavfsizlik deb belgilangan

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 manfaatlar*i* 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 tajovuzlardanhimoyalash 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 tavsifigaega.

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 imoyalanganligi;

− fuqarolar, alohida guruhlar va ijtimoiy qatlamlar, umuman olgandaaholining 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 shaxslaryoki 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. 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.

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.

3. Axborot tizimlarida malumotlarga nisbatan xavflar.

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:

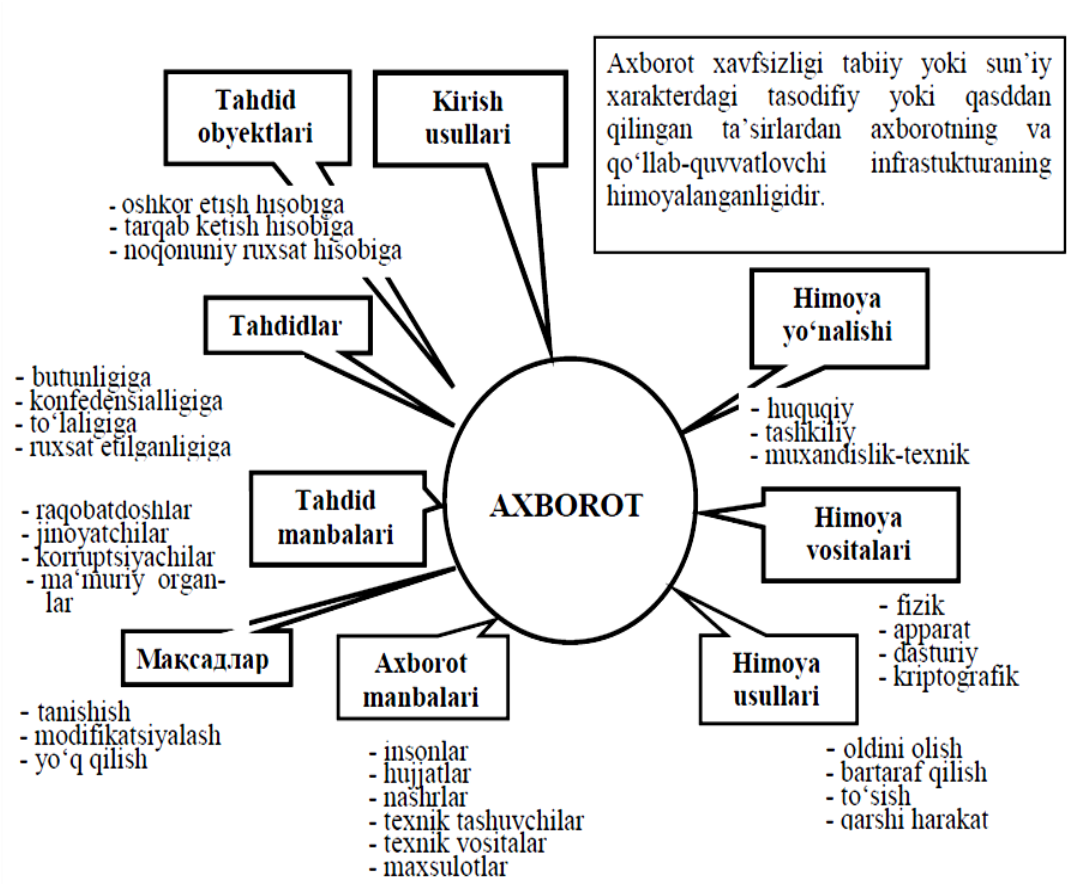
– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– 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 oydalanishni 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.

