# KIBERJINOYATDAN HIMOYALANISH CHORALARI TAHLILI

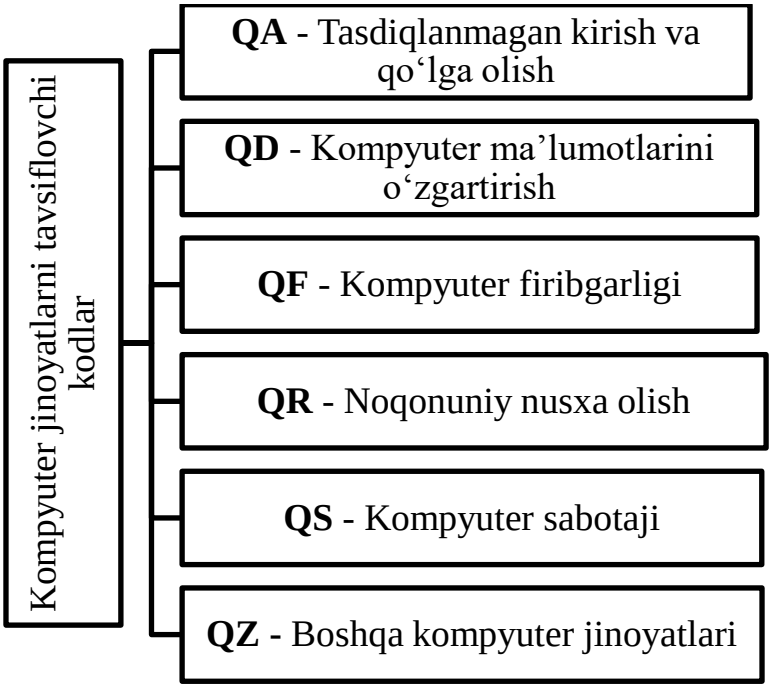
**Radjabova M.Sh**
**Obidov B.X**
**Suyunov K**
**Mardonov S.F**
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnalogiyalari universiteti*

**Anatatsiya:** *Kiberjinoyatlar korxonalarga katta zarar yetkazishi, ma'lumotlar o'chirilishi yoki xavfsizlikka tegishli tizimlarga zarar yetkazishi mumkin. shu sababli korxonalarning kiberjinoyatlarga qarshi qo'llash uchun kiberxavfsizlik choralari va tahlillarini amalga oshirish kerak. Kiberjinoyatdan himoyalanish choralari tahlili, korxona tizimlarini himoya qilish uchun muhim hisoblanadi.*

**Kalit so'zlar:** *QA, QD, QF, QR, QS, QZ, Assinxron, Kriptografik himoyalash, DES, CRIPPER, PGP algoritmlari.*

Xorijiy mamlakatlar tomonidan kompyuter jinoyatlarini sodir etish bo'yicha turlicha tasniflar ishlab chiqilgan. Quyida shu kabi sodir etiladigan jinoyat turlarining nomlanishi Interpol bosh kotibiyati kodifikatoriga muvofiq keltirilgan. 1991-yilda ushbu kodifikator qidiruv avtomatlashtirilgan tizimiga biriktirilgan va hozirda 100 dan ortiq mamlakatlarning NSB si mavjud.

Kompyuter jinoyatlarini ifodalovchi barcha kodlar Q harfi bilan boshlanuvchi identifikatorlarga ega. Jinoyatning tavsiflanishi uchun kamayib borish tartibida joylashgan beshtagacha kod ishlatilishi mumkin.




2.1.-rasm. Kompyuter jinoyatlarini tavsiflovchi kodlar

Keltirilgan kodifikatorga muvofiq bir nechta kompyuter jinoyati turlarining

qisqacha tavsifi:

Tasdiqlanmagan kirish va qo‘lga olish (QA) quyidagi kompyuter jinoyatlarini o‘z ichiga oladi.

QAH – “Kompyuterni qo‘lga olish” (xaking - hacking): Kirish xuquqiga ega bo‘lmagan xolda kompyuter yoki tarmoqqa kirish. Ushbu kompyuter jinoyati turi odatda xakerlar tomonidan o‘zga axborot tarmog‘iga kirishda qo‘llaniladi.

