O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI JIZZAX FILIALI

Abdumalikov Akmaljon Abduxoliq o‘g‘li

INFOKOMMUNIKATSIYA TIZIMLARIDA FOYDALANUVCHI AXBOROTLARINI HIMOYALASH VOSITALARI VA USULLARINI TADQIQ ETISH

MONOGRAFIYA

Jizzax - 2026

UDK: 004.738.5:004.056
KBK: 32.811.4
A 15

Abdumalikov, A.A. Infokommunikatsiya tizimlarida foydalanuvchi axborotlarini himoyalash vositalari va usullarini tadqiq etish: monografiya / A.A. Abdumalikov .- Jizzax: D-Press Services nashriyoti, 2026.- 102 b.

Mazkur monografiyada infokommunikatsiya tizimlarida foydalanuvchi axborotlarini himoyalashning nazariy va amaliy jihatlari tadqiq etilgan. Unda axborot xavfsizligining asosiy tamoyillari, foydalanuvchi ma'lumotlariga tahdid soluvchi omillar hamda zamonaviy himoya vositalari va usullari tahlil qilingan. Shuningdek, kriptografik himoya, autentifikatsiya, avtorizatsiya va tarmoq xavfsizligi texnologiyalarining samaradorligi o'rganilib, axborot xavfsizligini oshirish bo'yicha ilmiy-amaliy tavsiyalar ishlab chiqilgan. Monografiya axborot xavfsizligi, kiberxavfsizlik va infokommunikatsiya tizimlari sohasida faoliyat yurituvchi tadqiqotchilar, mutaxassislar hamda talabalar uchun mo'ljallangan.

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

S.P. Xalilov - Muhammad al-Xorazmiy nomidagi TATU "Sun'iy intellekt" kafedrasi dotsenti, t.f.f.d. (PhD).

D.R.Xasanov - Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti Jizzax filiali "Kompyuter ilmlari va dasturlashtirish" kafedrasi mudiri, t.f.f.d., (PhD) dotsent.

Ushbu monografiya Mirzo Ulug'bek nomidagi O'zbekiston milliy universiteti Jizzax filialining 2026-yil 14-apreldagi 4-sonli ilmiy-texnik kengashida chop etishga ruxsat berildi.

ISBN: 978-9910-5042-8-0

KIRISH

Bugungi kunda zamonaviy jamiyat taraqqiyoti axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi bilan chambarchas bog‘liqdir. Raqamli transformatsiya jarayonlari barcha sohalarga chuqur kirib borayotgan bir vaqtda, axborot resurslari strategik ahamiyatga ega bo‘lgan muhim aktivga aylanmoqda. Natijada, foydalanuvchi axborotlarini himoya qilish masalasi nafaqat texnik, balki ijtimoiy, iqtisodiy va huquqiy jihatdan ham dolzarb muammolardan biri sifatida shakllanmoqda.

Hozirgi kunda dunyo miqyosida axborot texnologiyalarining jadal sur’atlar bilan rivojlanib borishi qulayliklar bilan bir qatorda yangi muammolarni o‘rtaga qo‘ymoqda. Avtomatlashtirilgan axborot tizimlarida va telekommunikasiya tizimlarida aylanayotgan axborotlar to‘plamiga bo‘lgan tahdidlar keskin oshdi, ayniqsa, Internet paydo bo‘lgandan boshlab, axborot o‘g‘irlash va axborot mazmunini buzib qo‘yish hollari ko‘paydi. Natijada axborot xavfsizligi muammosi O‘zbekiston Respublikasi uchun ham dolzarb muammoga aylandi. O‘zbekiston Respublikasida so‘nggi yillarda axborot xavfsizligini ta’minlashga, chet eldan valyutaga sotib olinayotgan dasturiy va dasturiy-apparat vositalarning mahalliylashtirishga davlatimiz rahbariyati tomonidan katta ahamiyat berilmoqda.

Jahonda infokommunikatsiya tizimlari monitoringida axborotlarni taqsimlashning turli signal o‘zgartgichlarini keng qo‘llash, ular yordamida doimiy monitoring jarayonlarini amalga oshirishda infokommunikatsiya vositalarini uzluksiz va sifatli ishlashini ta’minlash bo‘yicha signallar bilan ta’minlovchi apparatlar, qurilmalar, vositalar hamda algoritm va dasturiy vositalarini takomillashtirishga qaratilgan qator ilmiy tadqiqot ishlari olib borilmoqda.

Infokommunikatsiya tizimlari- bu axborotni yig‘ish, uzatish, qayta ishlash va saqlash jarayonlarini ta’minlovchi murakkab tizimlar majmuasidir. Ushbu tizimlar orqali katta hajmdagi shaxsiy, tijorat va davlat ahamiyatiga ega ma’lumotlar almashinuvi amalga oshiriladi. Shu sababli, mazkur tizimlarda axborot xavfsizligini ta’minlash, xususan foydalanuvchi ma’lumotlarini ruxsatsiz kirish, o‘zgartirish, yo‘q qilish va oshkor etishdan himoya qilish ustuvor

vazifalardan biri hisoblanadi. So‘nggi yillarda kiberxavfsizlik sohasida yuzaga kelayotgan tahdidlar ko‘lami va murakkabligi ortib bormoqda. Xakerlik hujumlari, zararli dasturlar, fishing, identifikatsiya ma’lumotlarini o‘g‘irlash kabi tahdidlar foydalanuvchi axborotlariga jiddiy xavf tug‘dirmoqda. Ayniqsa, bulutli texnologiyalar, mobil ilovalar va IoT qurilmalarining keng qo‘llanilishi axborot xavfsizligini ta’minlashni yanada murakkablashtirmoqda. Bu esa himoya vositalari va usullarini chuqur o‘rganish, ularni takomillashtirish va amaliyotga joriy etishni talab etadi.

Mazkur monografiyaning asosiy maqsadi infokommunikatsiya tizimlarida foydalanuvchi axborotlarini himoyalash vositalari va usullarini kompleks tarzda tadqiq etish, mavjud yondashuvlarni tahlil qilish hamda ularni rivojlantirish bo‘yicha ilmiy asoslangan taklif va tavsiyalar ishlab chiqishdan iboratdir.

Tadqiqot doirasida quyidagi vazifalar belgilab olingan:

- infokommunikatsiya tizimlarida axborot xavfsizligining nazariy asoslarini o‘rganish;
- foydalanuvchi axborotlariga tahdidlar va xavf omillarini aniqlash va tahlil qilish;
- zamonaviy himoya vositalari (kriptografik usullar, autentifikatsiya va avtorizatsiya mexanizmlari, tarmoq xavfsizligi vositalari)ni o‘rganish;
- mavjud himoya usullarining samaradorligini baholash;
- axborot xavfsizligini oshirishga qaratilgan innovatsion yondashuvlarni ishlab chiqish.

Tadqiqot obyekti sifatida infokommunikatsiya tizimlari va ularda qayta ishlanadigan foydalanuvchi axborotlari tanlangan bo‘lsa, tadqiqot predmeti esa ushbu axborotlarni himoyalash vositalari, texnologiyalari va usullaridan iboratdir. Mazkur ishning ilmiy yangiligi shundan iboratki, unda infokommunikatsiya tizimlarida foydalanuvchi axborotlarini himoya qilishning kompleks yondashuvi ishlab chiqiladi, zamonaviy tahdidlarga moslashgan himoya mexanizmlari taklif etiladi hamda mavjud usullarning samaradorligi tizimli ravishda baholanadi.

Tadqiqot natijalari amaliy jihatdan ham muhim ahamiyatga ega bo‘lib, ular axborot tizimlari xavfsizligini oshirish, foydalanuvchi ma’lumotlarini ishonchli himoya qilish va kiberxavfsizlik darajasini mustahkamlashda qo‘llanilishi mumkin. Shu tariqa, infokommunikatsiya tizimlarida foydalanuvchi axborotlarini himoyalash masalasi bugungi kunda dolzarb ilmiy-amaliy yo‘nalishlardan biri bo‘lib, uni chuqur tadqiq etish zamon talabiga to‘liq javob beradi.

I BOB. AXBOROT – KOMUNIKASIYA TIZIMLARIDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY VOSITALARINING TADQIQI

1.1-§.Axborot – komunikasiya tizimlarining boshqarishning funksional masalalari

Zamonaviy axborot texnologiyalaridan muvaffaqiyatli foydalanish uchun nafaqat tarmoqlarning o‘zini, balki tarmoq xavfsizligi vositalarini ham ishonchli va samarali boshqarish zarur. Hozirgi vaqtda kompaniyaning butun infrastrukturasini qamrab oluvchi boshqarishning kompleks tizimini yaratish birinchi galdagi vazifa hisoblanadi. Bunday boshqarish tizimi axborot tizimining murakkabligi va masshtabidan qat’iy nazar, quyidagilarga imkon yaratadi:

- butun axborot infrastrukturasiga markazlashtirilgan va operativ boshqarish ta’sirni ko‘rsatish;

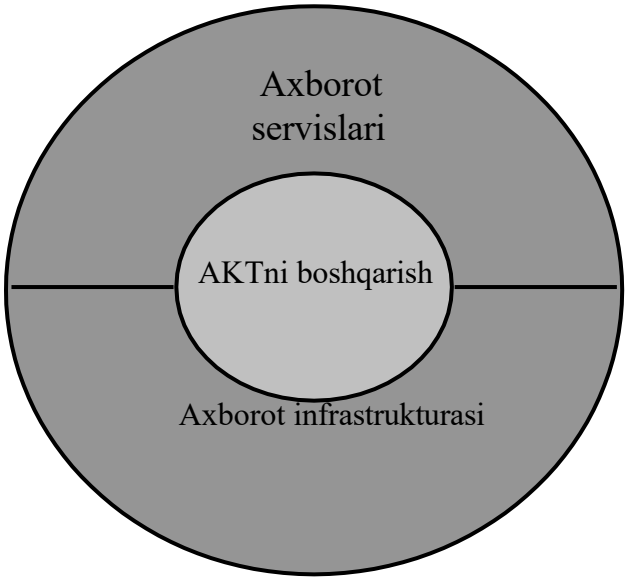
- operativ yechimlarni qabul qilish uchun axborot xavfsizligi holati xususidagi obyektiv axborotni beruvchi muntazam auditni va keng ko‘lamdagi monitoring o‘tkazish;

- axborot infrastrukturasi rivojini bashoratlash uchun uning ishlashi xususidagi statistik ma’lumotlarni to‘plash.

Axborot tizimlarini boshqarishning ITIL metodologiyasi

ITIL (IT Infrasructure Library) metodologiyasiga muvofiq axborot tizimi ikkita yirik blokdan – axborot infrastrukturasi va axborot servislaridan iborat (1-rasm).

Axborot infrastrukturasi axborot servislari ishlovchi moddiy asos, muhit hisoblanadi. Axborot servislariga Internet-servislar, ilovalar servisi, boshqarish, yechim qabul qilish servislari va h. kiradi. Axborot infrastrukturasi servislar ishlashini ta’minlovchi texnik vositalar, aloqa liniyalari, muolajalar, me’yoriy xujjatlar va h. majmuidir. Axborot servislarining sifati bevosita axborot infrastrukturasi va uni boshqarish sifatiga bog‘liq.



1-rasm. ITIL metodologiyasi nuqtai nazarida axborot tizimining ko‘rinishi

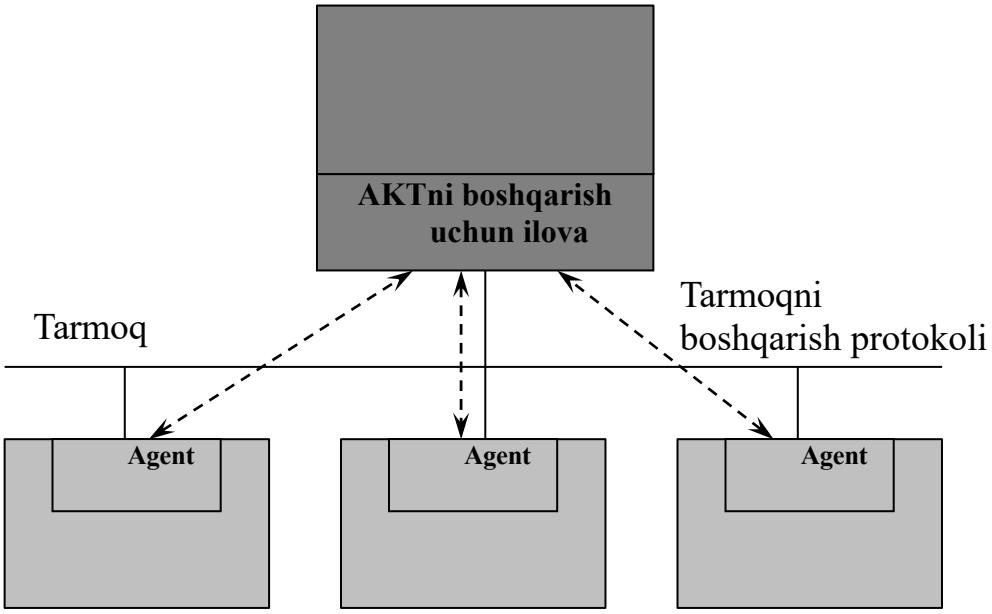
Axborot infrastrukturasini asosida axborot resurslari (hisoblash platformalari, serverlar, shaxsiy kompyuterlar, ma’lumotlarni uzatish tarmoqlari, aloqa liniyalari) yotuvchi piramida sifatida tasavvur etish mumkin (2-rasm).

2–rasm. Axborot infrastructurasini tashkil etuvchilari

Piramidaning ikkinchi sathini turli ilovalar tashkil etadi. Bu ilovalar birinchi sath resurslaridan foydalanib tatbiqiy dastur ta’minoti, elektron pochta, kafolatlangan yetkazish tizimi, ma’lumotlar bazasi, Web-serverlar va h. kabi

muayyan ilovalar ishlashini ta’minlaydi. Va nihoyat, eng yuqori sathda biznes va ishlab-chiqarish jarayonlarining o‘tishini ta’minlovchi ilovalar ishlaydi. Ikkala pastki sathdan foydalanuvchi bu ilovalar ishlab-chiqarishni boshqarish, buyurtmachilar va ta’minlovchi bilan o‘zaro aloqa, moliyaviy hisob va yechimni qabul qilishni madadlash kabi biznes masalalarni yechishga yo‘naltirilgan.

Umumiy holda, tarmoqni boshqarish tizimining arxitekturasi 13.3- asmda keltirilgan ko‘rinishga ega. Tarmoqni boshqarish ilovasi tarmoq ma’murining ish joyida yoki boshqa kompyuterda bajarilishi mumkin. Uning vazifasi boshqariluvchi qurilmalarda bajariladigan agent - ilovalardan yoki operasion tizim servislaridan keluvchi boshqariluvchi obyekt xususidagi axborotni yig‘ish.



3–rasm. AKTning boshqarish tizimining umumlashtirilgan sxemasi.

Bunday ilovalarni agentlar bilan o‘zaro aloqasi uchun odatda SNMP (Simple Network Management Protocol) yoki CMIP (Common Management Information Protocol) protokollaridan foydalaniladi. Birinchisi, odatda, lokal tarmoqda ishlatilsa, ikkinchisi telekommunikasiyadan foydalanuvchi taqsimlangan tarmoqlarda ishlatiladi. Ammo dastur ta’minotini ba’zi ishlab chiqaruvchilari tarmoqni boshqarishda xususiy tarmoq protokollaridan foydalanishadi.

Tarmoqni boshqaruvchi zamonaviy vositalar quyidagi vazifalarni bajara oladi:

- Boshqariluvchi kompyuter va qurilmalardagi buzilishlarni kuzatish,

sabablarni aniqlash va bartaraf etish (ko‘pincha avtomatik tarzda), oqibatlarini tuzatish va buzilishlarni oldini olish (masalan tashhislash amalini bajarish orqali);

- kompyuterlarning va tarmoq qurilmalarining konfigurasiyalanishini boshqarish (xususan, inisializasiyalash, qayta konfigurasiyalash va tarmoq qurilmalari va kompyuterlarni uzib qo‘yish);

-foydalanuvchilar va foydalanuvchilar guruhi tomonidan tarmoq resurslaridan foydalanishni tartibga solish (masalan, diskli va boshqa kvotalarni tartibga solish);

- tarmoq qurilmalari va servislar unumdorligini boshqarish (tarmoq qurilmalari ishlatilishi jadalligi statistikasini va xatoliklar chastotasini yig‘ish va tahlillash hamda olingan ma’lumotlar asosida ular unumdorligini sun’iy tarzda o‘rnatish);

- oldindan belgilangan xavfsizlik siyosati asosida tarmoq resurslaridan foydalanishni nazoratlashdan foydalanib ma’lumotlar himoyasini boshqarish va ularni buzishga urinishlardan ma’murni habardor etish.

Korxona axborot xavfsizligi tizimi korporativ tarmoqni boshqarish tizimining eng muhim komponenti hisoblanadi. Korxona masshtabidagi taqsimlangan tarmoqda axborotni himoyalash vositalarini boshqaruvchi tizim quyidagi vazifalarni bajarishi lozim:

- korxona tarmog‘i doirasida xavfsizlik siyosatini boshqarish, alohida qurilmalar xavfsizligining lokal siyosatini shakllantirish va uni axborotni himoyalovchi barcha qurilmalarga yetkazish;

- foydalanish obyektlarini va subyektlarini konfigurasiyalashni boshqarish; himoya qurilmalari va dasturiy ta’minoti tarkibini, versiyasini, komponentlarini boshqarishni o‘z ichiga oladi;

- taqsimlangan tatbiqiy tizimlarga himoya servislarini taqdim etish, himoyalangan ilovalar va ular resurslarini ruyxatga olish. Ilovalarning bu guruhi, avvalo, tatbiqiy tizimlar tomonidan himoya servislarini boshqarish uchun interfeysni ta’minlash lozim;

- kriptovositalarni boshqarish, xususan kalitli boshqarish (kalitli

infratsruktura). Kalitli infrastruktura infrastruktura xizmati tarkibida ishlashi lozim;

- xodisaviy protokollash; turli qurilmalarga loglarni berishni sozlashni, loglarni detallashtirish satxini boshqarishni, protokol olib boriluvchi xodisalarni tarkibini boshqarishni o‘z ichiga oladi;

- axborot tizimi xavfsizligini auditlash; axborot tizimlari himoyalanishining joriy holati xususidagi obyektiv ma’lumotlarni baholashni ta’minlaydi;

- tizim xavfsizligini monitoringlash; qurilmalar va qurilmalarda kechuvchi xodisalar (himoyalash konteksti bo‘yicha) holati, faolligi xususida, masalan, bo‘lishi mumkin bo‘lgan xujumlar xususida real vaqtda axborot olinishini ta’minlaydi;

- maxsus himoyalangan ilovalar, masalan amallar ustidan notarial nazorat ishini ta’minlash hamda reglamentda ko‘zda tutilgan tadbirlarni (kalitlarni, parollarni, himoya qurilmalarini almashtirish, smart-kartalarni ishlab chiqarish va h.) madadlash;

- ilovalarning loyiha-inventarizasiyalash guruhi ishini ta’minlash. Ilovalarning bu guruhi korxona tarmog‘iga himoya vositalarini o‘rnatishni, qo‘llaniladigan himoya vositalarini hisobga olishni, himoya vositalarining modul tarkibini nazoratlashni, himoya vositalari holatini nazoratlashni va h. bajaradi.

Tarmoqlarni an’anaviy boshqarish tizimi va tarmoqdagi axborotni himoyalash vositalarini boshqarish tizimi orasida o‘zaro aloqani komplekslash va tashkil etish muammosi mavjud.

Axborot – komunikasiya tizimlarining xavfsizlik vositalarini boshqarish arxitekturasi

Kompaniyaning taqsimlangan axborot tizimida o‘zining xavfsizlik siyosatini muvaffaqiyatli amalga oshirishi uchun xavfsizlikni boshqarish markazlishtirilgan bo‘lishi va ishlatiladigan operasion tizimga va tatbiqiy tizimlarga bog‘liq bo‘lmasligi lozim. Undan tashqari, korporativ axborot tizimida kechuvchi jarayonlarni (ruxsatsiz foydalanish, foydalanuvchilar imtiyozini o‘zgarishi va h.)

ro‘yxatga olish tizimi yagona bo‘lishi va ma’murga korporativ axborot tizimidagi barcha o‘zgarishlarning to‘liq ko‘rinishini tasavvur etishiga imkon berishi lozim.

Korporativ axborot tizimi xavfsizligini markazlashtirilgan boshqarish asosida global boshqarish konsepsiyasi GSM (Global Security Management) yotadi. Ushbu konsepsiya korxona axborot resurslarini quyidagi xususiyatlarga ega bo‘lgan kompleks boshqarish tizimini qurishga imkon beradi:

- korxonaning barcha resurslari (xavfsizlik siyosati obyektlari) uchun himoyalashning yaxlitligini, ziddiyatlik emasligini va qoidalar naborining to‘laligini ta’minlovchi, barcha mavjud himoya vositalarini korxona xavfsizligi siyosati asosida boshqarish;

- resurslarni tavsiflovchi shaxsiy vositalar hamda korxonaning boshqa kataloglari bilan aloqasi bo‘yicha faollashuvchi korxona muhitining yagona (taqsimlangan) katalogi orqali korxonaning barcha resurslarini aniqlash;

- xavfsizlik siyosatiga asoslanib, axborotni himoyalashning lokal vositalarini markazlashtirilgan boshqarish;

- korxona muhitida siyosat obyektlarini tokenlar va ochiq kalitlar infrastrukturasidan foydalanib qat’iy autentifikasiyalash;

- katalogda belgilangan korxona resurslaridan yoki butun katalog qismlaridan foydalanishni ma’murlashning kengaytirilgan imkoniyatlari;

- hisob-kitoblikni (korporativ tarmoq masshtabida tizimning taqsimlangan obyektlarining o‘zaro aloqasidagi barcha amallarini ruyxatga olish) va auditni, xavfsizlik monitoringini, xavotirli signalizasiyani ta’minlash;

- umumiy boshqarish tizimlari va xavfsizlikning infrastruktura tizimlari bilan integrasiyalanishi;

Ushbu konsepsiya doirasida «xavfsizlik siyosatiga asoslangan PBM (Policy Based Management) boshqarish» deganda korxona biznes-obyekti uchun ta’riflangan qoidalar nabori tushuniladi. Bu qoidalar nabori obyektlarning biznes-sohani to‘liq qamrab olishini va ishlatiluvchi boshqarish qoidalarining ziddiyatlik emasligini kafolatlaydi.

PBM prinsiplariga asoslangan, korxona xavfsizligini boshqarishga

mo‘ljallangan GSM boshqarish tizimi quyidagi talablarga javob beradi:

- korxona xavfsizligi siyosati mantiqiy va semantik bog‘langan, shakllanuvchi, tahrirlanuvchi va tahlillanuvchi ma’lumotlarning bir butun strukturasidan iborat;

- korxona xavfsizligi siyosati yagona kontekstda himoyaning barcha sathlari uchun himoyaning tarmoq siyosati va korxona axborot resurslari xavfsizlik siyosatining bir butuni sifatida belgilanadi;

- korxona resurslarini va xavfsizlik siyosatini ma’murlashni yengillashtirish maqsadida siyosat parametrlari soni minimallashtiriladi.

GSM boshqarish tizimi xavfsizlik siyosatining korxona xavfsizligi konsepsiyasi modeliga mosligini tekshiruvchi ko‘p mezonli vositalar evaziga xavfsizlik siyosatini tahlillashning turli-tuman mexanizmlarini ta’minlaydi.

Xavfsizlikning global va lokal siyosatlari

Korxona xavfsizligining global siyosati axborot xavfsizligi kontekstida korporativ tarmoq obyektlari o‘zaro aloqasining parametrlarini tavsiflovchi xavfsizlik qoidalarining chekli to‘plamidir.

Bunda xavfsizlikning global siyosati obyekti sifatida alohida ishchi stansiyalari va qism tarmoqlar hamda o‘z ichiga kompaniyaning butun strukturaviy bo‘limlarini oluvchi (masalan, marketing bo‘limi yoki moliyaviy departament) obyektlar guruhi yoki hatto alohida kompaniya ko‘rilishi mumkin.

Xavfsizlikning global siyosati tarmoqdagi o‘zaro aloqaga, hamda tizimning nazoratlash va boshqarish funksiyalariga taalluqli bo‘lishi mumkin. Bajaradigan funksiyalari bo‘yicha xavfsizlikning global siyosati quyidagi guruhlarga bo‘linadi:

- VPN qoidalari. Qoidalarning bu guruhi IPSec protokollari yordamida amalga oshiriladi;

- paketli filtrlash qoidalari. Bu qoidalar Stateful va Stattles xilidagi paketli filtrlashni ta’minlaydi.

- proxy-qoidalar. Bu qoidalar berilgan tatbiqiy protokllar boshqaruvida uzatiluvchi trafikni filtrlashga javob beradi;

- autentifikasiyalangan/avtorizasiyalangan foydalanish qoidalari;

- signalizasiyaga va xodisaviy protokollashga javob beruvchi qoidalar.

Xavfsizlikning global siyosati tarmoq sathida xavfsizlik siyosatining mantiqiy yaxlit va semantik to‘liq tavsifi bo‘lib, uning asosida alohida qurilmalar xavfsizligining lokal siyosati qurilishi mumkin.

Xavfsizlikning lokal siyosati axborot xavfsizligining qandaydir servisini amalga oshiruvchi har qanday himoyalash vositasiga zarur hisoblanadi. An’anaviy yondashishda ma’murga har bir himoya vositasini alohida sozlashga yoki eng oddiy sozlashni uzellarning katta soniga qaytarishga (replikasiyalashga) to‘g‘ri kelar edi. Ravshanki, bu ma’murlashning katta sonli xatoligiga olib kelar va natijada korporativ tarmoqning himoyalanish darajasi jiddiy pasayar edi.

Ma’mur tomonidan xavfsizlikning global siyosati shakllantirilganidan so‘ng boshqarish markazi uning asosida har bir himoya vositasi uchun avtomatik tarzda himoyalashning alohida lokal siyosatini hisoblaydi va mos himoya vositasining boshqarish moduliga zaruriy sozlashlarni avtomatik tarzda yuklaydi.

Tarmoqda xavfsizlikning global siyosatini va muayyan qurilmada xavfsizlikning lokal siyosatini amalga oshirish qoidalarining bir-biridan farqi shundaki, xavfsizlikning global siyosatidagi qoidalarda foydalanish obyektlari va subyektlari tarmoq chegarasida ixtiyoriy ravishda taqsimlanishi mumkin, xavfsizlikning lokal siyosatidagi qoidalardan esa faqat tarmoq qurilmalaridan birining muhiti chegarasida foydalanish mumkin.

Axborot xavfsizligi vositalarini boshqarish tizimining umumiy struktura sxemasi 4–rasmda keltirilgan. Asosiy xavfsizlik vositalarining vazifalari quyidagicha. Mijoz shaxsiy kompyuterida o‘rnatilgan xavfsizlik agenti odatda «mijoz-server» ilovalarida mijoz sifatida qatnashuvchi alohida foydalanuvchini himoyalashga mo‘ljallangan.