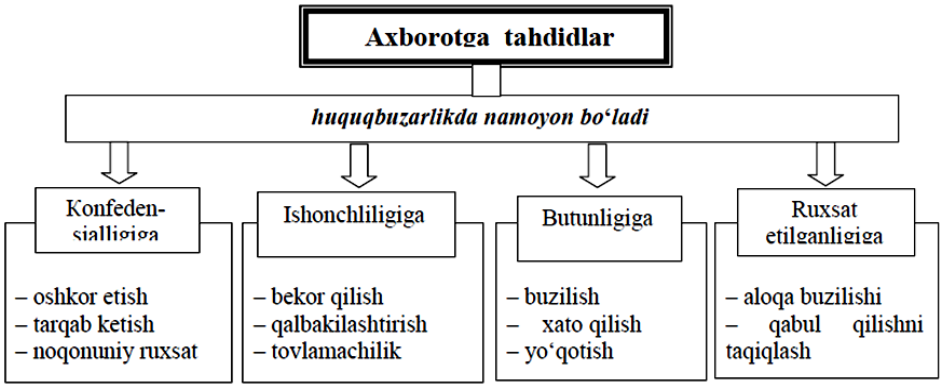
Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida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

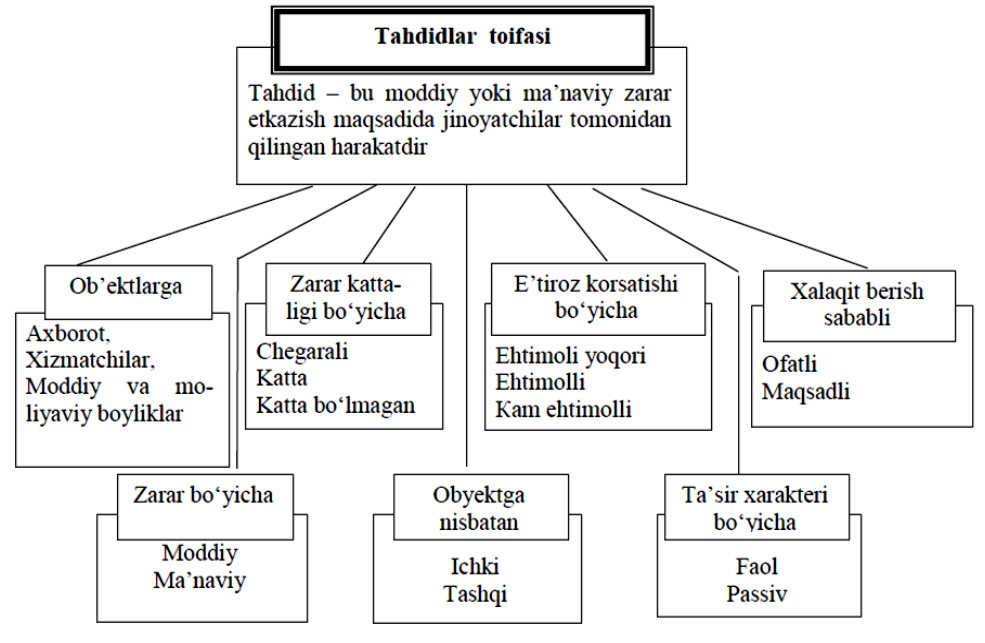
– intellektul mulk obyektlariga tahdid.

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.



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.

Tahdid – bu moddiy yoki ma'naviy zarar etkazish maqsadida jinoyatchilar tomonidan qilingan harakatdir

Tahdidlar toifasi

Axborot, Xizmatchilar, Moddiy va moliyaviy boyliklar Ob'ektlarga Ehtimoli yoqori Ehtimolli Kam ehtimolli E'tiroz korsatishi bo'yicha Ofatli Maqsadli Xalaqit berish sababli Ichki Tashqi Obyektga nisbatan Moddiy Ma'naviy Zarar bo'yicha Faol Passiv Ta'sir xarakteri bo'yicha

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, nazorato‘ 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.

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.

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);

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:

– ***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);

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).

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:

O‘zbekiston Respublikasi Adliya vazirligi Me’yoriy-huquqiy hujjat loyihasini ishlab chiquvchi organ Me’yoriy-huquqiy hujjatlarni Davlat ro‘yxatiga taqdim etish Me’yoriy-huquqiy hujjat loyixasini qabul qiluvchi organga kiritish Loyihani tayyorlovchi komissiya Me’yoriy-huquqiy hujjatni tayyorlashda uning amaliyotda qo‘llanilishi va jamoatchilik fikrini o‘rganish Me’yoriy-huquqiy hujjat loyihalarini ekspertiza qilish Me’yoriy-huquqiy hujjatning rasmiy matnini tasdiqlash Me’yoriy-huquqiy hujjatni chop etish, kuchga kirishi va amal qilinishi
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.

