O’ZBEKSITON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

H i m o y a g a
kafedra mudiri
Irgasheva D.Ya._____
«___»_____2015 y.

BAKALAVR BITIRUV ISHI

Mavzu: «Server ximoyasini ta’minlashda apparat va dasturiy vositalarning samaradorligini oshirish usullari»

Bitiruvchi	_____ (imzo)	Oqboyev A.Q.
Rahbar	_____ (imzo)	Karimov M.M.
Taqrizchi	_____ (imzo)	_____ (f.i.sh)
HFX maslahatchisi	_____ (imzo)	_____ (f.i.sh)

Toshkent – 2015

Mundarija

Kirish

Bugungi kunda AKT ning iqtisodiyotning va ijtimoiy hayotning barcha sohalariga joriy qilinishi, uning turmush farovonligi va qulayligidagi tutgan o‘rni, ish samaradorligini oshirishdagi ahamiyati oshib borishi mas’ul idoralar oldiga bu yo‘nalishdagi say-harakatlarni yanada jadallashtirish vazifasini qo‘ymoqda.

Shuningdek, “elektron hukumat” tizimini rivojlantirish loyihalari doirasida jismoniy va yuridik shaxslarning identifikatsiya tizimi yo‘nalishidagi istiqbolli rejalar amalga oshirilmoqda.

Umumjahon axborot globallashuvi jarayonlari axborot-kommunikatsiya texnologiyalarini nafaqat mamlakatlar iqtisodiyoti va boshqa sohalariga joriy etish, balki axborot tizimlari xavfsizligini ta’minlashni ham taqozo etayotir. O‘zbekiston axborot va kommunikatsiya texnologiyalari sohasidagi xalqaro xavfsizlik tizimiga Markaziy Osiyoda birinchilardan bo‘lib qo‘shildi.

Axborot xavfsizligini ta’minlash bo‘yicha O’zbekiston Respublikasi prezidentining 2015 yil 4 fevraldagi qaroriga asosan tashkil etilgan O’zbeksiton Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi tomonidan axborot xavfsizligi bo’yicha bir necha chora-tadbirlar amalga oshirilmoqda. Va ushbu ishlar bilan shug’ullanishni Axborot xavfsizigini ta’minlash markaziga yuklatilgan edi[1].

Mazkur Markazning asosiy maqsadi etib, «Elektron hukumat» tizimining axborot tizimlari, resurslari va ma’lumotlar bazalarining, shuningdek Internet tarmog‘i milliy segmentining axborot xavfsizligini ta’minlash sohasidagi normativ-huquqiy bazani takomillashtirish bo‘yicha takliflar ishlab chiqish, davlat organlari tizimlari va axborot resurslarida axborot xavfsizligini ta’minlash belgilangan.

Markaz xodimlari axborot xavfsizligiga hozirgi vaqtdagi tahdidlar to‘g‘risidagi ma’lumotlarni yig‘ish, tahlil qilish va to‘plash bilan shug‘ullanadilar, «Elektron hukumat» tizimi axborot tizimi, resurslari va ma’lumotlar bazalariga noqonuniy kirib olish holatlarining oldini olishni ta’minlaydigan tashkiliy va

dasturiy-texnik yechimlarni samarali qabul qilish bo‘yicha tavsiyalar va takliflar ishlab chiqishda ishtirok etadilar.

“Elektron hukumat” tizimi axborot xavfsizligini ta’minlashning me’yoriy-huquqiy asoslarini takomillashtirish bo‘yicha takliflarini ishlab chiqish ham markazning maqsad-vazifalari hisoblanadi.

Mamlakatimiz siyosatining ustuvor yo‘nalishlariga kiritilgan kompyuter va axborot texnologiyalari, telekomunikatsiya, ma’lumotlarni uzatish tarmoqlari, Internet xizmatlaridan foydalanish rivojlanmoqda va modernizatsiyalashmoqda. Jamiyatimizning barcha sohalariga kundalik hayotimizga zamonaviy axborot texnologiyalarini keng joriy etish istiqboldagi maqsadlarimizga erishishni ta’minlaydi. Har bir soha faoliyatida Internet tarmog‘idan foydalanish ish unumdorligini oshirmoqda[2].

Aynan tarmoqdan foydalangan holda tezkor ma’lumot almashish vaqtdan yutish imkonini beradi. Xususan, yurtimizda Elektron hukumat tizimi shakllantirilishi va uning zamirida davlat boshqaruv organlari hamda aholi o‘rtasidagi o‘zaro aloqaning mustahkamlanishini tashkil etish tarmoqdan foydalangan holda amalga oshadi. Tarmoqdan samarali foydalanish demokratik axborotlashgan jamiyatni shakllantirishni ta’minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha tezkor natijaga ega bo‘linadi.

Biroq tarmoqqa noqonuniy kirish, axborotlardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Ish faoliyatini tarmoq bilan bog‘lagan korxona, tashkilotlar hamda davlat idoralari ma’lumot almashish uchun tarmoqqa bog‘lanishidan oldin tarmoq xavfsizligiga jiddiy e’tibor qara-tishi kerak. Tarmoq xavfsizligi uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotni ishonchli tizimli tarzda ta’minlash maqsadida turli vositalar va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirish orqali amalga oshiriladi. Tarmoq xavsizligini ta’minlash maqsadida qo‘llanilgan vosita xavf-xatarni tezda aniqlashi va unga nisbatan qarshi chora ko‘rishi kerak.

Tarmoq xavfsizligiga tahdidlarning ko‘p turlari bor, biroq ular bir necha toifalarga bo‘linadi:

— axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (Eavesdropping);

— xizmat ko‘rsatishdan voz kechish; (Denial-of-service);

— portlarni tekshirish (Port scanning).

Tarmoq orqali ma’lumot almashish mobaynida yuborilayotgan axborotni eshitish va o‘zgartirishga qarshi bir necha samarali natija beruvchi texnologiyalar mavjud:

— IPSec (Internet protocol security) protokoli;

— VPN (Virtual Private Network) virtual xususiy tarmoq;

— IDS (Intrusion Detection System) ruxsatsiz kirishlarni aniqlash tizimi.

Bakalavr bitiruv ishining maqsadi: Server ximoyasini ta’minlashda apparat va dasturiy vositalarning samaradorligini oshirish usullarini ishlab chiqishdan iborat.

Ishni bajarishda quyidagi vazifalarni bajarish lozim:

— Axborot xavfsizligini ta’minlovchi vositalarni ko’rib chiqish;

— Server himoyasini tashkil etish.

Bitiruv malakaviy ishi kirish, 3 ta qism, xulosa, adabiyot ro’yhati va ilovadan iborat.

1-qism nazariy qism: axborot kommunikatsiya tizimlarida tahditlar va zaifliklar, ularning turlari, zarar darajalari berilgan. Shuningdek, ushbu tahditlarni oldini olishning dasturiy va apparat vositalari keltirilgan.

2-qism amaliy qism: korparativ tarmoqda serverga qo’yiladigan asosiy talablar, uni himoyalashning usullari va xavfsizligini ta’minlash samaradorligini oshirishning mantiqiy sxemasi ishlab chiqilgan.

3-qism hayot faoliyati xavfsizligi muammolari keltirilgan.

1. Nazariy qism. Axborot kommunikatsiya tizimlarida zaifliklar va tahditlar

1.1. Axborot xavfsizligiga tahdid va uning turlari

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;

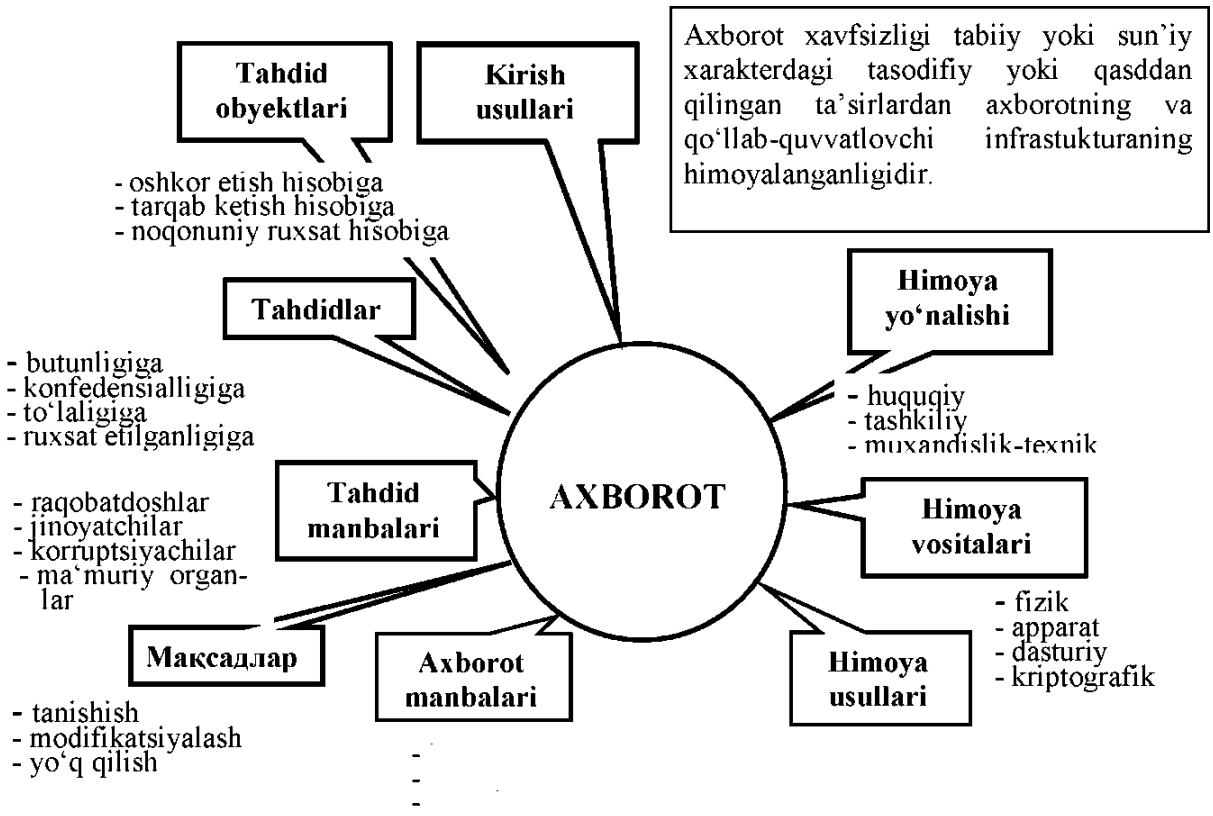
—axborot tizimida mavjud bo'lgan shaxsiy ma'lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

— 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[11].

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:



1.1-rasm. Axborotning tashkil etuvchilari

— 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[4].

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

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.

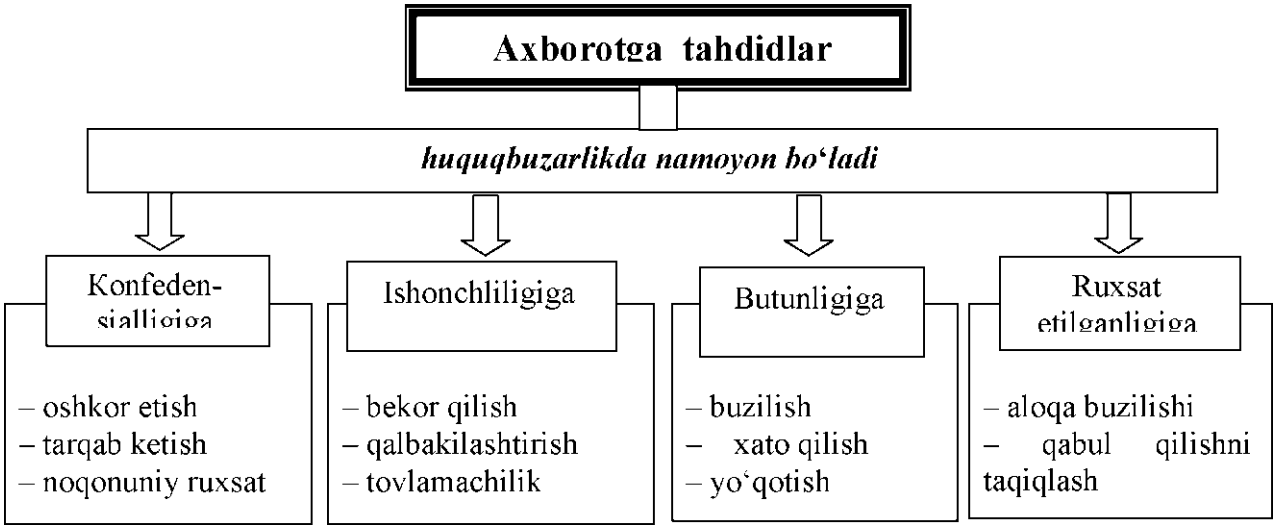
Tahdidning uchta ko'rinishi mavjud.

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'zgar- tirishni o'zida mujassamlaydi. Jinoyatchilar axborotni qasddan o'zgar- tirganda, 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 mavjud- ligidir[5].

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.