QAI – qo‘lga olish (interception): Kirish xuquqiga ega bo‘lmagan xolda texnik vositalar yordamida ma’lumotni qo‘lga olish. Bu jarayon to‘g‘ridan to‘g‘ri tizimning tashqi kommunikatsion kanali, yoki qo‘shimcha qurilmalarga bevosita bog‘lanish orqali amalga oshirilishi mumkin. Bunda kabel-sim tizimlari, yer usti mikroto‘lqinli tizimlari, suniy yo‘ldosh aloqa xamda tizimi xamda maxsus xukumat aloqa tizimi, kuzatilayotgan obekt xisoblanadi. Bunday turdagi kompyuter jinoyatlariga shuningdek elektromagnit qo‘lga kiritish xam kiradi. Zamonaviy texnikalar kompyuter tizimiga bog‘lanmasdan ma’lumotlarni qo‘lga kiritishga imkon beradi. Qo‘lga kiritish markaziy protsesor, monitor, kommunikatsion kabel, printer va x.k. nurlanishi tufayli amalga oshadi. Buning xammasini obektdan yetarli masofada turib xam amalga oshirish mumkin.

Tasdiqlanmagan kirish va qo‘lga olish metodlarini tasniflashda quydagi maxsus terminlar qo‘llaniladi:

“Juchok”(bugging) - "qo‘ng‘izcha" deganda, xizmat ko‘rsatilayotgan tarkibning suxbatini qo‘lga kiritish maqsadida kompyuterga mikrofon o‘rnatish tushuniladi;

“Otkachivaniye dannых” (data leakage) – “ma’lumotlarni sug‘urib olish” tizimga taaluqli asosiy ma’lumotni qo‘lga kiritish maqsadida kerakli ma’lumotlar to‘plash;

“Uborka musora” (scavening) – "axlatni tozalash" foydalanuvchi kompyuterda ishni yakunlaganidan so‘ng ma’lumotlarni qidirish. Bu usul ikki turga bo‘linadi – jismoniy va elektron. Jismoniy turida axlat qutilarini ko‘zdan kechirish va x.k. nazarda tutiladi.

QAT – vaqtni o‘g‘irlash: pul to‘lamaslik maqsadida kompyuter tizimi va tarmog‘idan noqonuniy foydalanish.

Kompyuter ma’lumotlarini o‘zgartirish (QD) o‘z ichiga quyidagi jinoyatlarni oladi:

QDL/QDT - mantiqiy bomba (logic bomb), troya oti (Trojan horse): mantiqiy bomba va troya otini joriy etish yo‘li bilan noqonuniy kompyuter ma’lumotlarini o‘zgartirish.

Mantiqiy bomba dasturga komandalar to‘plamini maxfiy o‘rnatadi, natijada muayyan muddatda faqatgina bir marta ishga tushadi.

Troya otining maqsadi tizimning ish faoliyati saqlanib qolgan holda dasturga foydalanuvchi rejalashtirmagan o‘zga funksiyalarni bajarish komandalarini kiritishdan iborat.

QDV - virus (virus): kompyuter virusini tarqatish orqali noqonuniy kompyuter ma’lumotlari yoki dasturlarini o‘zgartirish.

Kompyuter virusi – bu kompyuterda salbiy oqibatlarga olib keluvchi, o‘zini

boshqa dasturga yozish, koʻpayish va yangi viruslar yaratish imkoniga ega maxsus yozilgan dastur.

Virus dasturi bilan kompyuterni yuqtirish va uni davolash tibbiy amaliyot kabi bir qancha xususiyatga ega. Umuman olganda bu termin tibbiyotga juda yaqin:

- rezervlash – FAT nusxa koʻchirish, fayllarning oʻzgarishi xaqida kunlik arxiv toʻldirish - bu viruslardan himoyalanishning eng muxim va asosiy usuli xisoblanadi. Boshqa usullar umumiy ximoya darajasini yuqori ta'minlasada, kunlik arxivlashni oʻrnini egallay olmaydi;

- profilaktika – yangi sotib olingan va ekspluatatsiya qilingan dasturlarni alohida saqlash, disklarni aloxida "suv oʻtmaydigan boʻlinma", "faqat oʻqish uchun" rejimi oʻrnatilgan qismlarda saqlash, ishllatilmagan dasturlarni arxivlarda saqlash, disketlardan yangi dasturlarni yozish uchun maxsus "inkubatsion" qismdan foydalanish, ishlatilayotgan disketlarning VOOT-sektorini tizimli tekshirish va x.k.;