– 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, umumfoydalaniluvchi obyektlarning butunligini ta’minlash maqsadida ularga ruxsatni vaqtincha chegaralovchi xavfsizlik funksiyalari, ruxsat berish huquqini tarqatishni boshqarish kabilar);
– hisobot berishlilik (protokollashtirish);
– audit (mustaqil nazorat);
– obyektlardan qayta foydalanish;
– axborotning aniqligi (ma’lumot turli qismlarining o‘zaro mosligini ta’minlash (aloqa aniqligi) hamda axborotni uzatishda uni o‘zgarmasligini ta’minlash (kommunikatsiya aniqligi));

– xizmat ko‘rsatishning ishonchliligi (qisqa vaqt ichida vaqt bo‘yicha
kritik harakatlar bajarilishini ta’minlovchi funksiyalar; kritik bo‘lmagan, ya’ni kerakli vaqtda ma’lumotni olish imkonini berish; xatolarni topish va ularni bartaraf etish funksiyalari; kommunikatsiya xavfsizligini ta’minlovchi rejalovchi funksiyalar);
– ma’lumot almashish.
6. Xavfsizlik mexanizmlarini ifodalash.
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.

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?

Nazorat savollari

1. Axborot xavfsizligi milliy xavfsizlik tizimida nima tushuniladi?

2. Axborot xavfsizligining zamonaviy konsepsiyasi nima?

3. Axborot xavfsizligiga tahdid deganda nima tushuniladi?

4. Axborotni ximoyalashda qanday usullari va turlari mavjud?

5. Axborotni muhofaza qilish qanday obyektlarga ega?

6. Axborotni muhofaza qilish vositalariga nimalar kiradi?

FOYDALANILGAN ADABIYOTLAR:

1. Ganiev S.K., Karimov M.M.Tashev K.A. Axborot xavfsizligi. O'quv qo'llanma. T

2. Informatika. Bazovo'y kurs. Pod redaktsiey S.V.Simonovicha Sank — Peterburg. 2001 g.

3. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka? 2001 g.

4. Informatika. Pod redaktsiey prof. N.V.Makarovoy M.: 1997 g.

5. Axborot tizimlari va texnologiyalari. Akad. S.G'ulomov va boshkalar. T.: "Shark", 2000 y.

2 Mavzu: AXBOROT XIMOYASI VA UNING TURLARI.

Reja:

1. Axborot ximoyasi va uning turkumlari.

2. Tarmoq xavfsizligini nazorat qilishni texnik vositalari.

3. Avtomatlashtirilgan axborot tizimlarida ma'lumotlarga nisbatan xavflar.

4. Avtomatlashtirilgan axborot tizimlarida ximoyalash zarurati.

Tayanch ibora va tushunchalar*:* Passif va aktif xujumlar,texnik ximoya, kodlash, ohiq kalit, yopiq kalit, terroristik guruxlar, iqtisodiy ayroqchilik, "mantiqiy bomba", axborotlar urushi, axborotlarni himoyalash, siyosiy dissident.

1. Axborot ximoyasi va uning turkumlari.

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;

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 koʻrinish – obyektning tuzilishi va toʻlaligicha koʻrinishini aks ettiradigan kattaliklarini (tarkibi, soni va alohida obyektlarning joylashuvi, shakli va geometrik oʻlchamlari) aniqlovchi belgilar;

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

Texnik demaskirovka belgilarini ikki toifaga boʻlish mumkin:

– toʻgʻridan-toʻgʻri demaskirovka belgilari – himoya obyektining faoliyati va uning fizik maydonlari (elektromagnit, akustik, radiatsion va boshqalar) bilan bogʻliq boʻlgan, himoya qilinadigan axborotga bogʻliq boʻlmagan atrof-muhitning fizik maydoni fonidan farq qiladigan belgilar;

– bilvosita demaskirovka belgilari – obyektning faoliyat koʻrsatishi natijasida atrof-muhitdagi oʻzgarishlar natijasida yuzaga keladigan belgilar (faoliyatning optik-vizual belgilari, geometrik oʻlchamlar, yoritilganlikning keskin farq qilinishi, ishlab chiqarish faoliyatidan qolgan izlar va hokazo).