1.2-rasm. Taxdit turlari

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;

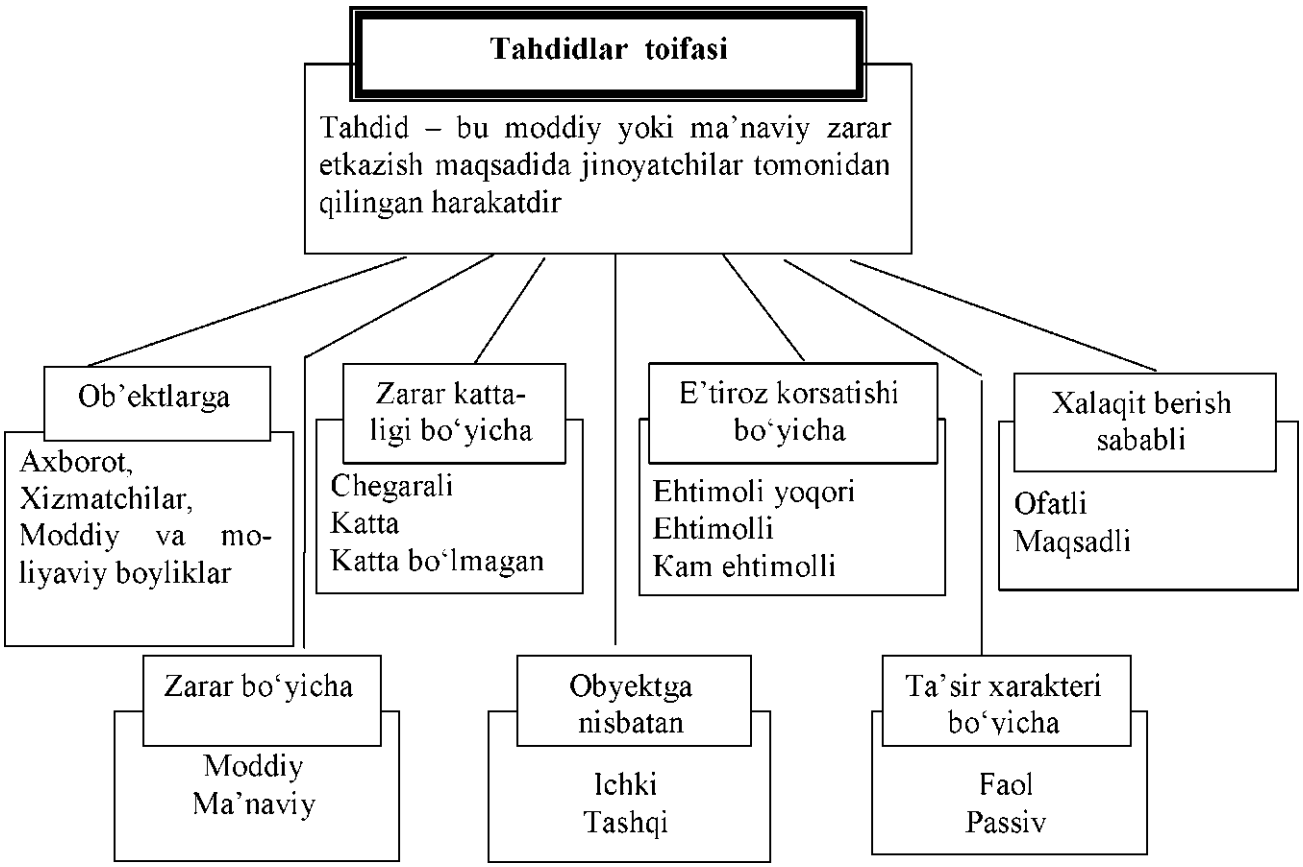
- intellektul mulk obyektlariga tahdid.

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.



1.3-rasm. Taxditlar toifalari bo'yicha turlari

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.

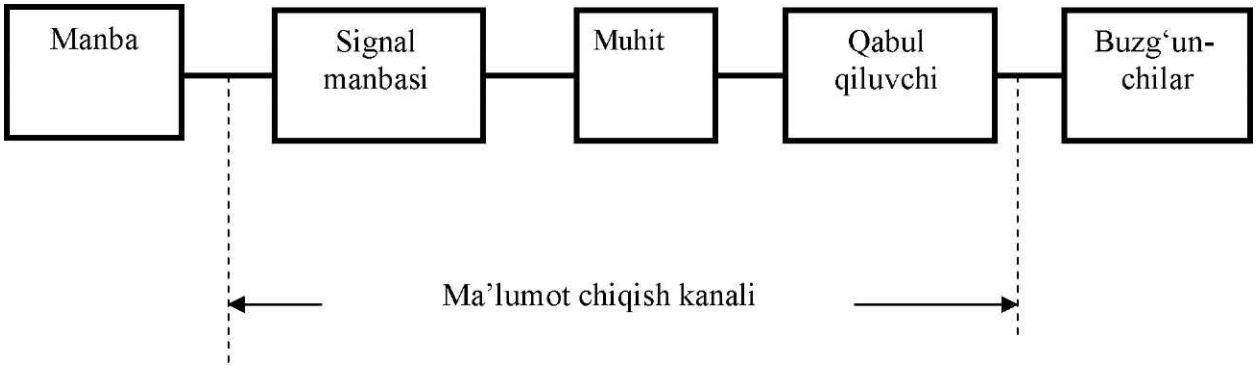
Turli axborot tizimlarida foydalanuvchilar xizmat ko'rsatuvchi personal hisoblanib, axborot manbai va tashuvchilari bo'lishi mumkin.

1.2. 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 qan- day 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[6].



1.4-rasm. Ma’lumot chiqib ketuvchi texnik kanalning bosqichlari

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.

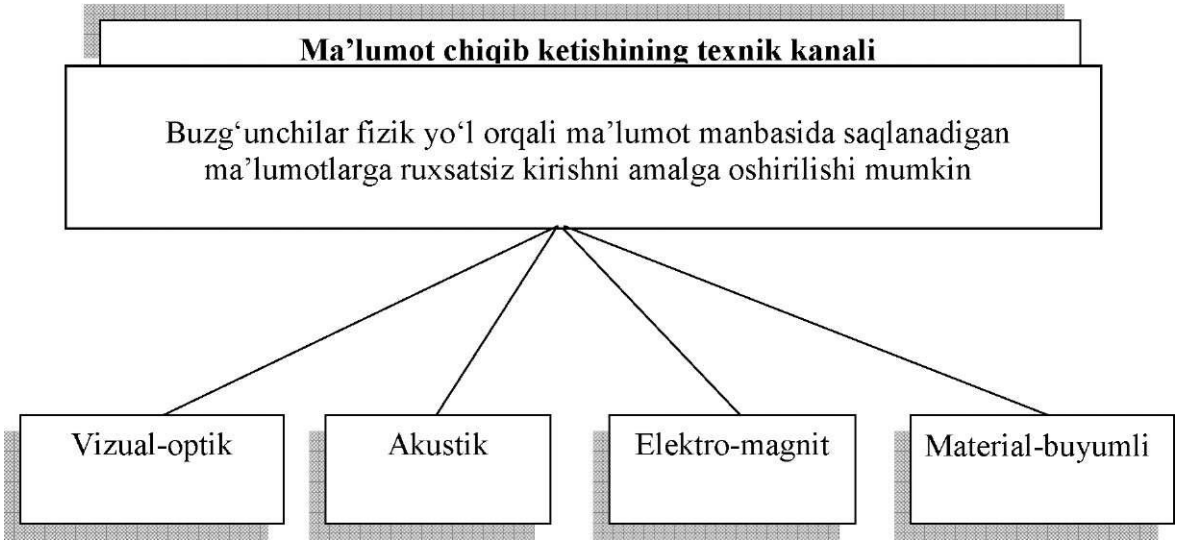
Fizik xususiyatlarini inobatga olgan holda ma'lumotlar chiqib ketish kanalining paydo bo'lishini quyidagi guruhlarga ajratish mumkin:

— 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).

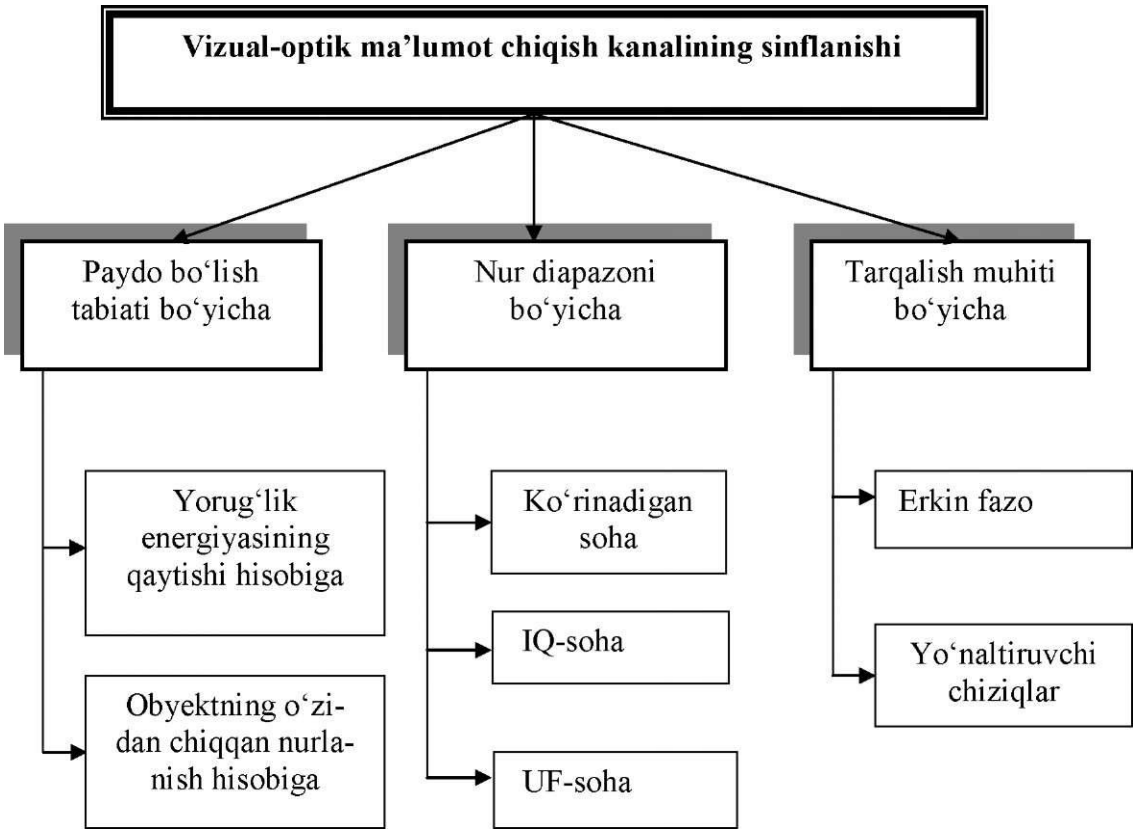


1.5-rasm. Ma’lumot chiqib ketuvchi texnik kanallar

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.



1.6-rasm. Axborot chiqib ketuvchi optik kanallar

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[7].

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

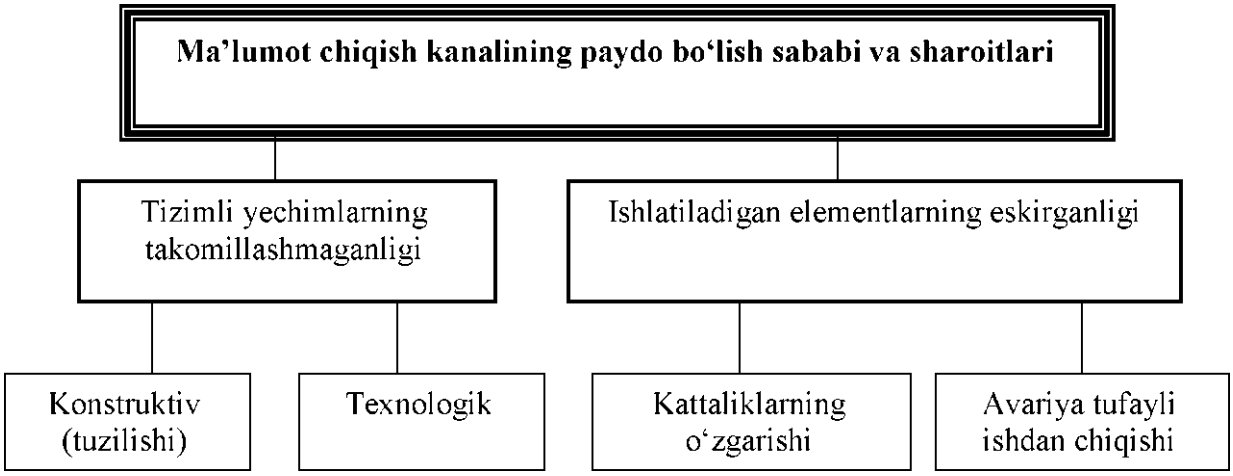
hamda zararli aloqa va navodkalar hisoblanadi. YOEMNN ixtiyoriy elektron qurilmaga, tizimlarga, tabiiy xususiyatlarga ega bo'lgan mahsulotlarga xosdir.

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.



1.7-rasm. Ma’lumot chiqish kanalining paydo bo’lish sababi

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.

1.3. Server ximoyasini ta’minlashda texnik vositalarning roli

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.

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[8].

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.

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 chega-ralash);

- 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[9].

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.

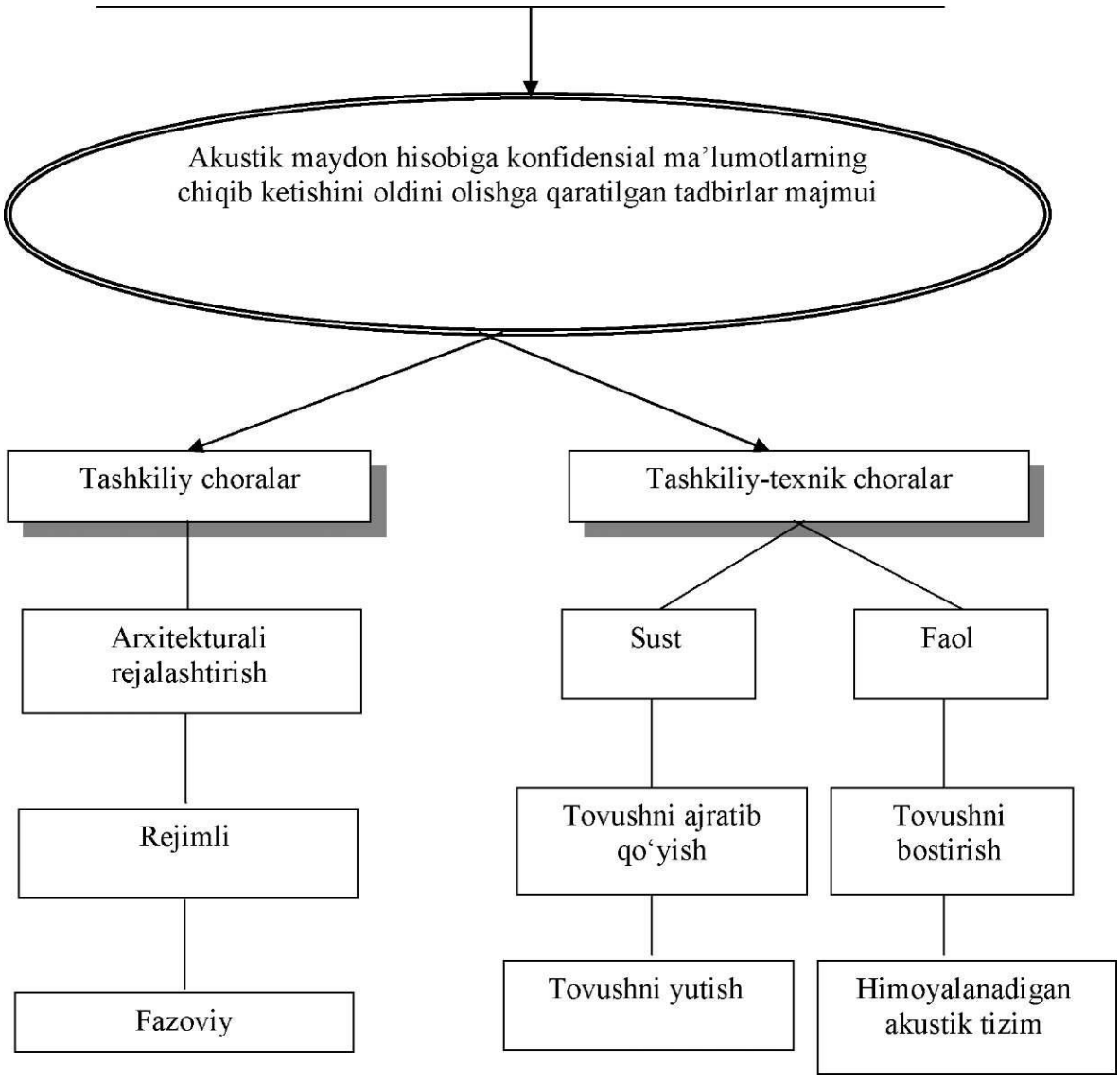
Himoyaning bu turidagi asosiy tadbirlarga tashkiliy va tashkiliy-texnik choralar kiradi.