Ilovalar serveriga o‘rnatilgan xavfsizlik agenti taqsimlangan ilovalarning server komponenti xavfsizligini ta’minlashga mo‘ljallangan. Shlyuz kompyuteriga o‘rnatilgan xavfsizlik agenti turli tarmoq xavfsizligi siyosatini muvofiqlashtirish masalasini yechgan holda, korxona ichida yoki korxonalar orasida tarmoq agentlarini ajratilishini ta’minlaydi.

Boshqarish markazi tarmoq masshtabida xavfsizlikning global siyosatini tavsiflashni, global siyosatni himoyalash qurilmasi xavfsizligining lokal siyosatiga translyasiyalashni, himoyalash qurilmasini yuklashni va tizimning barcha agentlari holatini nazoratlashni ta’minlaydi.

Boshqarish konsoli ma’mur (ma’murlar) ish joyini tashkil etishga mo‘ljallangan. GSMning har bir serveri uchun bir necha konsollar o‘rnatilishi mumkin.

Xavfsizlikning lokal agenti oxirgi qurilmada (mijozda, serverda, shlyuzda) joylashtiriluvchi dastur bo‘lib, quyidagi funksiyalarni bajaradi:

- xavfsizlik siyosati obyektlarini autentifikasiyalash, jumladan autentifikasiyalashning turli servislarini integrasiyalash;
- tizimdagi foydalanuvchini va u bilan bog‘liq xodisalarni aniqlash;
- xavfsizlik vositalarini markazlashtirilgan boshqarishni va foydalanish nazoratini ta’minlash;
- ilovalar manfaati uchun resurslarni boshqarish, tatbiqiy sath resurslaridan foydalanishni boshqarishni madadlash;
- trafikni himoyalash va autentifikasiyalash;
- trafikni filtrlash;
- xodisaviy protokollash, monitoring, xavotirli signalizasiya.

Lokal agentning markaziy elementi – xavfsizlikning lokal siyosatining prosessori (LSP processor) xavfsizlikning lokal siyosatini izohlaydi va boshqa komponentlar orasida chaqirishlarni taqsimlaydi.

Axborot xavfsizligini ta’minlash usullari va vositalarining tasnifi

Axborot xavfsizligi deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan qilingan ta’sirlardan axborot va uni qo‘llab-quvvatlab turuvchi infrastukturaning himoyalanganligi tushuniladi [5]. Bunday ta’sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo‘llab-quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin. O‘zbekiston Respublikasining 2002 yil 12 dekabrdagi №439 II sonli «Axborot erkinligi prinsiplari va

kafolatlari to‘g‘risida»gi qonunida axborot xavfsizligi axborot borasidagi xavfsizlik deb belgilangan va u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

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

Bugungi kunda axborot xavfsizligini ta’minlaydigan uchta asosiy tamoyil mavjud [6]:

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

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

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

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

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

Quyida axborot xavfsizligining asosiy tashkil etuvchilari va jihatlari keltirilgan [6]:

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

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

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

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

Axborotni muhofaza qilish – axborot xavfsizligining (ma’lumotlarning butunligi, foydalana olish va zarur bo‘lganda, ma’lumotlarni kiritish, saqlash, qayta ishlash va uzatishda foydalaniluvchi axborot va uning zaxiralari konfedensialligi) muhim jihatlarini ta’minlashga yo‘naltirilgan tadbirlar majmuidir [5].

Axborot xavfsizligi axborotni muhofaza qilishning kompleks tashkiliy-texnik chora-tadbirlari va dasturiy-apparat vositalarini o‘z ichiga oluvchi tizim bilan ta’minlanishi kerak. Davlat axborot resurslarining axborot xavfsizligini ta’minlash tizimi davlat organining o‘z axborot resurslarini muhofaza qilishga yondashuvini aks ettiruvchi xavfsizlik siyosatiga muvofiq amalga oshirilishi kerak. Xavfsiz tizimda tegishli apparat va dasturiy vositalardan foydalanib, axborotni o‘qish, yozish, hosil qilish va o‘chirish huquqiga ega shaxslar yoki ular nomidan amalga oshiradigan jarayonlar orqali axborotdan foydalana olish boshqariladi. Ma’lumki, absolyut xavfsiz tizimlar mavjud emas, lekin «ishonish mumkin bo‘lgan tizim» ma’nosidagi ishonchli tizimlardan foydalaniladi. Yetarlicha apparat va dasturiy vositalardan foydalanib, bir vaqtning o‘zida turli maxfiylik darajasidagi ma’lumotlarni foydalanuvchilar guruhi tomonidan foydalanish huquqlarini buzmagan holda qayta ishlash imkonini beruvchi tizim ishonchli hisoblanadi [7].

Axborotni muhofaza qilishning asosiy obyektlariga quyidagilar kiradi:

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

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

Axborot himoyasi turlari ikki asosiy belgiga ko‘ra tasniflanadi: birinchidan, axborot xususiyligi, aniqrog‘i qo‘riqlanadigan sirlar turiga ko‘ra; ikkinchidan, axborot himoyasi uchun qo‘llaniluvchi kuchlar, vositalar va usullar guruhlari bo‘yicha [7].

Axborotni muhofaza qilishda foydalaniladigan asosiy usullar quyidagilar hisoblanadi: yashirish, ranjirlash, noto‘g‘ri ma’lumot berish, bo‘laklash, sug‘urta qilish, hisobga olish, kodlash va shifrlash [8].

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

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

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

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

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

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

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

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

Umumiy olganda, axborot xavfsizligini ta’minlash vositalari deganda, axborotni muhofaza qilish masalalarini hal etish uchun foydalaniluvchi

muhandislik-texnik, elektr, elektron, optik va boshqa qurilma vositalar to‘plami tushuniladi [8].

Mavjud axborot xavfsizligini ta’minlash vositalarini 4 ta asosiy sinfga ajratish mumkin:

1. Tashkiliy vositalar;
2. Huquqiy vositalar;
3. Apparat-dasturiy vositalar;
4. Kriptografik vositalar.

Axborot xavfsizliginining tashkiliy vositalari axborotni himoyalash tizimlari tarkibida eng asosiysi hisoblanadi va u 50-60% ni tashkil qiladi. Tashkiliy chora-tadbirlar yuridik va jismoniy shaxslarni davlat axborot resurslarini tashkil etish, shakllantirish, ulardan foydalanish va ularni qo‘llab-quvvatlashga jalb etish tartibini boshqaradigan xatti-harakatlar va talablar ro‘yxatini o‘z ichiga olishi kerak [9].

Ular quyidagilar:

- binoni qo‘riqlashni tashkil etish;
- kompyuter tizimini qo‘riqlash;
- xodimlarni tanlash, joylashtirish va o‘rgatish;
- xizmatchilarni qimmatli axborotlarni niqoblash va tarqatmaslik majburiyatlarini yuklash;
- keluvchilar ustidan nazorat qilish;
- tizim ishdan chiqqandan keyin uning ishlash qobiliyatini tiklash rejasining mavjudligi.

Axborot xavfsizligini ta’minlashda huquqiy vosita ham muhim o‘rin egallaydi. Huquqiy vosita asosini axborotni qayta ishlash va uzatish, ulardan foydalanish qoidalariga rioya qilishni ta’minlaydigan qonunlar tashkil etadi.

Qonun hujjatlarida kuyidagi masalalar ko‘rib chiqiladi:

- kompyuter jinoyatchiligi uchun jazolash me’yorlarini ishlab chiqish;
- dasturlovchilarning mualliflik huquqlarini himoya qilish;
- axborotlashtirish sharoitlarida axborot sohasidagi huquq va erkinliklarni

himoya qilish;

- axborot xavfsizligi bo‘yicha xalqaro shartnomalarni qabul qilish va unga amal qilish me’yorlarini ishlab chiqish. Axborot xavfsizligini huquqiy ta’minlash bo‘yicha milliy huquqiy normativ asosni rivojlantirish va takomillashtirish to‘g‘risida farmon, qaror hamda qonunlar qabul qilingan. Ushbu huquqiy hujjatlar O‘zbekiston Respublikasining axborot xavfsizligini ta’minlash maqsadlari, vazifalari, tamoyillari va asosiy yo‘nalishlarini o‘zida mujassam etgan. Bu O‘zbekiston Respublikasining axborot xavfsizligini ta’minlashda davlat siyosatini shakllantirish, axborot xavfsizligini huquqiy, metodik, ilmiy-texnik va tashkiliy jihatdan takomillashtirish bo‘yicha takliflar tayyorlash, axborot xavfsizligining maqsadli dasturlarini ishlab chiqish uchun huquqiy asos bo‘lib xizmat qiladi.

Axborot xavfsizligini huquqiy ta’minlashning asosini O‘zbekistan Respublikasi Konstitusiyasi, O‘zbekistan Respublikasi Jinoyat kodeksi normalari,
—Axborotlashtirish to‘g‘risida‖gi qonun, —Elektron raqamli imzo to‘g‘risida‖gi [1],
—Elektron tijorat to‘g‘risida‖gi va shunga o‘xshash qator qonunlarda ko‘zda tutilgan moddalar tashkil etadi.

Davlat va nodavlat tashkilotlarning axborot xavfsizligi sohasidagi sa’y-harakatlarini birlashtiradigan O‘zbekiston Respublikasining axborot xavfsizligini ta’minlash dasturining ishlab chiqilishini tashkil etish, jahon axborot tarmoqlari va tizimlarining baynalmilallashuvi hamda jahon axborot hamjamiyatiga O‘zbekistonning teng huquqli hamkorlik shartlarida qo‘shilishiga imkoniyat yaratish ham davlatning axborot xavfsizligini ta’minlash borasidagi vazifalari sirasiga kiradi.

Axborot xavfsizligini ta’minlashning 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 tarkibiga kiritilishi bilan belgilanadi [10].

Axborot xavfsizligini ta’minlashning asosiy apparat vositalariga quyidagilarni kiritish mumkin:

- foydalanuvchini identifikasiyalovchi 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).

Axborot xavfsizligini ta’minlashning 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 (signalizasiya beruvchi) qurilmalar va boshqalar.

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.

Axborotlarni muhofaza qilishning dasturiy vositalari deganda, faqatgina axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlar tushuniladi [10].

Axborotlarni muhofaza qilishning asosiy dasturiy vositalariga quyidagilarni kiritish mumkin:

- kompyuter tizimlarida foydalanuvchilarni identifikasiyalovchi va autentifikasiyalovchi 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. Himoyalovchi dasturiy-apparat komplekslarning ko‘pchiligi maksimal sondagi himoyalash mexanizmlaridan foydalaniladi. Bu mexanizmlarga quyidagilar kiradi [8]:

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

Foydalanishni cheklash vositalari yordamida noqonuniy foydalanishdan himoyalashning usul va vositalaridan tashqari kompyuterni himoyalash uchun quyidagi usul 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 biri ekanligini nazarda tutish lozim. Ushbu o‘zgartirishlar ro‘yxatdan o‘tkazilmagan qurilmalarni ulash yoki kompyuter tizimlarining tarkibiy vositalarini almashtirish orqali amalga oshiriladi [11].

Bunda tahdidlarni oldini olish uchun quyidagi usullardan foydalaniladi:

- qurilmaning o‘ziga xos xususiyatlarini tekshirish;
- qurilmalarni identifikasiyalashdan foydalanish.

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

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

Axborot xavfsizligini ta’minlashning 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 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 [12].

Kriptografik usul muhim ahamiyatga ega bo‘lib, ma’lumotlar himoyasini uzoq vaqtga saqlashni ta’minlaydigan vosita hisoblanadi. Ma’lumotlarni himoyalash vositalarini bunday taqsimlash shartli hisoblanib, amaliyotda ular

ko‘pincha: bir-birini to‘ldiradi, kompleks (ma’lumotlarni yashirish algoritmlaridan keng foydalanuvchi apparat-dasturiy modul) shaklda namoyon bo‘ladi [13].

Kriptografiya axborotni muhofaza qilish usullaridan biri hisoblanadi. Kriptografiya axborot (ma’lumotlar)ni o‘zgartirish tamoyillari, vositalari va usullarini tadqiq etadi. Bundan maqsad axborot mazmunidan ruxsat etilmagan foydalanishdan muhofazalash va uni buzishni bartaraf qilish. Kriptografiya ma’lumotlarni aloqa kanallari orqali uzatishda yoki saqlashda konfedensiallikni yoki haqiqiylikni ta’minlash usullari bilan shug‘ullanadi. Shu bilan birga, kriptografiya ma’lumotlarni xabardor bo‘lmagan shaxslar uchun tushuna olmaydigan qilish maqsadida o‘zgartirish usuli hamdir. U ma’lumotlar xavfsizligi tizimining muhim tarkibiy bo‘lagi. Uning mohiyati ma’lumotlarni uzatishdan oldin ma’nosiz belgilar yoki signallar jamlanmasiga aylantirish va ma’lumotlarni oluvchi qabul qilib olgandan so‘ng, ularni dastlabki shakliga qayta tiklashdir.

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

Zamonaviy kriptografiya axborot xavfsizligining konfedensiallik, butunlik, autentifikasiya va tomonlarning mualliflikni inkor eta olmasliklari muammolarini hal etuvchi bilim sohasi hisoblanadi [14]. Konfedensiallikni ta’minlash deganda axborot bilan tanishish huquqi bo‘lmagan shaxslardan bu axborotni himoyalash tushuniladi.

Raqib tomonidan nazoratda bo‘lgan aloqa kanali orqali uzatiladigan xabarning konfedensialligini ta’minlash muammosi kriptografiyaning an’anaviy masalalaridan hisoblanadi.

Butunlikni ta’minlash deganda axborotni ruxsatsiz o‘zgartirib bo‘lmasligining kafolati tushuniladi [15]. Butunlikni kafolatlash uchun ma’lumotlar bo‘yicha biron-bir o‘zgartirishlarni amalga oshirishni aniqlaydigan sodda va ishonchli mezon bo‘lishi kerak. Bu o‘zgartirishlar matnni o‘chirish, almashtirish, yangisini qo‘yish orqali amalga oshirilishi mumkin. Axborot butunligini nazorat qilishning ko‘proq maqbul bo‘lgan metodlaridan biri xesh-funksiyadan foydalanish hisoblanadi. Xesh-funksiyaning qiymatini uning kalitini bilmasdan turib qalbakilashtirib bo‘lmaydi, shu sababli xeshlash kalitini shifrlangan ko‘rinishda yoki jinoyatchining «qo‘li yetmaydigan» joydagi xotirada saqlash kerak.

Autentifikasiyalashni ta’minlash axborotli o‘zaro munosabat jarayonida axborotning o‘zini va tomonlarning haqiqiyligini tasdiqlash usullarini ishlab chiqishni anglatadi. Aloqa kanali orqali uzatilayotgan axborot manbasi, yaratilgan sanasi, tashkil etuvchi ma’lumotlari, uzatish sanasi va shu kabilar bilan autentifikasiya qilinishi kerak.

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

Yuqorida keltirilgan axborotni himoyalash vositalari va usullari bilan bir qatorda axborot xavfsizligini ta’minlovchi amaliy vositalarni qo‘llash ham yaxshi samara beradi. Bunday amaliy vositalar qatoriga brandmauyerlarni o‘rnatish, zaif joylarni skanerlab turish, parol ochuvchi maxsus dasturlarni ishlatib turish kabi vositalar kiradi. 1–rasmda axborot xavfsizligini ta’minlash vositalarining tasnifi keltirilgan.

Umuman olganda, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash kompyuter bezorilari tomonidan uyushtirilgan hujum va xavflarni boshqarish holatlarini tahlil qilish va ularning oldini olish vositalarini ishlab chiqishni taqozo etadi.

1.2-§. Axborot xavfsizligini ta’minlashning dasturiy vositalariga qo‘yiladigan talablar

Axborot xavfsizligini ta’minlashning dasturiy-apparat vositalari – axborotni muhofaza qilish funksiyalarini (foydalanuvchilarni identifikasiyalash va autentifikasiya qilish, resurslardan foydalana olishni cheklash, voqyealarni qayd qilish, axborotni kriptografik himoyalash va shu kabilar) bajaradigan (mustaqil yoki boshqa vositalar bilan birgalikda) turli elektron qurilmalar va maxsus dasturlardir.

Axborot xavfsizligini ta’minlashning apparat vositasi - bu, maxsus himoya qurilmasi yoki axborotni qayta ishlash texnik vositasining komplektiga kiruvchi moslama.

Axborot xavfsizligini ta’minlashning dasturiy vositalari axborotlar xavfsizligini taminlashga 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 [14].

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.

Davlat organlarining axborot tizimlarida qo‘llanadigan axborotlarni xavfsizligini ta’minlashning dasturiy-apparat vositalari lisenziyalangan, sertifikatlangan bo‘lishi va quyidagilarni:

- himoya qilinadigan axborot resurslarni identifikasiyalashni;
- axborot tizimidan foydalanuvchilarni autentifikasiya qilishni;
- tizimda aylanayotgan axborotlarning maxfiyligini;
- autentifikasiyalangan ma’lumot almashinuvini;

- axborotlarni shakllantirish, uzatish, foydalanish, ishlash va saqlashda ma’lumotlarning butligini;
- normal foydalanish sharoitlarida tizimdagi barcha resurslardan ruxsat bilan foydalanishni;
- foydalanuvchilarning axborot izimi resurslaridan foydalanishi chegaralanishini;
- boshqaruvni (axborot tizimlari resurslaridan foydalanish huquqlarini belgilash, ro‘yxatga olish daftarlaridagi axborotlarni ishlash, himoya tizimini o‘rnatish va olib tashlash);
- foydalanuvchilarning tizimga kirish va chiqish bo‘yicha harakatlarini hamda kirish huquqlarini buzishga urinishlarini qayd etishni;
- axborot xavfsizligini ta’minlash tizimining butligi va ish qobiliyatini nazorat qilishni;
- axborot xavfsizligi bo‘yicha xavflarni aniqlash va oldini olishni;
- favqulodda vaziyatlarda tizimning xavfsiz va uzluksiz ishlashini ta’minlashi kerak.

Axborot tizimlarining dasturiy-apparat ta’minoti xavfsizlik va axborot muhofazasi bo‘yicha qonun hujjatlarida belgilangan tartibda davriy attestasiyadan o‘tishi lozim.

Axborot xavfsizligini ta’minlash, ya’ni tashqaridan begonalarning kirishini va axborotni o‘g‘irlanishining oldini olish uchun server xonalarga quyidagi talablar qo‘yiladi:

- mustahkam devorlar, ishonchli to‘siqlar va panjaralar;
- maxsus kodli yoki boshqa turdagi ishonchli qulflar bilan jihozlangan mustahkam eshiklar;
- tashqi kuzatuvga qarshi himoya vositalari;
- yong‘in xavfsizligi va qo‘riqlash signalizasiyasining mavjudligi.

Serverlarni tashqi ta’sirdan himoyalash uchun tarmoqlararo ekranlar hamda axborotni muhofaza qiluvchi lisenziyalangan apparat va dasturiy vositalar o‘rnatilishi kerak [16].

Axborotlar almashinuvi qatnashchilarini autentifikasiya qilish va axborot tizimlarini parol va antivirus bilan himoyalash choralari ko‘rilishi kerak.

Kompyuter va boshqa jihozlar ishdan chiqqan hollarda, uzilishsiz faoliyat yuritishini ta’minlash maqsadida tizimning zaxira tiklanish rejasi hamda zarur dastur va vositalar bo‘lishi kerak.

Server va eng muhim kompyuterlarni elektr energiyasi bilan uzilishlarsiz ta’minlash uchun uzluksiz elektr ta’minoti qurilmalari (UPS) va dizel-generator bo‘lishi kerak.

Axborot xavfsizligini taminlashning dasturiy va dasturiy-apparat vositalaridan foydalanishga qo‘yiladigan asosiy talablar esa quyidagilardan iborat. Xavfsizlik modelini to‘g‘ri tanlash operasion tizim (OT) mutaxassislarinigina emas, xavfsizlik bo‘yicha mutaxassislarning asosiy vazifasi hisoblanadi. Hozirda mavjud standartlar modellarning majburiy ro‘yxatini faqat ikki model, ya’ni foydalanish huquqini boshqarishning diskret va mandatli turlari bilan cheklaydi. Ko‘p hollarda ushbu ikki modelning qo‘llanilishi yetarli hisoblanadi.

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

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

2. Obyektlar va subyektlarning ishonchli identifikasiyalash va autentifikasiyalashdan o‘tkazish. Ushbu muammo texnik xarakterga ega. Hozirda, ishonchli identifikasiyalashni va berilgan aniqlikda autentifiksiyalashni ta’minlaydigan tizimlar mavjud. Identifikasiyalashning ishonchliligi foydalanilayotgan belgilarning noyobligi (unikalligi) bilan, autentifikasiyalashniki esa - qalbakilashtirishning qiyinligi bilan ta’minlanadi. Foydalanuvchilarni identifikasiyalash va autentifikasiyalashni ishonchli algoritmlarini qo‘llash uchun maxsus apparat vositalar - magnit kartalar, foydalanuvchining fiziologik kattaliklari (barmoq izlari, ko‘z to‘r pardasi va hokazo)ni o‘quvchi qurilmalar zarur. Ushbu usullarni dasturiy jihatdan ixtiyoriy mavjud tizimlarga joriy etish mumkin. Subyektlar va obyektlarning dasturiy (inson ishtirokisiz) identifikasiyalash va autenfikasiyalash uchun keyingi paytlar keng qo‘llanilayotgan

elektron imzodan foydalanilmoqda. Identifikasiyalash va autenfikasiyalashning muayyan bir mexanizmi, qurilmasi va vositasini tanlash muayyan tizimga qo‘yiladigan talablardan kelib chiqadi va axborot xavfsizligini ta’minlashda qo‘llanilayotgan boshqa qarorlarga bog‘liq bo‘lmagan holda amalga oshirilishi mumkin. Xavfsizlikni ta’minlash tizimini dasturiy amalga oshirishdagi xatoliklarni kamaytirish yoki to‘liq bartaraf etilishiga erishish. Boshqa dasturiy ta’minotlar singari himoyalashning usul va vositalari ham joriy etish xatoliklaridan holi emas. Himoya tizimining ixtiyoriy tashkil etuvchisidagi biror xatolik butun tizimning xavfsizligini shubha ostida qoldirishi tabiiydir. Shu sababli xavfsizlikka javobgar bo‘lgan dasturiy ta’minotdagi xatoliklar nafaqat o‘z vazifasini bajara olmay qoladi, balki butun tizimni izdan chiqaradi. Ushbu muammoni hal etilishiga qaratilgan chora-tadbirlar dasturlash texnologiyasi va OTning ishonchlilik sohasiga taalluqli bo‘ladi.

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

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

5. Administrasiyalashdagi xatoliklarni minimumga keltirish. Ushbu muammo inson faktori bilan bog‘liqligi sababli sof texnik vositalar yordamida hal

etila olmaydi. Shu kabi xatoliklarni vujudga kelish ehtimolligini kamaytirish uchun xavfsizlikni boshqarish va foydalanishga ruxsat berishni nazorat qilish vositalarini qulay va ishlashga oson bo‘lgan interfeys bilan ta’minlash lozim, hamda imkoniyatga qarab boshqaruvning avtomatlashtirilgan tizimidan foydalangan ma’qul. Bundan tashqari, hisoblash tizimi konfigurasiyasini administrasiyalashning adekvat emasligini tekshiradigan verifikasiyalovchi vositalarning qo‘llanilishi ham nazarda tutilishi mumkin.

Ma’lumotlar bazasida axborotlarni qayta ishlash jarayonini himoyalash, fayldagi ma’lumotlarni himoyalashdan farq qiladi va quyidagi o‘ziga xos xususiyatlarga ega:

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

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

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

Zamonaviy ma’lumotlar bazasida ma’lumotlardan foydalanishga ruxsat berishni cheklash, ma’lumotlarning fizik butunligini va mantiqiy saqlanganlik masalasi yetarli darajada muvaffaqiyatli hal etilgan [17]. Hozirda foydalanuvchi tomonidan ma’lumotlar bazasi yozuvlaridan va yozuv maydonlaridan foydalanishga ruxsatni cheklash algoritmlaridan unumli foydalanilmoqda, ushbu himoyani jinoyatchi zararlovchi dasturlarni joriy etish yoki foydalanuvchi huquqlarini qalbakilashtirish yordamida yengib o‘tishi mumkin. Ma’lumotlar bazasi faylidan va bazaning qismlaridan foydalanishga ruxsat berish ma’lumotlar bazasini boshqarish tizimi tomonidan, foydalanuvchining huquqlarini belgilab berish va ruxsat berilishi kerak bo‘lgan obyektlardan foydalanishga ruxsat berish huquqlarini nazorat qilish yo‘li bilan amalga oshiriladi.

Foydalanuvchi huquqlari ma’lumotlar bazasini boshqarish tizimi administratori tomonidan belgilanadi. Odatda, foydalanuvchining standart

identifikatori bo‘lib, shifrlangan ko‘rinishda uzatiladigan parol hisoblanadi. Taqsimlangan KTda foydalanuvchining haqiqiyligini tasdiqlash jarayoni, masofaviy jarayonlarni o‘zaro autentifikasiyalash kabi maxsus prosedura bilan to‘ldiriladi [11].

Axborot xavfsizligiga potensial tahdidlarning juda xilma-xilligi, axborotni himoyalash maqsadiga faqat axborotni himoyalashning kompleks tizimini (AHKT) yaratish yo‘li bilan erishish mumkin. Bunda yagona belgilangan maqsad va kompyuter tizimida axborotni zarur samaradorlikda himoyasini ta’minlash uchun birlashtirilgan usul va vositalar majmui tushiniladi [14].

Axborotni himoyalashning kompleks sitemasiga asosiy talablar:

- Axborot xavfsizligini ta’minlashning qoida va mavjud qonunlar talablari, standartlari va normativ-metodik hujjatlari asosida yaratish;
- Kompyuter tizimining himoyasi uchun dasturiy-texnik vositalar va tashkiliy choralar kompleksini qo‘llash;
- Ishonchlilik, maxsuldorlik, konfigurasiyalanuvchanlik;
- Iqtisodiy maqsadga muvofiqlik (AHKT narxi kompyuter tizimi narxi ichiga kiradi, himoya vositasi narxi axborotni yo‘qotishdan keladigan zarardan yuqori bo‘lmasligi lozim);
- Kompyuter tizimida axborotni qayta ishlash hayot siklining barcha darajalarini bajarish (shu bilan birga ta’mirlash va reglamentlash ishlarini olib borishda);
- Takomillashish imkoniyati;
- Buzg‘unchining e’tiborini yolg‘on axborotga qaratib, maxfiy axborotdan foydalanishni belgilash (faqat passiv emas aktiv himoyani ham ta’minlash);
- Himoyalanmagan kompyuter tizimlari bilan o‘zaro aloqani, o‘rnatilgan foydalanishlarni belgilash qoidalariga binoan amalga oshirilishi;
- Kompyuter tizimida axborot xavfsizligini buzilish hollarini tekshirish va hisob olib borishni ta’minlash;
- Foydalanish uchun murakkablik (unda ruxiy qarshi harakat va uning

vositalarini qo‘llamasdan kifoyalanishga urinishlarni uyg‘otmasligi lozim);

- Uni qo‘llashning samaradorligini baholash imkoniyati.