Axborotni muhofaza qilishning samaradorlik koʻrsatkichi himoya obyektining texnik demaskirovka belgilari kattaligi boʻlib, unga nisbatan axborotni muhofaza qilish samaradorligining me’yorlari belgilanadi.

Xavfli signal, obyekt belgisining koʻrsatkichi boʻlib, undan konfedensial ma’lumotlarni olish uchun texnik razvedkada (TR) foydalaniladi. Obyektni aniqlash – TR vositalarining faoliyati boʻlib, 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 boʻlishi mumkin, biroq obyektni aniqlashda bu belgilarning ma’lum toʻplamidan foydalaniladi.

Texnik vositalar bilan himoyalanadigan ma’lumotlarning manbasi va tashuvchilari:

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

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

– obyektning shakli, rangi, oʻlchami va elementlarini 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 boʻyicha amalga oshiriladi. Bu belgilar *koʻrinishi, faoliyat belgisi va joylashuvi* boʻyicha uchta guruhga boʻlinadi. *Koʻrinishi boʻyicha*

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.

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;

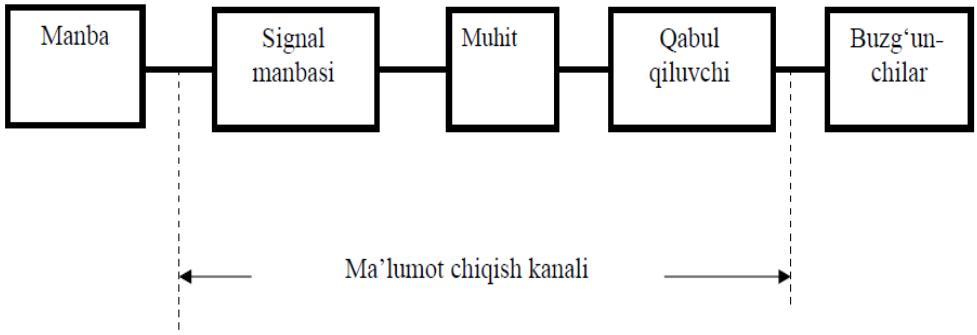
nurlanish turi; chastotani qayta sozlash tartibi va chegarasi; modulyatsiya qilinuvchi signalning turi va o‘zgarish qonuniyati; signal kattaliklarining qiymatlari (tashuvchi chastotalar, impuls davomiyligi, impulsning chiqish chastotasi va boshqalar).

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. Tarmoq xavfsizligini nazorat qilishni texnik vositalari.

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.

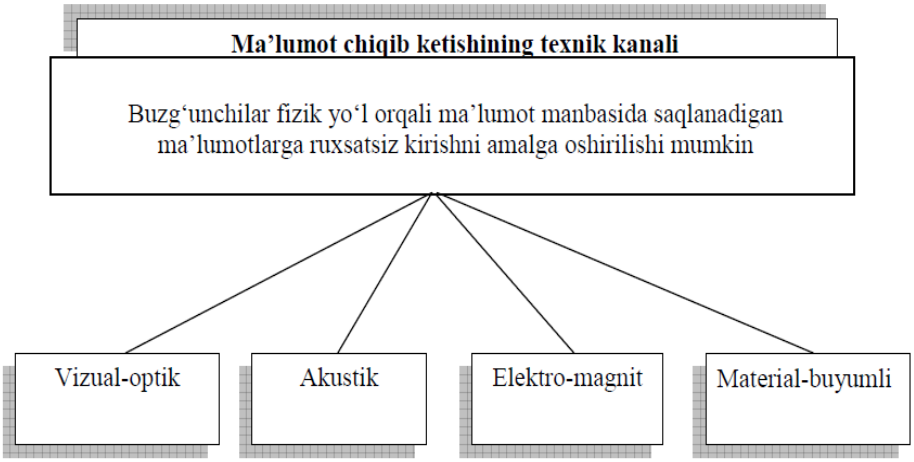
Fizik xususiyatlarini inobatga olgan holda ma’lumotlar chiqib ketish kanalining paydo bo‘lishini quyidagi guruhlarga ajratish mumkin:

– vizual-optik;

– akustik;