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.

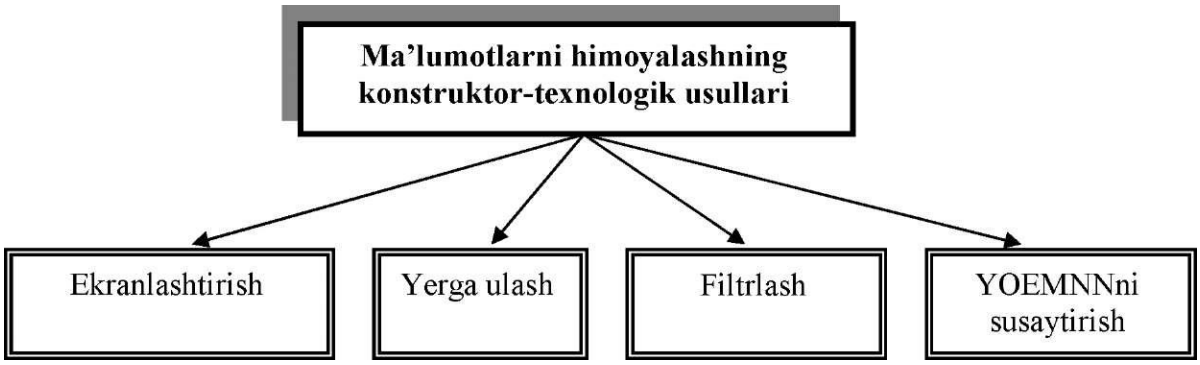
Tovushni o'tkazmaydigan qilish bilan himoyalashning samaradorligini aniqlash uchun shovqin o'lchagichlar ishlatiladi. *Shovqin o'lchagich* - tovush bosimi tebranishlarini tovush bosimi darajasiga mos ko'rsatkichlarga aylantiruvchi o'lchov asbobidir. Odam tovushini akustik himoya qilish sohasida analogli shovqin o'lchagichlardan foydalaniladi[10].

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.

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).



1.8-rasm. Akustik kanal orqali ma'lumotlarni chiqib ketishini oldini olish



1.9-rasm. Ma'lumotlarni himoyalashning konstruktor-texnologik usullari

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 konfidensial ma'lumotlarni ruxsatsiz olishdir.

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

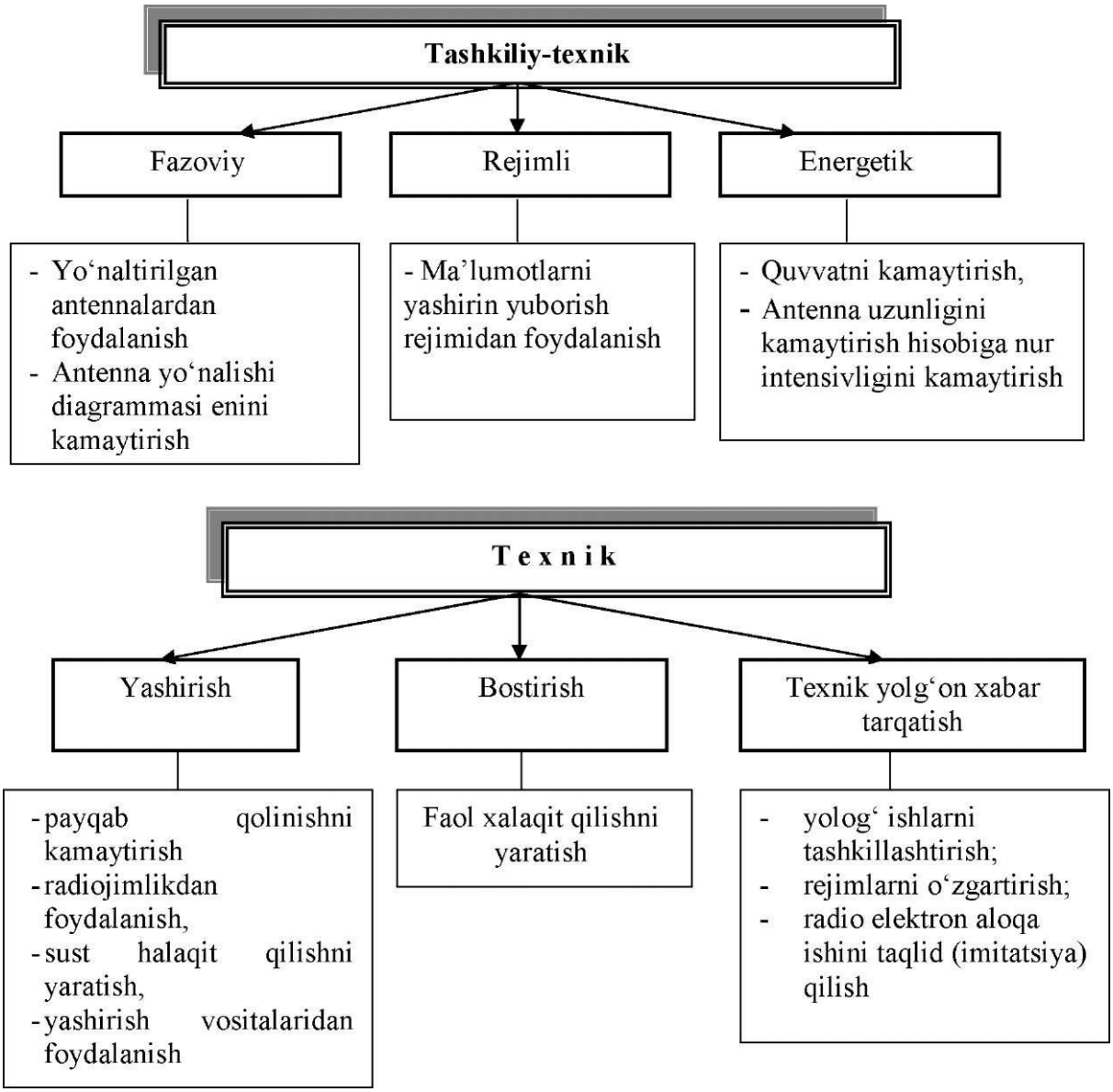
- kriminal qiziqishli obyekt bilan bevosita bog'lanmasdan amalga oshiriladi;
- turli diapazondagi radioto'lqinlarning tarqalish chegarasi bilan aniqlanadigan katta masofa va fazoda o'rinli;
- yil va kunning ixtiyoriy vaqtida va turli ob-havoda uzluksiz ta'minlanadi;
- ma'lumot aynan manbadan chiqqani 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).

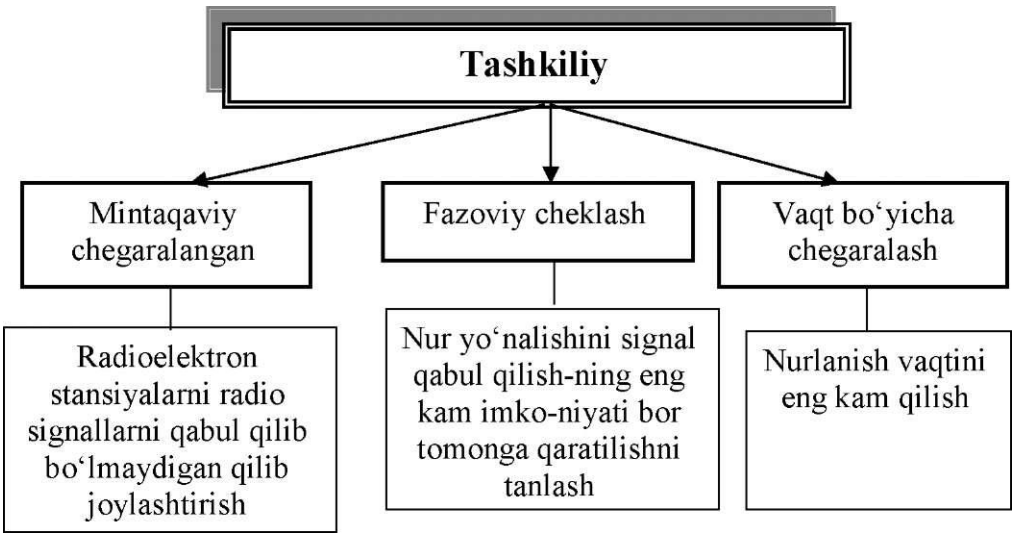
Tutib olishdan himoyalash usullari: tashkiliy, tashkiliy-texnik, texnik.



1.10-rasm. Axborotlarni himoyalashning tashkiliy-texnik usullari

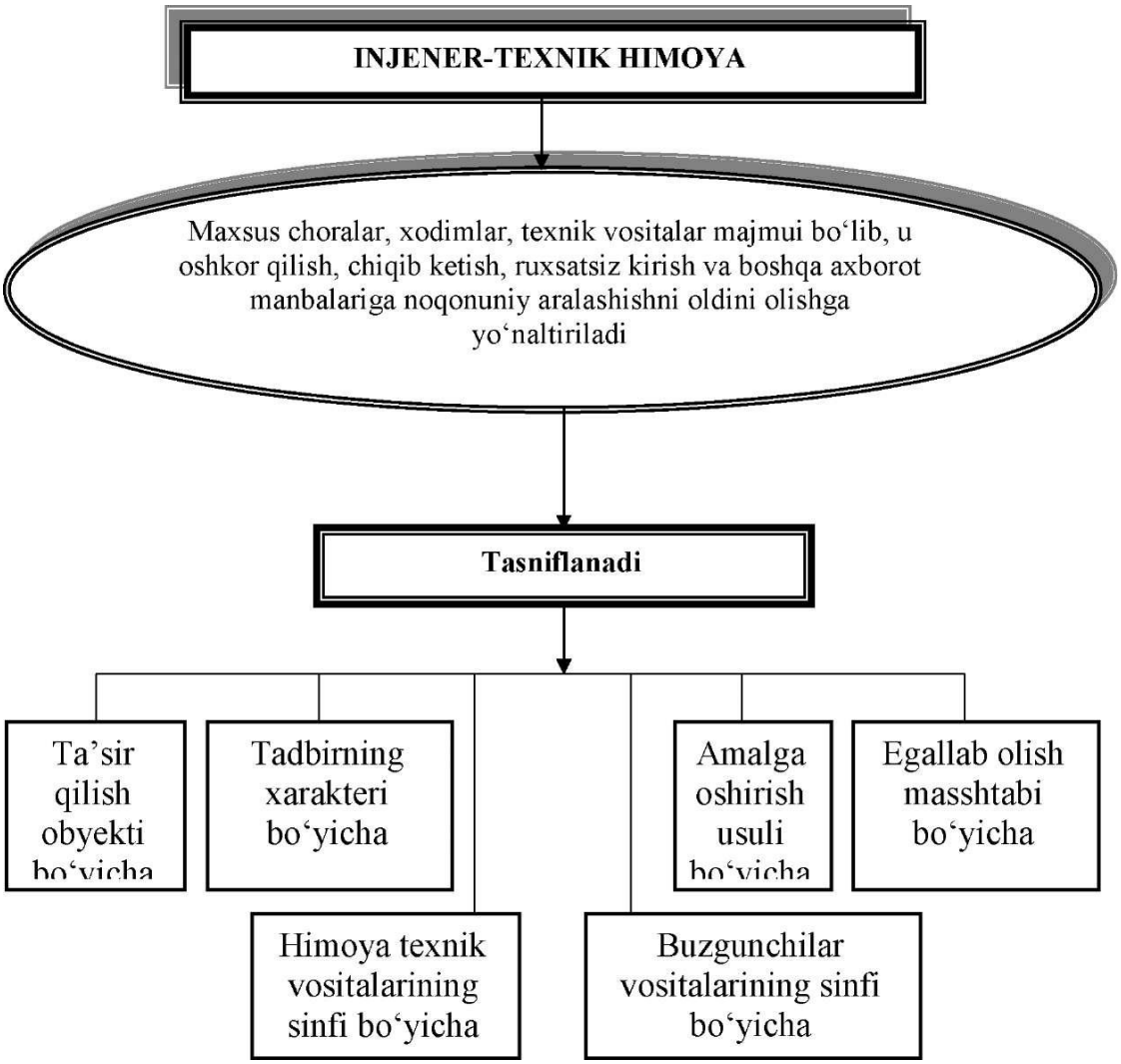
Injener-texnik himoyaning tasnifi - bu konfedensial ma'lumotlarni himoyalashga qaratilgan maxsus idoralar, texnik vositalar va tadbirlar majmuidir.

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.



1.11-rasm. Axborotlarni himoyalashning tashkiliy usullari

Quyidagi rasmda injener-texnik himoyaning taxminiy sinflanish tuzilishi keltirilgan:



1.12-rasm. Axborotlarni himoyalashning injiner texnik usullari

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 klassifi-katsiyalash.