Kompyuter tizimining himoyalanganligiga talablarning asosiy darajalari birinchi marta 1985 yil AQSh ning ―Trusted Computer System Evaluation Criteria‖ (―Kompyuter tizimlari xavfsizligini baholashning darajalari‖, yoki ―Olov rang kitob‖) Mudofaa vazirligi hujjatlarida ta’riflangan [12]. Bu hujjatda talablarning uch asosiy darajasi keltirilgan.

1. Siyosat:

- Xavfsizlikni ta’minlashning yaqqol va yaxshi belgilangan siyosatiga egalik;

- Kompyuter tizimlaridan foydalanishni boshqarish uchun kompyuter tizimi obyektlarini markirovkalashdan foydalanish.

2. Hisobot berishga majburlik:

- Kompyuter tizimi subyektlarining individual identifikasiyasi;

- Audit axborotini saqlanishi va himoyasi.

3. Kafolatlar:

- 1 va 2 darajalardagi talablarning bajarilishiga kafolat olish uchun kompyuter tizimi tarkibiga dasturiy-apparat vositalarining qo‘shilishi;

- Kompyuter tizimlarida axborot xavfsizligini ta’minlash vositalarining ularga egalik qilish va (yoki) ruxsatsiz o‘zgartirishdan doimiy himoyalanganligi.

―Olov rang kitob‖da kompyuter tizimining himoyalanganligining yettita sinfi keltirilgan edi – minimal himoyadan (D1 sinfi) verifikasiyalangan (rasmiy isbotlangan) himoyagacha (A1 sinfi). ―Olov rang kitob‖ talablari loyihachilar, ishlab chiqaruvchilar (dasturchilar), shunga o‘xshash tizim foydalanuvchilari va ularni sertifikatlash mutaxassislari tomonidan hisoblab chiqilgan, kompyuter tizimi xavfsizligining yagona standartini yaratishga birinchi urinishga sabab bo‘ldi.

Bu standartning farqlanuvchi jihati, davlat (birinchi navbatda harbiy) tashkilotlari va operasion tizimlariga mo‘ljallanganligi.

Hisoblash texnikasi vositalarini va avtomatlashtirilgan tizimlarni ruxsatsiz foydalanishdan himoyalash bo‘yicha boshqaruvchi hujjatlar to‘plami birinchi marta 1992 yilda Rossiyaning Gostexkomissiyasi tomonidan nashr qilindi.

1.3-§. Aloqa tarmoqlarida xavf-xatarlarni tahlillash va boshqarish.

Xavf-xatarlarni tahlillash va boshqarish axborot tizimidagi taxdidlar, zaifliklar va xavf-xatarlarni baholash, hamda ushbu axborot tizimi xavfsizligining etarli darajasini ta’minlovchi qarshi choralarni aniqlash uchun ishlatiladi.

Xavf-xatarlarni tahlillash-taxdidlarni, zaifliklarni va korporativ axborot tizimi xavfsizligiga bo‘lishi mumkin bo‘lgan zararlarni aniqlash jarayoni. Xavf-xatarlarni tahlillashdan maqsad mavjud xavf-xatarlarni aniqlash va ular me’yorini baholash (ularga miqdoriy baho berish). Xavf-xatarlarni tahlillash kompyuter axborot tizimi xavfsizligini tekshirish bo‘yicha tadbirni o‘z ichiga oladi. Bu tadbirga binoan qaysi resurslarni qaysi taxdidlardan himoyalash zarurligi hamda u yoki bu resurslar qanday darajada himoyaga muhtoj ekanligi aniqlanadi.

Xavf-xatarlarni tahlillashga turli yondashishlar mavjud. Yondashishni tanlash tashkilotda axborot xavfsizligi rejimiga quyiladigan talablar darajasiga va e’tiborga olinuvchi taxdidlar xarakteriga (taxdidlar ta’siri spektriga) bog‘liq. Talablarning ikkita darajasi farqlanadi:

- axborot xavfsizligi rejimiga minimal talablar;
- axborot xavfsizligi rejimiga oshirilgan talablar.

Axborot xavfsizligi rejimiga minimal talablar axborot xavfsizligining bazaviy darajasiga mos keladi. Bu darajadan, odatda, namunaviy loyiha echimlarida foydalaniladi. Xavf-xatarlarni tahlillash soddalashtirilgan sxema bo‘yicha o‘tkaziladi: xavfsizlikka taxdidlarning ko‘p tarqalgan nabori ularning ehtimolligini baholamasdan ko‘riladi. Viruslar, asbob-uskunalarning buzilishi, ruxsasiz foydalanish va h. kabi ehtimolligi yuqori tahdidlarning minimal nabori ko‘riladigan qator standartlar va spesifikasiyalar mavjud. Bunday tahdidlarni betaraflashtirish uchun ularning amalga oshirilishi ehtimolligi va, resurslarning

zaifligidan qat’iy nazar, qarshi choralar ko‘rilishi lozim, ya’ni bazaviy darajada taxdidlar xarakteristikalarini ko‘rish shart emas.

Axborot xavfsizligi rejimiga oshirilgan talablar, axborot xavfsizligi rejimining buzilishi og‘ir oqibatlarga sabab bo‘lganida va axborot xavfsizligi rejimiga minimal talablar etarli bo‘lmaganida ishlatiladi.

Axborot xavfsizligi rejimiga oshirilgan talablarni ta’riflash uchun resurslar ahamiyatini aniqlash, tadqiqlanuvchi axborot tizimi uchun dolzarb bo‘lgan taxdidlar ruyxati bilan standart naborni to‘ldirish, tahdidlar ehtimolligini baholash va resurslar zaifligini aniqlash zarur.

Xavf-xatarni tahlillash jarayonini quyidagi bosqichlarga ajratish mumkin:

- korporativ axborot tizimining tayanch resurslarini identifikasiyalash;
- u yoki bu resursning muhimligini aniqlash;
- tahdidlarning amalga oshirilishiga imkon beruvchi mavjud xavfsizlik taxdidlarni va zaifliklarni identifikasiyalash;
- xavfsizlikka taxdidlarni amalga oshirilishi bilan bog‘liq xavf-xatarlarni hisoblash.

Resurslar uchta kategoriyaga – axborot resurslariga, dasturiy ta’minotga va texnik vositalarga (fayl serverlari, ishchi stansiyalar, ko‘priqlar, marshrutizatorlar va h.) bo‘linadi. Har bir kategoriya ichida resurslarni sinflarga va qism sinflarga ajratish mumkin. Faqat korporativ axborot tizimi funksionalligini belgilovchi va xavfsizlikni ta’minlash nuqtai nazaridan muhim bo‘lgan resurlar identifikasiyalanishi lozim.

Resursning muhimligi (narhi) bu resursning konfidensialligi, yaxlitligi yoki foydalanuvchanligi buzilganida etkazilgan zarar miqdori bilan belgilanadi. Resurslar narxini baholashda resurslarining har bir kategoriyasi uchun bo‘lishi mumkin bo‘lgan zarar miqdori belgilanadi. Namunaviy xavfsizlik taxdidlariga korporativ axborot tizimi resurslariga lokal masofadan xujumlar, tabiiy ofat, xodimlar xatosi, dasturiy ta’minotdagi xatolik yoki apparaturaning nosozligi sabab bo‘luvchi korporativ axborot tizim ishidagi buzilishlar taalluqli. Taxdid darajasi deganda uning amalga oshirilishi ehtimolligi tushuniladi.

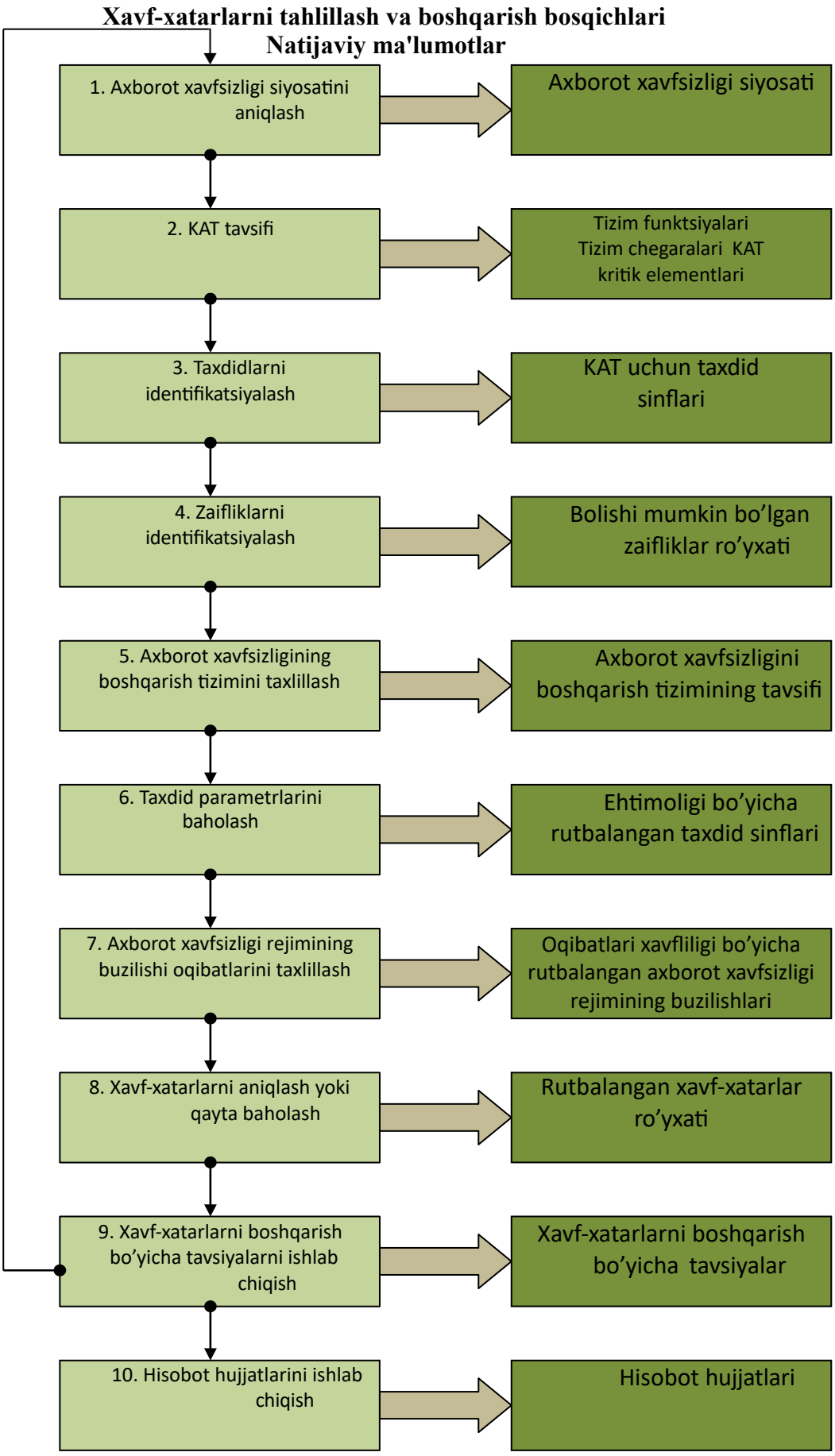
Himoyaning bo‘shligi korporativ axborot tizimidagi zaifliklarga sabab bo‘ladi. Zaifliklarni baholash xavfsizlik taxdidlarining muvaffaqiyatli amalga oshirilish ehtimolligini aniqlashni nazarda tutadi. Shunday qilib, zarar etkazish ehtimolligi taxdidlarning amalga oshirilishi ehtimolligi va zaiflik miqdori orqali aniqlanadi.

Xavf-xatar darajasi resurs narxi, taxdid darajasi va zaiflik miqdori asosida aniqlanadi. Resurs narxi, taxdid darajasi va zaiflik miqdori oshishi bilan xavf-xatar darajasi ham oshadi. Xavf-xatarlar darajasini baholash asosida xavfsizlik talablari belgilanadi.

Xavf-xatarlarni boshqarish masalasi, xavf-xatar darajasini maqbul miqdorgacha kamaytirishga imkon beruvchi qarshi choralarni asosli tanlashni va amalga oshirish narxini baholashni o‘z ichiga oladi. Tabiiyki, qarshi choralarni amalga oshirish narxi bo‘lishi mumkin bo‘lgan zarar miqdoridan kam bo‘lishi kerak. 3-rasmda xavf-xatarlarni boshqarish texnologiyasining bosqichlari keltirilgan.

Axborot xavfsizligi siyosatini aniqlash. Bu bosqichda axborot xavfsizligi sohasidagi qo‘llanma-xujjatlar, standartlar, axborot xavfsizligining asosiy qoidalari, xavf-xatarlarni boshqarishga yondashishlar aniqlanadi hamda qarshi choralar strukturizasiyalanadi va korporativ axborot tizimini sertifikasiyalash tartibi belgilanadi.

Korporativ axborot tizimini (KAT) tavsiflash. Ushbu bosqichda axborot xavfsizligi sohasidagi halqaro, davlat va kor3porativ standartlarga binoan korporativ axborot tizimning funksional vazifalari tavsiflanadi.



4–rasm. Xavf-xatarlarni boshqarish texnologiyasining varianti

Kompaniyaning kritik axborot resurslari, jarayonlari va servislari tavsiflanadi; korporativ axborot tizimining chegaralari hamda boshqarish va ma’lumotlar bo‘yicha eng muhim komponentlarining tarkibi va bog‘lanishlari aniqlanadi.

Taxdidlarni identifikasiyalash. Ushbu bosqichda taxdidlar ruyxati tuziladi va ularning darajasi baholanadi. Bunda turli tashkilotlarning taxdidlar sinflari ro‘yxatidan ham berilgan taxdidni amalga oshirish ehtimolligining reytingi yoki o‘rtacha qiymatidan foydalanish mumkin.

Zaifliklarni identifikasiyalash. Ushbu bosqichda berilgan korporativ axborot tizimining zaifliklari ro‘yxati, ularning amalga oshirilishidagi joiz natijalar ko‘rsatilgan holda tuziladi. Mavjud korporativ axborot tizimi uchun ro‘yxatlar qator manbalardan foydalanilib tuziladi. Bu manbalarga zaifliklarni tarmoq skanerlari, turli tashkilotlarning zaifliklar katalogi, xavf-xatarlarni tahlillovchi ixtisoslashtirilgan usullar kiradi.

Korporativ axborot tizimining boshqarish tizimini tahlillash. Ushbu bosqichda boshqarish, tizimi, aniqlangan taxdidlarga va zaifliklarga joiz bo‘lgan ta’sir nuqtai nazaridan tahlillanadi.

Taxdidlar parametrlarini baholash. Ushbu bosqichda xodisaga olib keluvchi zaiflikning amalga oshirilishi imkoniyati baholanadi. Baholashning namunaviy shkalasi – bir necha rutbali (masalan, past, o‘rta, va yuqori sath) sifatiy (balli) shkaladir. Bunday baho ekspert tomonidan mavjud obektiv faktorlarni hisobga olgan holda beriladi.

Axborot xavfsizligi rejimining buzilishi oqibatlarini tahlillash. Ushbu bosqichda axborot xavfsizligi rejimining buzilishi bahosi aniqlanadi. Buzilish oqibatlari moliyaviy yo‘qotishlarga, obro‘sizlanishga, rasmiy strukturalar tomonidan ko‘ngilsizliklarga va h. sabab bo‘lishi mumkin. Buzilish oqibatlarini baholash uchun mezonlar tizimi tanlanadi va oqibatlar og‘irligini baholash uchun integrasiyalangan shkala belgilanadi. Xavf-xatarlarni baholash. Ushbu bosqichda axborot resurslari xavfsizligining buzilishi xavf-xatar darajasi baholanadi. Xavf-xatar darajasi qiymati taxdidlar, zaifliklar darajasiga va bo‘lishi mumkin bo‘lgan

oqibatlar og‘irligiga bog‘liq. Xavf-xatarlarni baholashda sifatiy va miqdoriy usullardan foydalaniladi. Sifatiy usul ishlatilganda axborot xavfsizligi buzilishining bo‘lishi mumkin bo‘lgan xavf-xatarlar xavfliligi darajasi bo‘yicha rutbalanishi lozim. Miqdoriy usul ishlatilganda xavf-xatarlar miqdoriy shkalalarda baholanishi mumkin. Bu tavsiya etilayotgan qarshi choralarning narhi/samaradorligini tahlillashni osonlashtiradi. Ammo bu holda dastlabki ma’lumotlarni o‘lchash shkalalariga va ishlatilayotgan modelning adekvatligiga juda yuqori talablar quyiladi. Oddiy holda xavf-xatarni baholashda ikkita omil-xodisa extimolligi va bo‘lishi mumkin bo‘lgan oqibatlar og‘irligi ishlatilishi mumkin.

Xavf-xatarlarni boshqarish bo‘yicha tavsiyalarni ishlab chiqish. Ushbu bosqichda turli sathlar (tashkiliy, dasturiy-texnik) va xavfsizlikning alohida jihatlari bo‘yicha strukturizasiyalangan qarshi choralarning kompleksi tavsiya etilishi lozim. Taklif etiluvchi qarshi choralar kompleksi xavf-xatarlarni boshqarishning tanlangan strategiyasiga binoan quriladi.

Hisobot xujjatlarni ishlab chiqish. Ushbu bosqichda xavf-xatarlarni tahlillash va boshqarishning barcha bosqichlari bo‘yicha ish natijalari akslantirilgan hisobot xujjatlari tayyorlanadi.

Ta’kidlash lozimki, hozirda axborot xavf-xatarlarini baholashni avtomatlashtirish maqsadida dasturiy mahsulotlar ishlab chiqilgan.

Aloqa tarmoqlarida foydalanuvchi axborotlarini axborot xavfsizligini ta’minlash usullari va vositalarining tasnifi

Hozirgi kunda O‘zbekiston Respublikasida zamonaviy axborot texnologiyalari, kompyuter texnikasi va telekommunikasiya vositalarini jamiyatning barcha sohalariga joriy etish, hamda ulardan foydalanish, fuqarolarning axborotga ortib borayotgan talab-ehtiyojlarini yanada to‘laroq qondirish, jahon axborot jamiyatiga kirish, hamda jahon axborot resurslaridan foydalanishni kengaytirish uchun qulay shart – sharoitlar yaratilmoqda. Kompyuter tarmoqlarida almashinadigan elektron ma’lumotlarni buzg‘unchilardan himoyalash va tarmoqlarda maxfiy ma’lumotlar almashish uchun muhofazalangan kanalni tashkil etish muhim masalalardan biri hisoblanadi [5].

Internet rivojlanishi davomida individual va korporativ foydalanuvchilarning elektron aloqalari shakllandi. Internet ayniqsa alohida shaxslarga ham foydalanish imkoniyatini yaratdi. Milliy, shaxsiy va korporativ kompyuter tarmoqlarining yagona Internet tarmog‘iga birlashishi tarmoq xizmatlarining rivojlanishiga qattiq turtki berdi va u elektron xizmat biznesini rivojlanishiga va mustahkamlanishiga sezilarli ta’sir ko‘rsatdi.

Kompyuter tarmoqlarida almashinadigan elektron ma’lumotlarni buzg‘unchilardan himoyalash va tarmoqlarda maxfiy ma’lumotlar bilan almashinish uchun muxofazalangan kanalni tashkil etish muhim masalalardan biri hisoblanadi [4].

Internetdan keng foydalanishning asosiy shartlaridan biri u orqali o‘tkaziladigan barcha tranzaksiyalar uchun xavfsizlikning bir xil darajasini ta’minlash bo‘lgan va bo‘lib qoladi. Bu foydalanuvchilar o‘rtasida uzatiladigan axborotga, savdo tizimlarining ma’lumotlar bazalarida saqlanadigan axborotga, moliyaviy tranzaksiyalarga ilova qilinadigan axborotga taalluqlidir.

Axborot xavfsizligi tushunchasini axborot egalarining yoki axborotdan foydalanuvchilarning moddiy zarar ko‘rishiga olib keladigan axborotning yo‘q qilinishi, buzilishi va fosh etilishi uchun yo‘l qo‘yib bo‘lmaydigan xavflarni bartaraf etuvchi tasodifiy yoki ataylab qilingan ta’sirlarga bardosh berish holati kabi ta’riflanadi. Tarmoq tashqaridan kirish uchun to‘liq ochiq bo‘lganligi sababli ushbu usullarning ahamiyati juda katta. Xavfsizlik omillarning katta ahamiyatga egaligi Internetda o‘tkaziladigan ko‘p sonli tadqiqotlar bilan belgilanadi.

Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash deb foydalanuvchilarni ruxsasiz tarmoq elementlari va zahiralariga egalik qilishni man etishdagi texnik, dasturiy va kriptografik usul va vositalar, hamda tashkiliy tadbirlarga aytiladi [5].

Axborot xavfsizligini ta’minlash usullarini 4 ta asosiy sinfga ajratish mumkin:

1. Tashkiliy-huquqiy usullar;

2. Injener-texnik usullar;
3. Dasturiy va dasturiy-apparat usullar;
4. Kriptografik usullar.

Axborot xavfsizliginining tashkiliy-huquqiy usullari tashkiliy va huquqiy usullarni o‘z ichiga oladi. Tashkiliy chora-tadbirlar yuridik va jismoniy shaxslarni davlat axborot resurslarini tashkil etish, shakllantirish, ulardan foydalanish va ularni qo‘llab-quvvatlashga jalb etish tartibini boshqaradigan xatti-harakatlar va talablar ro‘yxatini o‘z ichiga olishi kerak. Huquqiy usullar asosini axborotni qayta ishlash va uzatish, ulardan foydalanish qoidalariga rioya qilishni ta’minlaydigan qonunlar tashkil etadi. Axborot xavfsizligini huquqiy ta’minlash bo‘yicha milliy huquqiy normativ asosni rivojlantirish va takomillashtirish to‘g‘risida farmon, qaror hamda qonunlar qabul qilingan. Ushbu huquqiy hujjatlar O‘zbekiston Respublikasining axborot xavfsizligini ta’minlash maqsadlari, vazifalari, tamoyillari va asosiy yo‘nalishlarini o‘zida mujassam etgan. Bu O‘zbekiston Respublikasining axborot xavfsizligini ta’minlashda davlat siyosatini shakl-lantirish, axborot xavfsizligini huquqiy, metodik, ilmiy-texnik va tashkiliy jihatdan takomillashtirish bo‘yicha takliflar tayyorlash, axborot xavfsizligining maqsadli dasturlarini ishlab chiqish uchun huquqiy asos bo‘lib xizmat qiladi [6].

Axborot xavfsizligini ta’minlashning injener-texnik usullari 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 asosida amalga oshiriladi. Tashkilotlarning ish faoliyatida juda ko‘p qurilmalar, telefon apparatlaridan tortib avtomatlashtirilgan tizimlargacha ishlatiladi. Texnik usullarning asosiy vazifasi – ishlab chiqarish faoliyatidagi texnik vositalar orqali ma’lumotlarning oshkora bo‘lishi, chiqib ketishi va ularga ruxsasiz kirishdan qat’iy himoya qilishdan iborat[6].

Kompyuter tarmog‘ida dasturiy himoyalanish usullariga eng avvalo himoyalangan kriptoprotokollarni kiritish mumkin. Ushbu protokollardan foydalanilganda ulanishni ishonchli himoya qilish imkoniyati paydo bo‘ladi.

Masofadan turib hujum qilishdan dasturiy himoyalanish usullarning boshqa sinfiga bugungi kundagi mavjud dasturlar kiradi. Axborotlarni muhofaza qilishning dasturiy usullari faqatgina axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlar yordamida amalga oshiriladi. Axborot xavfsizligini ta’minlashning apparat usullari keng tarqalgan. Biroq, ular etarlicha o‘zgaruvchanlikka ega bo‘lmaganligi sababli himoyalangan ishlash prinsiplarining oshkora bo‘lishi ulardan ko‘pincha kelajakda foydalanishni yo‘qqa chiqaradi. Himoyaning dasturiy usullari ishonchli bo‘lib, ularning kafolatli ishlatilishi apparat usullarga nisbatan ancha keng.

Kompyuter tarmoqlarida axborot xavfsizligi muammosini echish uchun kriptografik usullardan foydalaniladi. Kriptografiya ma’lumotlar xavfsizligini ta’minlash to‘g‘risidagi fan hisoblanadi.

Zamonaviy kriptografiya axborot xavfsizligining konfedensiallik, butunlik, autentifikasiya va tomonlarning mualliflikni inkor eta olmasliklari muammolarini hal etuvchi bilim sohasi hisoblanadi. Konfedensiallikni ta’minlash deganda axborot bilan tanishish huquqi bo‘lmagan shaxslardan bu axborotni himoyalash tushuniladi.

Raqib tomonidan nazoratda bo‘lgan aloqa kanali orqali uzatiladigan xabarning konfedensialligini ta’minlash muammosi kriptografiyaning an’anaviy masalalaridan hisoblanadi.

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

Autentifikasiyalashni ta’minlash axborotli o‘zaro munosabat jarayonida

axborotning o‘zini va tomonlarning haqiqiyligini tasdiqlash usullarini ishlab chiqishni anglatadi. Aloqa kanali orqali uzatilayotgan axborot manbasi, yaratilgan

sanasi, tashkil etuvchi ma’lumotlari, uzatish sanasi va shu kabilar bilan autitenfikasiya qilinishi kerak.

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

Shunday qilib kompyuter tarmoqlarida axborot xavfsizligini ta’minlashning asosiy kriptografik usullariga shifrlash, elektron raqamli imzo kiradi. Autentifikasiya elektron raqamli imzo va sertifikat bilan ta’minlanadi.

Butunlikni ta’minlash deganda axborotni ruxsasiz o‘zgartirib bo‘lmasligining kafolati tushuniladi. Butunlikni kafolatlash uchun ma’lumotlar bo‘yicha biron-bir o‘zgartirishlarni amalga oshirishni aniqlaydigan sodda va ishonchli mezon bo‘lishi kerak. Bu o‘zgartirishlar matnni o‘chirish, almashtirish, yangisini qo‘yish orqali amalga oshirilishi mumkin. Axborot butunligini nazorat qilishning ko‘proq maqbul bo‘lgan metodlaridan biri xesh-funksiyadan foydalanish hisoblanadi. Xesh-funksiyaning qiymatini uning kalitini bilmasdan turib qalbakilashtirib bo‘lmaydi, shu sababli xeshlash kalitini shifrlangan ko‘rinishda yoki jinoyatchining «qo‘li etmaydigan» joydagi xotirada saqlash kerak.