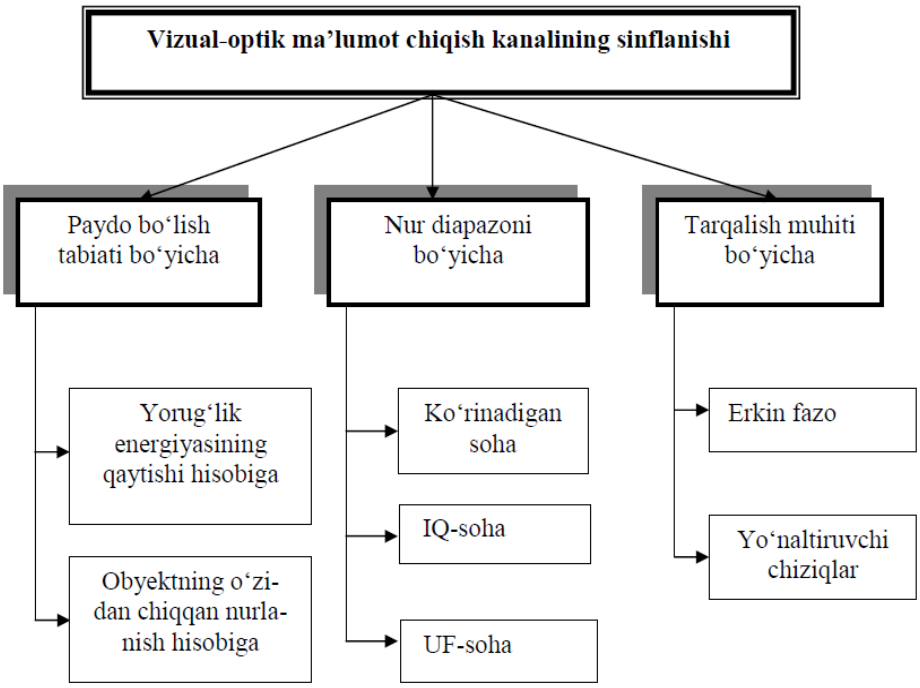
– elektromagnit (magnit va elektrik maydonni o‘z ichiga oladi);