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: l.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

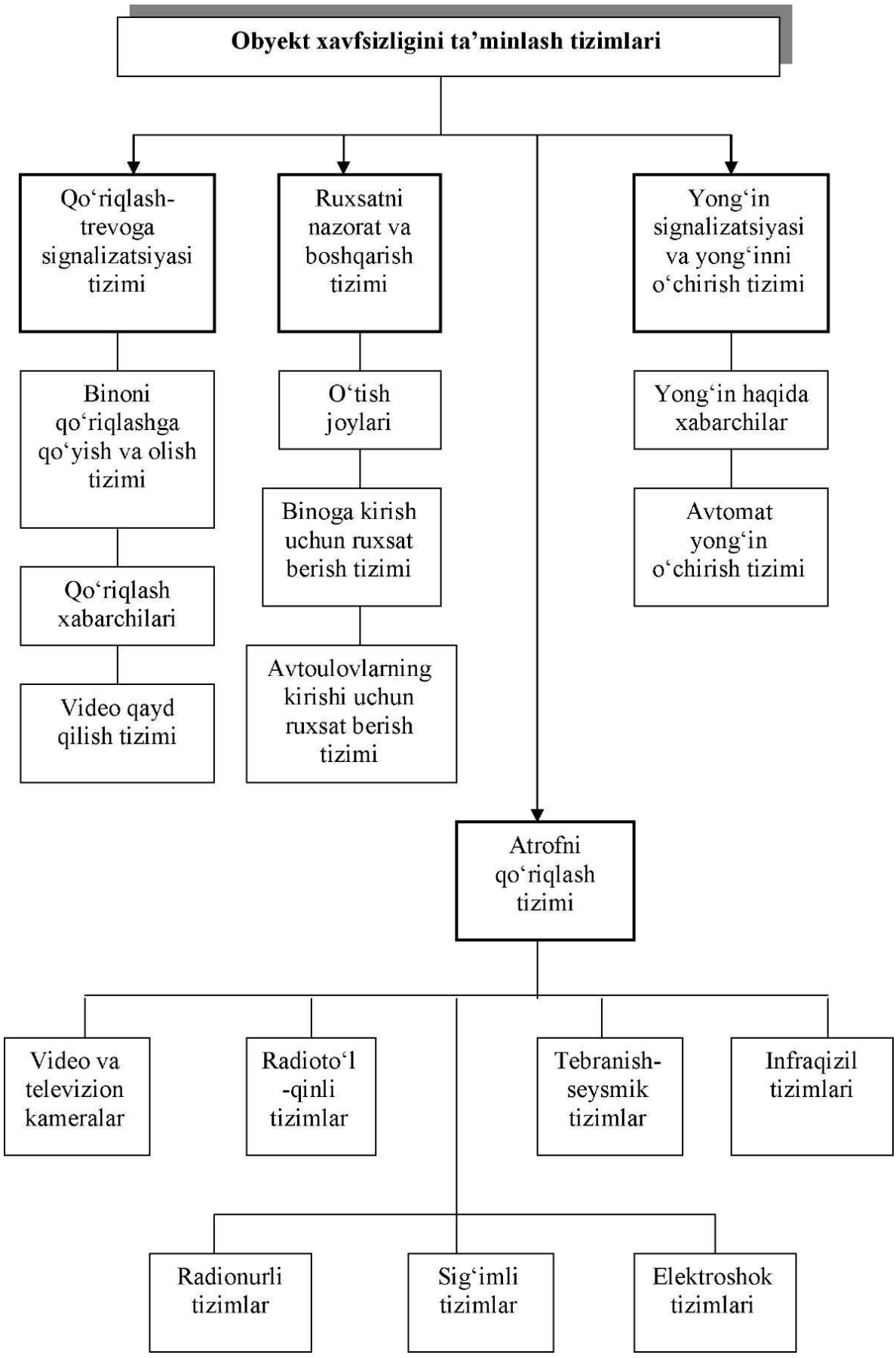
bayonnoma yuritadi hamda uni ko'rish va chop etish imkonini beradi; standart va nostandart holatlarda operator faoliyatini qayd etuvchi elektron jurnalni yuritadi.

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;
- 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.



1.13-rasm. Ob’ekt xavfsizligini ta’minlash tizimlari[11]

1.4. Axborotni muhofaza qilishning apparat-dasturiy vositalari

Bu vositalar **-** 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.

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;

- 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 foyda- lanishdan 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.

2. Asosiy qism. Server ximoyasini ta’minlashda apparat vositalarining samaradorligini oshirish

2.1. Korparativ serverga qo’yiladigan asosiy talablar

Server – bu tarmoqning barcha ishchi stansiyalar so‘rovlarini qayta ishlash uchun ajratilgan ko‘p foydalanuvchili kompyuter bo‘lib, u bu ishchi stansiyalarga umumiy tizim resurslariga(hisoblash quvvatlariga, ma’lumotlar omboriga, dasturlar kutubhonalariga, printerlarga, fakslarga va boshqa) murojat qilish imkonini beradi va bu resurslarni taqsimlaydi.

Server – o‘zining tarmoqli operatsion tizimiga ega bo‘lib, tarmoq barcha bug‘unlarining ishi uning boshqaruvi ostida o‘tadi.

Serverga qo‘yiladigan eng muhim talablar ichida yuqori ish unumdorligini va ishonchliligini ajratib o‘tish lozim.

Ishchi stansiyalarga tarmoq resurslarini taqdim etishdan tashqari, serverning o‘zi ham muroatlarning so‘rovi bo‘yicha ma’lumotlarni mazmunli qayta ishlashni bajarishi mumkin – bunday serverni qo‘shimcha ilovali server deb atashadi.

Server tarmoqga ko‘pincha ihtisoslashtiriladi.

Ihtisoslashgan serverlar ma’lumotlar omborirni va ma’lumotlar arhivini yaratish va boshqarish, ko‘p adresli faksimal aloqa va electron pochtani qo‘llash, ko‘p foydalanuvchili terminallarni (printerlarni, plotterlarni va boshqa) boshqarih bo‘yicha tarmoq ishidagi eng “zaif” joylarni bartaraf etish uchun ishlatiladi.

Ihtisoslashgan serverlarga misollar :

File server (Fayl server) – qiymatlar ombori bilan shlash uchun ko‘pincha sigimi terabaytgacha bo‘lgan RAID diskli massivlardagi hajmli diskli eslab qolish qurilmalariga egadir.

Novell Netware operatsion tizimida tarmoqning asosiy buguni fayl server hisoblanadi. Unda tarmoq operatsion tizimi, m’lumotlar ombori va foydalanuvchilarning amaliy dasturi joylashtiriladi. Shuning uchun fayl server tarmoqdagi eng kuchli kompyuter bo‘lishi kerak, chunki butun tarmoqning unumdorligi va funksional imkoniyatlari unga bog‘liqdir.

Fayl server sifatida tezkor xotirasining sig‘imi 16-32 MB dan kam bo‘lmagan kompyuter ishlatilishi kerak. Fayl server qattiq diskining (qullab quvvatlaydigan tarmoq resursi asosiy taqsimlovchining) – sigi’mi 1200-3000 MB ni tashkil etishi lozim.

Fayl server ishining ishonchliligi tarmoq ishining ishinchliligini aniq belgilagani uchun qattiq diskdagi ma’lumotlarni adashishlarda va yo‘qotishlardan himoya qilish uchun maxsus choralarni ko‘rish kerak.

Arhivli server (zahirali nushalash serveri- storage express system) - ma’lumotlarni zahirali nushalash uchun yirik ko‘p serverli tarmoqlarda, sig‘imi 5 gegabaytgacha bo‘lgan almashtiriladigan kartridjli magnit lentadagi yiguvchilar (stremmiterlar) ihlatiladi; Odatda, trmoq ma’muriyati tomonidan senariy bo‘yicha (tabiiyki, arhiv katalogini tuzish bilan) serverlardan va ishchi stansiyalardan olingan ma’lumotlarni siqishtirish kundalik avtomatik arhivlashtirish ishlarini bajaradi.

Fax server (Net Statisfaxion server) – samarali ko‘p adresli faksimal aloqani tashkil etish uchun, bir nechta fax-modemli platali, uzatish jarayonida ruhsat etilmagan murojat qilishdan ma’lumotlarni maxsus himoyali electron fakslarni saqlash tizimli ajratilgan ishchi stansiyasidir.

Pochtali – server (Mail server) – huddi faks server kabi, lekin electron pochtani tashkil etish uchun electron pochta qutilari ishlatiladi.

Bosma serveri (Print server) – tizimli printerlarni samarali ishlatish uchun.

Appratli vositalar bilan bir qatorda tarmoq o‘zining tarkibiga murakkab dasturli va ma’lumotli ta’minotni ham olishi kerak.

Ishchi stansiyalar (Work station) – bu tarmoqqa ulangan kompyuter bo‘lib u orqali foydalanuvchi tarmoq resurslariga murojat qila oladi. Tarmoqning ishchi stansiyasi ham tarmoqli, ham lokal rejimlarda ishlay oladi. U hususiy operatsion tizim bilan johozlangan va foydalanuvchini o‘zning amalaiy masalalarini echish uchun barcha kerakli narsalar bilan ta’minlaydi. Ishchi stansiyalar ba’zida grafik, muhandislik, noshirlik va boshqa ishlarni bajarish uchun ihtisoslashadi.

Serverning asosiy vazifalari:

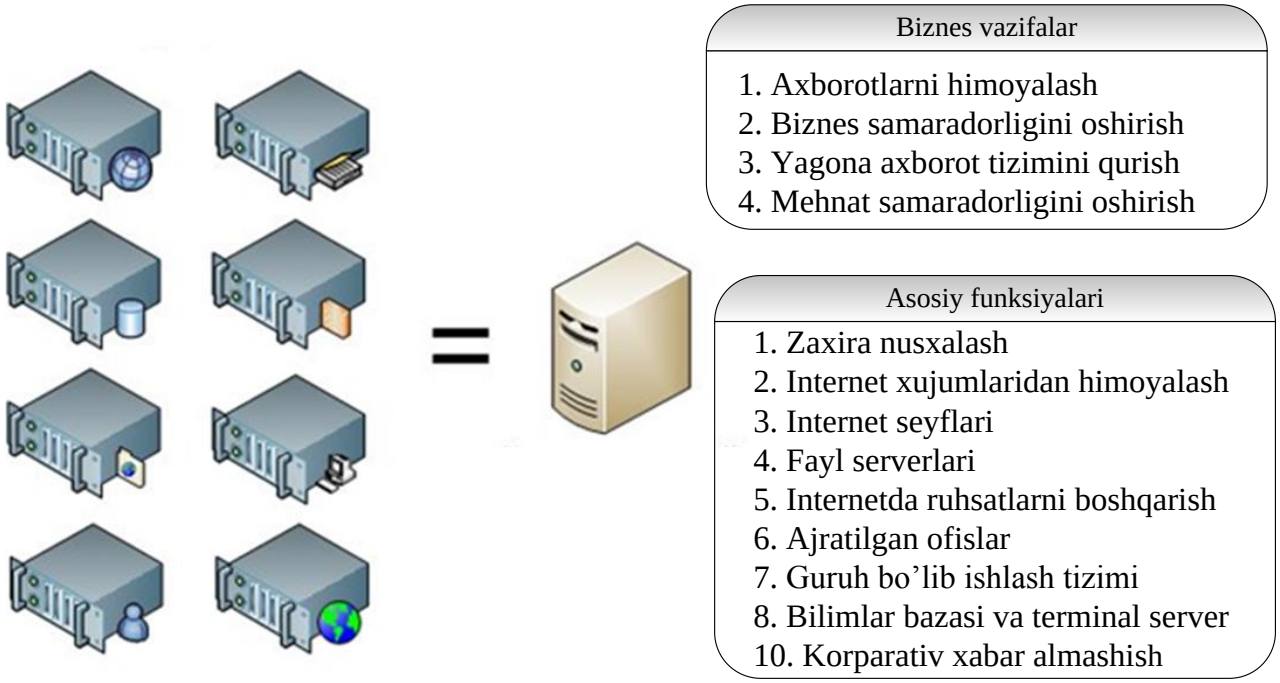
— Axborotlarni himoyalash: tashkilotning asosiy fayllari va ma’lumotlari;

— Tshkilotning ichki tarmog’ini himoyalash: Internetdan bo’ladigan asosiy xujumlar;

— Biznes samaradorligini oshirish: axborot texnologiyalari yordamida;

— Yagona axborot tizimini qurish;

— Ishlab chiqarish samaradorligini oshirish: tashkilotning xodimlari ustidan to’liq nazorat[12].



2.1-rasm. Serverlar va ularning asosiy vazifalari

Serverning xavfsizligini ta’minlashning quyidagi asosiy talablari mavjud:

— Tarmoqlararo ekran o’rnatilishi shart;

— Agar tashqi tarmoqdan murojat bo`lsa (serverga murojat to`g`ridan to`g`ri emas web ilova orqali bo’lishi kerak. Bu degani aloxida 1 ta serverga autentifikatsiyadan o’tish tizimi qo`yiladi hamma foydalanuvchiga Login va Parol yoki qo`shimcha tarzda ERI berilishi mumkin. Autentifikasiyadan o`tgandan keyin berilgan huquqiga qarab serverga murojat qiladi);

— parol mukammalligi (An@1>Q9'Hf56) va vaqida har oyda bir marta to`liq yangilanishi lozim;

— Korxona boshqa ofis bn VPN kanal orqali bog`lanishi (bunda ham korxona o’rtada boshqa serverda kerakli malumotlar saqlanadi va korxona serveriga o’sha server orqali o’tadi);

— AD(active directoriy) yoki DLP tizimi bo’lishi lozim;

— Korporativ pochtadan foydalanish (Kerio mail server yoki ICWarp mail server) lozim;

— Tashqi pochta aloqalari uchun xam (Kerio mail server yoki ICWarp mail server) bo’lishi lozim. Bunda hodimlar qayerga qanday ma’lumot yuborayotganini nazotar qilinadi;

— Barcha korparativ tarmoq pochta xizmatlaridan boshqalari yopilishi lozim;

— Internet nazorati o`rnatilishi kerak (Proksi orqali);

— 1-bobda sanalgan fizik xavfsizlik talablari bajarilgan bo’lishi lozim;

— Korxonaga xar bir xodimning kirib chiqishi kartochka(smart kartalar, e-tokenlar) orqali amalga oshirilishi kerak.

2.2. 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[13].

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.

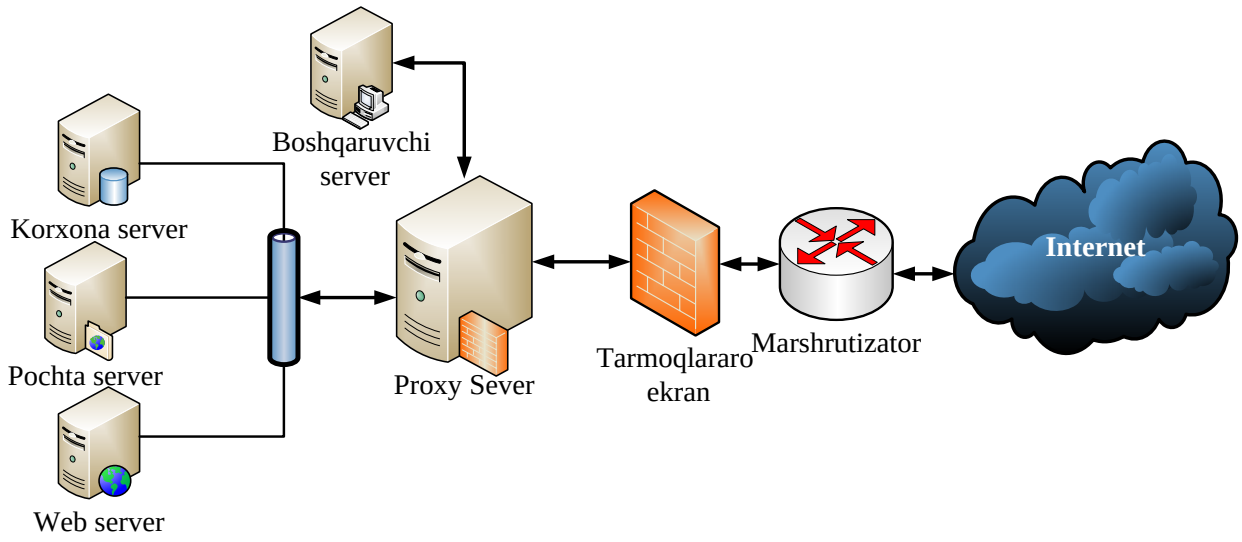
Tarmoqlararo ekran filtrlashni kanallar, tarmoqlar, transport va amaliy sathlarda amalga oshiradi. Ekran qancha ko'p sathni o'z ichiga olsa, shuncha takomillashgan hisoblanadi.