Autentifikasiyalashni ta’minlash axborotli o‘zaro munosabat jarayonida axborotning o‘zini va tomonlarning haqiqiyligini tasdiqlash usullarini ishlab chiqishni anglatadi. Aloqa kanali orqali uzatilayotgan axborot manbasi, yaratilgan sanasi, tashkil etuvchi ma’lumotlari, uzatish sanasi va shu kabilar bilan autentifikasiya qilinishi kerak.

Mualliflikni inkor etolmaslikni ta’minlash bu subektlar tomonidan amalga oshirilgan harakatlarni tan olmaslik holati mumkinligining oldini oladi [13].

Yuqorida keltirilgan axborotni himoyalash vositalari bilan bir qatorda axborot xavfsizligini ta’minlovchi amaliy vositalarni qo‘llash ham yaxshi samara beradi. Bunday amaliy vositalar qatoriga brandmauerlarni o‘rnatish, zaif joylarni skanerlab turish, parol ochuvchi maxsus dasturlarni ishlatib turish kabi vositalar kiradi.

Brandmauerlar (tarmoqlararo ekran) tashkilotning eng asosiy himoya vositasi bo‘lib, ular tarmoqda kiruvchi, undan chiquvchi axborot oqimini nazorat

qiladi. U axborot oqimining biror turini to‘sib qo‘yishi yoki tekshirib turishi va xakerlarning tajovuzidan saqlashi mumkin.

Axborot xavfsizligini ta’minlash vositalarini tahlil etish natijasida ularni quyidagi 5 ta sinfga ajratish maqsadga muvofiq deb topildi.

1-rasmda axborot xavfsizligini ta’minlash vositalarining turkumlanishi turlari tasvirlangan.

5-rasm. Axborot xavfsizligini ta’minlash vositalarining turkumlanishi

Niyati buzuq odamlarni yolg‘iz foydalanuvchilar emas, balki korporativ kompyuter tarmoqlari qiziqtiradi. Aynan bunday tarmoqlarda axborotning yo‘olishi, ruxsasiz modifikasiyalanishi jiddiy oqibatlarga olib kelishi mumkin.

Kompyuter tarmoqlarini himoyalash uyda foydalanuvchi kompyuterlarni himoyalashdan farqlanadi (garchi individual ishchi stansiyalarni himoyalash-tarmoq himoyasining ajralmas qismi). Chunki, avvalo, bunday masala bilan savodli mutaxassislar shug‘ullanadilar. Shu bilan birga korporativ tarmoq xavfsizligi tizimining asosini chetki foydalanuvchilar uchun ishlash qulayligi va

texnik mutaxassilarga quyiladigan talablar o‘rtasida murosaga etishish tashkil etadi.

Kompyuter tizimiga ikki nuqtai nazardan qarash mumkin: unda faqat ishchi stansiyalardan foydalanuvchilarni ko‘rish mumkin, yoki faqat tarmoq operasion tizimining ishlashini hisobga olish mumkin.

Simlar bo‘yicha o‘tuvchi axborotli paketlar majmuini ham kompyuter tarmog‘i deyish mumkin. Tarmoqni ifodalashning bir necha sathlari mavjud. Xudi shunday tarmoq xavfsizligi muammosiga turli sathlarda yondashish mumkin. Mos holda har bir sath uchun himoyalash usuli turlicha bo‘ladi. Tizimning ishonchli himoyalanishi himoyalangan sathlar soni bilan belgilanadi.

Birinchi, ko‘rinib turgan va amalda eng qiyin yo‘l-xodimlarni tarmoq xujumlarini qiyinlashtiruvchi xatti-harakatga o‘rgatish. Bu bir qarashda osonday tuyulsada, ammo mushkul ish. Internet dan foydalanishni chegaralash lozim.

Aksariyat foydalanuvchilar chegaralanishlar sababini bilmaydilar. Shuning uchun taqiqilar aniq ifodalanishi lozim.

Kompyuter tarmoqlari axborotini himoyalashga himoyalash tadbirlarining yagona siyosatini hamda huquqiy, tashkiliy-ma’muriy va injener-texnik xarakterga ega choralar tizimini o‘tkazish orqali erishiladi.

Tarmoqda axborotni himoyalashning zaruriy darajasini ishlab chiqishda xodimlar va rahbariyatning o‘zaro javobgarligi, shaxs va tashkilot manfaatlariga rioya qilish, xuquqni muhofaza qiluvchi organlar bilan o‘zaro aloqa hisobga olinadi. Raqobatli sharoitda xizmatlarning katta sonini taqdim etish va xizmat qilish vaqtini qisqartirish orqali etakchi o‘rinni saqlab qolish va yangi mijozlarni jalb etish mumkin. Bunga faqat barcha amallarni avtomatlashtirishning zaruriy darajasini ta’minlash evaziga erishish mumkin. Ayni zamonda hisoblash texnikasining ishlatilishi bilan nafaqat paydo bo‘lgan muammolar hal etiladi.

Yangi axborotni buzilishi va yo‘qotilishi, tasodifan va atayin modifikasiyalanishi hamda axborotni begonalar tarafidan ruxsasiz olinishi bilan bog‘liq no‘ananaviy tahdidlar paydo bo‘ladi.

Mavjud holatning tahlili ko‘rsatadiki, axborotni himoyalash uchun qilinadigan tadbirlar darajasi, odatda, avtomatlashtirish darajasidan past. Bunday orqada qolish jiddiy oqibatlarga olib kelishi mumkin.

Avtomatlashtirilgan komplekslarda axborotning zaifligiga hisoblash resurslarining konsentrasiyalanishi, ularning xududiy taqsimlanganligi, magnit eltuvchilarida ma’lumotlarning katta hajmini uzoq vaqt saqlanishi, ko‘pgina foydalanuvchilarning resurslardan bir vaqtda foydalanishi sabab bo‘ladi.

Bunday sharoitda himoyalash choralarini ko‘rish zaruriyatiga shubha qilmasa bo‘ladi. Ammo quyidagi qiyinchiliklar mavjud:

- hozirgi kunda himoyalangan tizimlarning yagona nazariyasi yo‘q;
- himoya vositalarini ishlab chiqaruvchilar xususiy masalalarni echish uchun asosan alohida komponentlarni tavsiya etadilar, himoyalash tizimini shakllantirish va bu vositalarning birga ishlatilishi masalalari esa iste’molchi ixtiyoriga qoldiriladi;
- ishonchli himoyani ta’minlash uchun texnik va tashkiliy muammolari kompleksini hal etish va mos xujjatlarni ishlab chiqish zarur.

Axborot xavfsizligi axborotni muhofaza qilishning kompleks tashkiliy-texnik chora-tadbirlari va dasturiy-apparat vositalarini o‘z ichiga oluvchi tizim bilan ta’minlanishi kerak. Davlat axborot resurslarining axborot xavfsizligini ta’minlash tizimi davlat organining o‘z axborot resurslarini muhofaza qilishga yondashuvini aks ettiruvchi xavfsizlik siyosatiga muvofiq amalga oshirilishi kerak. Xavfsiz tizimda tegishli apparat va dasturiy vositalardan foydalanib, axborotni o‘qish, yozish, hosil qilish va o‘chirish huquqiga ega shaxslar yoki ular nomidan amalga oshiradigan jarayonlar orqali axborotdan foydalana olish boshqariladi. Ma’lumki, absolyut xavfsiz tizimlar mavjud emas, lekin «ishonish mumkin bo‘lgan tizim» ma’nosidagi ishonchli tizimlardan foydalaniladi. Yetarlicha apparat va dasturiy vositalardan foydalanib, bir vaqtning o‘zida turli maxfiylik darajasidagi ma’lumotlarni foydalanuvchilar guruhi tomonidan foydalanish huquqlarini buzmagan holda qayta ishlash imkonini beruvchi tizim ishonchli hisoblanadi [7].

Axborot xavfsizligini ta’minlash, ya’ni tashqaridan begonalarning kirishini va axborotni o‘g‘irlanishining oldini olish uchun server xonalarga quyidagi talablar qo‘yiladi:

- mustahkam devorlar, ishonchli to‘siqlar va panjaralar;
- maxsus kodli yoki boshqa turdagi ishonchli qulflar bilan jihozlangan mustahkam eshiklar;
- tashqi kuzatuvga qarshi himoya vositalari;
- yong‘in xavfsizligi va qo‘riqlash signalizasiyasining mavjudligi.

Serverlarni tashqi ta’sirdan himoyalash uchun tarmoqlararo ekranlar hamda axborotni muhofaza qiluvchi lisenziyalangan apparat va dasturiy vositalar o‘rnatilishi kerak [16].

Axborotlar almashinuvi qatnashchilarini autentifikasiya qilish va axborot tizimlarini parol va antivirus bilan himoyalash choralari ko‘rilishi kerak.

Kompyuter va boshqa jihozlar ishdan chiqqan hollarda, uzilishsiz faoliyat yuritishini ta’minlash maqsadida tizimning zaxira tiklanish rejasi hamda zarur dastur va vositalar bo‘lishi kerak.

I bob bo‘yicha xulosa

Dissertasiya ishining birinchi bobi bo‘yicha quyidagi natijalar olindi:

1. Axborot xavfsizligi axborotni muhofaza qilishning kompleks tashkiliy-texnik chora-tadbirlari va dasturiy-apparat vositalarini o‘z ichiga oluvchi tizim bilan ta’minlanishi kerakligi bayon etildi.

2. Axborot himoyasi turlari ikki asosiy belgiga ko‘ra tasniflanishi, shuningdek mavjud axborot xavfsizligini ta’minlash vositalarini 4 ta asosiy sinfi bo‘lgan tashkiliy vositalari, huquqiy vositalari, dasturiy-apparat vositalari va kriptografik vositalari tadqiq etildi.

3. Yuqori quvvatli kompyuterlarning, tarmoq va neyron hisoblash texnologiyalarining paydo bo‘lishi avval o‘ta mustahkam, amalda yechimi yo‘q deb hisoblangan kriptografik tizimlarni obro‘sizlantirganligi sababli zamonaviy kriptografik usullardan foydalanish o‘ta dolzarb masalalardan biriga aylanganligi yoritib o‘tildi.

4. Yuqorida keltirilgan axborotni himoyalash vositalari va usullari bilan bir qatorda axborot xavfsizligini ta’minlovchi amaliy vositalarni, ya’ni brandmauyerlarni o‘rnatish, zaif joylarni skanerlab turish, parol ochuvchi maxsus dasturlarni ishlatib turish kabi vositalarni qo‘llash ham yaxshi samara berishi ko‘rib chiqildi.

5. Axborotlar almashinuvida qatnashchilarni autentifikasiya qilish va axborot tizimlarini parol va antivirus bilan himoyalash choralari ko‘rilishi kerakligi, OTda axborot xavfsizligini samarali ta’minlash uchun bajarish lozim bo‘lgan tavsiyalar keltirib o‘tildi.

6. Ma’lumotlar bazasida axborotlarni qayta ishlash jarayonini himoyalash, fayldagi ma’lumotlarni himoyalashdan farq qilishi va uning o‘ziga xos xususiyatlari, axborot xavfsizligiga potensial tahdidlarning juda xilma-xilligi, axborotni himoyalash maqsadiga faqat axborotni himoyalashning kompleks tizimini yaratish yo‘li bilan erishish mumkinligi o‘rganib chiqildi.

II BOB. INFOKOMUNIKASIYA TIZIMLARIDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING DASTURIY VOSITALARINING TAHLILI

2.1-§.Ruxsatsiz kirishlardan himoyalovchi dasturiy vositalar

Axborot tarmoqlarida keng tarqalgan axborotni himoyalashning dasturiy-apparat vositalariga quyidagilar kiradi: ―Spektr - Z tizimi; SecretNet tizimi; DAALLAS LOCK dasturiy-apparat kompleksi va boshqalar [19].

Spektr-Z – bu himoyalashning kompleks tizimi bo‘lib, Windows 95 yoki Windiws 98 operasion tizimlarining barcha versiyalarida ishlovchi IBM PC ShEXM guruhiga mansub kompyuterlarda o‘rnatiladi.

Spektr-Z tizimining asosiy imkoniyatlari:

- Keng ko‘lamdagi zamonaviy va loyihalashtirilayotgan dasturiy kompleks va ma’lumotlar bazasini ruxsatsiz kirishlardan har bir alohida loyiha doirasida himoya vositalarini ishlab chiqish kabi qo‘shimcha kuch sarflashlarsiz himoyalash, huddi alohida ishchi stansiya bazasidagi avtomatlashtirilgan tizim kabi lokal tarmoq bazasidagi avtomatlashtirilgan tizim doirasi ham;
- Internet bilan ishlashning himoyalangan ishchi o‘rnini yaratish;
- Logik disklar uchun foydalanuvchilar vakolatini (umumiy ruxsat, faqat o‘qish, o‘zgartirish rejimi, ruxsat yo‘q) boshqarishni ta’minlash;
- Ro‘yxatga olingan foydalanuvchi yo‘qligida klaviatura, monitor va sichqonchani blakirovkalash;
- Xavfsizlik admininstratori tomonidan shakllantirilib belgilangan bir qancha disketalardan foydalanishda foydalanuvchi ishini chegaralash;
- Kompyuter viruslari hujumini, dastur va ma’lumotlardagi tasodifiy yoki qasddan ma’lumotlarning buzib ko‘rsatilishini aniqlash;
- Foydalanuvchilarning kompyuterdagi ishini qayd qilish.

SecretNet tizimi Novell Netware operasion tizimi boshqaruvidagi lokal hisoblash tarmoqlarida saqlanuvchi va qayta ishlanuvchi axborotlarni himoyalash uchun mo‘ljallangan.

SecretNet tizimi quyidagilarni ta’minlaydi:

- Foydalaniluvchini autentifikasiyalash apparat vositalari nomenklaturasini

kengaytirish imkoniyatiga ega maxsus apparat vositalari (TouchMemory va SmartCard) yordamida foydalanuvchilarni autentifikasiyalash;

- Kompyuter lokal disklarida saqlanuvchi ma’lumotlardan, shuningdek turli qurilmalardan (printer, kommunikasion portlar) foydalanuvchilar foydalanishini diskresion (tanlangan) boshqarish;

- Xuddi lokal kabi, tarmoq fayllari va kataloglaridan foydalanishni konfedensiallikni uch darajasi (umumfoydalanuvchi, maxfiy va juda maxfiy)dan foydalangan holda vakolatli (mondatli) boshqarish;

- Ma’lumotlarni kriptografik himoyalash vositalarini ulash;

- Xavfsizlikka aloqador bo‘lgan tizimda sodir bo‘layotgan xodisalarning to‘liq ro‘yxatga olinishi, shu bilan birga ro‘yxatga olishni moslashuvchan holda boshqarish;

- Himoya mexanizmlarini doimiy (zarurat bo‘lganda) qo‘shish;

- Dastur ishga tushganda tarmoq resurslariga ruxsat berish vakolatlarini foydalanuvchilarga dinamik o‘zlashtirish;

- Himoya vositalarini markazlashtirilgan holda boshqarish;

- Foydalanuvchilar ishini tezkor boshqarish (monitoring);

- Operasion tizim va foydalanuvchi tomonidan foydalanilayotgan dastur yaxlitligini boshqarish;

- Sozlashlarning moslashuvchanligi va tizimni ekspluatasiyalashning odddiyligi.

DAALLASLOCK dasturiy-apparat kompleks hisoblanadi.

DAALLASLOCK 4.1 dasturiy ta’minoti quyidagilarni o‘z ichiga oladi:

- Yaxlitlikni nazorat qilish moduli;

- Ichiga o‘rnatilgan antivirus himoyasini;

- Foydalanuvchilarning ruxsat etilgan va taqiqlangan masalalar ro‘yxatini tayinlay olish imkoniyati;

- Kompyuter ma’lumotlariga ruxsatga aloqador hodisalarni ro‘yxatga olish;

- Foydalanuvchi yo‘qligida ekran va klaviaturani blakirovkalash.

DAALLASLOCK 5.0 versiyasi ixtiyoriy IBM – Windows NT Workstation operasion tizimi bilan mos keluvchi kompyuterlar bilan ishlashga mo‘ljallangan.

2.2-§.Axborot xavfsizligini ta’minlashning dasturiy-apparat vositalari.

Axborotlarning kriptografik himoya vositalari (AKHV) – apparat, dasturiy va dasturiy-apparat vositalar ko‘rinishida bo‘lishi mumkin va ular o‘zida bir yoki bir nechta kriptografik usullarni qamrab olgan bo‘lishi mumkin [8].

AKHV quyidagi asosiy vositalardan tashkil topgan:

- kriptografik dasturiy vositalar - bir yoki bir nechta kriptografik usullarni o‘zida mujassam etgan, yuqori yoki quyi dasturlash tillarida yozilgan alohida biblotekalar yoki belgilangan dasturlar to‘plami;
- kriptografik apparat vositalar – kriptografik usullarni maxsus mikrosxemalar, prosessorlar, maxsus bloklar yoki dasturiy modullarda amalga oshirilgan ko‘rinishi bo‘lib, avtomatik ravishda ishlaydi;
- kriptografik dasturiy-apparat vositalar – kriptografik himoya usullarini kompleks, ya’ni ham dasturiy ham apparat vositalar orqali amalga oshiriladi.

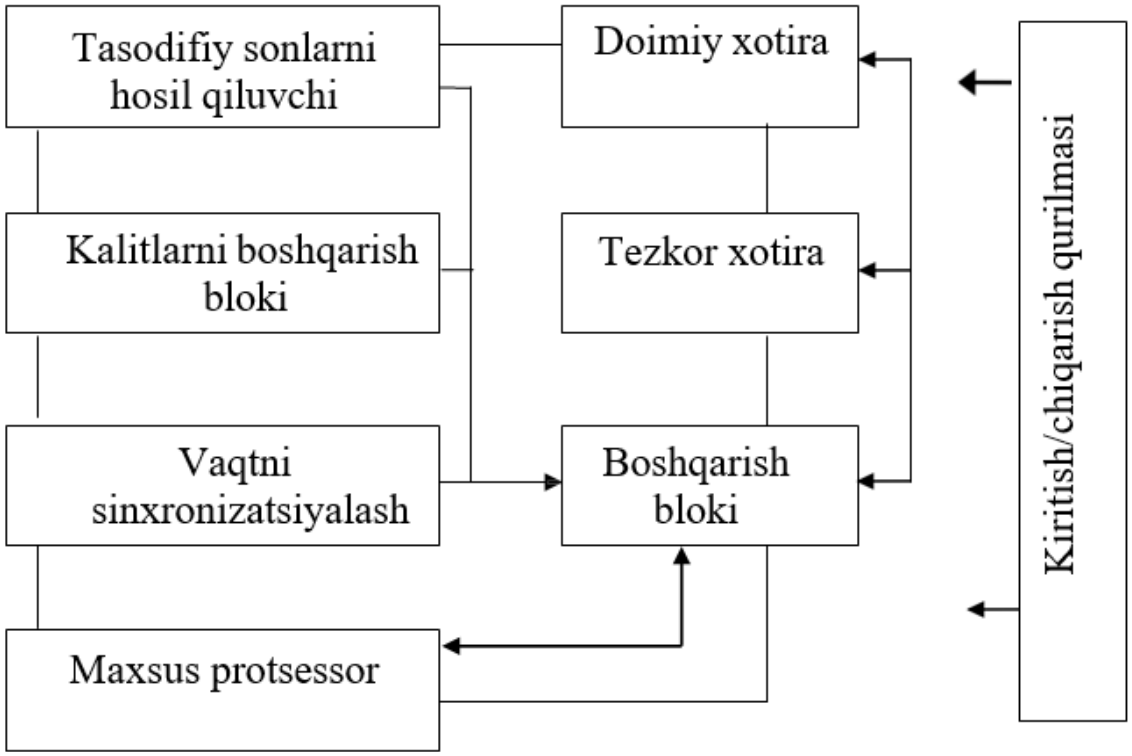
Kriptografik apparat himoya vositalar – maxsus blok bo‘lib, bu blok ma’lumotlarni shifrlash uchun foydalaniladigan qurilmalardan tashkil topgan. Kriptografik apparat himoya vositalari, shuningdek qo‘shimcha himoya funksiyalaridan iborat. Masalan, ruxsatsiz foydalanishlardan himoyalovchi funksiya. Bundan tashqari, kriptografik apparat vositalar dasturiy vositalarga talab etilmaydigan quyidagi qo‘shimcha bloklardan iborat:

- kriptografik kalitlarni boshqarish bloki;
- tasodifiy sonlarni hosil qiluvchi generator;
- xotira, doimiy va tezkor xotira;
- vaqtni sinxronizasiyalash bloki;
- xesh-qiymatni saqlovchi va nazorat qiluvchi blok.

Shuningdek apparat kriptografik himoya vositalari qo‘shimcha maxsus shifrlovchi prosessorlardan, identifikasiya, autentifikasiya va avtorizasiyani tekshiruvchi bloklardan iborat bo‘lishi mumkin. Hattoki, apparat vositalar maxsus

hisoblovchi kompyuter ham bo‘lishi mumkin. Bunda u markaziy prosessor bilan maxsus shina (tizim shinasi) orqali bog‘lanadi.

Kriptografik apparat himoya vositalar odatda kompyuterga ulanadigan plata ko‘rinishida bo‘ladi va u quyidagi bloklardan iborat bo‘ladi:



6 - rasm. Kriptografik apparat himoya vositalarining asosiy sxemasi.

Boshqarish bloki kriptografik apparat himoya vositasining turli xil bloklarini bir-biriga bog‘lash vazifasini bajaradi, ma’lumotlarni boshqaradi va tizim shinasi orqali uzatilishini ta’minlaydi.

Apparatning xotirasi ikki blokdan tashkil topgan:

- tezkor xotira – kriptografik himoya vositasining dasturiy ta’minotini, dastur tashkil etuvchilarini, o‘zgaruvchi parametrlarni o‘zida saqlaydi;
- doimiy xotira maxsus buyruqlar, himoyani amalga oshiruvchi funksiyalar va apparat AKHV dasturiy ta’minoti yuklanishlari yig‘indisi.

Bulardan tashqari qolgan manbalar qo‘shimcha ikki xotira blokida saqlanadi:

- jurnal uchun xotira;
- kalitlarni saqlash uchun xotira.

Tasodifiy sonlar generatori apparat AKHV uchun tasodifiy sonlar ketma-ketligini hosil qilib beradi. Tasodifiy sonlar generatorining apparat ko‘rinishida fizik jarayonlar orqali tasodifiy ketma-ketliklar olinadi.

Vaqtni sinxronizasiyalash bloki apparat AKHVda amallar bajarilishini nazorat qiladi, ma’lumot uzatilishini vaqt sinxronizasiyasida amalga oshiradi.

Kiritish/chiqarish bloki tashqaridan kiruvchi signalni ichki signalga aylantirib beradi. Apparat AKHV kiritish/chiqarish bloki quyidagi qurilmalar bilan bog‘liq muhim bog‘lanishlarni amalga oshiradi:

- kompyuterning tizimli shinasi yoki ma’lumotlarni uzatuvchi liniyalarda qabul qiluvchi/uzutuvchi qurilma, bu to‘g‘ridan-to‘g‘ri shifrlash uchun foydalaniladi;
- kalit ma’lumotlarni saqlovchi qurilma, ular identifikasiya/autentifikasiya jarayonlariga yordam beradi, shuningdek apparat AKHV vazifalarini nazorat qilishga yordam beradi;
- qattiq disk boshqaruvchisi va ma’lumotlarni zaxirada saqlash qurilmasi, bular ma’lumotlarni xavfsizligini ta’minlashda va zaxirada saqlashda ishlatiladi.

Shunday qilib, apparat kriptografik himoya vositalar o‘zida murakkab bo‘lgan ko‘p funksiyalarni qamrab olgan [17]. Kriptografik apparat vositalar quyidagi afzalliklarga ega:

- shifrlash algoritmini o‘zgartirib bo‘lmaslik;
- kriptografik kalitlarni hosil qilishda tasodifiy sonlar generatoridan foydalanishlik;
- shaxsiy identifikatorlardagi kalitlar bilan shifrlash to‘g‘ridan-to‘g‘ri apparatning maxsus prosessorida amalga oshirilishi;
- kalitlarni kompyuterning xotirasida emas, balki shifrlovchi prosessor xotirasida saqlanilishi;
- tizim yuklangunga qadar foydalanuvchilarni identifikasiya va autentifikasiyadan o‘tkazish imkoniyati;
- ma’lumotlarni shifrlash yuqori tezlikda amalga oshirilishi.

Dasturiy-apparat himoya vositalari dasturiy va apparat tashkil etuvchilar yig‘indisidan tashkil topgan bo‘lib, ular quyidagi tayanch modullardan tashkil topgan:

- shifrlash bloki (nosimmetrik shifrlash tizimlari dasturiy modullar, simmetrik shifrlash apparat modullar uchun), dasturiy, apparat ko‘rinishida yoki ularning kombinasiyasi asosida amalga oshiriladi;
- elektron raqamli imzo bloki;
- kalitlarni boshqarish bloki;
- identifikasiya/autentifikasiya moduli;
- tashqi interfeysni boshqarish moduli;
- tizim ishlashini nazorat etuvchi modul.

Axborotni kriptografik himoyalashning dasturiy-apparat vositalaridan biri autentifikasiya vositalari hisoblanadi [21]. Ularga quyidagilarni kiritish mumkin:

- eToken;
- USB – kalit / eToken PRO smart-kartasi;
- USB – kalit/ eToken PRO smart-kartasi (Java);
- Kombinasiyalashgan eToken NG – OTP USB – kaliti;
- Kombinasiyalashgan eToken NG - FLASH USB – kaliti;
- eToken PASS breloki va boshqalar.

eToken elektron kaliti - avtorizasiya, autentifikasiya va ma’lumotlarni himoyalangan saqlash shaxsiy vositasi, raqamli sertifikatlar va elektron raqamli imzoni qo‘llovchi dasturiy-apparat vositasi.

eToken USB-kalit smart-kartalari yoki brelok shaklida chiqariladi. eToken modellari Rossiya tomonidan sertifikatlangan bo‘lib, uni foydalanuvchilar autentifikasiyasi va himoyalanganlik sinfi G1 gacha bo‘lgan maxfiy axborotni qayta ishlovchi avtomatlashtirilgan tizimlarda kalitli axborotlarni saqlash uchun qo‘llagan ma’qul. Ular sertifikatlangan axborotni himoyalashning kompleks sitemasi (KriptoPro CSP, Kripto-KOM, Domen-K, Verba-OW va b.) uchun kalit ma’lumotlarni tashishga tavsiya qilinadi.

eToken PRO smart-kartalar va USB-kalitlar smart-karta mikrosxemalari bazasida qurilgan, autentifikasiya va raqamli sertifikatlar va elektron raqamli imzo bilan ishlashni apparat jihatdan qo‘llab quvvatlovchi ma’lumotlarni himoyalangan saqlash uchun mo‘ljallangan.

Mumkin bo‘lgan ko‘rinishlari:

- bajarilish form-faktori bo‘yicha: USB-kalit, smat-karta;
- smart-karta xotira hajmiga ko‘ra: 32, 64 KB;
- sertifikatlangan turi (Rossiya);
- ichki o‘rnatilgan radio-belgilarga egaligi bo‘yicha;
- USB-kalit korpusiga relyefli logotipni kiritish, smart-karta yuzasiga chop qilish, USB-kalit qurilmasiga tampopechat usulida logotipni kiritish;
- USB-kalit qurilmasi uchun korpus rangi bo‘yicha.