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

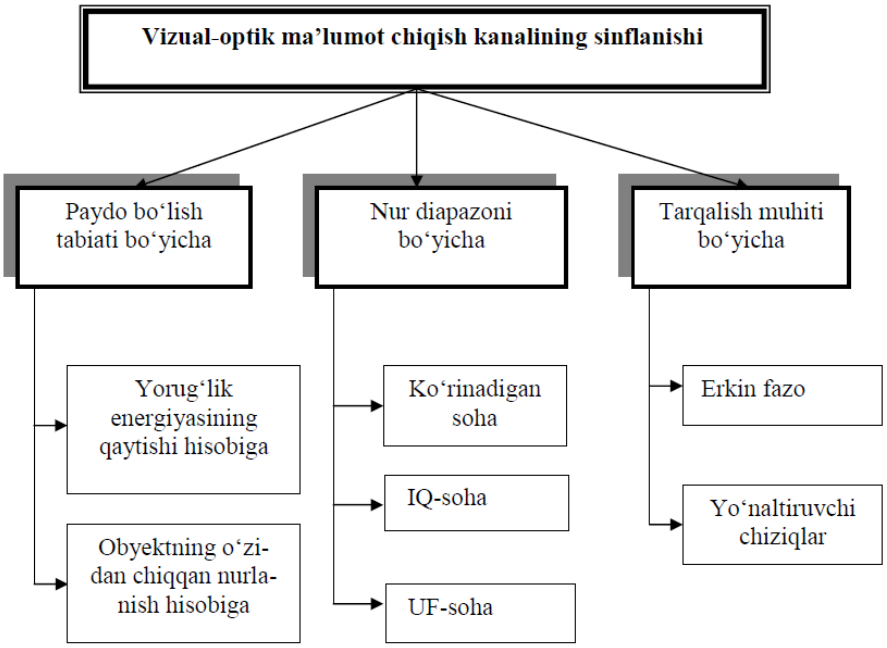


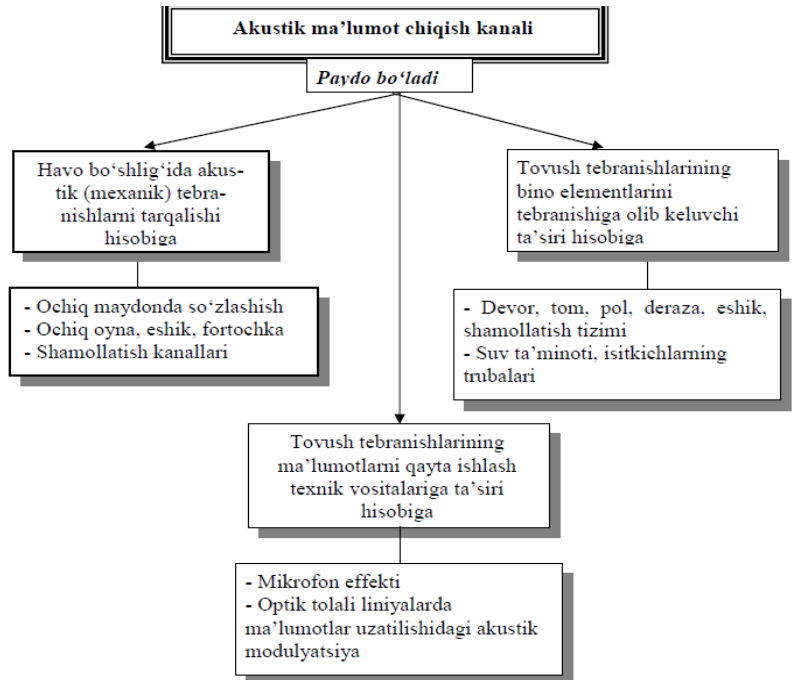
Vizual-optik kanallar – bu bevosita yoki uzoqdan (jumladan televizion) kuzatishdir. Ma’lumot tashuvchi bo‘lib, konfedensial ma’lumot manbasi chiqaradigan yoki undan qaytuvchi Ko‘rinadigan, infraqizil va ultrafiolet diapazondagi yorug‘lik xizmat qiladi.

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.

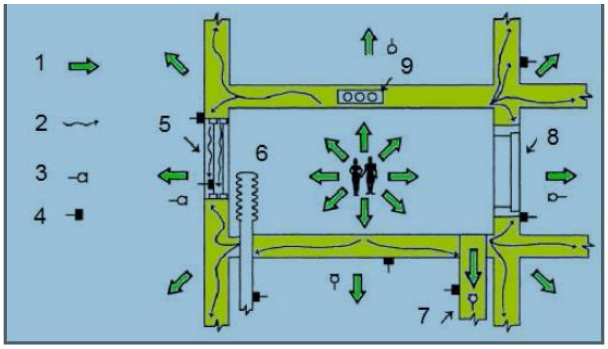


Havoda akustik to‘lqin tarqalganda havo zarralari tebranadi va buning natijasida biridan-biriga energiya uzatiladi. Agar tovush yo‘lida to‘siq bo‘lmasa, u hamma tomonga birday tarqaladi. Agar tovush to‘lqinlari yo‘lida devor, oyna, eshik, tom va kabi boshqa to‘siqlar bo‘lsa, tovush to‘lqini ularga ma’lum 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.