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[14].



2.2-rasm. Tarmoqlararo ekranlarning ishlash sxemasi

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.

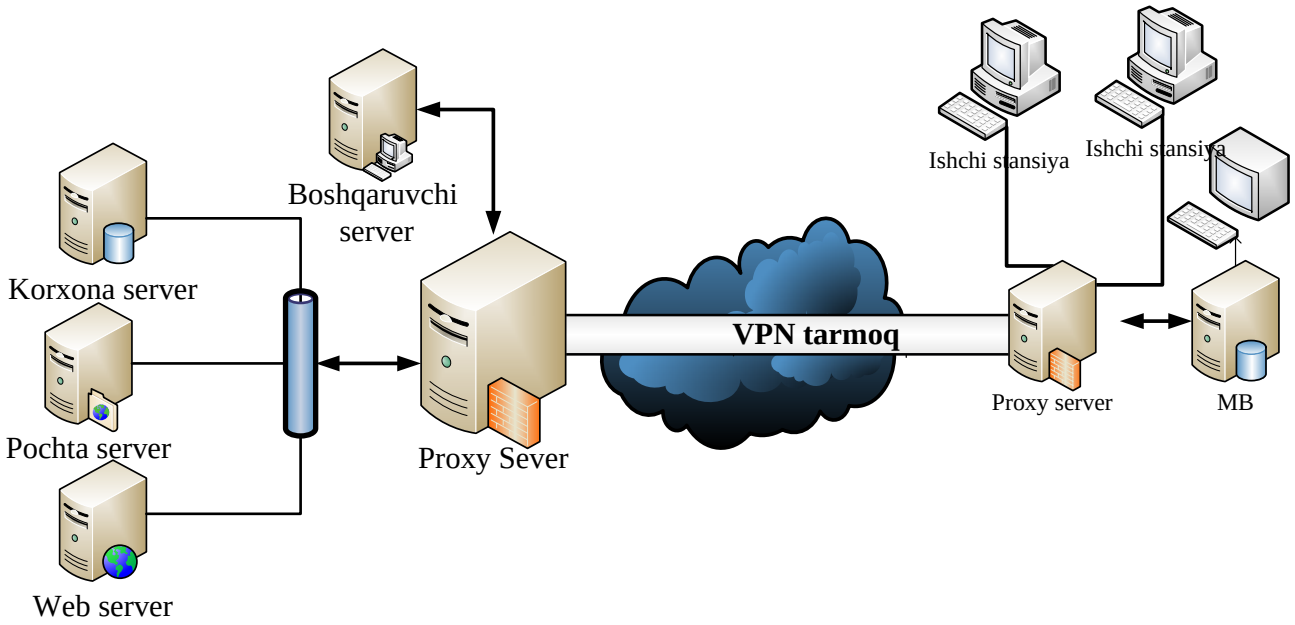
6. Ekranni boshqaruv tizimi olisdagi filiallar uchun ham yagona xavfsizlik siyosatini yuritishni markazlashgan holda ta'minlash imkoniyatiga ega bo'lmog'i lozim.

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.

VPN tarmoqlaridan foydalanish

Internetning hamma yerda tarqalishidan manfaat ko’rish maqsadida tarmoq xujumlariga samarali qarshilik ko’rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq VPN yaratish ustida ishlar olib borildi. Natijada 1990 yilning boshida virtual xususiy tarmoq VPN konsepsiyasi yaratildi. "Virtual" iborasi VPN atamasiga ikkita uzel o’rtasidagi ulanishni vaqtincha deb ko’rilishini ta’kidlash maqsadida kiritilgan.

Haqiqattan, bu ulanish doimiy, qat’iy bo’lmay, faqat ochiq tarmoq bo’yicha trafik o’tganida mavjud bo’ladi[15].



2.3. Ishchi stansiya va ofis o’rtasida VPN kanal

Axborotni VPN tunneli bo’yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

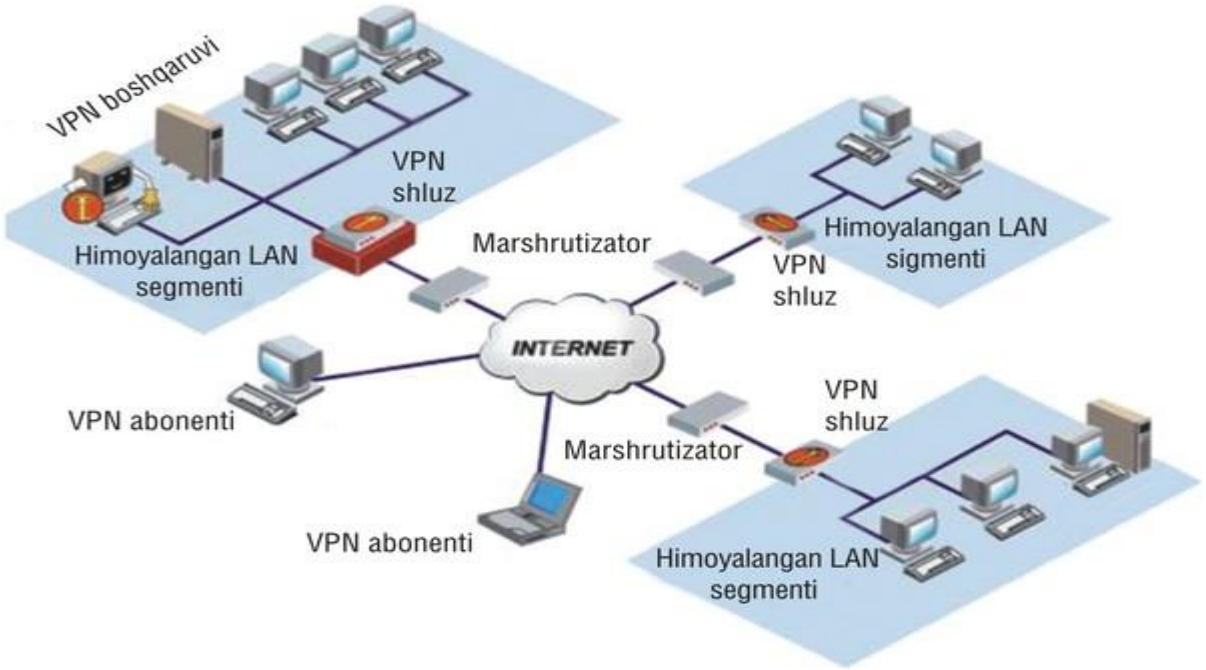
— o’zaro aloqadagi taraflarni autentifikasiyalash;

— uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash);

— yetkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish.

VPN qurilmalari tomonidan shakllantirnluvchi VPN tunneli himoyalangan ajratilgan liniya xususiyatlariga ega bo’lib, bu himoyalangan ajratilgan liniyalar umumfoydalanuvchi tarmoq, masalan Internet doirasida, saflanadi. VPN qurilmalari virtual xususiy tarmoqlarda VPNmijoz, VPNserver yoki VPN xavfsizligi shlyuzi vazifasini o’tashi mumkin.

URI mijoz odatda shaxsiy komp’yuter asosidagi dasturiy yoki dasturiy apparat kompleksi bo’lib, uning tarmoq dasturiy ta’minoti u boshqa VPN mijoz, VPN server yoki VPN xavfsizligi shlyuzlari bilan almashinadigan trafikni shifrlash va autentifikaqiyalash uchun modifi- kasiyalanadi. Odatda VPNmijozning amalga oshirilishi standart operasion ti- zim Windows N/2000 yoki Unixni to’ldiruvchi dasturiy yechimdan iborat bo’ladi.



2.4. Xar bir tarmoq o’zaro VPN orqali aloqani amalga oshiradi

VPN server vazifasini o’tovchi, komp’yuterga o’rnatiluvchi dasturiy yoki dasturiy apparat kompleksidan iborat. VPNserver tashqi tarmoqlarning ruxsatsiz foydalanishidan serverlarni himoyalashni hamda alohida komp’yuterlar va mos VPN mahsulotlari orqali himoyalangan lokal tarmoq segmentlaridagi komp’yuterlar bilan himoyalangan ulanishlarni tashkil etishni ta’minlaydi. VPNserver VPNmijozning server platformalari uchun funkqional analog hisoblanadi. U avvalo VPN mijozlar bilan ko’pgina ulanishlarni madadlovchi kengaytirilgan resurslari bilan ajralib turadi. VPN server mobil foydalanuvchilar bilan ulanishlarni ham madadlashi mumkin[16].

VPN xavfsizlik shlyuzi. (Security gateWay) ikkita tarmoqqa ulanuvchi tarmoq qurilmasi bo’lib, o’zidan keyin joylashgan ko’p sonli xostlar uchun shifrlash va autentifikaqiyalash vazifalarini bajaradi. VPN xavfsizli¬gi shlyuzi shunday joylashtiriladiki, ichki korporativ tarmoqqa atalgan barcha trafik u orqali o’tadi. VPN xavfsizligi shlyuzining adresi kiruvchi tunnellanuvchi paketning tashqi adresi sifatida ko’rsatiladi, paketning ichki adresi esa shlyuz orqasidagi muayyan xost adresi hisoblanadi.

Marshrutizatorlar asosidagi VPN. VPN qurishning ushbu usuliga binoan himoyalangan kanallarni yaratishda marshrutizatorlardan foydalaniladi. Lokal

tarmoqdan chiquvchi barcha axborot marshrutizator orqali o’tganligi sababli, unga shifrlash vazifasini yuklash tabiiy. Marshrutizator asosidagi VPN asbob-uskunalariga misol tariqasida Cisco-Systems kompaniyasining qurilmalarini ko’rsatish mumkin.

Tarmoqlararo ekranlar asosidagi VPN. Aksariyat ishlab chiqaruvchilarning tarmoqlararo ekrani tunnellash va ma’lumotlarni shifrlash vazifalarini madadlaydi. Tarmoqlararo ekranlar asosidagi yechimga misol tariqasida Check Point Software Technologies kompaniyasining Fire Wall-1 mahsulotini ko’rsatish mumkin. Shaxsiy kompyuter asosidagi tarmoqlararo ekranlar faqat uzatiluvchi axborot hajmi nisbatan kichik bo’lgan tarmoqlarda qo’llaniladi. Ushbu usulning kamchiligi bitta ishchi o’rniga hisoblanganda yechim narhining yuqoriligi va unumdorlikning tarmoqlararo ekran ishlaydigan apparat ta’minotiga boqliqligi.

Dasturiy ta’minot asosidagi VPN. Dasturiy usul bo’yicha amalga oshirilgan VPN mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan qurilmadan qolishsada, VPN-tarmoqlarni amalga oshirilishida yetarli quvvatga ega. Ta’kidlash lozimki, masofadan foydalanishda zaruriy o’tkazish polosasiga talablar katta emas. Shu sababli, dasturiy mahsulotlarning o’zi masofadan foydalanish uchun yetarli unumdorlikni ta’minlaydi. Dasturiy mahsulotlarning shubhasiz afzalligi—qo’llanilishining moslanuvchanligi va qulayligi, hamda narxining nisbatan yuqori emasligi.

Ixtisoslashtirilgan apparat vositalari asosidagi VPN. Ixtisoslashtirilgan apparat vositalari asosidagi VPNlarning eng muhim afzalligi unumdorligining yuqoriligidir. Ixtisoslashtirilgan VPN tizimlarda shifrlashning mikrosxemalarda amalga oshirilishi tezkorlikning ta’minlanishiga sabab bo’ladi. Ixtisoslashtirilgan VPN-qurilmalar xavfsizlikning yuqori darajasini ta’minlaydi, ammo ularning narhi anchagina yuqori.

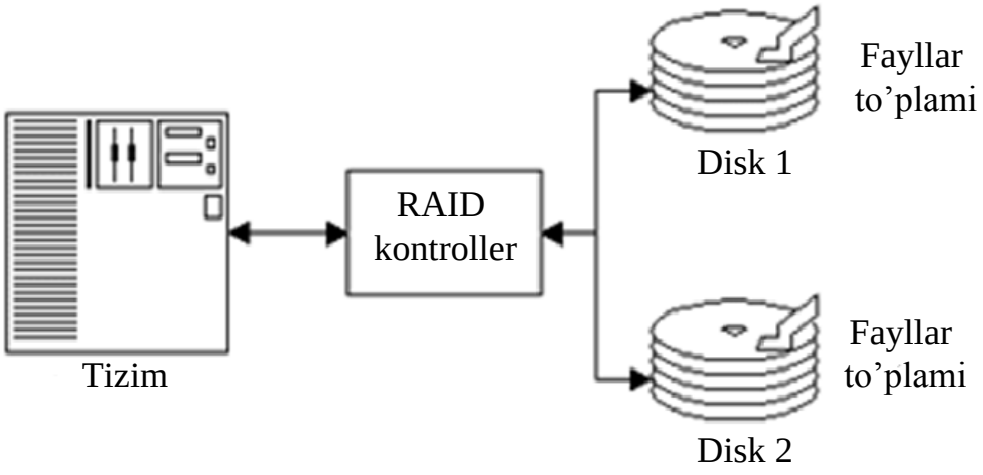
2.3. Ma’lumotlarning zaxira nusxalarini yaratuvchi RAID kontrollerlari

Ma’lumotlarni saqlashda hozirgi kunda RAID sistemalari juda keng qo’llaniladi. RAID inglizcha Redundant array of independent/inexpensive disks

(«izbытochnыy massiv nezavisimых diskov») so’zlarining bosh harflaridan kelib chiqqan. RAID nazariyasi beshta asosiy prinsipdan – beshta sirli so’zdan tashkil topgan. Bu Massiv (Array), Akslantirish (Zerkalirovaniye Mirroring), Dupleks (Duplexing), Navbatma– navbat(Cheredovaniye Striping) va Juftlik (Chetnost Parity).