- tahlil – yangi olingan dasturlarni maxsus vositalar orqali tekshirish va nazoratdagi muxitda ishga tushirish, dasturni saqlashda va uzatishda kontrol summani tizimli qoʻllash. Xar bir kontrol summasiz olingan yangi dastur vakolatli mutahassislar tomonidan kamida kompyuter viruslarining ma'lum turlariga tekshirilishi va ma'lum bir vaqt ichida uning ustidan nazorat olib borilishi;

- filtrlash – Flushot plus, Mace Vaccinee kabi rezident dasturlardan va boshqa noqonuniy xarakatlarni amalga oshirishga urinishlarni aniqlovchi dasturlardan foydalanish;

- vaksinalashtirish – fayllar, disklar, kataloglarni maxsus qayta ishlash, dastur yoki diskning shikastlanganligi ushbu virus turi bilan mos keladigan maxsus rezident-vaksina dasturlarini ishga tushiradi;

- terapiya (davolash) – maxsus antivirus dasturlar orqali dasturlarda aniqlangan viruslarni deaktivatsiya qilish yoki dastur-fag yordamida shikastlangan fayllar va disklarni barcha virus nusxalarini yoʻq qilish yoʻli bilan dasturning dastlabki xolatini tiklash.

Shuni aytish mumkinki, kompyuter virusidan xalos boʻlish profilaktika oʻtkazishni ta'minlashdan koʻra ancha qiyin.

QDW - chuvalchang: chuvalchangni kompyuter tarmogʻiga yuborish, joriy etish yoki tarqatish, kompyuter ma'lumotlari va dasturlarini noqonuniy oʻzgartirish.

Kompyuter firibgarligi (QF) oʻzining tarkibiga turli xil jinoyat sodir eish usullarini jamlagan:

QFS - bankomatlardan naqd pul oʻgʻirlash bilan bogʻliq kompyuter firibgarligi

QFF - kompyuter soxtaliklari: soxta qurilmalar (kartochka) yaratish orqali kompyuter tizimlarida firibgarlik va oʻgʻirlik

QFG - oʻyin avtomatlari bilan bogʻliq firibgarlik va oʻgʻirlik

QFM – kiritish-chiqarish dasturlari bilan manipulyatsiya qilish: kompyuter tizimlariga notoʻgʻri kiritish va chiqarish orqali firibgarlik va oʻgʻirlik qilish yoki shu orqali dasturni manipulyatsiya qilish. Bu turdagi kompyuter jinoyati turlariga

ma’lumotlarni kiritish-chiqarish jarayonida amalga oshuvchi Ma’lumotlarni almashtirish usuli (data diddling code change), kiritish mumkin. Bu eng oddiy va shuning uchun eng ko‘p qo‘llaniladigan usul hisoblanadi.

QFP - To‘lov vositalari bilan bog‘liq kompyuter firibgarligi va o‘g‘irligi. Ushbu tur kompyuter orqali pul vositalarini o‘g‘irlash bo‘yicha. Kompyuterdan foydalanishdagi jinoyatlarning 45 % ni aksariyati ushbu tur, ya’ni pul vositalarini o‘g‘irlash bilan bog‘liq jinoyatlar tashkil etadi.

QFT - telefon firibgarligi: telefon tizimiga xizmat ko‘rsatuvchi telekommunikatsion xizmatlarga kompyuterning protokollari va protseduralariga tajovuz qilish orqali kirish

Ma’lumotdan noqonuniy nusxa olish (QR) o‘z ichiga quyidagi jinoyatlarni oladi:

QRG/QRS – kompyuter o‘yinlarini va qonun himoyasidagi boshqa dasturiy ta’minotdan noqonuniy nusxa olish, tarqatish yoki chop etish.

QRT – yarimo‘tkazgichli qurilmalarning topografiyasidan noqonuniy nusxa olish: qonun himoyasidagi yarimo‘tkazgichli qurilmalar topografiyasidan noqonuniy nusha olish, yarimo‘tkazgichli qurilma yoki uning topografiyasini noqonuniy tijorat qilish yoki shu maqsadda import qilish.