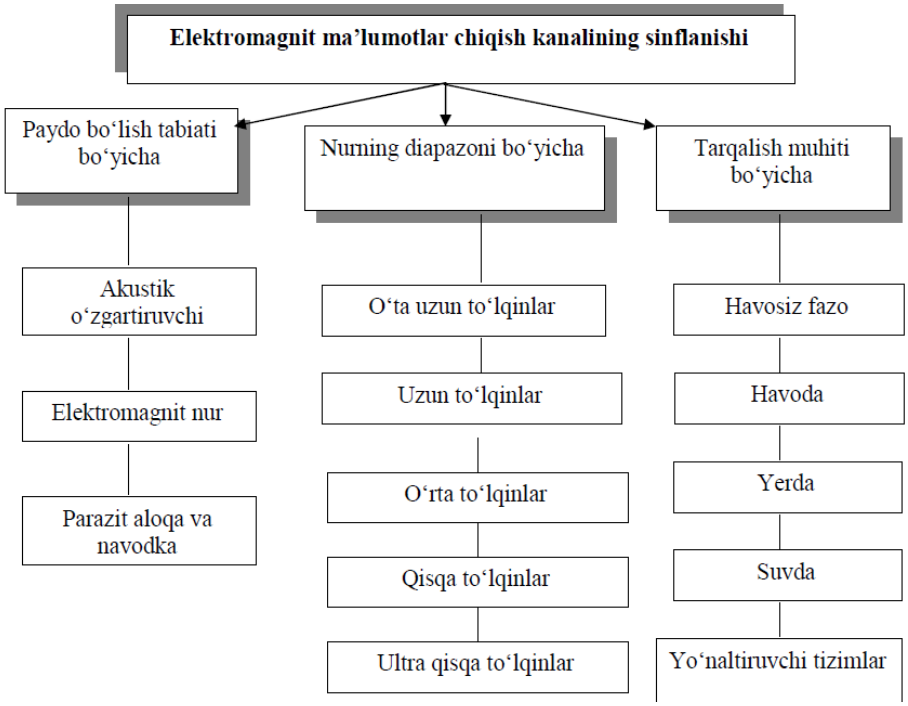


Quyidagi rasmda akustik va vibratsion tebranishlar orqali ma’lumotlar chiqib ketish kanallarining chizmasi keltirilgan bo‘lib, unda akustik tebranish va tovushlarning qattiq muhitda, metal buyumlarda va binoning boshqa elementlarida tarqalishi tasvirlangan.



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.



3. Avtomatlashtirilgan axborot tizimlarida ma’lumotlarga nisbatan xavflar.

Ma’lumotlarni vizual-optik kanal bo‘yicha chiqib ketishidanhimoyalash – 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;

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;

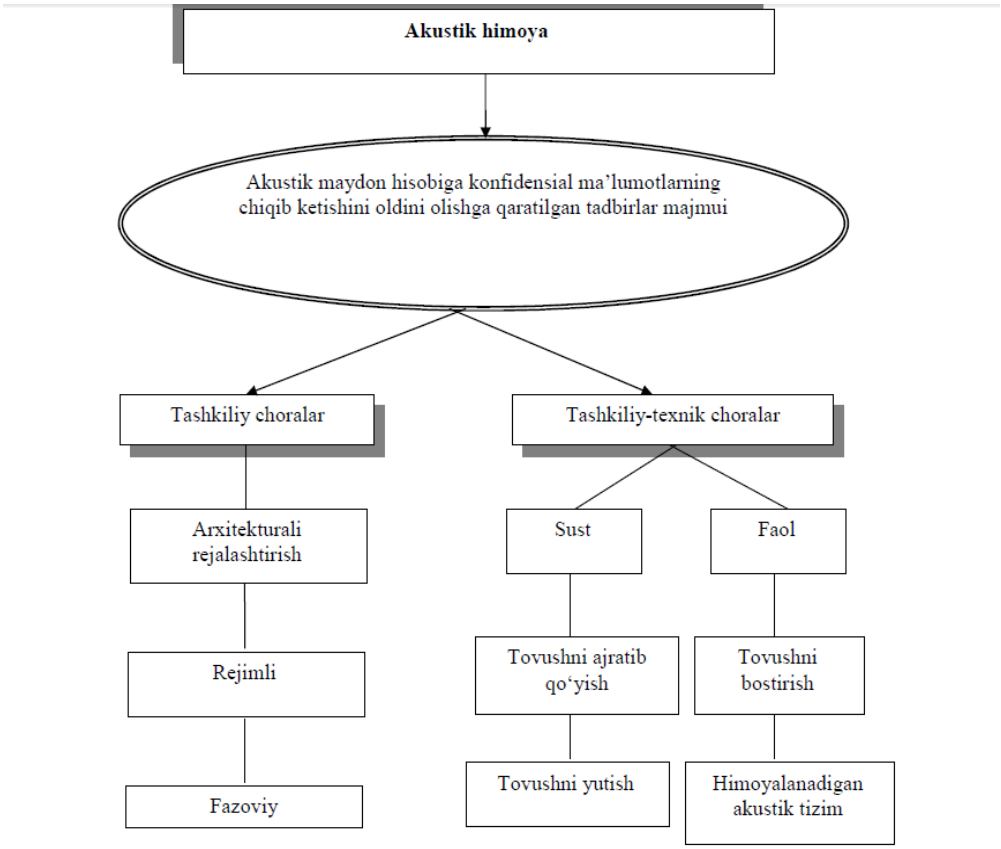
– ma’lum bir vaqtdan keyin kompyuter monitori va umumfoydalanish

ekranlarini o‘chiruvchi vositalardan foydalanish (vaqt bo‘yicha ishlash rejimi).