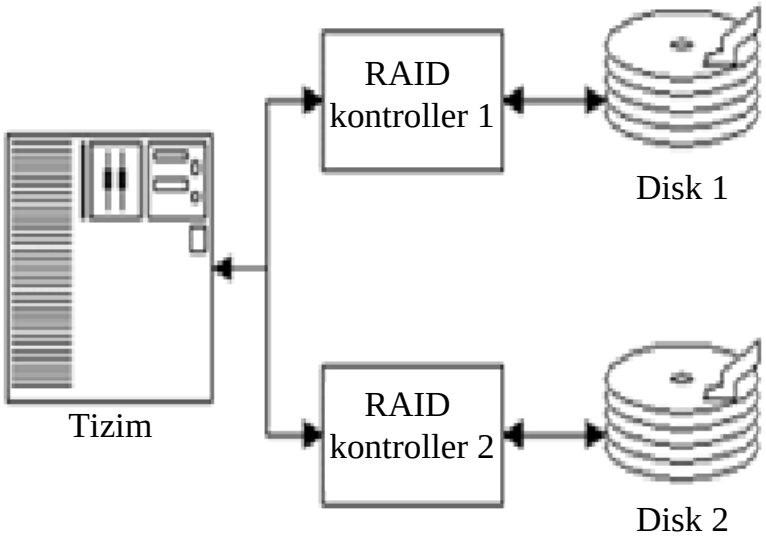
Massiv deb, markazlashgan holda sozlanadigan, shakllantiriladigan, va boshqariladigan bir nechta jamlagichlarga aytiladi. Mantiqiy massiv – bu yuqori darajali ko’rsatkich bo’lib, tizimning fizik tavsiflari hisobga olinmaydi. Mantiqiy disklar soni va xajmi jihatidan fizik disklar bilan mos tushmaydi. Operasion tizim uchun massiv bir butun katta disk deb qaraladi.

Akslantirish – tizimning ishonchliligini oshirish imkonini beruvchi texnologiya. Akslantirish texnologiyada ishlovchi RAID massiv axborotni bir vaqtni o’zida ikkita diskka yozadi, ya’ni ma’lumotlar «ko’zgu(aksi)»si yaratiladi. Bitta disk ishdan chiqsa, ikkinchi diskda axborot saqlanib qoladi.



2.5-rasm. Akslantirish

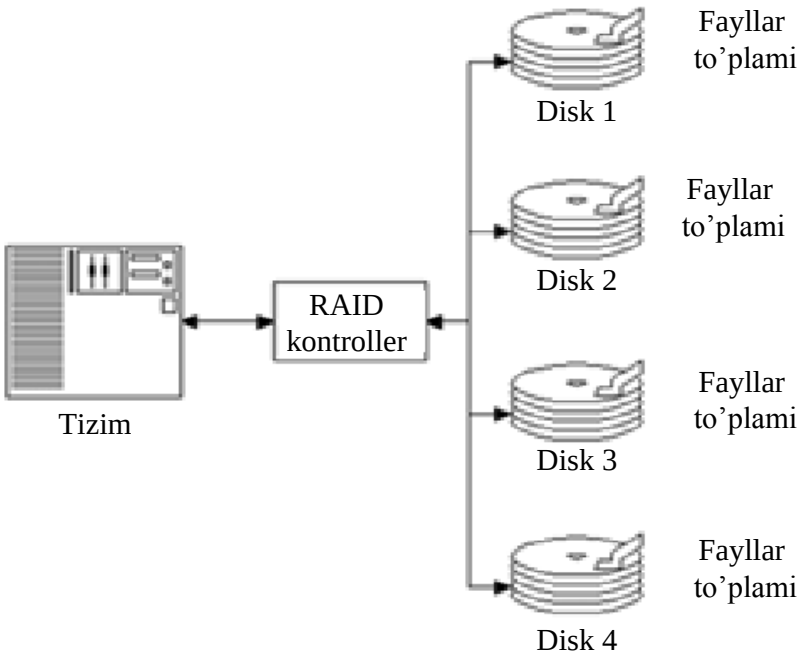
Bunday himoya juda qimmatga tushadi, chunki bitta vinchester tizimning unumdorligiga ta’siri yo’q[15].



2.6-rasm. Dupleks

Dupleks – akslantirish g’oyasining rivojlanganligidir. Bu holatda ishonchlilik darajasi juda yuqori bo’lib, qattiq diskning ikki barobar ko’p bo’lishini talab qiladi. Bunda xarajat ham ikki barobar bo’lib, tizimga ikkita mustaqil ravishda ishlaydigan RAID kontroller o’rnatiladi.

Navbatma– navbat – tizimning tezligining oshirishning a’lo darajadagi imkoniyatidir. Ko’rinib turibdiki, agar o’qish va yozishni bir nechta diskda parallel olib borilsa, tezlikda yutib chiqish mumkin.



2.7-rasm. Navbatma– navbat

Bu qanday amalga oshiriladi? Yozilayotgan faylni ma’lum o’lchamdagi qismlarga bo’lib, bir vaqtning o’zida hamma jamlagichlarga yuboriladi. Shunday bo’laklar ko’rinishida fayllar saqlanadi. O’qilganda ham, «bo’lak»lab o’qiladi. «Bo’lak» o’lchami minimal 1 bayt bo’ladi, odatda yirik bo’laklar 512 bayt (sektor) qo’llaniladi.

Juftlik o’zida akslantirishning (yuqori ishonchliligi) va navbatma–navbatning (yuqori tezlikda ishlashi) fazilatlarini birlashtirgan alternativ qarordir.

Agar axborotning I bloki bo’lsa va u asosida yana bitta qo’shimcha ekstrablok hisoblansa, hosil bo’lgan (I+1) blokdan bitta disk ishdan chiqsa ham, axborotni qayta tiklash imkoniyati mavjuddir.

Bloklarning disk bo’ylab tarqatilishi navbatma– navbat texnologiyasi kabi amalga oshiriladi. Ekstrablok alohida jamlagichga ham yozilishi mumkin, disklarga bo’lib tashlanishi ham mumkin.

Ekstrablokda nima saqlanadi? Odatda, ekstrablokning xar bir biti hamma I bloklar bitining yig’indisidan iborat, aniqrog’i XOR mantiqiy amalining bajarilish natijasidan iborat. XOR – antiqiy operator bo’lib, uni takroran ishlatilishi boshlang’ich natijani beradi, ya’ni (A XOR B) XOR B = A. Bu qoida operandlarning xar qanday miqdorida qo’llaniladi.

Juftlikni qo’llash juda afzaldir, chunki navbatma–navbatlik hisobiga ishlash tezligi ortadi, akslantirish hisobiga ishonchliligi saqlanib qoladi, ammo massivning «ishlatilmaydigan» xajmi kamayadi va sig’imi bitta diskni tashkil qiladi, ya’ni massivda beshta disk bo’lsa, 20% sig’imni yo’qotadi.

Juftlikni o’ziga yarasha kamchiligi bor. Ekstrablokni shakllantirish uchun hisob– kitob talab qilinadi. Buni juda tez bajarish kerak. Agar bu ishni markaziy prosessorga yuklansa, tizim juda sekin ishlaydi. Shuning uchun «hisoblashni o’z zimmasiga oladigan» narxi qimmat bo’lgan RAID-kontrollerlardan foydalanish kerak bo’ladi.

Shaxsiy kompyuterlar uchun maxsus qurilma orqali RAID sistemasini tashkil qilsa bo’ladi. Masalan, **PCI** **IDE** RAID qurilmasi. RAID sistemalari ikki

turga bo'linadi: oddiy (single) va tarkibiy (multiple) RAID massiv. Tarkibiy (multiple) RAID massiv tarkibi ikkita oddiy massivdan iborat.

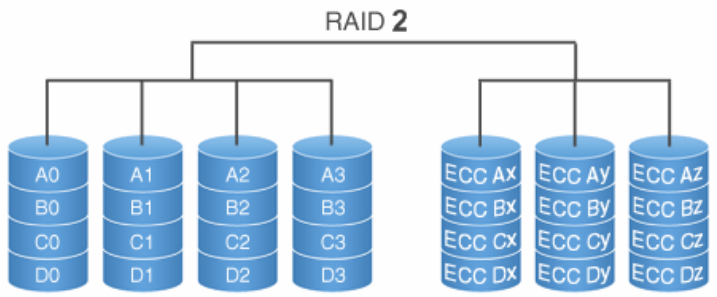
Jumladan RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5 va ularning kombinasiyasidan yana RAID 0+1, RAID 1+0 kabilari xam mavjud.

RAID 0 ("*Striping— «cheredovaniye»*") **–** ikki yoki undan ortiq bo'lgan disklardan iborat bo'lib, unga yozilayotgan ma'lumotlar (A_i massiv ko'rinishida) ketma – ketlik bilan xar diskka yoziladi.

2.8-rasm. RAID 0 va RAID 1 ning ko'rinishi

RAID 1 (*Mirroring — «zerkalo»*) – ikkita vinchesterdan iborat bo'lib, ikkita vinchesterga ham ma'lumot massiv ko'rinishida yoziladi. Lekin bu holatda ma'lumotlar faqat birinchi vinchesterdan o'qilib, ikkalasiga ham yoziladi. Buning afzalligi ma'lumotlar bir xil nusxalanib, bitta vinchester ishdan chiqqan paytda xam ikkinchi vinchestorda saqlanib qolishidir.

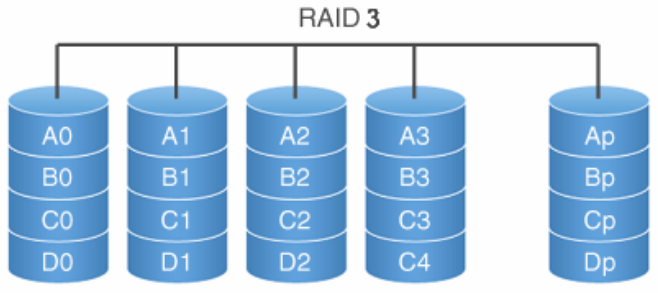
RAID 2 – ma'lumotlar va xatolik kodlar saqlanadigan ikkita gurux jamlamasidan iboratdir. Bunda xam ma'lumotlarni yozish RAID 0 kabi amalga oshiriladi.



2.9-rasm. RAID 2 ning ko'rinishi

RAID 3 – bir nechta disklar jamlamasidan iborat bo'lib, unga yozilayotgan ma'lumot o'lchami 1 baytdan bo'lgan qismlarga ajratiladi. Ajratilgan ma'lumotlar n-1 ta (n – umumiy disklar soni) diskka yoziladi. Qolgan bittasiga esa ajratilgan

qismlar haqida ma’lumot yoziladi. Buning afzalligi, bitta disk zararlanganda umumiy ma’lumotning 1 bayti zararlanadi. Bu esa ma’lumotning birdaniga yo’qolib ketishining oldini oladi.



2.10-rasm. RAID 3 ning ko’rinishi

RAID 4 – bu xuddi RAID 3 kabi bo’lib, bunda ma’lumotlar 1 baytdan emas, n ta diskka teng taqsimlanadi.

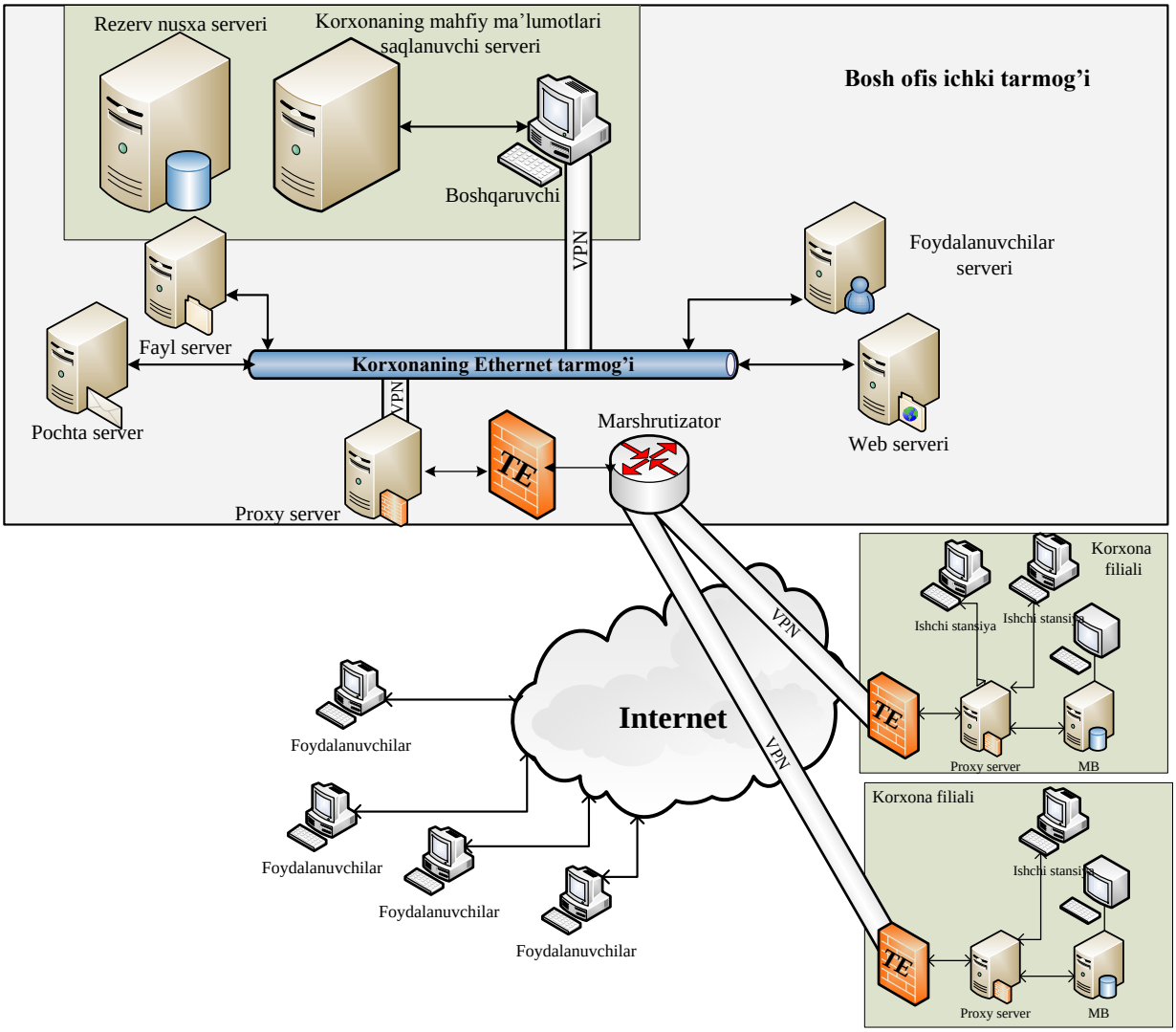
RAID 5 – bunda xam disklar massiv ko’rinishida bo’ladi. Ma’lumotlarni o’qish va yozishda yordamchi ma’lumotlardan foydalaniladi, ya’ni yordamchi ma’lumotlar xar bir faylning qismini (massiv ko’rinishida) qayerda joylashganligi xaqidagi ma’lumotdan foydalanadi. Afzalligi, RAID 5 tejamkorligi va yuqori darajali bo’lganligi uchun qolganlaridan oldingi o’rinda turadi.