Kompyuter sabotaji (QS) o‘z ichiga quyidagi jinoyatlarni oladi:

QSH – apparat ta’minot yordamida sabotaj: kiritish, o‘zgartirish, o‘chirish, kompyuter a’lumotlari yoki dasturlarini bostirish; kompyuter yoki telekommunikatsiya tizimining faoliyatiga xalal berish maqsadida kompyuter tizimiga aralashish.

QSS – dasturiy ta’minotli kompyuter sabotaji: kompyuter ma’lumotlarini yoki dasturlarni noqonuniy o‘chirish, zarar yetkazish, yaroqsiz holatga keltirish.

Boshqa turdagi kompyuter jinoyatlari (QZ) quyidagicha tasniflanadi:

QZB - elektron e’lonlar taxtasi yordamida (BBC) jinoiy faoliyatga taaluqli ma’lumotlarni saqlash, almashish va tarqatish;

QZE – tijorat siri hisoblangan ma’lumotni o‘g‘irlash: moliyaviy zarar yetkazish yoki moliyaviy manfaat olish maqsadida noqonuniy tijorat sirini qo‘lga kiritish yoki uzatish.

QZS - Maxfiy turdagi ma’lumotlarni saqlash, almashish va tarqatish yoki joyini almashtirish uchun kompyuter tizimlari va tarmoqlaridan foydalanish.

Ba’zi bir kompyuter jinoyati bo‘yicha mutaxassislar quyida keltirilgan noananviy nomli manipulyatsiya usullarini aloxida guruhda keltirishadi.

“Vaqtinchalik bomba” - aniq bir vaqtda ishga tushuvchi mantiqiy bombaning bir turi;

“Asinxron xujum” (asynchronous attack) kompyuter tizimi tomonidan ikki va undan ortiq foydalanuvchilari komandalarining bajarilishi va aralashuvi natijasida xosil bo‘ladi

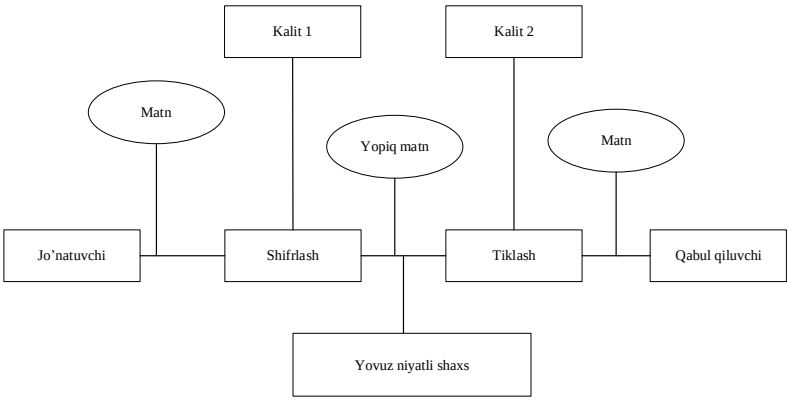
Turli xil adabiyotlarda kriminalistik xarakteristikaning tashkiliy qismlarining turli variantlari mavjud. Har bir kriminalistning kriminalistik xarakteristika haqida,

uning darajalari haqida qarashlari turlichadir. Lekin har bir variantlar qaysidir tomonlari bo‘yicha bir-biriga o‘xshash. Tadqiqotchilarning katta qismi kriminalistik xarakteristikani Jinoyat Kodeksining (278, 273, 274-moddalar) moddalari bo‘yicha uch xil jinoyat ko‘rinishida tasvirlashadi. Jinoyat Kodeksining birgina “kompyuter jinoyatlari”ga tegishli moddalari juda ham ko‘pdir, ular bir-biridan jinoyatchining shaxsiyati, jinoyat holatlari va qoladirgan jinoyat izlari bilan farqlanadi. Masalan, bir dasturchi asabiy holatda virus yaratdi va uni tarmoqga joyladi, butun dunyoga zarar yetkazish maqsadida. Yana bir misol, reklama tashkiloti hodimi zombi tarmoq yordamida (bot_net) o‘zining spam habarlarini tarqatadi. Ikkala holatda ham Jinoyat Kodeksining $278^6$-moddasiga (“zararkunanda dasturlarni yaratish va tarqatish”) binoan jinoyat sodir etilmoqda. Kriminalistik harakteristika tajribadan kelib chiqib, buning uchun juda ko‘p jinoyatlarni tahlil qilish lozim. Kompyuter jinoyatlari bilan tahlil ishlari kvartira o‘g‘riligi yoki mashina o‘g‘rilari kabi keng tarqalgan emas. Kompyuter jinoyatlari sohasida qonunbuzarliklar kam kuzatiladi, aniqlanadi va sodir etiladi. Bu sohada tajriba yillar davomida izlanishlar natijasida yuzaga keladi. Bir jinoyatni misol qilib olamiz: zombiye tarmoqlarni qurish. Bu qonunbuzarlik JK ning $278^6$-moddasiga asoslangan. Ammo bu jinoyatni fosh etish holatlari O‘zbekiston Respublikasida umuman kuzatilmagan, butun dunyo bo‘ylab esa, 3 yoki 4-marta kuzatilgan.