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



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;

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

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;

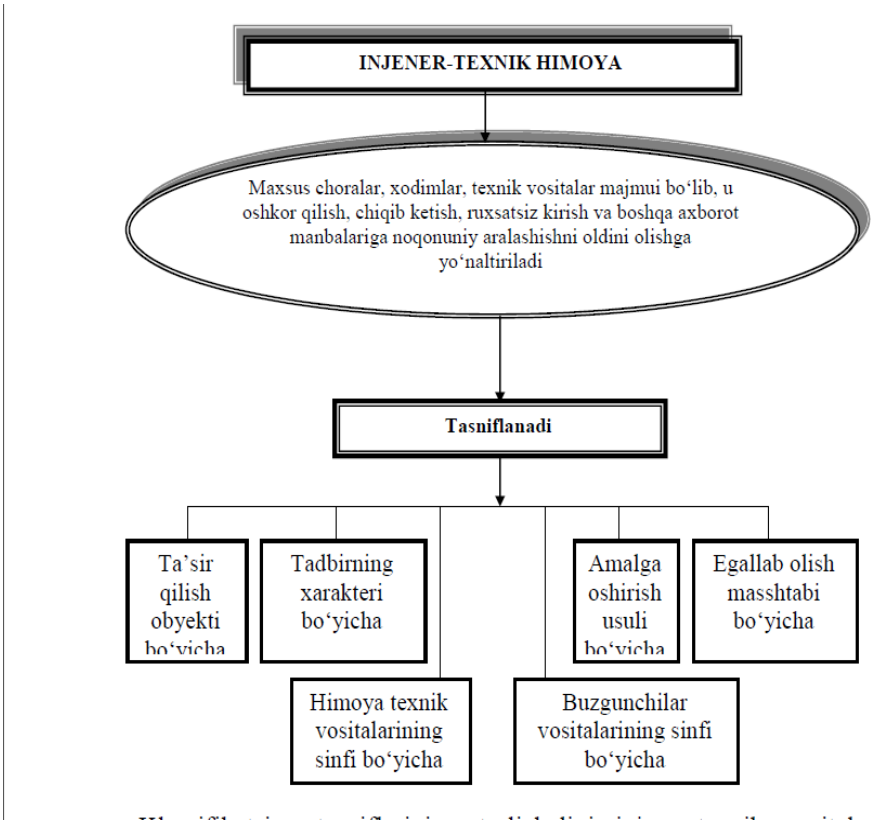
– radiomikrofon signallari;

4. Avtomatlashtirilgan axborot tizimlarida ximoyalash zarurati.

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. 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.

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?

Nazorat savollari.

1. Axborot xavfsizligi milliy xavfsizlik tizimida nima tushuniladi?
2. Axborot xavfsizligining zamonaviy konsepsiyasi nima?
3. Axborot xavfsizligiga tahdid deganda nima tushuniladi?
4. Axborotni ximoyalashda qanday usullari va turlari mavjud?
5. Axborotni muhofaza qilish qanday obyektlarga ega?
6. Axborotni muhofaza qilish vositalariga nimalar kiradi?

FOYDALANILGAN ADABIYOTLAR:

1. Ganiev S.K., Karimov M.M.Tashev K.A. Axborot xavfsizligi. O’quv qo’llanma. T
2. V. Passikov. Zahita kompyuternoy informatsii. M.: Nauka? 2001 g.
3. Informatika. Pod redaktsiey prof. N.V.Makarovoy M.: 1997 g.
4. Axborot tizimlari va texnologiyalari. Akad. S.G’ulomov va boshkalar. T.: "Shark", 2000 y.