2.4. Server xavfsizligini ta’minlashning samaradorligini oshirish sxemasi

Server xavfsizligini ta’minlashda tarmoq strukturasini to’g’ri tanlash juda muhimdir.

Korxonaning bosh ofisida fayl serveri, pochta serveri, web server, foydalanuvchilar haqidagi ma’lumotlar serveri va asosiy serverdan iborat. Tarmoqdan keladigan va tarmoq ichidagi so’rovlar VPN orqali boshqaruvchiga boradi va u bu so’rovlarni qayta ishlaydi. Barcha so’rovlar VPN kanali orqali boshqaruvchidagi CISCO ASA tarmoqlararo ekran orqali tekshiriladi.

Internetdan keladigan barcha so’rovlar marshrutizator va tarmoqlararo ekran tekshiruvidan o’tib, proxy serverga boradi. Proxy serverning shrtlarini qanoatlantirgan so’rovgina VPN kanali orqali korxona ichki tarmog’iga boradi va yuqorida sanab o’tgan serverlarda qayta ishlanadi.



2.11-rasm. Server xavfsizligini ta'minlashning samaradorligini oshirish arxitekturasi

Xar bir korxona filiali tashkilot bilan VPN kanali yordamida bog'lanadi va ma'lumot almashinadi. Filiallarning o'zi xam internet tarmog'iga Tarmoqlararo ekran va proxy server yordamida bog'lanadi.

Masofaviy boshqa foydalanuvchilar uchun esa, marshrutizator, tarmoqlar aro ekran va proxy serverning xavfsizlik parametrlari yetarli hisoblanadi.

Asosiy serverning xavfsizligini ta'minlash maqsadida undagi ma'lumotlar web ilovalar yordamida namoish etilganligi sababli ularni o'zgartirish mumkin emas, faqat o'qish huquqi beriladi. Serverning RAID kontrollerlari bilan zahira nusxasi yaratiladi.

3. Hayot faoliyati xavfsizligi

3.1. Xavfsizlik muammolari

Mamlakatimizda mustaqillikning dastlabki yillaridanoq fuqarolarni jumladan ishchi va xizmatchilarni ijtimoiy holatini yaxshilash, ularning turmush darajasini yuksaltirishga, ishlash sharoitlarini texnika xavfsizligi va sanitariya talablari darajasidagi asosini yaratishga katta e'tibor qaratib kelinmoqda. Ta'lim jarayonida ham keng qamrovli islohotlar amalga oshirilmoqda. Qabul qilingan Kadrlar tayyorlash milliy dasturi, Ta'lim to'g'risidagi Qonunlar asosida ta'lim sohasida katta yutuqlarga erishildi. Ta'lim mazmuni tubdan ijobiy o'zgarishga yuz tutmoqda. Ta'lim tizimining barcha tizimida eng zamonaviy o'qitish vositalaridan foydalanilmoqda. Ishlab chiqarish ham eng qudratli, zamonaviy ishlab chiqarish vositalari bilan qurollantirilmoqda. Ijtimoiy hayot tarzi faollashmoqda. Mamlakatda qabul qilingan «Kadrlar tayyorlash milliy dasturi», «Ta'lim to'g'risida»gi Qonun ta'lim tizimi mazmunini tubdan o'zgartirib yubordi. Jumladan oliy ta'lim o'quv rejalariga zamon va hayot talablaridan kelib chiqib katta o'zgartirishlar kiritildi. Yosh mutaxassislarga har bir sohada chuqur va keng qamrovli ma'lumot berish, ularga berilgan bilim ishlab chiqarishda va jamiyatda o'z aksini va dolzarbligini yo'qotmaydigan bo'lishiga va ularning bilim darajalari dunyo ta'lim standartlari qo'ygan talabga javob berishiga asosiy ahamiyat qaratilmoqda.

Zamonaviy hayotdagi ishlab chiqarish samaradorligini yetuk kadrlarsiz tasavvur etish mumkin emas. Har sohada inson omili, uning qadr-qimmati birinchi o'ringa qo'yilib ish tashkil etilgan joyda yutuqlar barqaror bo'lishi shubhasiz.

Inson tug'ilishi bilan yashash, erkinlik va baxtga intilish huquqiga ega bo'ladi. Inson o'zining yashash, dam olish, sog'ligi haqida qayg'urish, qulay atrof-muhit, xavfsizlik va gigiyena talablariga javob beradigan mehnat sharoitida ishlashga bo'lgan xuquqlarini hayot faoliyati jarayonida amalga oshiradi. Uning bu huquqlari O'zbekiston Respublikasi Konstitusiyasida kafolatlangan.

Hayot faoliyati – bu insonning kunlik faoliyati, dam olishi va yashash tarzidir.

Inson hayoti jarayonida uni o’rab turgan borliq muhiti bilan uzluksiz aloqada bo’ladi va shu bilan birga har doim uni o’rab turgan muhitga bog’liq bo’lib kelgan va shunday qolaveradi. Inson shuning uchun ham o’zini o’rab turgan atrof-muhit hisobiga oziq-ovqat, havo, suv, dam olish uchun zarur moddiy narsalar va boshqalarga bo’lgan ehtiyojini qanoatlantiradi.

Atrof-muhit – insonni o’rab turgan muhit bo’lib, insonning hayot faoliyatiga, uning sog’ligi va nasliga to’g’ridan to’g’ri, birdan urinma yoki masofadan ta’sir etishga qobiliyatli omillarning (jismoniy, ximiyaviy, biologik, informasion, ijtimoiy) shartli yig’indisidir.

Inson va atrof-muhit uzluksiz o’zaro ta’sirda bo’lib, doimiy harakatdagi «Inson – atrof muhit» sistemasini tashkil etadi. Dunyoning evolyusion jarayonida bu sistemani tashkil etuvchilar uzluksiz o’zgarib bordi. Inson mukammallashdi, yer sharining aholisi va uning oqimi o’sdi, jamiyatning ijtimoiy asosi o’zgardi. Atrof-muhit o’zgardi: inson o’zlashtirgan yer yuzi va yer osti hududi kattalashdi; tabiiy tabiat muhiti insoniyat jamiyatining o’sib borayotgan ta’sirini boshdan kechirmoqda, inson tomonidan sun’iy yaratilgan maishiy, shahar va ishlab chiqarish muhiti paydo bo’ldi.

Tabiiy muhit o’zi yetarli bo’lib, inson ishtirokisiz mustaqil mavjud bo’la oladi va rivojlana oladi. Inson tomonidan yaratilgan boshqa barcha borliq muhiti mustaqil rivojlana olmaydi va ular paydo bo’lganidan so’ng eskirishga va yemirilishga mahkum.

Insoniyat o’zining dastlabki rivojlanish bosqichida tabiiy atrof-muhit bilan o’zaro uyg’un harakat qilgan. Atrof-muhit asosan biosfera, yer osti, gallaktika va cheksiz koinotdan tashkil topadi.

Biosfera - barcha turdagi organizmlar, jumladan inson yashashi mumkin bo’lgan atrof-muhit bo’lib, u murakkab tuzilishdagi yer sharining muhim qobig’idir. Biosfera bir necha milliard yillar davomida shakllangan. Zamonaviy olimlar biosferani moddalarni planeta bo’yicha harakatini ta’minlovchi yirik, global ekosistema sifatida qarashadi. Hozirgi erada hayot yer qatlamining yuqori (litosfera) qismida, yerning pastki havo (atmosfera) qobig’ida va yer sharining

suvli qobig'i (gidrosfera) da tarqalgan. Bu shu bilan izohlanadiki, litosferada yer osti suvlari va tog' cho'kmalarida chuqurlikni sekin-asta ortib borishi bilan harorat ham ortib 2 km dan 16 km chuqurlikda 100 ^{o}S va yuqori (vulqonik faollik zonasida esa 200 dan 1500 ^{o}S cha) ni tashkil etadi.

Yerning yuzasida hayotning konsentrasiyasi va faolligi eng yuqoridir.

Inson evolyusiyasi jarayonida o'zining oziq-ovqat, moddiy boylik, iqlim va ob-havo ta'siridan himoyalanish, o'ziga qulaylikni oshirish bo'yicha ehtiyojlarini samaraliroq qanoatlantirishga intilib tabiiy muhitga birinchi o'rinda biosferaga to'xtovsiz o'z ta'sirini o'tkazdi. Bu maqsadga yetish uchun u biosferani bir qismini texnosfera band etgan joyga aylantirdi.

Texnosfera - o'tmishda biosferaga taalluqli bo'lgan keyinchalik insonlarning o'zining moddiy va ijtimoiy-iqtisodiy ehtiyojlarini yanada yaxshilash maqsadida to'g'ridan to'g'ri yoki sirtdan texnik vositalar bilan ta'sir etgan hududdir.

Texnosfera insonlar tomonidan texnik vositalar yordamida yaratilgan shaharlar, qo'rg'onlar, qishloq aholi punktlari, sanoat va korxonalar zonasi band etgan hududlar hisoblanadi.

Inson hayot faoliyati jarayonida nafaqat tabiiy muhit bilan balki, ijtimoiy muhit deb ataluvchi odamlar bilan ham uzluksiz aloqada bo'ladi. Insonni ijtimoiy muhit bilan aloqasi tug'ilishni davom ettirish, bilim, tajribalarni almashtirish, o'zining ma'naviy ehtiyojlarini qanoatlantirish, intellektual qobiliyatlarni oshirishda foydalaniladi va shakllanadi.

3.2. Favqulodda holatlarda xavfsizlik tadbirlarini rejalashtirish

Xalq xo'jalik obyektlarining turg'unligi ularni favqulodda holatlarning xavfli va zararli omillari ta'siriga chidamliligi, ya'ni, favqulodda holatlar sharoitida rejalashtirilgan hajmda va nomenklaturada mahsulot ishlab chiqarish, ishchi va xizmatchilar hayot faoliyati xavfsizligini to'liq taminlash hamda ishlab chiqarishga zarar yetgan holatlarda o'z ish qobiliyatini tiklashga moslashishi orqali baholanadi.

Favqulodda holatlar vaqtida obyektning turg’un ishlashiga tashkiliy, muhandis-texnik va boshqa tadbirlarni kompleks ravishda amalga oshirish natijasida erishiladi.

Ushbu tadbirlar birinchi navbatda ishchilar va xizmatchilarni himoyalashga qaratilgan bo’lishi kerak. Chunki, inson resursi hamda xalq, xo’jaligi obe’ktlarini favqulodda holatlarning xavfli va zararli omillaridan himoyalamasdan turib, ularni turun ishlashini ta’minlab bo’lmaydi. Bunday tashqari, obyektdagi ishchilar va obyekt yaqinida yashovchi aholini hayot faoliyati xavfsizligini taminlashda favqulodda holatlarning buzuvchi omillari ta’sirida yuzaga keluvchi ikkilamchi xavfli omillar sodir bo’lish xavfining oldini olishga qaratilgan tadbirlar ham muhim rol o’ynaydi. Ikkilamchi xavfli omillar, ichki va tashqi sabablar natijasida vujudga kelishi mumkin.

Xalq xo’jaligi obe’ktlarining favqulodda holatlar vaqtida turun ishlashini taminlashga qaratilgan tadbirlar kompleksi ichidan asosiy ikkita tadbirga, ya’ni, aynan favqulodda holatlarda ishchi va xizmatchilarni hayot faoliyati xavfsizligini taminlash muammolariga hamda ikkilamchi xavfli omillar hosil bo’lishini bartaraf etishga qaratilgan tadbirlarga to’xtalamiz.

Ishchi-xizmatchilarni himoyalash tadbirlariga-texnologik jarayonlarda portlashga va yong’inga xavfli hamda zaharli va radioaktiv moddalar ishlatiladigan ish sharoitlarida ish rejimini tashkil etish; zaharlanish o’chog’ini bartaraf etishga qaratilgan ishlarni aniq bajarish yo’llari bo’yicha o’qitish; obyektdagi ishchi va xizmatchilar hamda obyekt yaqinidagi aholiga, obyektda hosil bo’lgan xavf to’g’risida xabar berishning lokal sistemasini tashkillashtirish va uni doimiy tayyor holatda saqlash kabi ishlar kiradi.

Favqulodda holatlarning xavfli va zararli omillari ta’sirida yuz beradigan yong’inlar, portlashlar, zaharli radioaktiv moddalarni muhitga tarqalishi ikkilamchi omillar jumlasiga kiradi. Ma’lumki, normal ish sharoitida obyektning xavfsiz va avariyasiz ishlashini taminlashga qaratilgan qator tadbirlar amalga oshiriladi. Lekin, bu omillar favqulodda holatlar vaqtida yetarli darajada bo’lmaydi. Shu sababli, favqulodda holatlarning ikkilamchi omillaridan himoyalashga qaratilgan

qo’shimcha tadbirlar ishlab chiqish talab etiladi. Bunday tadbirlarga saqlanadigan portlashga, yong’inga xavfli va zaharli moddalar zahirasini minimum darajagacha kamaytirish; saqlash omborxonalarini xavfsiz joyda, mustahkam qilib, shamol yo’nalishini, yong’in oraliqlari va yo’laklarini, yong’inga qarshi suv taminotini hisobga olgan holda qurish; ularni yong’in o’chiruvchi vositalar, zahira elektr manbalari, aloqa vositalari avtomat signalizasiya kabi vositalar bilan taminlash ishlari kiradi.

Rejalashtirish favqulodda holatlar vaqtida hayot faoliyat xavfsizligini taminlashning yetakchi funksiyasi va markaziy zvenosi hisoblanadi. Rejalashtirishda xavfsizlikni taminlash maqsadida amalga oshiriladigan tadbirlar vaqti, resursi va tadbirlarni bajaruvchi shaxslar aniqlashtiriladi.

Rejalashtirishda hujjat, reja tuziladi va u quyidagi qismlardan iborat bo’ladi: aniq ko’rsatkichlar (ish turi, tadbirlar); ushbu ishlarni bajarish vaqti; ishlarni bajarish uchun zarur resurslar (turi, soni, miqdori, manbai); ishni bajaruvchi mas’ul shaxs (har bir punkt bo’yicha); ishni bajarilishini nazorat qilish usuli.