USB-kalit/eToken PRO (Java) smart-kartasi USB-kalitlar va eToken smart-kartalarining yangi avlodi – eTokenning funksional imkoniyatlarini sezilarli darajada kengaytiruvchi va uning foydalanish ko‘lamini kengaytiruvchi Java-karta bazasida qurilgan, autentifikasiya va axborot xavfsizligini ta’minlovchi yechimdir.

eToken PRO (Java) eToken PROning barcha funksiyalariga ega va dasturiy jihatdan u bilan butunlay mos. Qo‘shimcha ravishda, eToken PRO (Java) foydalanuvchilar ma’lumotlarini (72 KB) himoyalangan holda saqlashda, xotira hajmini kattalashtirish imkoniyatiga ega va qo‘shimcha dasturlarni yuklash imkonini beradi. eToken PRO (Java) ERI kalitlarini generasiyasini apparat tomonidan amalga oshiradi va GOST R 34.10-2001 standarti bo‘yicha ERI larni shakllantiradi.

eToken PRO (Java) USB–kalitlarini Windows Vista operasion tizimida ishlatish uchun drayverlarni o‘rnatish talab qilinmaydi (drayverlar operasion tizim tarkibida kiradi).

Mumkin bo‘lgan ko‘rinishlari:

- Amalga oshirish form-faktori bo‘yicha: USB-kalit, smart-karta;
- sertifikatlangan versiyasi (Rossiya) – sinov sertifikati bosqichida;
- ichki o‘rnatilgan radio-belgilariga egaligi bo‘yicha;

- USB-kalit korpusiga relyefli logotipni kiritish, smart-karta yuzasiga chop qilish, USB-kalit qurilmasiga tampopechat usulida logotipni kiritish;
- USB-kalit qurilmasi uchun korpus rangi bo‘yicha.

eToken PRO sertifikatlangan modellari hisoblangan, Aladdin kompaniyasining eToken PRO modellari bo‘lgan NG-OTP va NG-FLASH lar 2008 yil 5 martdagi №925/5 sertifikatiga muvofiq, axborotni himoyalash vositalarini sertifikatlash tizimi (Rossiya) tomonidan sertifikatlangan.

eToken NG-OTP kombinasiyalangan USB–kalitlari axborot xavfsizligi sohasidagi yechimlardan biri. U funksional smart-karta, kalitlarni tasvirlash uchun suyuq kristall displey va generasiyalash tugmasiga ega bo‘lgan ichki o‘rnatilgan bir martalik kalitlar apparat generatoridan tashkil topgan.

Mumkin bo‘lgan ko‘rinishlari:

- smart-karta xotira hajmi bo‘yicha: 32, 64 KB;
- sertifikatlangan versiyasi (Rossiya);
- ichki o‘rnatiluvchi radio-belgilariga egaligi bo‘yicha;
- korpus rangi bo‘yicha.

eToken NG-FLASH kombinasiyalangan USB-kaliti ichki o‘rnatilgan flash-xotira modulida foydalanuvchilar ma’lumotlarining katta hajmini saqlaydigan funksional smart-kartaga ega [23]. Shuningdek eToken NG-FLASH kompyuterning operasion tizimi yuklanishini va flash-xotiradan foydalanuvchi ilovalarini ishlatishni amalga oshira oladi.

Mumkin bo‘lgan ko‘rinishlari:

- ichki o‘rnatiluvchi flash-xotira moduli hajmi bo‘yicha: 512 MB; 1,2 va 4 GB;
- sertifikatlangan versiyasi (Rossiya);
- ichki o‘rnatiluvchi radio-belgilariga egaligi bo‘yicha;
- korpus rangi bo‘yicha.

eToken PASS o‘zining ishlashi uchun kompyuterga ulashni talab qilmaydigan bir martalik parollar avtonom generatori. eToken PASS bir martalik kalitlarni tasvirlash uchun suyuq kristall displey va generasiyalash tugmasiga ega.

ruToken [24] – bu shifrlash va autentifikasiya algoritmlaridan foydalanuvchi va o‘zida bir necha xalqaro xavfsizlik standartlarini birlashtirgan, autentifikasiyalash va axborotni himoyalashning apparat vositasidir. U Rossiyaning ―ANKAD [23] firmasida ishlab chiqarilgan.

ruToken kompyuterning USB-portiga ulanuvchi, unchalik katta bo‘lmagan elektron qurilmani o‘zida nomoyon qiladi (USB-brelok). U smart kartaning analogi hisoblanadi, lekin u bilan ishlashda qo‘shimcha qurilmalar talab etilmaydi.

Sanoat standartlarini qo‘llab-quvvatlashi ruTokenni umumfoydalanuvchi dasturiy ta’minot sifatida o‘rnatishga, shifrlash algoritmlarining qo‘llanilishi esa ruToken identifikatorlari bazasida axborot xavfsizligi tizimini yaratishga imkon beradi.

ruToken ixtiyoriy ilovalarda qo‘llanilishi mumkin, masalan parollar, smart-kartalar va boshqa identifikatorlarning odatiy ishlatiluvchi joylarda. Dasturiy-apparat vositalari kompleksida mos holda ruToken quyidagi masalalarni hal qilishda ishlatilishi mumkin:

Autentifikasiya:

- dasturiy-apparat autentifikasiyasiga mo‘ljallangan ma’lumotlar bazasi, Web-serverlar, VPN-tarmoqlar va ilovalarga kirishda parolli himoyani o‘zgartirishni;
- pochta serverlari, ma’lumotlar bazasi serverlari, Web-serverlar, fayl-serverlar, masofaviy foydalanishda autentifikasiyadan foydalanishda himoyalangan bog‘lanishni.

Ma’umotlar himoyasi:

- axborot himoyasini (GOST 28147 algoritmiga asosan shifrlash);
- elektron pochta himoyasini (ERI, shifrlash);
- kopyuterga kirishdan himoyalash (foydalanuvchini operasion tizimga kirishda avtorizasiyalash).

ruToken ISO/IEC 7816 standartiga javob beruvchi ichki o‘rnatilgan fayl tizimini o‘z ichiga oladi. GOST 28147 ga ko‘ra ruTokenning har bir nusxasi uchun

noyob hisoblanuvchi ma’lumotlar asosidagi butun fayl tizimini shaffof shifrlanishi ta’minlanadi.

Xavfsizlikning apparat modullari ichida birmuncha taniqli va ishonchlilaridan biri KRIPTON seriyali platalari hisoblanadi [14].

—KRIPTON seriyali ma’lumotlarni kriptografik himoyalash qurilmasi apparat vositalarining qo‘llanilishida yaxlitlikni ta’minlash muammaosini hal qiladi. Ruxsatsiz foydalanishlardan himoyalashning ko‘plab zamonaviy tizimlarida doimiy xotira qurilmasiga dasturiy ta’minot yoki analogik mikrosxema birlashtirish amalga oshirilgan. Shu yo‘l bilan, dasturiy ta’minotga o‘zgartirish kiritish zarur bo‘lsa, tegishli plataga ruxsat olish zarur va keyin mikrosxemani o‘zgartirish mumkin.

—KRIPTON davlat hamda tijorat tuzilmalarida qo‘llaniladi.

—KRIPTON qurilmasi —ANKAD [23] firmasi tomonidan ishlab chiqilgan, ishlab chiqarilmoqda va tadbiq qilinmoqda. Ular shu firma tomonidan yaratilgan prosessorning ixtisoslashtirilgan 32 razryadli shifrida qurilgan. KRIPTON seriyasidagi qurilmalar davlat aloqa va axborot federal agentligi (Rossiya) tomonidan sertifikatlangan.

—KRIPTON seriyasining afzalliklari:

- Kriptografik qayta qurish algoritmining apparatda tadbiq qilinishi *algoritm yaxlitligini* ta’minlaydi;
- *Kompyuter operativ xotirasida* emas, platada shifrlashning amalga oshirilishi va shifrlash kalitining saqlanishi;
- Smart-karta va *Touch Memory* identifikatorlaridan —KRIPTON qurilmasiga shifrlash kalitlarining yuklanishi kompyuternig tezkor xotira qurilmasi va tizim shinalaridan xolos bo‘lgan holda to‘g‘ridan-to‘g‘ri amalga oshiriladi, bu kalitlarni ushlab olish imkoniyatini bartaraf etadi;
- Kriptografik qayta qurishlarni amalga oshirish uchun ixtisoslashtirilgan shifrprosessorining qo‘llanilishi, kompyuterning markaziy prosessori ishini yengillashtiradi.

—KRIPTON qurilmalari uchun maxsus dasturiy ta’minot ishlab chiqilgan va u quyidagilarni ta’minlaydi:

- Kompyuter axborotini (fayllar, fayllar guruhi va disk qismlarini) maxfiyligini ta’minlash uchun shifrlashni;

- Fayllarni butunligi va avtorligini tekshirgan holda, ularning elektron raqamli imzolanishini amalga oshirishni;

- Foydalanuvchilarning maxfiy axborot bilan ishlashini imkoni boricha yengillashtirish va osonlashtirish uchun shaffof shifrlanuvchi logik disklarni tashkil qilish;

- Kriptografik himoyalangan virtual tarmoqlarni tashkil qilish, IP-trafikni shifrlash;

- Axborotni ruxsatsiz foydalanishlardan himoyalash tizimlarini yaratish va kompyuterdan foydalanishni belgilash.

Shifrlash algoritmi - GOST 28147 – 89. Shifrlash kaliti o‘lchami - 256 bit**.** Ma’lumotlarni kriptografik himoyalashning KRIPTON/Crypton seriyali dasturiy vositalari shifrlash, ERI va tijorat, bank, sug‘urta, soliq siri, shaxsiy ma’lumotlar va hakozolar ko‘rinishidagi turli maxfiy axborotlarni xavfsizligini ta’minlash uchun axborotni kompleks himoyalash funksiyasini ta’minlaydi.

KRIPTON/Crypton seriyasidagi dasturiy mahsulotlar avtonom holda yoki shifratorlarni —ANKAD [23] firmasining ixtiyoriy dasturiy ta’minoti bilan hamkorligini ta’minlovchi *Crypton API* asl kutubxonasi vositasidagi KRIPTON shifratori bazasida ishlaydi. Bundan tashqari, —ANKAD firmasi tomonidan *Crypton Emulator* dasturiy mahsuloti ham ishlab chiqilgan. U —KRIPTON seriyasidagi ma’lumotlarni kriptografik himoyalash qurilmalari shifrlash funksiyalarini emulyasiya qiladi.

—VERBA-O, —VERBA-OW axborotni kriptografik himoyalash vositasi

—Moskva ilmiy-tadqiqot elektrotexnika instituti‖ tomonidan ishlab chiqarilgan va u quyidagi masalalarni hal qiladi [20]:

- Fayl sathida axborotni shifrlash/deshifrlash;
- Elektron raqamli imzo (ERI) generasiyasi;

- ERIni tekshirish; himoyalangan axborotga yovuz niyatli shaxs yoki viruslar tomonidan kiritilgan xatoliklarni topish.

—Verba seriyasidagi axborotlarni kriptografik himoyalash vositalari avtonom ish o‘rni yoki buyurtmachi dasturiy ta’minotiga o‘rnatiladigan modul ko‘rinishida tashkil etiladi.

Ushbu vositalarning qo‘llanilishi virtual xususiy tarmoq qurishni va ular o‘rtasida maxfiy almashuvni ta’minlashni, Internetga himoyalangan holda chiqish va masofaviy (mobil) foydalanuvchilarning xususiy tarmog‘idan himoyalangan *on-line* foydalanish imkoniyatlarini beradi

—Grot telefon sklembleri maxfiy axborot himoyasi uchun mo‘ljallangan [16]. U umumiy qo‘llanish telefon tarmog‘i orqali uzatiluvchi nutq signalini shifrlashni va faksimil xabar himoyasi uchun mo‘ljallangan.

Aloqa kanalida ishlash xarakteristikasi va foydalanuvchi xususiyatlari:

- Abonent liniyasidagi doimiy tok kuchlanishi: 30...60 V;
- Yuqori to‘siqlarga bardoshlilik;
- Abonent telefon apparatiga, abonent liniyasiga, ATS yo‘nalishi chiziqlimasligiga avtomatik ravishda adaptasiya;
- Ixtiyoriy zichlikdagi radiorele qo‘shimchali shaxarlararo va davlatlararo aloqani o‘z ichiga oluvchi, Rossiya va MDH davlatlari real telefon kanallarida ishlashning bardoshliligini;
- Aks sadoga yuqori bardoshlilik;
- Telefon tarmog‘ida shovqin darajasining pastligi;
- Nutqni qayta tiklashning yuqori sifati;
- Individual kalit-identifikatori xotirasining energiyadan mustaqilligi;
- Individual kalit-identifikatori kiritish algoritmining individual kalitlar elektron yon daftarchasidan foydalangan holda soddalashtirilganligi.

Shifrlash:

- Shifrlash metodi – mozaikali: chastotali va vaqtinchalik joy almashtirish;
- Kalitlarni tanlashning qo‘l mehnatisiz ishlashini ta’minlovchi kalitlarni ochiq taqsimlash metodi;

- Kalit kombinasiyalarining umumiy miqdori $2*10^{18}$;

- Abonentlar identifikasiyasi uchun qo‘shimcha yetti ma’noli kalit kiritish imkoniyati;

- Buyurtmachi xohishiga binoan o‘rnatiluvchi qo‘shimcha master kalitlar hisobiga kriptografik himoyaning yuqori darajasi.

Nutq va hujjatli axborotni kafolatlangan kriptografik himoyalashning Ye-20 apparati quyidagilarni ta’minlaydi:

- Umumiy foydalanish telefon apparati rejimi;

- Nutqni kriptografik himoyalash rejimi;

- Uzatish va ichki o‘rnatiluvchi imitohimoya qurilmasi bilan ma’lumotlarni kriptografik himoyalash rejimi.

Yopiq rejimdagi ish *Data Key* o‘rnatilgan kalit tashuvchisida amalga oshiriladi.

―Ye14‖ apparati raqamli axborot potoklarini shifrlash apparati hisoblanadi. Ye14 va Ye14A [6] mahsulotlari dupleks kabellari, optik tolali, radioreleli kanallari raqamli tizimlarida uzatiluvchi, yuqori tezlikdagi maxfiy axborot oqimlarini kriptografik himoyalash uchun mo‘ljallangan. Kalit uzunligi 256 bit.

―GAMMA-M telefon faksimilli va hujjatli axborotni abonent shifrlashi apparati hisoblanadi. ―Gamma-M [21] apparati raqamli shifrator birlashtirilgan standart telefon apparat hisoblanadi. Dupleks rejimida kafolatlangan o‘zgarishsiz va ma’lumotlarni imitohimoya bilan telefon va hujjatli axborotlarni shifrlash uchun mo‘ljallangan.

Apparatning kalit tizimi quyidagilarni o‘z ichiga oladi:

- obro‘sizlantirishga bardoshli juft aloqa kaliti;

- har bir muloqotda ―kalitlarni ochiq taqsimlash‖ prinsipida ishlab chiqariluvchi seans kaliti;

- tarmoq apparatlari soni 5000 gacha;

- tarmoq kalitining amal qilish muddati 3 oy;

- kalit uzunligi 256 bit.

Mahsulot foydalanishga ruxsat kodini va o‘rnatish jarayonida DATA-KEY turidagi kalit olib yuruvchi apparatga identifikasion axborotni kiritishni ta’minlaydi.

―Cancort‖ kriptosmart telefoni GSM 900/1800 standarti maxsus kriptografik mobil telefoni, kriptografik himoya maxsus vositalarini qo‘llagan holda, kriptografik rejimda GSM tarmog‘i orqali ovozli xabar va ma’lumotlarni qabul qilish va uzatish uchun mo‘ljallangan GSM tarmoqlarida aloqani ta’minlaydi [25].

Ovoz va ma’lumotlarni ishonchli shifrlash birgina GSM telefonida ta’minlanadi.

Ma’lumotlarni shifrlash algoritmiga ega barcha telefon aloqasi turlari bilan to‘liq munosabat o‘rnatadi. Kompyuterga ulanganda shifrlangan xabarlarni Internet tarmog‘i orqali elektron pochtaga yuborish imkoniyatini beradi.

Cancort quyidagi funksiyalarni amalga oshiriladi:

- Ovozli axborotni shifrlash/deshifrlash;
- Qisqa xabarlarni (SMS xizmati) shifrlash/deshifrlash;
- Ma’lumotlarni (BS26 va GPRS xizmatlari) shifrlash/deshifrlash;
- Elektron pochtani shifrlash/deshifrlash;
- Telefonning barcha direktoriyalari axborotlarini shifrlash/deshifrlash;
- MMS axborotlarini shifrlash/deshifrlash.

―ZASLON [18] zamonaviy telekommunikasion tizimlarda axborotni kriptografik himoyalash uchun mo‘ljallangan keng qamrovli IP-shifrator apparatini o‘zida namoyon qiladi.

Shifrlash GOST 28147 algoritmi asosida amalga oshiriladi.

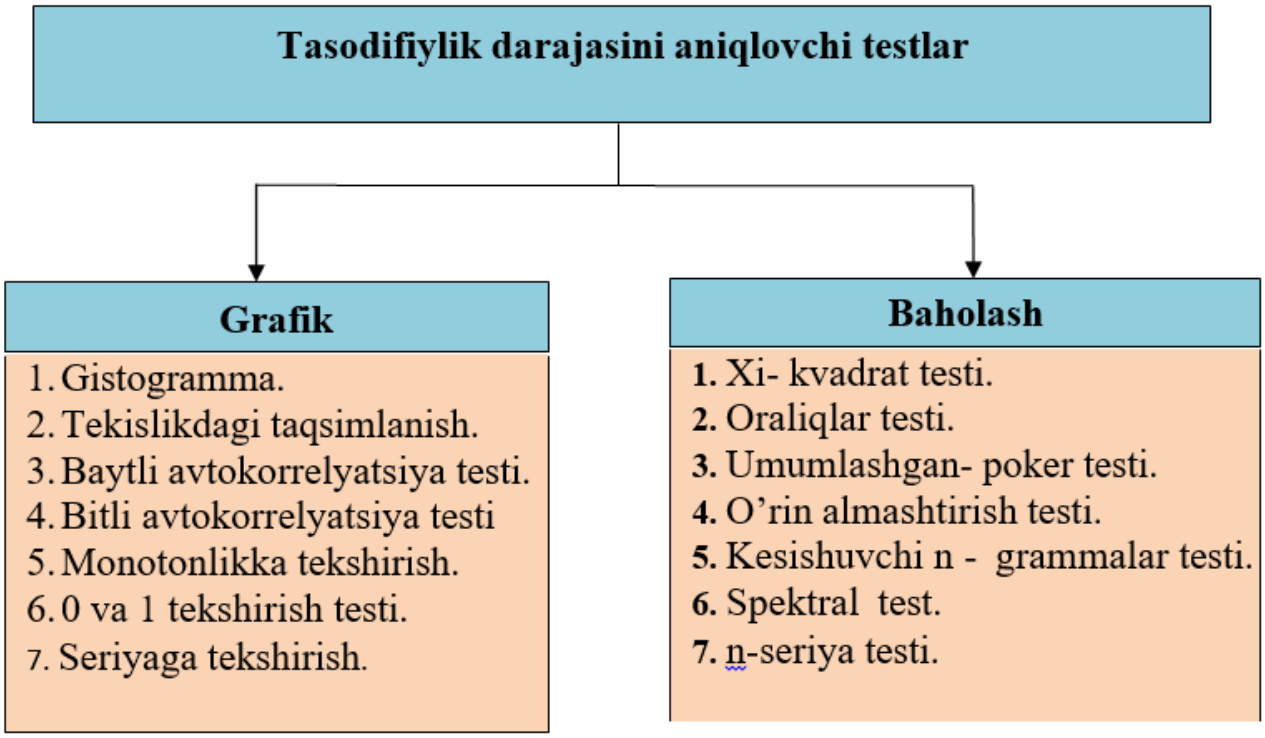
Mavjud blokli simmetrik shifrlash algoritmlari DES, AES, GOST 28147-89 mos ravishda 56 bit, 128 bit, yoki 256 bit, yoki 512 bit va 256 bit uzunlikdagi oldindan belgilab qo‘yilgan qoida bo‘yicha generasiya qilingan kalitlardan foydalanadi. Biroq standart algoritmlarda belgilab qo‘yilgan qoida bo‘yicha generasiya qilingan barcha kalitlar har doim ham shifrmatnni ochish maqsadida ochiq aloqa tarmog‘ini nazorat qiluvchi kriptoanalitik tomonidan uyushtiriladigan

turli kriptohujumlarga bardoshli bo‘lmasligi mumkin. Masalan, kalitni tashkil etuvchi bitlar ketma-ketligi faqat nollardan yoki birlardan yoki bo‘lmasa, nol va birlarning kombinasiyasi fiksirlangan davr bilan takrorlanishi yordamida tuzilgan bo‘lsa, bu toifa kalitlar bardoshsiz hisoblanadi. Chunki ushbu tur bitlar ketma-ketligida, shu ketma-ketlikni tashkil etuvchi nol va bir elementlari davriy takrorlanishining matematik qonuniyatini oldindan aytish imkoniyati mavjud. U holda bu kabi generasiya qilingan bitlar ketma-ketligidan simmetrik shifrlash algoritmlari uchun maxfiy kalit sifatida foydalanish maqsadga muvofiq emas. Demak, yuqoridagi fikr-mulohazalardan kelib chiqib, «kriptoalgoritmlar mahfiy kalit bloklari uchun tasodifiy bitlar ketma-ketligi qanday quriladi?» degan savolning tug‘ilishi tabiiy, yani agar biror qoida bo‘yicha kalit blokining $k = k_1 k_2 ... k_m$, ketma-ketligi olingan bo‘lsa, bu yerda $k_i \in \{0;1\}$, va m=56, 128, 192, 256 bo‘lishi mumkin. U holda $k = k_1 k_2 ... k_m$, kalit blokida k_i - bitlarning taqsimoti tasodifiy yoki tasodifiy emasligi qanday aniqlanadi? Ushbu savolga javob olish uchun kalit blokida k_i -bitlarning taqsimotini amaliyotda keng tarqalgan va boshqa mavjud tasodifiylik testlarining asoslarini tashkil etuvchi Xi-kvadrat taqsimotidan foydalanib aniqlash kerak bo‘ladi.

Tasodifiylikka tekshiruvchi testlar 2 xil bo‘ladi:

Grafik testlar **-** Grafik testlar foydalanuvchiga tekshirilayotgan ketma-ketlikning ma’lum bir grafik bog‘liqligi haqidagi ma’lumotni berib, u bo‘yicha tekshirilayotgan ketma-ketlik xossalari to‘g‘risida xulosa chiqarish imkoniyatini beradi.

Baholash testlari **-** Baholash testlari tekshirilayotgan ketma-ketlik statistik xossalarini tahlil qilib, uning chin tasodifiylik darajasi haqida xulosa chiqarish imkoniyatini beradi [14]:



7-rasm. Tasodifiylik darajasini aniqlovchi testlarning turlari.

Kalit blokini tashkil etuvchi belgilar taqsimotini tasodifiylikka tekshirishda, avvalo, bu kalit blokini biror qoida bo‘yicha hosil qilib olish zarur. Bu kabi ishlar. Odatda, psevdotasodifiy ketma-ketliklar generatorlari orqali amalga oshiriladi. Psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar haqida, ularning tuzilish asoslariga ko‘ra turkumlari, xususiyatlari, xossalari, kriptografik masalarni yechishdagi qo‘llanishlari V bobda batafsil tahlil qilingan. Xususan:

1) Chiziqli kongruent;

2) Kvadratik kongruent;

3) Bir tomonlama unikasiyalarga, shifrlash va xeshlash algoritmlariga asoslangan;

4) Sonlar nazariyasi muammolariga asoslangan generatorlar tahlil qilingan.

Bundan tashqari, V bobda tasodifiylik darajasi yetarli yuqori va akslantirishlari kriptoxujum turlariga bardoshli va samarali:

1) Differensial va chiziqli kriptotahlil usullariga bardoshli bo‘lgan 256 baytli S-blok va 16x16 o‘lchamli siqish jadvali (SJ) akslantirishlari asosida;

2) Ikkita ustuni proporsional va barcha elementlari har-xil bo‘lgan o‘lchami

2^t x4 bo‘lgan to‘g‘ri to‘rtburchakli $A_{2\times 4}^{t}$ - matrisa, hamda, o‘lchami 16x16, bo‘lib, elementlari yarim baytdan iborat bo‘lgan (0 dan 15 gacha sonlarni tekis taqsimotidan iborat) siqish jadvali (SJ) akslantirishlari asosida;

3) To‘rtta 4 argumentli mantiqiy funksiya va o‘lchami 16x16, elementlari yarim baytdan iborat bo‘lgan (0 dan 15 gacha sonlarni tekis taqsimotidan iborat) siqish jadvali (SJ) akslantirishlari asosida;

4) Baytlar va bitlar o‘rnini bog‘liqsiz almashtirishga asoslangan psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlarni 5 marta kombinasiyalashga asoslangan (boshqa sinfga tegishli bo‘lgan generator ham olish mumkin) yangi generatorlar ishlab chiqilgan hamda ularning kriptobardoshli uzuluksiz shifrlash algoritmlari sifatida qo‘llanilishi mumkinligi ilmiy asoslangan.

2.3-§.Tarmoqlararo ekranlarning axborot xavfsizligini ta’minlashdagi ahamiyati.

Tarmoq texnologiyasining keng ko‘lamda qo‘llanishi natijasida umumiy resurslardan foydalanish imkonini beruvchi lokal tarmoqqa kompyuterlar birlashtirildi. Klient-server texnologiyasining tadbiq 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 [6].

Zamonaviy telekommunikasiya 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 obekti bo‘lsa, hujumni amalga oshirayotgan shaxsga uning qaerda (qo‘shni xonada yoki boshqa kontinentda) joylashgani katta ahamiyatga ega emas.