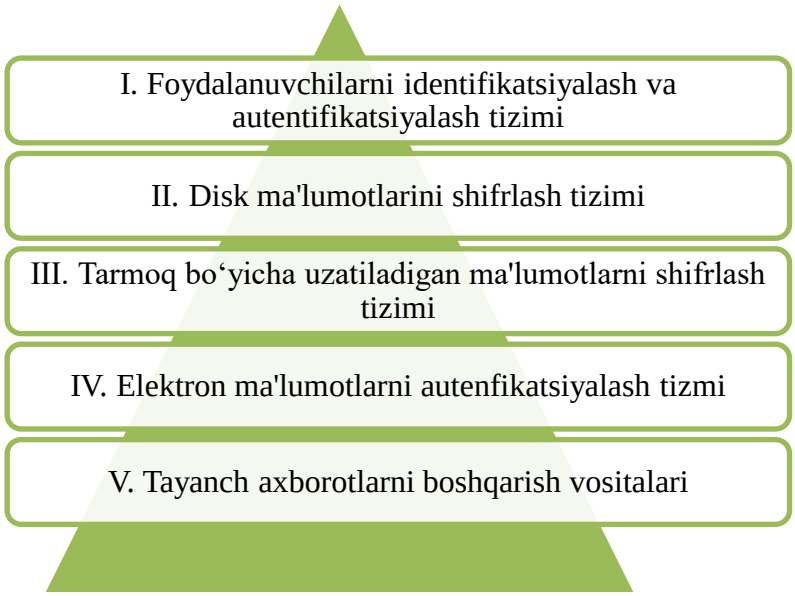
Amerika qo‘shma shtatlari jinoyat kodeksining 18-moddasi jinoyatlar va jinoiy protsedura qismi, 1-bob Jinoyatlar, tovlamachilik va noto‘g‘ri rasmiy hisobotlar qismi 1030-bo‘limda tovlamachilik va kompyuterlar bilan bog‘liq jinoiy faoliyat bo‘yicha quyidagicha tavsiflangan: kimda kim bila turib ruhsatsiz kompyuterga kirsa va ruhsat berilmagan kirishdan oshib ketsa bunday xatti-harakat orqali qo‘shma shtatlar hukumatiga tegishli bo‘lgan ma’muriy buyruq yoki chet aloqalar milliy mudofaa sabablariga ko‘ra ruhsat berilgan va har qanday cheklangan ma’lumotlarni oshkor qilishga qarshi himoya ehtiyojidan kelib chiqqan qonun 1954-yilgi atom energiyasi akti bo‘limida tushuntirilganidek bunday axborot qo‘shma shtatlarga zarar yetkazsa yoki har qanday chet el millatiga xabar qilsa, yetkazsa, translyatsiya qilish yoki xabar qilishga, yetkazishga sabab bo‘lish yoki xabar qilish vakolatlari hech kimga berilm.