Rejaning matn qismi ikki bo’limdan iborat bo’lib, birinchi bo’limda favqulodda holatlar vaqtidagi shart-sharoitlarni baholash bo’yicha xulosalar, ikkinchi bo’limda esa favqulodda holatlar xavfidan aholini himoyalash tadbirlari ko’rsatiladi. Ushbu tadbirlarga asosan quyidagilar kiritilishi mumkin, ya’ni: favqulodda holat to’g’risida xabar berish tartibi; kuzatish va razvedkani tashkil etish; qutqaruv va boshqa muhim ishlarni bajarish uchun kuch va vositalarni tayyorlash; favqulodda holatlar ta’sirini bartaraf etish yoki susaytirish tadbirlari; odamlar va moddiy boyliklarni himoyalash tadbirlarini tezkor bajarish usullari; tibbiy taminlash, dozimetrik va ximiyaviy nazorat; ishlab chiqarishni avariyasiz to’xtatish tartibi; odamlarni himoyalashni tashkil etish, shaxsiy himoya vositalari bilan taminlash; evakuasiya tadbirlarini tashkil etish; ularni boshqarish; har xil sharoitlarda qutqaruv ishlarini tashkil etish tartibi; yuqori tashkilotlarga va favqulodda holatlar bo’yicha tuzilgan komissiyalarga axborot hamda ma’lumotlar berish tartibi.

Rejaga turli xil zarur lug’aviy va tushuntiruvchi xarakterdagi materiallar ham ilova qilinadi. Reja real qisqa mazmo’nli, lekin, to’liq ifoda etilgan, iqtisodiy jihatdan maqbul bo’lishi hamda obyektning barcha imkoniyatlarini ifoda etishi zarur.

Rejaning realligi tabiiy va texnogen ko’rinishdagi favqulodda holatlar vaqtida haqiqiy ishlab chiqarish sharoitida hayot faoliyatni taminlash bo’yicha sistemali ravishda turli xil mashg’ulotlar va amaliy mashqlar o’tkazish yo’li bilan tekshiriladi.

3.3. Favqulodda holatlar oqibatlarini bartaraf etish

Avariyalarda halokatlar va tabiiy ofatlar oqibatlarini bartaraf etish, mamlakatning avariya-qutqaruv xizmatini doimiy tayyor holatini taminlash hamda ishlab chiqarish korxonalarida avariyalar va halokatlarni oldini olishga qaratilgan chora-tadbirlarni bajarilishi ustidan nazorat qilish maqsadida O’zbekiston Respublikasida favqulodda holatlar qo’mitasi tuzilgan.

Favqulodda holatlar oqibatlarini bartaraf etishga qaratilgan barcha vazifalar bosqichma-bosqich, aniq ketma-ketlik asosida maksimal qisqa muddatlar ichida bajarilishi lozim.

Birinchi bosqichda aholini tezkor himoyalash masalalari, favqulodda holatlar xavfli omillarini tarqalishini cheklash va uning ta’sir darajasini kamaytirish chora-tadbirlari hamda qutqaruv ishlarini amalga oshirish kabi vazifalar amalga oshiriladi.

Aholini tezkor himoyalashning asosiy tadbirlariga xavf to’g’risida xabar berish; himoya vositalaridan foydalanish; favqulodda holatlardagi rejimga rioya qilishni taminlash; xavfli zonalardan evakuasiya qilish; tibbiy va boshqa turdagi yordamlar ko’rsatish kabi ishlar kiradi.

Favqulodda holatlar ta’sir doirasini cheklash va uning oqibatlarini susaytirishga qaratilgan tadbirlar asosan: avariyalarni lokalizasiyalash, ishlab chiqarish texnologik jarayonlarini to’xtatish yoki o’zgartirish, yong’inni oldini olish yoki uni o’chirish kabi vazifalarni o’z ichiga oladi.

Qutqarish va boshqa turdagi kechiktirib bo’lmaydigan tadbirlar jumlasiga boshqarish organlarini, kuch va vositalarni tayyor holatga keltirish, zararlanish o’chog’ini razvedka qilish va mavjud holatni baholash kabi vazifalar kiradi.

Ikkinchi bosqich vazifalariga favqulodda holatlar oqibatlarini bartaraf etish bo’yicha qutqaruv hamda boshqa kechiktirib bo’lmaydigan ishlarni amalga oshirish kiradi. Bu ishlar uzluksiz ravishda, qutqaruvchilar va bartaraf etuvchilar smenalarini almashtirgan holda xavfsizlik texnikasi va ehtiyot choralariga to’liq amal qilib bajarilishi shart.

Qutqaruv ishlari jarohatlanganlarni qidirib topish, ularni yonadigan binolar, xarobalar, transport vositalari ichidan olib chiqish, odamlarni xavfli xonalardan evakuasiya qilish, jarohatlanganlarga birinchi yordam ko’rsatish va shu kabi boshqa yordamlarni amalga oshirish ishlarini o’z ichiga oladi.

Kechiktirib bo’lmaydigan ishlar jumlasiga esa yong’inni lokalizasiyalash va o’chirish, konstruksiyalarni mustahkamlash, qutqaruv ishlarini amalga oshirish maqsadida kommunal-energetik tarmoqlarni, aloqa va yo’llarni tiklash, odamlarga sanitar ishlov berish, dezaktivasiyalash va degazasiyalash ishlarini amalga oshirish kabi vazifalar kiradi.

Qutqaruv va boshqa kechiktirib bo’lmaydigan ishlar jumlasiga aholini barcha turdagi vositalar bilan taminlash, jumladan, ularni xavfsiz joylarga joylashtirish, oziq-ovqat va suv bilan taminlash, tibbiy yordam ko’rsatish hamda moddiy va moliyaviy yordamlar berishni amalga oshirish kabi vazifalar ham kiradi.

Uchinchi bosqich vazifalariga avariyalar, halokatlar va tabiiy ofatlar yuz bergan rayonlardagi aholi faoliyatini taminlash masalalari kiradi. Bu maqsadda turar joylarni tiklash yoki vaqtinchalik turar joylar barpo etish, energiya va suv ta’minotini, aloqa tarmoqlarini, kommunal xizmat obyektlarini tiklash, zararlanish o’chog’iga sanitar ishlov berish, aholiga oziq-ovqat mahsulotlari hamda birlamchi ehtiyoj buyumlari bilan yordam ko’rsatish ishlari amalga oshiriladi. Ushbu bosqich nihoyasida evakuasiya qilingan aholi o’z joylariga qaytariladi va xalq xo’jalik obyektlarining ishlashi tiklanadi.

Ayrim favqulodda holatlarning sodir bo’lishi oldindan aniqlanishi mumkin. Bunday holatlarda amalga oshirilishi lozim bo’lgan barcha ishlar oldindan ishlab chiqilgan reja asosida amalga oshiriladi. Rejada asosan ikki xil ko’rinishdagi tadbirlar belgilanadi.

Birinchi guruhdagi tadbirlar aholini himoyalash maqsadida amalga oshiriladi. Bu tadbirlarga - aholiga xavf to’g’risida ma’lumot berish va xabar berish; himoya vositalarini tayyor holga keltirish; boshqarish sistemalari va vositalarining tayyorligini tekshirib ko’rish; shaxsiy himoya vositalarini aholiga tarqatishga tayyorlash va tarqatish; tibbiy profilaktika, sanitar va epidemiyaga qarshi tadbirlarni o’tkazish; evakuasiyaga tayyorlanish va talab etilgan sharoitlarga xavf tahdid soladigan rayonlarda aholini evakuasiya qilish kabi vazifalar kiradi.

Ikkinchi guruh tadbirlariga favqulodda holatlarning xavfli va zararli omillarini bartaraf etishga qaratilgan vazifalar kiradi. Bu tadbirlarga-xalq xo’jaligi obyektlari ishini to’xtatish yoki ish rejimini o’zgartirish; energiya, suv, gaz sistemasi ish rejimini o’zgartirish yoki vaqtincha to’xtatish; mavjud muhandislik inshootlarini mustahkamlash yoki qo’shimcha qurish; yong’inga qarshi tadbirlar o’tkazish; xavfli rayonlardan moddiy boyliklar va chorva mollarini olib chiqish; oziq-ovqat, oziqa xom ashyosi va suv manbalarini himoyalash kabi ishlar kiradi.

Favqulodda holatlar sodir bo’lganligi to’g’risida xabar olingach, birinchi navbatda berilgan ma’lumotlarni to’g’riligi tekshirilib, qo’shimcha axborot va ma’lumotlar olish bo’yicha tadbirlar amalga oshiriladi. Chunki, turli xil favqulodda holatlarning har xil sharoitlardagi oqibatlari turlicha bo’lishi mumkin. Shu sababli dastlab favqulodda holatlar ta’sirida yuzaga kelishi mumkin bo’lgan ikkilamchi, uchlamchi va boshqa xavfli omillar aniqlanib, keyingina kompleks tadbirlar amalga oshiriladi.

3.4. Barqaror rivojlanish shartlari va xavfsizlik masalalari

O’zbekiston Respublikasi Prezidenti I. A. Karimov ta’kitlaganidek, «Ekologik xavfsizlik kishilik jamiyatining bugungi va ertasi uchun dolzarbligi, juda zarurligi bois eng muhim muammolar jumlasiga kiradi... Uni hal etish barcha

xalqlarning manfaatlariga mos bo’lib, sivilizasiyaning hozirgi kuni va kelajagi ko’p jihatdan ana shu muammoning hal qilinishiga bog’liqdir». Ushbu va boshqa ekologik muammolarni nazarda tutgan holda, mustaqillik davrida mamlakatimizda atrof-muhitni musaffoligi va tabiatni muhofaza qilish bo’yicha qator qonunlar, farmonlar va qarorlar qabul qilindi.

Mustabidlik davrida O’zbekistonda, jumladan Farg’ona vodiysida tabiat va jamiyat orasidagi murakkab va azaliy munosabatlarni tobora ziddiyatli tus olishi hududimizda ekologik muvozanat va barqarorlikni salbiy tomonga yo’nalishiga olib keldi. Bu holat, o’z navbatida xalq xo’jaligining barcha tarmoqlarini rivojlanishiga, hamda mavjud tabiiy resurslarning hajmi, miqdori va sifatiga salbiy ta’sir etdi.

Odatda, boshqa joylardagi kabi Farg’ona vodiysida ham ekologik holat o’zoq yillar davomida bir tekis rivojlanmagan, buni obyektiv va subyektiv sabablari mavjud, chunki tuproq, suv resurslaridan, o’simliklar va hayvonot dunyosi boyliklaridan o’ta samarasiz ravishda foydalanilgan. Natijada ushbu tabiiy resurslarning areallari qisqarib, tabiiy zahiralari kamayib borgan. O’simlik va hayvonot dunyosining tiklanish jarayonlari zaiflashib borgan. Hududimiz ekologik muammolarini atroflicha o’rganish, tadqiq qilishda, albatta ularni hududiy bioekologik holatlari va tarqalash hossalarini hisobga olish muhim hisoblanadi.

Etirof etish kerakki, mashxur ekolog akademik S.S.Shvarsning ta’kidlashicha har bir ekosistemaga tushayotgan antropogen ta’sirotlar

ko’lami va hajmini ta’sirini, ularni normasini aniqlash zarur. Bunda yana o’sha ekosistema yoki geomajmuani ushbu ta’sirotlari barqarorlik darajasini bilish muhim sanaladi.

Ekologik havfsizlik va barqaror rivojlanishni ta’minlashda muhit omillari ta’sirini optimallashtirish muhim sanaladi. Bu masalada yani iqlimni ta’sirini alohida ta’kidlash zarur. Ingliz ekologi Lorens ta’kidlagan ediki, «xokimiyatlar orasida iqlim xokimiyati eng kuchlidir».

Xulosa

Ushbu bitiruv malakaviy ishni bajarish natijasida quyidagilarga ega bo’lindi:

- Axborot xavfsizligiga bo’lishi mumkin bo’lgan na’munaviy taxditlar, ularning turlari va ko’rinishlari, axborotlarni chiqib ketishi mumkin bo’lgan texnik, optik kanallari, ma’lumot chiqish kanalining paydo bo’lish sabablari o’rganilgan;
- Server himoyasini ta’minlashda texnik vositalarning roli, yuqorida ko’rib chiqilgan kanallarda xavfsizlikni tashkil etish, ma’lumotlarni himoyalashning konstruktor-texnologik usullari ko’rib chiqilgan;
- Korparativ taroqda server tushinchasi, uning turlari, vazifalari bayon etilib bir biridan farqlari keltirilgan;
- Axborot xavfsizligining asosiy apparat-dasturiy vositalari: tarmoqlararo ekran, virtual himoyalangan tarmoqlar, ma’lumotlarni zaxira nusxalarini hosil qiluvchi RAID tizimlari berilgan;
- Ushbu vositlardan foydalangan holda server xavfsizligini ta’minlashning samaradorligini oshirish arxitekturasi ishlab chiqilib, uning tashkil etuvchilarini vazifalari va bu arxitekturadagi asosiy vazifalari yoritilgan.

Adabiyotlar ro’yhati

1. O’zbekiston Respublikasi prezidentining “O’zbeksiton Respublikasi Axborot Texnologiyalari va Kommunikatsiyalarini Rivojlantirish Vazirligini yaratish haqida”gi qarori. 2015 yil 4-fevral.
2. Karimov I.A. Jahon inqirozining oqibatlarini yengish, mamlakatimizni madernizasiya qilish Ba taraqqiy tapgan davlatlar darajasiga ko’tarish sari. T.18. - T., 2010.
3. S.K.G`aniev, M.M. Karimov, K.A. Toshev “Axborot xavfsizligi”. “Aloqachi”. 2008 yil, 378 b.
4. Давыдов А.С., Маслова Т.В. Информационные технологии в деятельнасти органов внутренних дел: Учебное пособие. - Челябинск, 2007.
5. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программно-аппаратные средства обеспечения информационнай безопасности: Учебное пособие. - М., 2006.
6. Информационные технологии управления в органах внутренных дел: Учебник / Шд ред. доцента Ю.А. Кравченка. - М., 2008.
7. Мельников В.П. и др. Информационная безопаснасть и защита информации: Учебное пособие. - М., 2008.
8. Левин М. Безопасность в сетях Internet и Intranet. - М., 2011.
9. Мельников В.П. Информационная безопасность. Учебное пособие. - М., 2009.
10. Миродова Ш. Проблемы обеспечения информационнай безопасности Республике Узбекистан в услaвиях глоболизации. - Т., 2008.
11. Мууаммадиев Ж.У. Ахборот хавфсизлиги: муаммо ва ечимлар: Манаграфия. - Т., 2011.
12. Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие. - М., 2002.
13. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. - М., 2000.

14. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. *Защита* информации в компьютерных системах и сетях. - М., 2008.

15. Серго А.Г. Интернет и право. - М., 2013. http://Cyber-Crimes.ru.

16. Соколов А., Степанюк О. Защита от компьютерного терроризма. СПб., 2012.

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

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