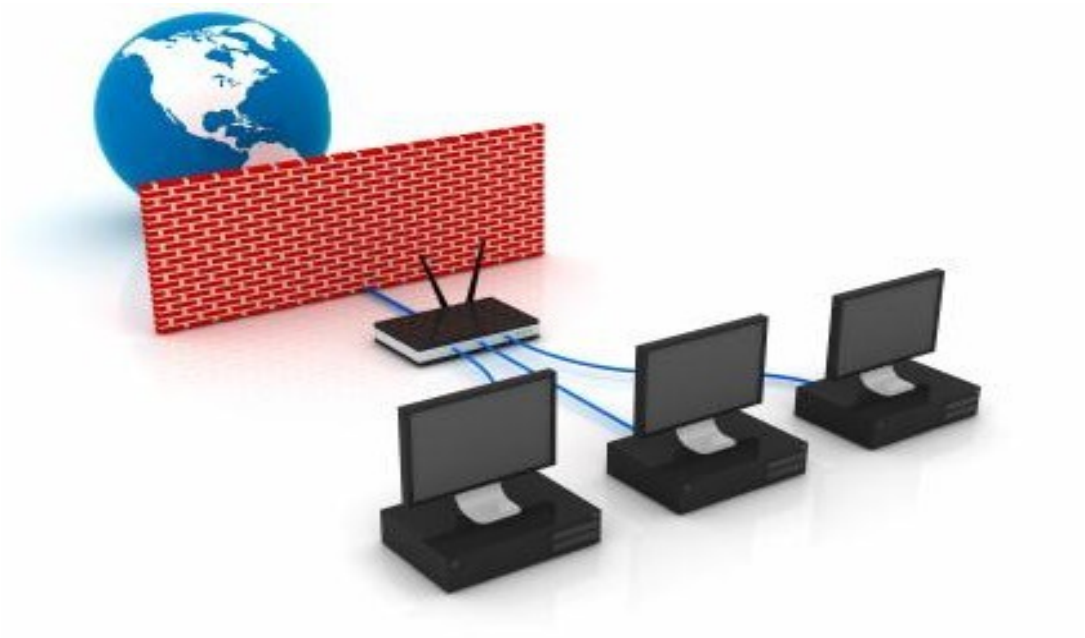
Internet tarmog‘ida masofaviy hujumlardan dasturiy-apparat himoyalash usullari haqida qisqacha to‘xtalib o‘tamiz. Internet tarmoqlarining aloqa vositalarida axborot xavfsizligini ta’minlashning dasturiy-apparat vositalariga quyidagilar kiradi:

- Tarmoq trafigi apparat shifratorlari;
- Dasturiy-apparat vositalar bazasida tashkil qilinuvchi Firewall (tarmoqlararo ekran) metodikasi;
- Himoyalangan tarmoq kriptoprotokollari;
- Tarmoq trafigi dasturiy-apparat analizatorlari;
- Himoyalangan tarmoq operasion tizimlari.

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

Tarmoqlararo ekranlar garchi korxona lokal tarmog‘i ulangan korporativ intratarmog‘idan qilinuvchi hujumlardan himoyalashda ishlatilishi mumkin bo‘lsada, odatda ular korxona ichki tarmog‘ini Internet global tarmoqdan suqilib kirishdan himoyalaydi. Aksariyat tijorat tashkilotlari uchun tarmoqlararo ekranlarning o‘rnatilishi ichki tarmoq xavfsizligini ta’minlashning zaruriy sharti hisoblanadi.

Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta’sir ko‘rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning himoyalanuvchi tarmog‘i va tashqi g‘anim tarmoq orasida joylanishi lozim (2-rasm) va bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtai nazardan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi.



8-rasm. Tarmoqlararo ekranni ulash sxemasi.

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

Tarmoqlararo ekran quyidagi to‘rtta funksiyani bajaradi:

- ma’lumotlarni filtrlash;
- ekranlovchi agentlardan foydalanish;
- manzillarni translyasiyalash;
- 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. Yekran qancha ko‘p sathni o‘z ichiga olsa, shuncha takomillashgan hisoblanadi.

Tarmoqlararo ekranda, dasturiy vositachi vazifasini bajaruvchi va subekt va obekt orasida ulanishni ta’minlovchi, so‘ngra axborotni qayd qilish va

nazoratini amalga oshirib jo‘natuvchi, *ekranlovchi agentlardan* (proxy-serverlar) foydalaniladi. Yekranlovchi agentlarning qo‘shimcha vazifasi foydalanishga ruxsat berilgan subektdan haqiqiy obektni yashirishdan iborat. Yekranlovchi agentlarning o‘zaro aloqa ishtirokchilariga ta’siri yuk.

Tarmoqlararo ekranning manzillarni *translyasiyalash* funksiyasi haqiqiy ichki manzillarni tashqi abonentlardan yashirish uchun mo‘ljallangan. Bu tarmoq topologiyasini yashirish va agar himoyalangan tarmoq uchun etarli 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.

Yekran simmetrik emas. U «tashqi» va «ichki» tushunchalarini farqlay oladi. Yekran ichki sohani nazorasiz va adovatli bo‘lgan tashqi muhitdan himoyasini ta’minlab beradi. Shu bilan birga ekran himoyalangan tarmoq subektlari tomonidan ommaviy tarmoq obektlaridan foydalanishni cheklashni ham ta’minlaydi. Foydalanishga ruxsat berilgan subektning 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 xavfsizligini ta’minlash va tashqaridan ulanishlar va aloqa seanslarini to‘liq nazorat qilish.

2. Yekranlovchi 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 prosessori tez ishlay olish, pik rejimlarida kiruvchi va chiquvchi oqimlarni etarli darajada samarali qayta ishlay olishga ulgurishi lozim.

5. Xavfsizlikni taminlash 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. Yekranni boshqaruv tizimi olisdagi filiallar uchun ham yagona xavfsizlik siyosatini yuritishni markazlashgan holda ta’minlash imkoniyatiga ega bo‘lmog‘i lozim.

7. Tarmoqlararo ekran foydalanuvchilarning tashqi ulanishlari orqali foydalanishga ruxsat berishning mualliflashtirish vositalariga ega bo‘lmog‘i kerak.

Taqsimlangan tarmoqlararo ekranlar, an’anaviy tarmoqlararo ekranlardan farqli ravishda, qo‘shimcha dasturiy ta’minot bo‘lib, xususan korporativ serverlarni, masalan Internet-serverlarni ishonchli himoyalashi mumkin. Korporativ tarmoqni himoyalashning oqilona echimi - himoyalash vositasini u himoya qiluvchi serveri bilan bir platformada joylashtirishdir [6].

Internetdan keng foydalanishning asosiy shartlaridan biri u orqali o‘tkaziladigan barcha tranzaksiyalar uchun xavfsizlikning bir xil darajasini ta’minlash bo‘lgan va bo‘lib qoladi. Bu foydalanuvchilar o‘rtasida uzatiladigan axborotga, savdo tizimlarining ma’lumotlar bazalarida saqlanadigan axborotga, moliyaviy tranzaksiyalarga ilova qilinadigan axborotga taalluqlidir [6].

Axborot xavfsizligi tushunchasini axborot egalarining yoki axborotdan foydalanuvchilarning moddiy zarar ko‘rishiga olib keladigan axborotning yo‘q qilinishi, buzilishi va fosh etilishi uchun yo‘l qo‘yib bo‘lmaydigan xavflarni bartaraf etuvchi tasodifiy yoki ataylab qilingan ta’sirlarga bardosh berish holati kabi ta’riflanadi. Tarmoq tashqaridan kirish uchun to‘liq ochiq bo‘lganligi sababli ushbu usullarning ahamiyati juda katta. Xavfsizlik omillarning katta

ahamiyatga egaligi Internetda o‘tkaziladigan ko‘p sonli tadqiqotlar bilan belgilanadi.

Internetning hamma erda tarqalishidan manfaat ko‘rish maqsadida tarmoq hujumlariga samarali qarshilik ko‘rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq VPN yaratish ustida ishlar olib borildi. «Virtual» iborasi VPN atamasiga ikkita uzel o‘rtasidagi ulanishni vaqtincha deb ko‘rilishini ta’kidlash maqsadida kiritilgan. Xaqiqatan, bu ulanish doimiy, qat’iy bo‘lmay, faqat ochiq tarmoq bo‘yicha trafik o‘tganida mavjud bo‘ladi.

Virtual tarmoq VPNlarni qurish konsepsiyasi asosida etarlicha oddiy g‘oya

orasida ochiq tarmoq orqali uzatilayotgan axborotning konfidensialligini va yaxlitligini ta’minlovchi virtual himoyalangan tunnel qurish zarur va bu virtual tunneldan barcha mumkin bo‘lgan tashqi faol va passiv kuzatuvchilarning foydalanishi haddan tashqari qiyin bo‘lishi lozim.

Shunday qilib, VPN tunneli ochiq tarmoq orqali o‘tkazilgan ulanish bo‘lib, u orqali virtual tarmoqning kriptografik himoyalangan axborot paketlari uzatiladi. Axborotni VPN tunneli bo‘yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

- o‘zaro aloqadagi taraflarni autentifikasiyalash;
- uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash);
- etkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish.

Bu vazifalar bir biriga bog‘liq bo‘lib, ularni amalga oshirishda axborotni kriptografik himoyalash usullaridan foydalaniladi. Bunday himoyalashning samaradorligi simmetrik va asimmetrik kriptografik tizimlarning birgalikda ishlatilishi evaziga ta’minlanadi. VPN qurilmalari tomonidan shakllantiriluvchi VPN tunneli himoyalangan ajratilgan liniya xususiyatlariga ega bo‘lib, bu himoyalangan ajratilgan liniyalar umumfoydalanuvchi tarmoq, masalan Internet doirasida, saflanadi. VPN qurilmalari virtual xususiy tarmoqlarda VPN-mijoz, VPN-server yoki VPN xavfsizligi shlyuzi vazifasini o‘tashi mumkin.

VPN-mijoz odatda shaxsiy kompyuter 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 autentifikasiyalash uchun modifikasiyalanadi. Odatda VPN-mijozning amalga oshirilishi standart operasion tizim - Windows NT/2000 yoki Unixni to‘ldiruvchi dasturiy echimdan iborat bo‘ladi. *VPN-server* server vazifasini o‘tovchi, kompyuterga o‘rnatiluvchi dasturiy yoki dasturiy-apparat kompleksidan iborat. VPN-server tashqi tarmoqlarning ruxsasiz foydalanishidan serverlarni himoyalashni hamda alohida kompyuterlar va mos VPN-mahsulotlari orqali himoyalangan lokal tarmoq segmentlaridagi kompyuterlar bilan himoyalangan ulanishlarni tashkil etishni ta’minlaydi. VPN-server VPN-mijozning server platformalari uchun funksional 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.

VPN xavfsizligi shlyuzi (Security gateway) ikkita tarmoqqa ulanuvchi tarmoq qurilmasi bo‘lib, o‘zidan keyin joylashgan ko‘p sonli xostlar uchun shifrlash va autentifikasiyalash vazifalarini bajaradi. VPN xavfsizligi 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. VPN xavfsizligi shlyuzi alohida dasturiy echim, alohida apparat qurilmasi, hamda VPN vazifalari bilan to‘ldirilgan marshrutizatorlar yoki tarmoqlararo ekran ko‘rinishida amalga oshirilishi mumkin.

VPN tunnellari turli foydalanuvchilar uchun yaratilishi mumkin. Korporasiyaning mavjud tarmoq infratuzilmalari VPNdan foydalanishga ham dasturiy, ham apparat ta’minot yordamida tayyorlanishlari mumkin.

Dasturiy ta’minot asosidagi VPN. Dasturiy usul bo‘yicha amalga oshirilgan VPN mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan

qurilmadan qolishsada, VPN tarmoqlarni amalga oshirilishida etarli quvvatga ega. Ta’kidlash lozimki, masofadan foydalanishda zaruriy o‘tkazish polosasiga talablar katta emas. Shu sababli, dasturiy mahsulotlarning o‘zi masofadan foydalanish uchun etarli unumdorlikni ta’minlaydi. Dasturiy mahsulotlarning shubxasiz 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 narxi anchagina yuqori. Ixtisoslashtirilgan apparat VPN vositalarda ma’lumotlarni shifrlash DES yoki 3-DES algoritmlari asosida amalga oshiriladi [6].

Axborot tarmoqlarida keng tarqalgan axborotni himoyalashning dasturiy-apparat vositalariga quyidagilar kiradi: —Spektr - Z tizimi; SecretNet tizimi; DAALLAS LOCK dasturiy-apparat kompleksi va boshqalar [19].

Spektr-Z – bu himoyalashning kompleks tizimi bo‘lib, Windows 95 yoki Windiws 98 operasion tizimlarining barcha versiyalarida ishlovchi IBM PC ShEXM guruhiga mansub kompyuterlarda o‘rnatiladi.

Spektr-Z tizimining asosiy imkoniyatlari:

- Keng ko‘lamdagi zamonaviy va loyihalashtirilayotgan dasturiy kompleks va ma’lumotlar bazasini ruxsasiz kirishlardan har bir alohida loyiha doirasida himoya vositalarini ishlab chiqish kabi qo‘shimcha kuch sarflashlarsiz himoyalash, huddi alohida ishchi stansiya bazasidagi avtomatlashtirilgan tizim kabi lokal tarmoq bazasidagi avtomatlashtirilgan tizim doirasi ham;
- Internet bilan ishlashning himoyalangan ishchi o‘rnini yaratish;
- Logik disklar uchun foydalanuvchilar vakolatini (umumiy ruxsat, faqat o‘qish, o‘zgartirish rejimi, ruxsat yo‘q) boshqarishni ta’minlash;

- Ro‘yxatga olingan foydalanuvchi yo‘qligida klaviatura, monitor va sichqonchani blakirovkalash;
- Xavfsizlik admininstratori tomonidan shakllantirilib belgilangan bir qancha disketalardan foydalanishda foydalanuvchi ishini chegaralash;
- Kompyuter viruslari hujumini, dastur va ma’lumotlardagi tasodifiy yoki qasddan ma’lumotlarning buzib ko‘rsatilishini aniqlash;
- Foydalanuvchilarning kompyuterdagi ishini qayd qilish.

SecretNet tizimi Novell Netware operasion tizimi boshqaruvidagi lokal hisoblash tarmoqlarida saqlanuvchi va qayta ishlanuvchi axborotlarni himoyalash uchun mo‘ljallangan.

SecretNet tizimi quyidagilarni ta’minlaydi:

- Foydalaniluvchini autentifikasiyalash apparat vositalari nomenklaturasini kengaytirish imkoniyatiga ega maxsus apparat vositalari (TouchMemory va SmartCard) yordamida foydalanuvchilarni autentifikasiyalash;
- Kompyuter lokal disklarida saqlanuvchi ma’lumotlardan, shuningdek turli qurilmalardan (printer, kommunikasion portlar) foydalanuvchilar foydalanishini diskresion (tanlangan) boshqarish;
- Xuddi lokal kabi, tarmoq fayllari va kataloglaridan foydalanishni konfedensiallikni uch darajasi (umumfoydalanuvchi, maxfiy va juda maxfiy)dan foydalangan holda vakolatli (mondatli) boshqarish;
- Ma’lumotlarni kriptografik himoyalash vositalarini ulash;
- Xavfsizlikka aloqador bo‘lgan tizimda sodir bo‘layotgan xodisalarning to‘liq ro‘yxatga olinishi, shu bilan birga ro‘yxatga olishni moslashuvchan holda boshqarish;
- Himoya mexanizmlarini doimiy (zarurat bo‘lganda) qo‘shish;
- Dastur ishga tushganda tarmoq resurslariga ruxsat berish vakolatlarini foydalanuvchilarga dinamik o‘zlashtirish;
- Himoya vositalarini markazlashtirilgan holda boshqarish;
- Foydalanuvchilar ishini tezkor boshqarish (monitoring);
- Operasion tizim va foydalanuvchi tomonidan foydalanilayotgan

dastur yaxlitligini boshqarish;

- Sozlashlarning moslashuvchanligi va tizimni ekspluatasiyalashning odddiyligi.

DAALLASLOCK dasturiy-apparat kompleks hisoblanadi.

DAALLASLOCK 4.1 dasturiy ta’minoti quyidagilarni o‘z ichiga oladi:

- Yaxlitlikni nazorat qilish moduli;
- Ichiga o‘rnatilgan antivirus himoyasini;
- Foydalanuvchilarning ruxsat etilgan va taqiqlangan masalalar ro‘yxatini tayinlay olish imkoniyati;
- Kompyuter ma’lumotlariga ruxsatga aloqador hodisalarni ro‘yxatga olish;
- Foydalanuvchi yo‘qligida ekran va klaviaturani blakirovkalash.

DAALLASLOCK 5.0 versiyasi ixtiyoriy IBM – Windows NT Workstation operasion tizimi bilan mos keluvchi kompyuterlar bilan ishlashga mo‘ljallangan.

Aloqa tarmoqlarida kriptografik himoya vositalari tahlili

Yuqorida ko‘rib o‘tilganidek, aloqa tarmoqlarida tizim xavfsizligini ta’minlashda kriptografik algoritmlardan keng foydalanildi. Ushbu algoritmlarni quyidagi turlarga ajratish mumkin:

- simmetrik shifrlash algoritmlari;
- assimetrik shifrlash algoritmlari;
- elektron raqamli imzo algoritmlari;
- kalit uzutish protokollari;
- xesh funksiyalar.

Ushbu kriptografik algoritmlar yordamida elektron to‘lov tizimida quyidagi amallarni bajarishda foydalaniladi:

- tranzaksiya ma’lumotlarini shifrlash;
- kalitlarni uzatish;
- ma’lumotni yaxlitligini ta’minlash;
- autentifikasiyalash va h.k.

Shularni hisobga olgan holda elektron to‘lov tizimlarida kriptobardoshli algoritmlardan foydalanish yuqori samara beradi. Quyida esa har bir turdagi algoritmlarning tahlili keltrilgan.

Simmetrik algoritmlarning tahlili. Simmetrik algoritmlar shifrlash va deshifrlash jarayonida bitta kalitdan foydalanadi. Ushbu shifrlash algoritmlari shifrlash va deshifrlash jarayonida assimetrik algoritmlarga qaraganda yufori tezlikka ega, kalit uzunligi esa bir xil bardoshlilikka erishganda kichikdir. Bu esa simmetrik shifrlash algoritmlaridan katta hajmdagi ma’lumotlarni shifrlashda foydalanish katta yutuq beradi. Quyida aynan elektron to‘lov protokollarida foydalanilgan simmetrik algoritmlarning qiyosiy tahlili keltirilgan.

1-jadval

Shifrlash algoritmlar tahlili

Xususiyat	**DES**	**AES**	**Blowfish**
Muallifi	IBM tashkiloti	Vinsent Rijman va Xuan Daymen	Bryus Shnaer
Kalit uzunligi (bit)	56	128, 192, 256	32-448, o‘zgaruvchan
Kirish blok uzunligi (bit)	64	128	64
Raund soni	16	10, 12, 14	16
Matematik asosi	XOR, surish va o‘rin almashtirish	Ko‘phadlar ustida amallar, XOR, surish	MOV, ADD, XOR
Yaratish asosi	Feystel tarmog‘i	SPN tarmoq	Feystel tarmog‘i
Yeng katta natijaga erishgan hujum turi	Brute-force hujumi	Side-channel hujumi	Kalit zaifligiga asoslangan hujum

Quyida ushbu algoritmlarning kriptotahlil tizimi sanalgan Crypto++ dasturiy taminoti orqali tahlil qilinganda olingan natijalar berilgan.

2-jadval

Shifrlashdagi tezliklar bo‘yicha tahlil

Algoritm	Shifrlanadigan ma’lumot (MB)	Vaqt	MB/Sek
Blowfish	256	3,976	64,386
Rijndael(128)	256	4,196	61,01
DES	128	5,998	21,34
3DES	128	6,159	20,783

Assimetrik shifrlash algoritmlari tahlili. Simmetrik algoritmlardan farqli ravishda assimetrik algoritmlar elektron to‘lov protokollarida ma’lumotlarni shifrlash uchun emas, asosan simmetrik shifrlash algoritmlari kalitlarini almashinishda, elektron qaramli imzo algoritmlari orqali autentifikasiyadan o‘tkazishda foydalaniladi. Hozirda assimetrik algoritmlar orasida keng foydalanilayotgani RSA va elliptik egri chiziqlarga asoslangan assimetrik algoritmlar keng foydalaniladi. Shularni hisobga olgan holda quyida ushbu ikki algoritmlarning qiyosiy tahlili keltirilgan [7,8].

Xesh funksiyalar. Xesh funksiyalar – ixtiyoriy uzunlikdagi kirish ma’lumotini chiqishda belgilangan uzunlikdagi xesh qiymatga aylantirib beruvchi bir tomonlama funksiyalarga aytiladi. Xesh funksiyalar kriptografiya va zamonaviy axborot xavfsizligi sohasida ma’lumotlarni to‘laligini tekshirishda foydalaniladi. Elektron to‘lov tizimlari protokollarida ham istemolchi kartasi ma’lumotlarini

bank-emitentga to‘liq etkazish uchun foydalaniladi. Quyida esa hozirda keng foydalanilayotgan xesh funksiyalar qiyosiy tahlili keltirilgan[7].

RSA va elliptik egri chiziqqa asoslangan algoritmlarning kalit uzunliklari bo‘yicha tahlili

3-jadval

Ochiq kalitli algoritmlar tahlili

RSA	YeCC
512	113
768	136

1024	160
2048	282
4096	409

4- jadval

RSA va elliptik egri chiziqqa asoslangan algoritmlarning xususiyatlari bo‘yicha tahlili

	RSA	**ECC**
Umumiy parametrlar	-	Qiyin. Tavsiya etilgan parametrlar
Kalit generasiyasi	O‘zgaruvchan. 0.2 s-14 min. 1024 bit kalit: 2.8 sek	0.054 s- 1.4 min. 161-bit kalit:0.09 sek
Shifrlash	0.02 sek-6.7 sek 1024 bit kalit, e=65537:0.025 sek	0.05 sek-2.8 min, 163 bit kalit, 2048 bayt mal:0.12 min
Deshifrlash	0.03sek-4.45 sek 1024 bit kalit:0.13 sek	0.03 sek-1.55 min 163 bit kalit, 22 bayt mal:0.05 sek
YeRI da imzolash	Deshifrlash	Deshifrlash
YeRI da imzoni tekshirish	Shifrlash	Shifrlash

5-jadval

Xesh funksiyalar tahlili

	Xeshlanadigan matn uzunligi	**Kirish blokining uzunligi**	**Xesh qiymat uzunligi**	**Har bir blokni xeshlash qadamlari soni**
GOST R 34.11-94	Ixtiyoriy	256	256	19
MD 2	Ixtiyoriy	512	128	1598
MD 4	Ixtiyoriy	512	128	72
MD 5	Ixtiyoriy	512	128	88
SHA-1	$<2^{64}$	512	160	80

SHA-256	$<2^{64}$	512	256	64
SHA-384	$<2^{128}$	1024	384	80
SHA-512	$<2^{128}$	1024	512	80
STB 1176.1 –99	Ixtiyoriy	256	142≤L≤256	77
O‘z DSt 1106:2006	Ixtiyoriy	128, 256	128, 256	16b+74, 16b+46, Bu erda b-bloklar soni

Elektron raqamli imzo algoritmlari. Elektron to‘lov tizimlarida istemolchini autentifikasiyadan o‘tkazishda ko‘plab usullar va protokollar foydalaniladi. Ushbu usullar asosida esa elektron raqamli imzo algoritmlari yotadi. Elektron raqamli imzo algoritmlarining asosiy maqsadi foydalanuvchilarni bank-emitent bilan aloqasida autentifikasiyadan o‘tkazish. Elektron raqamli imzo algoritmlari asosida ma’lumotlarning xesh qiymatlarini assimetrik shifrlash algoritmlari yordamida shifrlashdan iborat. Quyida keng foydalanilayotgan elektron raqamli imzo aolgoritmlari tahlili keltirilgan [7,8].

6-jadval

Elektron raqamli imzo algoritmlari tahlili

Belgilar	**O‘z DSt 1092:2005 O‘z DSt 1092:2009**	**DSA**	**GOSTR 34.10-2001**
Algebraik struktura	Parametrli algebra (parametrli chekli multiplikativ gruppa)	Chekli oddiy maydon	Chekli oddiy maydonda aniqlangan YeYeCh
Modul tipi va o‘lchamlari	Tub son $p > 2^{255}$ (Afzalligi *yuqori tezkorlikda*)	Tub son $2^{511} < p < 2^{1024}$	Tub son $p > 2^{255}$
Prosedura-larda foy-dalanilgan asosiy amallar	1. Parametrli ko‘pay-tirish 2. Parametr bilan darajaga oshirish 3. Parametr bilan teskarilash 4. Teskarilash	1 Ko‘paytirish 2. Qo‘shish 3. Darajaga oshirish 4. Teskarilash	1. Qo‘shish 2. Inkor 3. Ko‘p martalik qo‘shish 4. Konkatenasiya **(***Kamchiligi* amallarning murakkabligida)
Daraja asosi tipi	Maxfiy – *g* (Afzalligi *diskret logarifmlash masalasini qo‘yish murakkabligida*)	Oshkora - *g* (Kamchiligi *diskret logarifmlash masalasini qo‘yish*	Oshkora nuqta *R* (Kamchiligi *elliptik egri chiziqlarda dis-kret logarifm-*

		osonligida)	*lash masalasini qo‘yish osonligida)*
YeRI uzunligini	*Faktor((r-1) ning tub*	*Faktordan*	*Siklik gruppaning*
qisqarti-rishga yonda-shuv	*ko‘paytuvchisi)dan foydalanish* $2^{254} < q < 2^{256}$	*foydalanish* $2^{159} < q < 2^{160}$	*tartibidan foydalanish* $2^{254} < q < 2^{256}$, *q - gruppa tartibi*
Yopiq kalit shakli	Uchlik *(x, u, g)* (Afzalligi *maxfiylik darajasi oshishida)*	Parametr *x*	Parametr *d*
YeRI shakli	Juftlik *(r, s)* $\mu=0$ da**,** uchlik *(r, s, y_1)* $\mu=1$ da (Kamchiligi $\mu=1$ da)	Juftlik *(r, s)*	Juftlik *(r, s)*
Bardoshlilik	$\mu=1$ *da daraja parametri muammo-sining murakkabligiga* asoslangan **(**Afzalligi *DSA ga nisbatan yuqori bardoshliligida)*	Modul *512-1024* bit bo‘lganda *diskret logari-fmlashning murakkabligiga asoslangan*	Modul *255* bitdan katta bo‘lganda *YeYeChda diskret logarifmlashning murakkabligiga asoslangan*
Tekshirish kaliti shakli	Juftlik *(y, z)* $\mu=0$ da uchlik *(y, z, y_1)* $\mu=1$ da **(**Afzalligi *soxta imzoni aniqlashda)*	Juftlik *(g, y)*	Parametr – *Q*
Imzo tekshirish natijasi shakli	Xesh-funksiya qiymati yoki xeshlashdan foyda-lanilmaganda xabar bloki **(**Afzalligi xeshlanishi shart bo‘lmagan qisqa xa-barlarni uzatmaslik mumkinligi*)*	Ijobiy yoki salbiy	Ijobiy yoki salbiy
Foydalani-ladigan protokol	Standartga xos *(*$\mu=1$ *maromda* kamchiligi *kalitlarni ro‘yxatga olish markaziga qo‘shimcha yuklama tushishida)*	An’anaviy	An’anaviy
Foydalani-ladigan marom	1. Seans kalitisiz *(*$\mu=0$**)** 2. Seans kalitili *(*$\mu=1$*)* **(**Afzalligi *yangi imkoniyatlar tug‘ilishida***)**	Seans kalitisiz	Seans kalitisiz
Birgalikdagi kalitlar tipi	R, R_1 parametrlar **(**Afzalligi *maxfiylik darajasining ortishida***)**	Yo‘q	Yo‘q
Soxta imzoni aniqlash kaliti tipi	Juftlik *(R_1, y_1)* R_1 – nazorat kaliti y_1 – seans oshkora kaliti **(**Afzalligi**)**	Yo‘q	Yo‘q
Imzoni tan olmaslik imkoniyati	Mavjud **(**Afzalligi**)**	Yo‘q	Yo‘q

Kalitlarni taqsimlash protokollari. Ushbu protokollar istemolchi va bank-emitent o‘rtasida ma’lumot almashinishda dastlabki qilinadigan ish sanalab, bunda ikki tomon o‘rtasida maxfiy ma’lumotlarni (asosan kalitlar) almashinish amalga

oshiriladi. Ushbu jarayon o‘tkazilgan taqdirda ma’lumotlar almashinish boshlanadi. Yuboriladigan ma’lumotlar maxfiyligi aynan shu jarayonda almashingan kalitlarga bog‘liqdir. Shularni hisobga olgan holda quyida kalit taqsimlash protokollari tahlili keltrilgan [7].