Axborotlarni kriptografik himoyalash usullari. Kriptografiya - ma’lumotlarni o‘zgartirish usullarining to‘plami bo‘lib, ma’lumotlarni himoyalash bo‘yicha quyidagi ikkita asosiy muammolarni hal qilishga yo‘naltirilgan: maxfiylik; yaxlitlilik. Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o‘zgartira olmaslik haqida dalolat beradi. Kriptografiya tizimini sxematik ravishda quyidagicha tasvirlash mumkin: Bu yerda kalit qandaydir himoyalangan kanal orqali jo‘natiladi (chizmada punktir chiziklar bilan tasvirlangan). Umuman olganda, ushbu mexanizm simmetriyali bir kalitlik tizimiga taalluqlidir.Assimmetriyali ikki kalitlik kriptografiya tizimini sxematik ravishda quyidagicha tasvirlash mumkin:bu holda himoyalangan kanal bo‘yicha ochiq kalit jo‘natilib, maxfiy kalit jo‘natilmaydi. Yovuz niyatli shaxslar o‘z maqsadlariga erisha

olmasa va kriptotahlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u holda kriptotizim kriptomustahkam tizim deb aytiladi. Kriptotizimning mustaxkamligi uning kaliti bilan aniqlanadi va bu kriptotahlilning asosiy qoidalaridan biri bo‘lib hisoblanadi. Ushbu ta’rifning asosiy ma’nosi shundan iboratki, kriptotizim barchalarga malum tizim hisoblanib, uning o‘zgartirilishi ko‘p vaqt va mablag‘ talab qiladi, Shu bois ham faqatgina kalitni o‘zgartirib turish bilan axborotni himoyalash talab qilinadi. Foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash tizimi. Ushbu tizim foydalanuvchidan olingan ma’lumot bo‘yicha uning shaxsini tekshirish, haqiqiyligini aniqlash va shundan so‘ng unga tizim bilan ishlashga ruxsat berish lozimligini belgilab beradi.




2.2-rasm. Assimmetrik ikki kalitlik kriptografiya tizimini sxemasi(shriftni kattaroq qilish kerak)




2.3-rasm. Kompyuter ma’lumotlarini himoyalashning texnik-dasturiy vositalari

Ushbu tizim foydalanuvchidan olingan ma’lumot bo‘yicha uning shaxsini tekshirish, haqiqiyligini aniqlash va shundan so‘ng unga tizim bilan ishlashga ruxsat berish lozimligini belgilab beradi.

Bu holda asosan foydalanuvchidan olinadigan ma’lumotni tanlash muammosi mavjud bo‘lib, uning quyidagi turlari mavjud:

- foydalanuvchiga ma’lum bo‘lgan maxfiy axborot, masalan, parol, maxfiy kalit va boshqalar;

- shaxsning fiziologik parametrlari, masalan, barmoq izlari, ko‘zning tasviri va boshqalar.

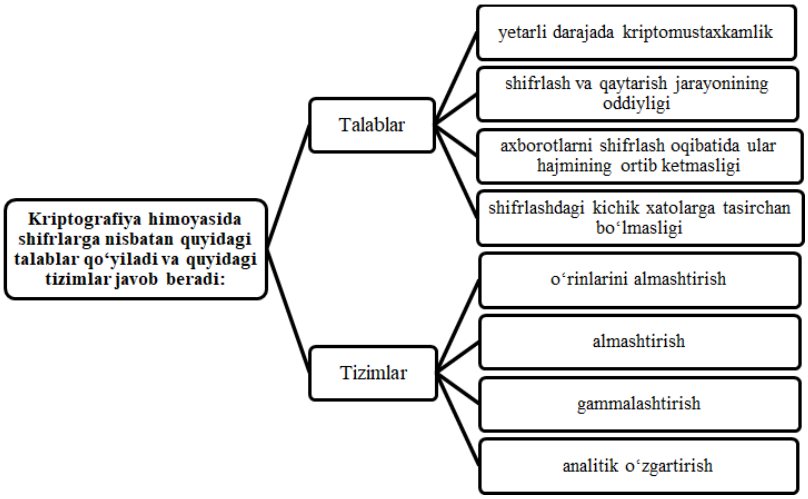
Birinchisi an’anaviy, ikkinchisi esa biometrik identifikatsiyalash tizimi, deyiladi. Disk ma’lumotlarini shifrlash tizimi. Ushbu tizimning asosiy maqsadi diskdagi ma’lumotlarni himoyalashdir. Bu xolda mantiqiy va jismoniy bosqichlar ajratiladi. Mantiqiy bosqichda fayl asosiy ob’yekt sifatida bo‘lib, faqatgina ba’zi bir fayllar himoyalanadi. Bunga misol qilib, arxivator dasturlarini keltirish mumkin. Jismoniy bosqichda disk to‘laligicha himoyalanadi. Bunga misol sifatida Norton Utilitiyes tarkibidagi Diskret shifrlovchi dasturni keltirish mumkin. Tarmoq bo‘yicha uzatiladigan ma’lumotlarni shifrlash tizimi. Ushbu tizimda ikki yo‘nalishni ajratish mumkin:

- kanal bo‘yicha, ya’ni aloqa kanallari bo‘yicha jo‘natiladigan barcha ma’lumotlarni shifrlash;

- abonentlar bo‘yicha, ya’ni aloqa kanallari bo‘yicha jo‘natiladigan ma’lumotlarning faqatgina mazmuniy qismi shifrlanib, qolgan xizmatchi ma’lumotlarni ochiq qoldirish.

Elektron ma’lumotlarni autentifikatsiyalash tizimi. Ushbu tizimda tarmoq bo‘yicha bajariladigan elektron ma’lumotlar almashuvida xujjatni va uning muallifini autentifikatsiyalash muammosi paydo bo‘ladi. Tayanch axborotlarni boshqarish vositalari. Ushbu tizimda tayanch axborotlar sifatida kompyuter tizimi va tarmog‘ida qo‘llaniladigan barcha kriptografik kalitlar tushuniladi. Bu xolda kalitlarni generatsiyalash, saqlash va taksimlash kabi boshqaruv funksiyalarini ajratishadi.

O‘rinlarini almashtirish shifrlash usuli bo‘yicha boshlangich matn belgilarining matnning ma’lum bir qismi doirasida maxsus koidalar yordamida o‘rinlari almashtiriladi. Almashtirish shifrlash usuli bo‘yicha boshlangich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtirilali. Gammalashtirish usuli bo‘yicha boshlangich matn belgilari shifrlash gammasi belgilari, ya’ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi. Tahliliy o‘zgartirish usuli bo‘yicha boshlangich matn belgilari analitik formulalar yordamida o‘zgartiriladi, masalan, vektorni matritsaga ko‘paytirish yordamida.



2.4-rasm. Kriptografiya himoyasida shifrlashga nisbatan qo‘yiladiga talab va tizimlar.

Bu yerda vektor matndagi belgilar ketma-ketligi bo‘lsa, matritsa esa kalit sifatida xizmat qiladi.O‘rinlarni almashtirish usullari ushbu usul eng oddiy va eng qadimiy usuldir. O‘rinlarni almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin:

- shifrlovchi jadval;
- sexrli kvadrat.

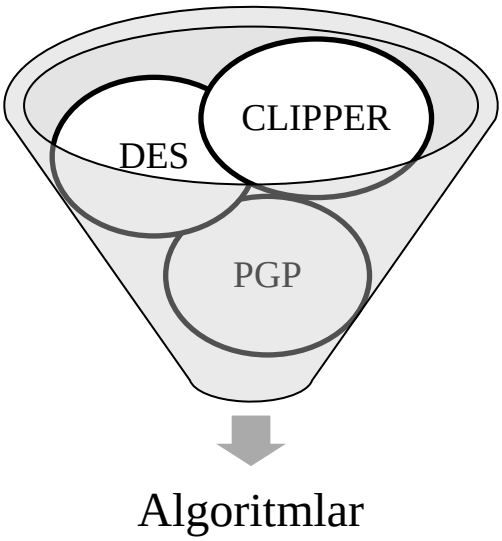
Shifrlovchi jadval usulida kalit sifatida quyidagilar qo‘llaniladi:

- jadval o‘lchovlari;
- so‘z yoki so‘zlar ketma-ketligi;
- jadval tarkibi xususiyatlari.

Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin:

- Sezar usuli;
- Affin tizimidagi Sezar usuli;
- Tayanch so‘zli Sezar usuli va boshqalar.

Xozirgi vaqtda kompyuter tarmoqlarida tijorat axborotlari bilan almashishda uchta asosiy algoritmlar, ya’ni DES, CLIPPER va PGP algoritmlari qo‘llanilmoqda.




2.5-rasm. Kompyuter tarmoqlarida tijorat axborotlari bilan almashishdagi asosiy algoritmlar.