7- jadval

Simmetrik algoritmlaridan foydalanilgan holda kalit almashinish protokollari tahlili

№	Protokol nomi	A	V	K_A	K_V	K	t	S	Bo‘lishi mumkin bo‘lgan hujum
1	**Vaqt metkasidan foydalanib kalitni uzutish protokoli**	+				+	-		Kriptoanalitik bu ma’lumotni ma’lum vaqtdan so‘ng V foydalanuvchiga qayta uzatishi mumkin.
		-				+	+		V foydalanuvchi bu ma’lumotni kim tomonidan uzutilganini bilmaydi.
2	**YeRI yordamidagi protokol**	+	+				+	-	V foydalanuvchi bu ma’lumotni kim tomonidan uzutilganini bilmaydi.
		+	+				-	+	Kriptoanalitik bu ma’lumotni ma’lum vaqtdan so‘ng V foydalanuvchiga qayta uzatishi mumkin.
3	**Tasodifiy sonlardan foydalanib kalitni generasiya qilish protokoli**	+		-	-				Protokol bajarilishi natijasida seans kalit generasiya qilinmaydi.
4	**Diffi-Xelman protokoli**	—O‘rtadagi kishi‖ hujumiga bardoshli emas							

8-jadval

Assimetrik algoritmlardan foydalanilgan holda kalit almashinish protokollari tahlili

№	Protokol nomi	A	V	r_A	r_V	r	t	Bo‘lishi mumkin bo‘lgan hujum
1	**Nidxem-Shreder protokoli**	-	-	+				Arbitr ma’lumotni kimdan kelgani va kimga yuborish kerakligi haqida hech narsa bilmaydi
		+	+	-		+		A foydalanuvchi ma’lumotni arbirtdan kelganiga to‘la ishonch hosil qilolmaydi
		-				+		V foydalanuchi kalitni kim tomonidan yuborilganini bilmaydi
		+				+		Kriptoanalitik bu kalitni ma’lum vaqtdan so‘ng qayta uzutishi mumkin
2	**Wide-Mouth Frog protokoli**	+	+				-	Kriptoanalitik bu ma’lumotni V foydalanuvchiga takroran uzatishi mumkmn.
		-	-				+	Foydalanuvchilar ma’lumotning kimdan kelganini bilmaydilar.
3	**Yahalom protokoli**	+	+	-	-	+		Foydalanuvchilar o‘rtasida o‘zaro identifikasiya ta’minlanmaydi
4	**Kerberos protokoli**	Tizim vaqtning sinxron ravishda ishlashi talab etiladi.						

II bob bo‘yicha xulosa.

Dissertasiya ishining ikkinchi bobi bo‘yicha quyidagi natijalar olindi:

1. Tarmoqlararo ekran dasturiy-apparat vositasi, uning funksiyalari, asosiy vazifalari, filtrlash olib boriladigan sathlar, tarmoqlararo ekranlarga qo‘yiladigan zamonaviy talablar, paketlarni filtrlashga asoslangan tarmoqlararo ekranlar va taqsimlangan tarmoqlararo ekranlar tadqiqi etildi.

2. Virtual xususiy tarmoq VPN ni axborot uzatilishi jarayonidagi himoyalashni amalga oshirishdagi imkoniyatlari yoritildi.

3. Axborot tarmoqlarida keng tarqalgan axborotni himoyalashning dasturiy-apparat vositalari hisoblangan ―Spektr - Z‖ va SecretNet tizimi, DAALLAS LOCK dasturiy-apparat komplekslari qo‘llanilishi, afzallik va kamchiliklari batafsil tahlil etildi.

4. Axborotlarning kriptografik himoya vositalarining apparat, dasturiy va dasturiy-apparat vositalar ko‘rinishlari qo‘llanilishi, afzallik va kamchiliklari tahlil

etildi. Shuningdek dasturiy-apparat himoya vositalarning autentifikasiya vositalari, axborotni kriptografik himoyalash apparatlari tahlil etildi.

5. Bardoshli kalitlar ishlab chiqish asoslari uzliksiz shifrlash algoritmlari asoslari kabi psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar masalalarining yechimlari bilan bog‘liqligi asoslandi.

6. Psevdotasodifiy ketma-ketlik bloklari belgilarini tasodifiylikka tekshiruvchi testlar haqida fikr va mulohazalar bildirilib, ularning grafik va baholash testlaridan iboratligi izohlandi.

III BOB. INFOKOMUNIKASIYA TIZIMLARIDA DASTURIY VOSITALARNI ISHLAB CHIQISHGA OID TAVSIYALAR AXBOROTLARINI HIMOYALASH ALGOROTMLARI

3.1-§. Infokomunikasiya tizimlarida dasturiy vositalarni ishlab chiqishga oid tavsiyalar

Axborot-kommunikasiya tizimida ma’lumotlar amashinuviga mos keluvchi kriptografik tizimni yaratish bilan bir qatorda shu tizimda kalitlar boshqarish masalasini optimal hal etish muhim o‘rin tutadi. Chunki tanlangan kriptotizim qanchalik murakkab va ishonchli bo‘lmasin, baribir undan amalda foydalanish jarayonlari kalitlarni boshqarish masalasi bilan bog‘liqdir. Agarda ma’lumotlarning mahfiy almashinuvi oz sonli foydalanuvchilar doirasida bo‘lsa, kalitlar almashinuvi jarayonida noqulayliklar tug‘ilmaydi. Ammo axborot-kommunikasiya tizimida ma’lumotlarning mahfiy almashinuvi yuzlab, minglab va xatto millionlab foydalanuvchilar doirasida bo‘lsa (misol uchun modem va INTERNET aloqa tizimlari orqali bank, savdo–sotiq, davlat ahamiyatiga bog‘liq hamda boshqa muhim sohalardagi aloqa jarayoni foydalanuvchilari doirasida) kalitlarni boshqarishning o‘ziga xos alohida muhim masalalari kelib chiqadi.

Kalitlar haqidagi ma’lumot deganda axborot-kommunikasiya kriptotizimida mavjud bo‘lgan barcha kalitlar to‘plami va ularning muhofazasi bilan bog‘liq ma’lumotlar tushuniladi. Agarda kalitlar haqidagi ma’lumotlarni yetarli darajadagi ishonchli muhofazali boshqaruvi ta’minlanmasa, tabiiyki, raqib tomonga axborot- kommunikasiya tizimidagi deyarli ihtiyoriy ma’lumotni olish uchun to‘la imkoniyat tug‘iladi.

Kalitlarni boshqarish jarayoni quyidagi uchta muhim bo‘lgan:

- barcha kalitlarning o‘zaro bog‘liq holda, ya’ni bir butun holda ishlash jarayonini ta’minlash (kalitlar generasiyasi);
- kalitlar to‘plamining maqsadli kengayib borishini ta’minlash (kalitlarlarning to‘planishi);
- kalitlarlarni foydalanuvchilar doirasida taqsimlash (kalitlarlarning taqsimlanishi) jarayonlariga ahamiyat berishni talab etadi.

Yana U. Diffi va M. Ye. Xellman bir tomonli funksiya sifatida taklif etgan ushbu

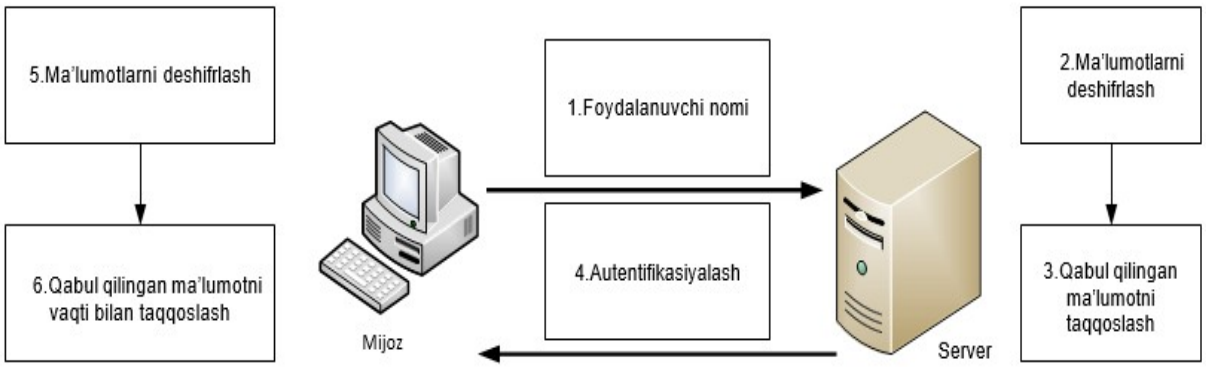
$$f(x) = \alpha^x \pmod p$$

p modul bo‘yicha diskret darajaga ko‘tarish funksiyasiga to‘xtalamiz. Ilgari ta’kidlanganidek, bu yerda: x-butun son bo‘lib, 1 dan (p–1) gacha bo‘lgan qiymatlarni qabul qilishi mumkin; p -yetarli katta bo‘lgan tub son; butun son bo‘lib, 1 danp gacha bo‘lgan qiymatlarni qabul qiladi va uning darajalari α , α 2 ,….,a qandaydir tartibda 1,..., p-1qiymatlarni qabul qiladi. Misol uchun, p = 7, α=3 bo‘lsa, α =3, α ^{2}=2, α ^{3}=6, α ^{4}= 4, α ^{5} =5, α ^{6} =1 ifodalarga ega bo‘lamiz.

Algebrada mana shunday α sonini chekli $GP(p)$ maydonning soda elementi deyiladi va ma’lumki, bunday α har doim mavjud bo‘ladi. Agarda $y = f(x) = a^x$ bo‘lsa, u holda tabiiyki, bu funsiyaga teskari funksiya bo‘lib, berilgan y lar bo‘yicha x qiymatlarni topish diskret lagorifmlarni topish masalasi deyiladi. Xattoki, p ning yetarli katta bo‘lgan qiymatlarida ham, misol uchun $p = 2^{1000}$ bo‘lganda ham, 1000 dan ko‘p bo‘lmagan kvadratga ko‘tarish va ko‘paytirish amallarini bajarib, $f(x)$ funksiyani oson hisoblash mumkin.

Agarda diskret darajaga ko‘tarish funksiyasi haqiqatan ham bir tomonlama bo‘lsa, u holda $\log_a y$ ifodani y ning barcha, ya’ni ushbu $1 \le y \le p$ tengsizlikni qanoatlantiruvchi, barcha qiymatlarida hisoblashni amaliy jihatdan imkoniyati yuq bo‘lishi kerak. M.Ye. Xellman va uning shogirdi Polig, faqatgina p soni katta tub son bo‘lgandagina emas, balki (p -1) soni katta tub kupaytuvchi q ga ega (yoki shu q tub son 2 ga kupaytirilgan) bo‘lganda, (1) ifoda bilan aniqlangan funksiyaning y qiymatlariga ko‘ra $\log_a y$ ifodani hisoblash amaliy jihatdan murakkab ekanligini ko‘rsatdilar. U. Diffi va M.Ye. Xellman mahfiy aloqa tizimlari foydalanuvchilari uchun, diskret logorifmlardan foydalanib, mahfiy kalitlarni o‘zaro almashuvini alohida maxfiy kanalsiz amalga oshirish algoritmini yaratdilar.

Axborot – komunikasiya tizimlarida ma’lumotlarni himoyalashning quyidagi kriptografik protokoli taklif etiladi (7-rasm).



9-rasm. Axborot – komunikasiya tizimlarida ma’lumotlarni himoyalash protokolining ishlash sxemasi

A - foydalanuvchi V - foydalanuvchi bilan ma’lumot almashishi uchun ularga seans kaliti quyidagicha amalga oshiriladi:

1. A - foydalanuvchi arbitrga o‘zining ismi va V - foydalanuvchining ismidan tashkil topgan ma’lumotni uzatadi:

$$\text{A—W: } A, B$$

2. Arbitr ikkita ma’lumotni hosil qiladi, birinchisi vaqt belgisi, hayotiy vaqt L, tasodifiy seans kalit va A - foydalanuvchining ismidan tashkil topgan. Arbitr bu ma’lumotni o‘zi va V - foydalanuvchi uchun umumiy bo‘lgan kalit bilan shifrlaydi, ikkinchisi vaqt belgisi, hayotiy vaqt, tasodifiy seans kalit va V - foydalanuvchining ismidan tashkil topgan. Arbitr bu ma’lumotni o‘zi va A -foydalanuvchi uchun umumiy bo‘lgan kalit bilan shifrlaydi. U ikkala shifrmatnni A -foydalanuvchiga uzatadi:

$$\text{W—A: } E_A(t, L, k, B), E_B(t, L, k, A) \ .$$

3. A - foydalanuvchi o‘zining kaliti bilan birinchi shifrmatnni deshifrlaydi. U o‘zining ismi va vaqt metkasini birlashtirib, k - seans kalit bilan shifrlaydi. Bu shifrmatnni va arbitrdan qabul qilgan ikkinchi shifrmatnni V - foydalanuvchiga uzatadi:

$$\text{A—V: } E_k(A, t), E_B(t, L, k, A) \ .$$

4. V-foydalanuvchi o‘zining kaliti yordamida ikkinchi shifrmatnni deshifrlaydi va seans kalitiga ega bo‘ladi. Bu seans kalit yordamida birinchi shifrmatnni deshifrlaydi. Natijada hosil bo‘lgan A -foydalanuvchining ismi va vaqt belgisi avvalgisi bilan mos bo‘lsa, V-foydalanuvchi A-foydalanuvchini identifikasiya qiladi. Endi A -foydalanuvchi uni identifikasiya qilishi uchun vaqt belgisiga 1 raqamini qo‘shib seans kalit bilan shifrlaydi. Hosil bo‘lgan shifrmatnni A -foydalanuvchiga uzatadi:

B — A : E_k (t+ 1) .

Agar har bir foydalanuvchining soatlari arbitrning soati bilan sinxron ravishda ishlasa Bu protokol yaxshi natija beradi.

3.2-§.Axborot komunikasiya tizimlarida dasturiy vosita ishlab chiqish uchun shifrlash algoritm.

Axborot – komunikasiya tizimlarida ma’lumotlarni himoyalashning dasturi ta’minoti uyidagi talablarni hisobga olgan holda yaratildi:

- bardoshli kriptografik tizimlardan foydalanish;
- tizimni himoyalashda axborot xavfsizligi usullaridan foydalanish;
- tizimdan foydalanish qulayligi.

Har bir dasturiy vositani yaratishda dasturlash tillariga ham alohida etibor beriladi. Chunki dasturlash tillari qanchalik yaratilayotgan tizim funksiyalariga mos bo‘lsa, bu imkoniyat dasturlovchiga ham, yaratilgan dasturiy vositaga ham qulaylik tug‘diradi. Shuning uchun ushbu kriptografik dasturiy vositani yaratishda dasturlash tiliga ham alohida e’tibor berildi va ularga quyidagi talablar qo‘yildi:

- dasturlash tili obektga mo‘ljallangan bo‘lishi;
- tizim resurslari bilan oson bog‘lanish imkoniyati mavjud bo‘lishi;
- dasturlash tilida xavfsizlik usullaridan foydalanish imkoniyati;
- foydalanilgan dasturlash tilida hisoblash amallari(katta sonlar ustida) mavjudligi va bajarish osonligi va boshqalar.

Ushbu talablarni hisobga olgan holda ushbu kriptografik dasturiy vositani yaratishda Mircosoft Visual Studio 2008 dasturiy vositalari komponentasi tarkibiga kiruvchi Visual C# dasturlash tili tanlandi.

Mircosoft Visual Studio 2008 dasturi Microsoft korporasiyasi tomonidan ishlab chiqilgan bo‘lib, bu dastur dasturchilar uchun mo‘ljallangandir. Bu dastur yordamida quyidagi dasturlash tillarida dasturlashni amalga oshirish mumkin:

- Visual Basic .NET
- Visual C# .NET
- Visual C++ .NET
- Visual J# .NET

Microsoft Visual Studio 2008 dasturi yordamida Windows muhiti uchun, telefonlar uchun, tarmoqlar uchun, Wyeb dasturlarni yaratish mumkin. Microsoft Visual Studio 2008 muhitida Visual C#, Visual Basic, Visual J# tillari yordamida Wyeb dasturlarni va Visual C#, Visual Basic, Visual J#, Visual C++ tillari yordamida Windows muhiti uchun dasturlar yaratish mumkin.

Quyida ushbu dasturlash tillari bilan tanishib chiqamiz:

Visual Basic .NET - Microsoft Visual Studio 2008 tarkibidagi yeng samaradorligi katta dasturlash tillardan biri bo‘lib, bu dasturlash tilini to‘liq obektga yo‘naltirilgan dasturlash tili deb aytishimiz mumkin. Visual Basic .NET dasturlash tili yordamida Windows ilovalarini va Wyeb ilovalarni yaratish mumkin.

Visual C# .NET - Microsoft korporasiyasi tomonidan ishlab chiqilgan bo‘lib, bu dasturlash tili aynan .NET platformasi uchun ishlab chiqilgan. Visual C# .NET dasturlash tili imkoniyatlari boshqa obektga yo‘naltirilgan dasturlash tillari(C, C++, Java va Delphi)dan ancha keng bo‘lib, bu dasturlash tilida Visual Basic .NET kabi Windows ilovalarini va Wyeb ilovalarni yaratish mumkin.

Visual C++.NET - dasturlash tili past sathdagi dasturchi uchun ilovalarni boshqarishda talab qilinadi. .NET platformasining Visual C++ dasturlash tili boshqa dasturlash tillaridan shu bilan farq qiladiki, bu dasturlash tili .NET platformasining kodli modeli (managed code model) va Windows (unmanaged native code model) kodli modelini qo‘llab quvvatlaydi.

Visual J# .NET - Microsoft .NET platformasi uchun Wyeb-servis va ilovalar yaratuvchi Java-dasturchilari ishlatishi mumkin. Visual J# .NET dasturlash tili.

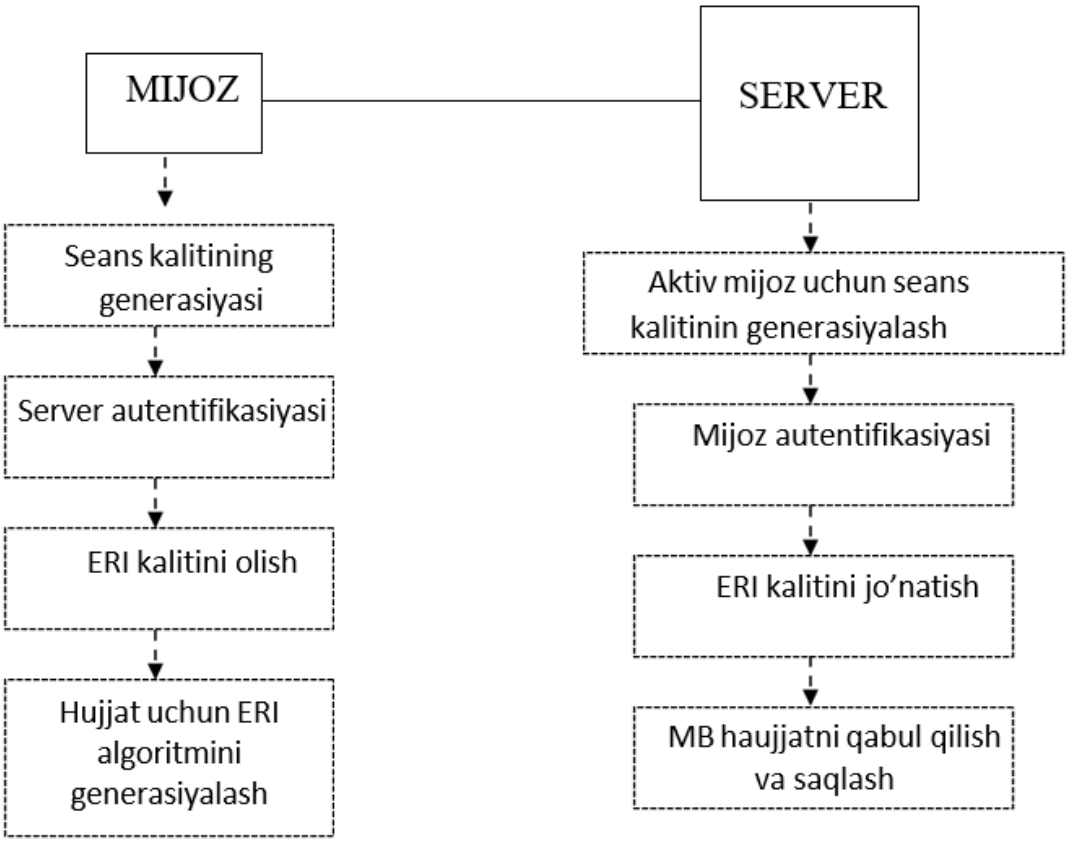
C# dasturlash tilining afzallik taraflari shundaki, bu dasturlash tilida juda ko‘plab kutubxonalar bor. Bu kutubxonalar dasturchi uchun qulaylik tug‘diribgina qolmasdan, kam hato qilishga olib keladi. C# dasturlash .NET Framework kutubxonalari bilan ishlaydi.

Yaratilgan kriptografik dasturiy modul faqat Microsoft, Macintosh operasion muhitlarida ishlaydi. Bu dastur ishlashi uchun bir talay qo‘shimcha dasturlar kerak bo‘ladi. Masalan yeng keraklisi .Net Framework dasturisiz ishlay olmaydi. Biz bu dasturning oynali (Windows Application) bo‘limida tuzdik. C# dasturlash tili C oilasi dasturlariga kiradi. Shuning uchun uni C dasturlash tilini bilgan dasturchiga u uncha qiyinchilik tug‘dirmaydi. C# dasturlash tili C++ dasturlash tilining ixchamlangan, foydalanuvchiga qulay ko‘rinishida chiqarildi. C++ dasturlash tilida qo‘lda yoziladigan dastur qismlari C# dasturlash tilida avtomatik tarzda maxsus buyruqlar orqali kiritiladigan bo‘ldi.

Ushbu dasturiy modulda, serverda orqali mavjud mijoz uchun va yangi foydalanuvchilar uchun elektron raqamli imzo orqali autentifikasiyalash mexanizmi qo‘llanilgan. Imzo algoritmi uchun asimmetrik algoritm, maxfiylik uchun yopiq kalitli algoritm qo‘llanilgan. Bu dasturiy modulning ishlash sxemasi 4-rasmda keltirilgan. Bu sxemadan ko‘rinib turibdiki algoritmning har bir qadamida autentifikasiyalash talab etiladi (8-rasm).

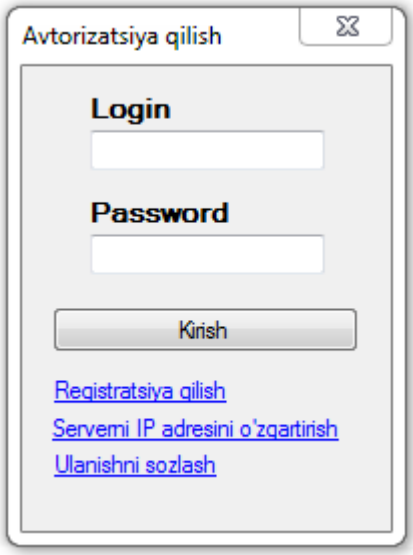
Server bilan mijoz ma’lumot almashinuvi uchun server mijozga ulanadi. Mijoz va server ishni keyingi qadamlarni bajarish uchun senans kalitlarining generasiyasidan boshlaydi. Senas kalitning generasiyasi uchun Diffi-Xelman algoritmi yoki kalitlar almashinuvining elliptik egri chiziqlar asosidagi algoritm tadbiq etiladi.

Bu dasturiy ta’minot axborot kommunikasiya tizimlarida server va mijozning axborot almashinuvida, shunigdek mijozning hujjatini ERI bilan muhrlanib serverda saqlanishini ta’minlaydi.