DES va CLIPPER algoritmlari integral sxemalarda amalga oshiriladi. DES algoritmining kriptomustaxkamligini quyidagi misol orqali ham baxolash mumkin: 10 mln. AQSH dollari harajat qilinganda DES shifrlash ochish uchun 21 minut, 100 mln, AQSH dollari harajat qilinganda esa 2 minut sarflanadi. CLIPPER tizimi SKIPJACK shifrlash algoritmini o‘z ichiga oladi va bu algoritm DES algoritmidan 16mln, marta kuchlirokdir.

PGP algoritmi esa 1991-yilda Filipp Simmerman (AQSH) tomonidan yozilgan va elektron pochta orqali kuzatiladigan xabarlarni shifrlash uchun ishlatiladigan PGP

dasturlar paketi yordamida amalga oshiriladi, FGP dasturiy vositalari Internet tarmog‘ida elektron pochta orqali axborot jo‘natuvchi foydalanuvchilar tomonidan shifrlash maqsadida keng foydalanilmokda. PGP (Pretty Good Privacy) kriptografiya dasturining algoritmi kalitli, ochiq va yopiq bo‘ladi.

PGP algoritmi esa 1991-yilda Filipp Simmerman (AQSH) tomonidan yozilgan va elektron pochta orqali kuzatiladigan xabarlarni shifrlash uchun ishlatiladigan PGP dasturlar paketi yordamida amalga oshiriladi, FGP dasturiy vositalari Internet tarmog‘ida elektron pochta orqali axborot jo‘natuvchi foydalanuvchilar tomonidan shifrlash maqsadida keng foydalanilmoqda. PGP (Pretty Good Privacy) kriptografiya dasturining algoritmi kalitli, ochiq va yopiq bo‘ladi.

Xulosa

Kiberjinoyatdan himoyalanish choralari tahlili korxonalarda kiberxavfsizlikni oshirish uchun muhim bir usul hisoblanadi. Bu tahlil, korxonalarda mavjud bo‘lgan ma‘lumotlar va tizimlar bilan bog‘liq xavfsizlik risklarini aniqlash va ularga qarshi qo‘llaniladigan choralar va tadbirlarni belgilashga yordam beradi. Tahlil jarayoni davomida quyidagi muhim nuqtalar ko‘rsatiladi:

- Ma‘lumotlarni tahlil qilish: Korxonalarda mavjud bo'lgan ma‘lumotlar, tizimlar va xavfsizlik tizimlari tahlil qilinadi. Bu tahlil korxonalarda risklarni belgilash, xavfsizlik ahamiyat darajalarini aniqlash mumkin.
- Choralar va tadbirlar: Tahlil natijalariga asosan korxonalarga choralar va tadbirlar tavsiya qilinadi. Bu choralar orqali xavfsizlik so‘rovlari va yangilanishlarni kuzatib borish, xavfsizlik xususiyatlari kengaytirilishi, xavfsizlik bilan bog‘liq kadrlar va xizmatlar belgilanishi kuzatiladi.
- Monitoring va tahlil: Tahlil davomida korxonalarda monitoring va tahlil jarayonlari amalga oshiriladi. Bu jarayonlar orqali jinoyatlar yuzasidan yuzaga kelgan o‘zgarishlar tez aniqlanib, xavfsizlik holatlarining tahlili va statistik analizlar olib boriladi.
- Natijalar va tavsiyalar: Tahlil natijalari asosida korxonalarga xavfsizlik resurslarini kengaytirish, xavfsizlik bilan bog‘liq kadrlarni tayyorlash, monitoring tizimlarini rivojlantirish va xavfsizlik siyosatini yangilash tavsiya qilinadi.

## FOYDALANILGAN ADABIYOTLAR:

- S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O’quv qo’llanma. – T.: «Aloqachi», 2020, 221 bet.
- Cyber Security Policy Guidebook
- Jennifer L. Bayuk Independent Cyber Security Governance Consultant Industry Professor at Stevens Institute of Technology, Hoboken
- NJ Jason Healey Director of the Cyber Statecraft Initiative Atlantic Council of the United States, Washington
- D.C. Paul Rohmeyer Information Systems Program Director Howe School of

Technology Management Stevens Institute of Technology, Hoboken

- NJ Marcus H. Sachs Vice President for National Security Policy Verizon Communications, Washington
- D.C. Jeffrey Schmidt Chief Executive Officer JAS Communications LLC, Chicago, IL
  Joseph Weiss Professional Engineer Applied Control Solutions, LLC, Cupertino, CA