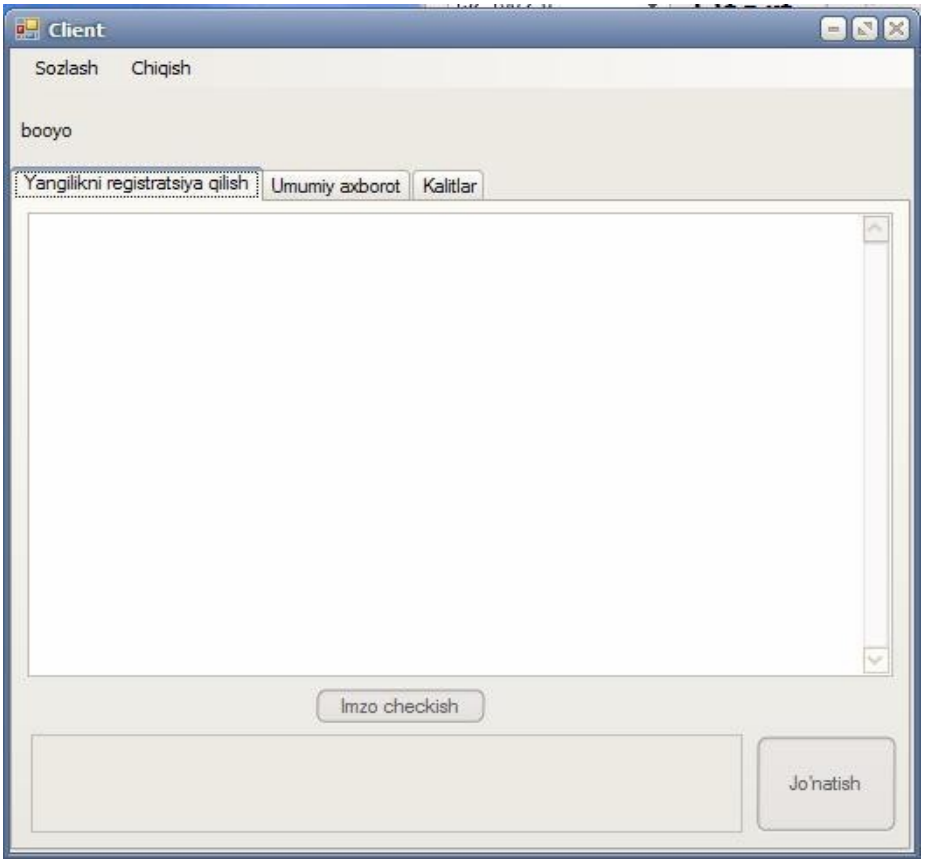
10-rasm. Dasturiy modul algoritmining ishlash sxemasi

Quyida ishlab chiqilgan dasturiy modulning oynacha ko‘rinishi tasvirlangan. Ushbu kriptografik dasturiy vosita Visual C# dasturlash tilida yaratilgan bo‘lib, ushbu dastur ishlashi uchun .Net Framework 3.5 komponentasini o‘rnatish talab etiladi. Dastur o‘rnatilgandan so‘ng tizim foydalanuvchisi dasturdan foydalanish uchun ro‘yxatdan o‘tiladi. Ushbu ma’lumot(parol, login) orqali foydalnuvchi dasturning asosiy sahifasiga kiradi va undan foydalanish imkoniyatiga ega bo‘ladi. Dasturning asosiy sahifasi ko‘rinishi quyidagicha:

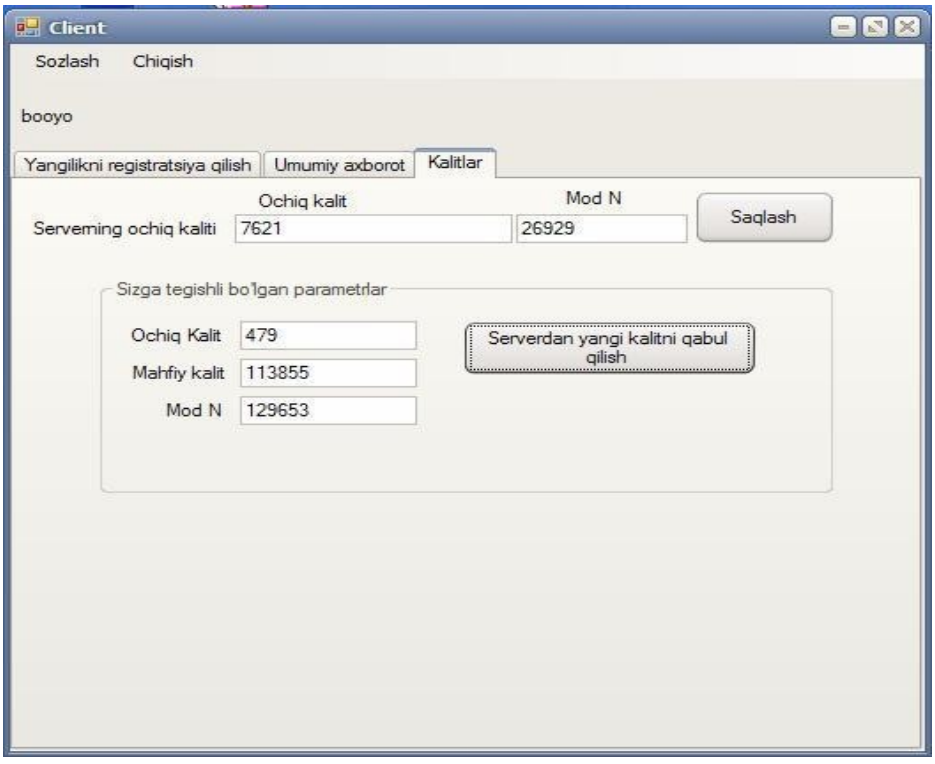


11-rasm. Mijozning serverga ulanish oynachasi.

12-rasm. Serverning kalitlar boshqaruvi va ma'lumotlar almashuvi dasturiy modulining oynachasi



13-rasm. Mijoz modulining oynachasi



14-rasm. Tizim kalitiga ega bo‘lgan mijozning foydalanish oynachasi.

Ushbu qo‘shimcha imkoniyatlar orqali foydalanuvchi ma’lumotlarni shifrlash standartlari orqali shifrlash, ularga ERI qo‘yish, ularni tekshirish, simmetrik va assimetrik tizimlar uchun kriptobardoshli kalitlarni ishlab chiqaruvchi generatorlardan foydalanish mumkin.

3.3-§. Infokomunikasiya tizimlarida foydalanuvchi axborotlarini ruxsasiz kirishlardan himoyalovchi dasturiy vositalarni ishlab chiqishga oid tavsiyalar.

Ushbu ilmiy tadqiqot ishida kriptografik apparat-dasturiy vositaning dasturiy qismi sanalgan dasturiy interfeys yaratildi. Ushbu dasturiy vosita S# dasturlash tilida yaratildi. Ushbu dasturlash tili xususiyatlari va uning imkoniyatlari haqida yuqoridagi bo‘limda to‘xtaldi.

Ishlab chiqilgan dasturning bardoshliligi quyidagi parametrlarga bog‘liq:

- Foydalanilgan dasturiy vositaning imkoniyati va xavfsizlik darajasiga bog‘liq;
- Foydalanilgan kriptografik tizimning bardoshliligiga;
- Kriptoalgoritmni shakllantirish jarayoni va usuliga.

Ushbu parametrlardan kelib chiqib, ishlab chiqilgan dasturiy vositani bardoshliligini quyidagilar bilan asoslash mumkin:

- Ushbu dastur S# dasturdash tilida yaratilganligi (uning imkoniyatlari yuqorida keltirilgan);
- Shifrlashda bardoshli sanalgan AES ishlatildi(asosiy qismda);
- Qo‘shimcha dasturiy vositalar sifatida esa quyidagilar ishlatildi:
- Shifrlash (AES, DES va GOST);
- ERI (RSA);
- Kalit generatori (tub son generatori va RS4 generatori).

AESning kriptobardoshligi. Ushbu shifrlash standarti kriptobardoshligi to‘g‘risida AQSh Milliy xavfsizlik agentligi tomonidan berilgan ma’lumotga ko‘ra 128 bit kalit yordamida shifrlaganda ma’lumotning maxfiylik darajasi

―SECRET‖, 192 yoki 256 bit holda ―TOP SECRET‖ maxfiylik darajasida bo‘ladi [31].

Ushbu xususida Bryus Shnayer quyidagicha yozgan: ‖AES ga biz to‘liq ishonmasligimiz kerak. Buning sababi AES sodda algebraik tuzulishga ega. Hech bir shifrlash tizimi hottoki bunday sodda tuzulishga ega emas. Lekin ushbu sabab AESning bardoshligiga bog‘liqligi hozirgacha bizga ma’lum emas‖ [12].

Nikolya Kartua va Yozef Pepshik 2002-yilda AES i Serpent shifrlash tizimlari ustida XSL-hujumini (ingl. eXtended Sparse Linearization) olib bordi. Hujum natijasi esa AES shifrlash tizimini buzish imkonini bermadi [31].

AES shifrlash tizimi quyidagi turdagi hujumlarga bardoshli [32]:

- kuchsiz kalitlar orqali yuzaga keladigan xujumlar;
- differensial kriptoanaliz;
- chiziqli (lineynogo) kriptoanaliz;
- Square hujumiga (kvadrat tuzulishigi ega bo‘lgan algoritmlarga xos);
- interpolyasiya (qo‘shimcha kiritish) usuliga.

2007- yilning may oyida kriptoanalizchilar tomonidan AES shifrlash tizimida quyidagi hujumlar olib borildi va quyidagi natijalar olindi:

- AES (192 bit, 12 raund) varianti uchun 10-raundgacha nazariy tomondan hujum qilinganligi;
- AES ga side-channel-atak hujumi orqali bir nechta hujumlar olib borildi.

Hozirgi zamon texnologiyasi rivoji va kriptoanalizning rivojlvnishini hisobga olid shuni aytish mumkinki AES 2100-yilga qadar o‘zining kriptobardoshligini yoqotmaydi. Shuni ham aytib olish kerakki, AES shifrlash tizimi muallifi hozirda uning kriptobardoshli sanalgan yangi AES-24 (24 raunddan iborat bo‘lgan) variantini tavsiya etgan [32].

Dastlab parmetrli algebra amali hisoblangan parmetrli darajaga oshirish va parametrli ko‘paytirish amallari bilan tanishib chiqsak. Quyida p modul bo‘yicha R parametrli ko‘paytirish va darajaga ko‘tarishning matematik asosi keltirilgan.

X ni Y ga p modul bo‘yicha R parametrli ko‘paytirish amali $X \circledR Y \ (mod\ p)$ ko‘rinishda belgilanadi va quyidagi ko‘rinishda aniqlanadi [6]:

$$X \circledR Y \ (mod\ p) = X + Y(1 + RX) \ (mod\ p).$$

Ushbu amal kommutativ va assosiativ amaldir.

X o‘zgaruvchini r modul bo‘yicha R parametrli teskarilash amali $X^{\backslash -1} \ (mod\ p)$ shaklida belgilanadi va quyidagi ko‘rinishda aniqlanadi:

$$X^{\backslash -1} \ (mod\ p) = -X(1 + RX)^{-1} \ (mod\ p),$$

bu erda $X^{\backslash -1} \circledR X \ \ 0 \ (mod\ p)$, 0 – parametrli gruppaning birlik elementidir.

Asos X ni p modul bo‘yicha R parametr bilan d-darajaga oshirish amali $X^{\backslash d} \ (mod\ p)$ ko‘rinishida ifodalanadi. Masalan, $d = 37$ bo‘lganda R parametr bilan $X^{\backslash d}$ quyidagicha hisoblanadi:

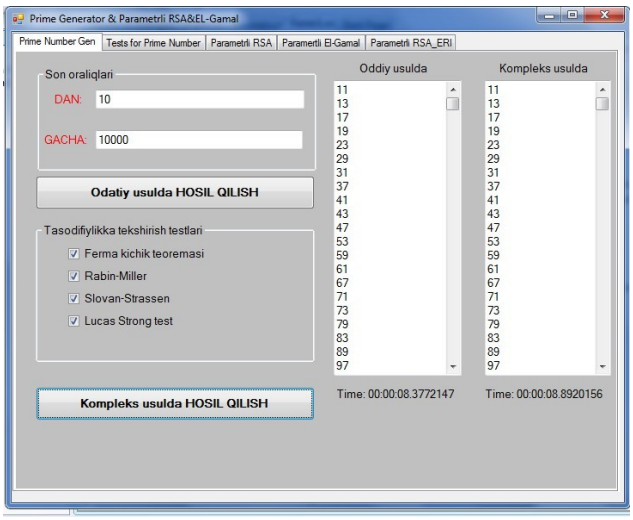
Ushbu kriptografik dasturiy vosita Visual C# dasturlash tilida yaratilgan bo‘lib, ushbu dastur ishlashi uchun .Net Framework 3.5 komponentasini o‘rnatish talab etiladi.

Ushbu dastur 5 ta qismdan iborat bular quyidagilar:

- tub sonlarni hosil qilish generatori;
- sonlarni tublikka tekshiruvchi algoritmlar;
- parametrli algebraga asoslangan RSA shifrlash algoritmi;
- parametrli algebraga asoslangan El-Gamal shifrlash algoritmi;
- parametrli algebraga asoslangan ERI (RSA asosida);

Ushbu amallar dasturiy ko‘rinishda amalga oshirilgan bo‘lib, dastur oynasining ko‘rinishi quyidagicha.

Tub sonlarni hosil qilish generatori. Dasturnig ushbu qismida oraliqlar bo‘yicha tub sonlar hosil qilinadi.



15-rasm. Tub son hosil qilish oynasining ko‘rinishi.

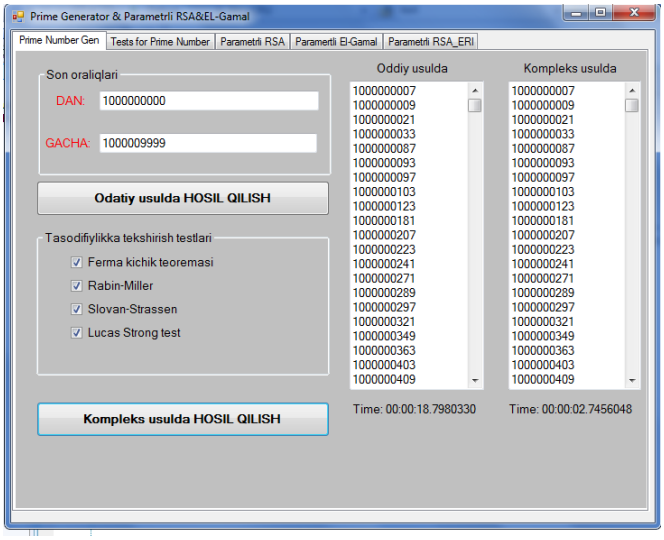
Ushbu oynadan ko‘rinib turibdiki, odatiy hosil qilingan va kompleks holda hosil qilingan tub sonlar generatorlari sarflagan vaqt bir-biridan katta farq qilmaydi. Boshqa tomondan testlashdan o‘tgan tub sonlar bardoshli sanalib, undan foydalanish katta samara beradi.

Agar algoritmlarda katta uzunlikdagi sonlar hosil qilinsa, u holda kompleks holda tashkil etilgan generator vaqtdan katta yutuq beradi. Ushbu ko‘rsatkichlar 5-rasmda ko‘rinib turibdi.

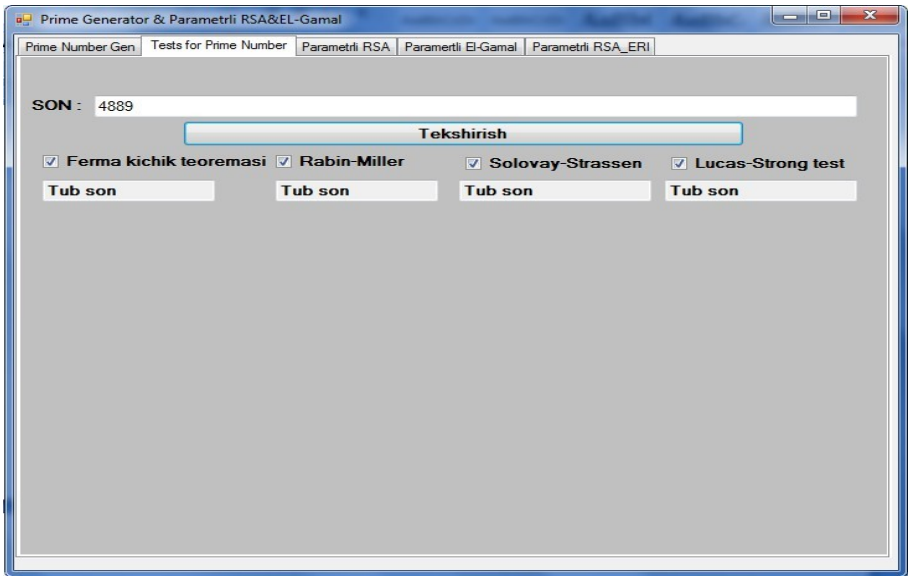
Sonlarni tublikka tekshiruvchi algoritmlar. Ushbu qismda tublikka tekshiruvchi testlar asosida sonlarni tekshirish dasturi ishlab chiqilgan. Ular quyidagilar:

- Fermaning kichik teoremasi asosida;
- Robin-Miller testi; Solovay-Strassen testi;
- Lukas strong test.

Ushbu testlar algoritmi haqida ikkinchi bo‘limda aytib o‘tildi. Dastur oynasi foydalanishga qulay bo‘lib, tekshirilayotgan son kiritiladi va testlash turi tanlanib, tekshirish tugmasi bosiladi. Natijada sonning tub yoki tub emasligiga qarab natija hosil qilinadi (9-rasm).



16-rasm. Tub son hosil qilish oynasining ko‘rinishi



17-rasm. Tub sonlarni tekshirish oynasi

Dasturiy vositaning qolgan uch qismi tub sonlarni amalda, faktorlash va diskret logarifmlash muammosiga asoslangan nosimmetrik tizimlarda qo‘llash ko‘rib chiqiladi.

Parametrli algebraga asoslangan RSA shifrlash algoritmi. Ushbu dastur ana’naviy RSA shifrlash algoritmining parametr asosida hosil qilingan ko‘rinishidir. Bunda har bir parametr uzunligi 256-bit bo‘lib, yakuniy n esa 512-bitni tashkil etadi. Ushbu dasturda foydalanilgan katta uzunlikdagi tub sonlar *BinInt* klassi asosida hosil qilinib, mavjud testlash asosida tekshiriladi. Tekshirishdan o‘tgan sonlar ushbu dasturda kiruvchi parametr sifatida

foydalaniladi. Har bir parametr avtomatik ravishda hosil qilinadi. Kiritilayotgan parametr uzunligini ixtiyoriy ravishda tanlash imkoniyati foydalanuvchiga qulaylik yaratiadi.

Parametrli algebraga asoslangan El-Gamal shifrlash algoritmi. Parametrli El-Gamal shifrlash tizimi dasturi kamida 64-bit uzunlikdagi R kalit asosida hosil qilinadi. Har bir kalit uzunligini oshishi bilan dasturning bardoshligi oshadi. *r(i)* va *r(j)* kalitlarni uzunligi ortishi tizimni ishlash tezligiga ta'sir ko'rsatadi. *e(i)* va *d(j)* kattiliklar kamida 64-bit uzunlikka ega. *r(i)* va *r(j)* maxfiy kalitlar esa kamida 2-bitni tashkil etib, tasodifiy sonlar generatori asosida tashkil etilib, tublikka tekshiruvchi testlar asosida testlanadi va shifrlashda foydalaniladi. Parametrlar uzunligini ortirish ixtiyoriy tanlash asosida amalga oshiriladi.

Parametrli algebraga asoslangan ERI (RSA asosida). Ushbu dasturda an'anaviy RSA shifrlash algoritmining parametrli algebraga o'tkazilgan shakli ishlab chiqilgan. Bunda qo'shimcha R parametr asosida darajaga oshirish amalga oshirilgan bo'lib, bu parametr tizimning xavfsizlik darajasini yana bir parametrga bog'liqligini isbotlab, uni maxfiy tutilishi asosida bardoshlik ta'minlanadi. Q va P qiymatlar kamida 256-bit o'lchamda olinib, parametr R kamida 2-bit uzunlikka ega. Olingan har bir parametr tasodifiy hosil qilinib, tublikka tekshiriladi va olingan son shifrlashda foydalaniladi.

Ishlab chiqilgan dasturiy kriptografik modulni bardoshliligini baholash

Ushbu amaliy qismda yaratilgan dasturiy vositalarning bardoshligini baholash har bir dasturning yaratilish maqsadi va uni amaliyotda beradigan foydasiga qarab amalga oshiriladi.

Shunga ko'ra yaratilgan tub sonlarni hosil qiluvchi generatorlarning afzallik va kamchiliklariga to'xtalib o'sak.

10-jadval

Ana'naviy va kombinasiyalashgan usullarning o'zaro tahlili

Xususiyatlar	Ana'naviy	Kombinasiyalashgan
	Hosil bo'layotgan sonning uzunligi ortishi bilan unga ketadigan vaqtni ko'payishi;	

Kamchiliklar	Sonlarni tublikka tekshirish testlari mavjud emasligi va buning natijasida sonlarni qo‘shimcha tublikka tekshirish amalga oshirilishi keragligi	Kichik uzunlikda ana’viy usulga qaraganda ko‘p vaqt sarflanishi
Yutuqlar	Kichik uzunlikda kombinasiyalashgan usulga qaraganda kam vaqt sarflanishi.	To‘rtta testlash turidan ixtiyoriy foydalanish imkoniyati mavjudligi. Katta uzunlikdagi tub son hosil qilishda vaqtni ana’naviy usulga qaraganda kam sarflanishi

Tub sonlarning amaliyotda qo‘llash uchun yaratilgan dasturiy vositaning bardoshligini baholashda quyidagi xususiyatlarga etibor berildi:

- Yaratilayotgan tub sonlarni ishonchligiga;
- Nosimmetrik tizimda foydalanilgan parametrli algebra murakkabligiga.

Yaratilgan nosimmetrik tizimlar parametrlari oldingi dasturda foydalanilgan tublikka tekshirish testlari asosida teslanib, so‘ngra foydalanildi. Bu esa tizimda foydalanilayotgan parametrlarning bardoshligini bildiradi.

Nosimmetrik tizimlarda kiritilgan qo‘shimcha murakkablik, daraja parametri asosida amalga oshiriladi. Shu o‘rinda daraja parametri muammosi uchta murakkablik pog‘onasi bilan farqlanib, quyidagicha ta’riflanadi:

Yaqoridagi tariflardan kelib chiqib parametrli RSA algoritmi uchun quyidagilarni keltirish mumkin:

- Ushbu algoritmi odatiy holda faktorlash muammosiga asoslanganligi va qo‘shimcha tarzda parametr muammosini kiritilishi bunga diskret logarifmlash muaamosini kiritadi.
- Agar ichki tomondan R parametr ma’lum bo‘lgan holda ham algoritm o‘zining bardoshligini kamida faktorlash muammosi darajasida ushlab turadi.

Ushbu dasturdan foydalanishda bardoshlilikka erishishda quyidagilarga ahamiyat berish shart:

- R parametrni etarli darajada katta uzunlikda tanlanishi ($2^{256} > R$,

$R^{-1} \geq 2^{160}$ shartni bajarishi);

- Kiruvchi parametrlarni 2048-bitdan kam bo‘lmagan holda tanlanishi (r^{160} uchun R parametrni topish imkoniyati amaliy yo‘qligi);

El-Gamal shifrlash tizimida ham shinga o‘xshash quyidagi afzalliklar mavjud:

- Diskret logarifmlash muammosining qo‘shimcha parametr muammosi asosida ortirilishi va buning natijasida ikki marta diskret logarifmlash muammomini vujudga keltirish.

- Maxfiy parametr R aniqlanganda ham tizim o‘zining kuchuni butunlay yoqotmasligi.

Bu tizim uchun ham RSA tizimiga keltirilgan shartlar o‘rinlidir. Umumiy holda sinalgan tub sonlarni amaliyotda qo‘llash nosimmetrik tizim uchun foydali bo‘lib, bunda tizim bardoshligi tub son ishonchlilik darajasi va uzunligiga bog‘liq bo‘ladi.

III bob bo‘yicha xulosalar

Magistrlik dissertasiyasining uchunchi qismi amaliy qism hisoblanib, ushbu bo‘limda kriptografik dasturiy vosita amalga oshirilish tartibi ko‘rib chiqildi.

Dasturilash tili sifatida S# dasturlash tili tanlanib, dastur Windows operasion tizimi uchun, Freamwork 3.5 platformasi asosida yaratildi. Ushbu dasturlash tilini tanlashdan asosiy maqsad qilib, dasturning ishlash tizimidan kelib chiqib, dasturchiga qulaylik tug‘dirishi olindi.

Dastur amalga oshirish vazifasiga ko‘ra ―SecretDisc‖ yutilitalariga o‘xshash bo‘lib, farqli ravishda himoyalash maqsadida AES shifrlash tizimi olinib, hosil qilingan vertual diskdagi barcha fayllar alohida kalitlar yordamida shifrlanib saqlanadi. Kalitlarni saqlashdagi xavflarni oldini olish maqsadida kalitlarni ko‘rsatilgan manzilga saqlash imkonini ko‘rsatish mumkin.

Dasturda qo‘shimcha ERI, shifrlash algoritmlari va kalit generatori yutilitalari mavjud bo‘lib, ular foydalanishda qulaylik tug‘diradi.

Ushbu yaratilgan dasturiy vositaning bardoshligini unda foydalanilgan dasturlash tili va foydalanilgan kriptografik tizim bardoshligi orqali belgilash mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi “O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida”gi PF-38-son Farmoni.
2. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston - 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni.
3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni.
4. O‘z DSt 1092:2009. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
6. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: NIST, 2024.
7. IoT Analytics. “Number of connected IoT devices growing 14% to 21.1 billion globally.” 2025. https://iot-analytics.com/number-connected-iot-devices/ (murojaat sanasi: 07.05.2026).

8. Fagan, M., Megas, K., Scarfone, K., Smith, M. NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology, 2020. https://csrc.nist.gov/pubs/ir/8259/a/final

9. OWASP Foundation. OWASP Internet of Things Project / OWASP IoT Top 10 2018 Mapping. https://owasp.org/www-project-internet-of-things/

10. Dodson, D. et al. NIST SP 1800-15: Securing Small-Business and Home Internet of Things (IoT) Devices. National Institute of Standards and Technology, 2021. https://csrc.nist.gov/pubs/sp/1800/15/final

11. Souppaya, M., Scarfone, K. NIST SP 800-83 Rev.1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST, 2013. https://csrc.nist.gov/pubs/sp/800/83/r1/final

12. Stratosphere Laboratory, AIC group, FEL, CTU University. IoT-23: A labeled dataset of Malware and Benign IoT Traffic. 2020. https://www.stratosphereips.org/datasets-iot23

13. Mehrban, A., Ahadian, P. “Malware Detection in IoT Systems Using Machine Learning Techniques.” arXiv:2312.17683, 2023. https://arxiv.org/abs/2312.17683

14. Farfoura, M. E., Alkhatib, A., Batyha, R. M., Mashal, I. “A novel lightweight Machine Learning framework for IoT malware classification based on matrix block mean Downsampling.” Alexandria Engineering Journal, 2025. https://www.sciencedirect.com/science/article/pii/S2090447924005860

15. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. “Internet of Things (IoT): A vision, architectural elements, and future directions.” Future Generation Computer Systems, 29(7), 1645–1660, 2013. DOI: 10.1016/j.future.2013.01.010.

16. ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

17. OWASP IoT Security Testing Guide. Firmware test cases and IoT penetration testing methodology. https://owasp.org/www-project-iot-security-testing-guide/

MUNDARIJA

INFOKOMMUNIKATSIYA TIZIMLARIDA FOYDALANUVCHI AXBOROTLARINI HIMOYALASH VOSITALARI VA USULLARINI TADQIQ ETISH

Abdumalikov Akmaljon Abduxoliq o‘g‘li

Monografiya

Muharrir: ***D.Kamolov***

Musahhih: ***M.Ismailova***

Kompyuterda sahifalovchi: ***M.Kamolova***

“D-PRESS SERVICES” nashriyoti
Jizzax-2026
Chop etishga ruxsat etildi: 2026-yil 8-may. Bichimi: 60x84 1/16.
“Times New Roman” garnitura. Ofset bosma.
Shartli bosma tabog‘i 6,25. Adadi:10. Buyurtma № 39/26.

Nashriyot litsenziyasi № 749316, 01/05/2025, “D-PRESS SERVICES” MCHJ bosmaxonasi, 131100. Jizzax viloyati, Sharof Rashidov tumani, Qo‘shbarmoq QFY, Istiqlol MFY, Dashtobod ko‘chasi 42-uy. Telefon: +99877-022-17-18

Nashrlarga kitobning ISBN xalqaro standart tartib raqamini berish ma’lumotnomasi:

Pin kod: 1547