4 – MAVZU: AXBOROT XAVFSIZLIGI VA AXBOROTLARNI HIMOYALASH USULLARI

1. Axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo‘ladigan taxdidlar, xujumlar va zaifliklar,

2. Axborot xavfsiligi sohasiga oid xalqaro va milliy me’yoriy-xuquqiy baza, xavfsizlik modellari.

3. Identifikatsiya va autentifikatsiya,

4. Kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlari,

5. Axborotni himoyalashda tarmoqlararo ekranlarning o‘rni, operatsion tizim himoyasi, axborot sirqib chiqish kanallari va ularni aniqlash hamda ob’ektlarni injener himoyalash va texnik qo‘riqlash masalalari.

6. Elektron raqamli imzo va undan foydalanish texnologiyalari.

1. Axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo‘ladigan taxdidlar, xujumlar va zaifliklar,

Komp`yuterni bexato, turi va puxta ishlashi undagi qimmatli ma`lumotlarni saqlanishini ta`minlaydi va ma`lumotlar himoyalanadi. Fuqarolarni tinchligini, xavfsizligini ta`minlashda qonun turadi.

Hisoblash texnika sohasida esa qonunlarni yaratish jarayoni hisoblash texnika va axborot kommunikatsiya texnologiyalarini rivojlanish tezligiga eta olmayapti. SHuning uchun Komp`yuter xavfsizligi ko`proq himoyalash tadbirlariga suyanadi.

Axborot xavfsizligi deb, ma`lumotlarni yo`qotish va o`zgartirishga yo`naltirilgan tabiiy yoki sun`iy xossali tasodifiy va qasddan ta`sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va xujjatlarni o`g`irlash yoki nusxa olishdan iborat bo`lsa, hozirgi paytdagi xavf esa komp`yuter ma`lumotlari to`plami, elektron ma`lumotlar, elektron massivlardan ularning egasidan ruxsat so`ramasdan foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta`minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta`minlovchi qat’iy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar etkazmokchi bo`lgan nohuquqiy muomaladan xar qanday xujjatlashtirilgan, ya`ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo`yilgan xolda moddiy jismda qayd etilgan axborot ximoyalanishi kerak.

Axborotni ximoyalashning maqsadlari kuyidagilardan iborat:

- axborotning kelishuvsiz chikib ketishi, ugirlanishi, yukotilishi, uzgartirilishi, soxtalashtirilishlarning oldini olish;
- shaxs, jamiyat, davlat xavfsizliligiga bo’lgan xavf – xatarning oldini olish;
- axborotni yuk qilish, uzgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish;
- xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta`minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish;
- axborot tizimida mavjud bo’lgan shaxsiy ma`lumotlarning shaxsiy maxfiyligini va konfidentsialligini saklovchi fukarolarning konstitutsion xukuklarini ximoyalash;
- davlat sirini, konunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saklash;
- axborot tizimlari, texnologiyalari va ularni ta`minlovchi vositalarni yaratish, ishlab chikish va kullashda sub`ektlarning xukuklarini ta`minlash.

2. Axborot xavfsiligi sohasiga oid xalqaro va milliy me’yoriy-xuquqiy baza, xavfsizlik modellari.

Axborotni qonunga xilof ravishda ishlatishiga to`sqinlik qiladigan uchinchi chegara ma’muriy usullardir. Barcha toifali ma’muriyatlar huquqiy me’yorlarni va ijtimoiy aspektlarni

hisobga olgan holda axborotni himoya qilishni ma’muriy choralarini aniqlaydilar. Bu choralar tashkiliy xarakterli choralarga tegishli bo`ladi. Ular reglamentlaydilar:

- KT va T larini ishlash jarayonini;
- tizimning barcha resurslarini ishlatishni;
- xodimlarning faoliyatini;
- foydalanuvchilarning tizim bilan o`zaro ta’sirlashish tartibini, bunda xavfsizlik xavflarini amalga oshirish imkoniyatini yuqori darajada kiyinlashtirish yoki inkor qilish ko`zda tutiladi.

Ma’muriy choralar o`z ichiga oladilar:

- KT va T larida axborotni qayta ishlash qoidalarini qayta ishlab chiqishni;
- jihozlarni, kompyuter tizimlari va tarmoqlari vositalarini loyihalashda va montaj qilishdagi harakatlar to`plamini (stixiyalarni, yong`inlarni, er qimirlashlarni, binolarni qo`riq-lashni va h.k. ta’sirlarini inobatga olish);
- mutaxassislarni va xodimlarni tanlashdagi va tayyorlashdagi harakatlar to`plami (yangi xodimlarni tekshirish, ularni maxfiy axborot bilan ishlash tartibi bilan tanishtirish, uni qayta ishlash qoidalarini buzganligi uchun javobgarlik choralari bilan tanishtirish; xodimlarni o`z mansablaridan foydalanishdan foyda bo`lmagan sharoitlarni yaratish va h.k.);
- ishonchli o`tish rejimini tashkil etish;
- hujjatlarni va maxfiy axborot tashuvchilarni hisobga olishni, saqlashni, ishlatishni va yo`qotishni tashkil etish;
- murojaat qilish cheklanishlarini rekvizitlarini taqsimlash (parollarni, kalitlarni, vakolatlarni va h.k.);
- tizimdan foydalanuvchilarni va xodimlarni ishlashi ustidan yopiq (bildirmasdan) nazorat qilishni tashkil etish;
- jihozlarni va dastur ta’minotini loyihalashda, ishlab chiqishda, ta’mirlashda va o`zgartirishda harakatlar to`plamini (ishlayotgan texnik va dasturli vositalarni sertifikatlash, barcha o`zgartirishlarga qat’iy ruxsat berish, ko`rib chiqish va tasdiqlash, himoya qilish talablariga qanoatlanganligini tekshirish, o`zgartirishlarni hujjat bilan qayd qilish va h.k.).

Alohida ta’kidlash joizki, tizimlarni ma’muriy himoya qilishning harakatdagi choralari qayta tashkil etilmaguncha, boshqa choralar shubxasiz, samarasiz bo`ladi.

Himoya qilishning ma’muriy-tashkiliy choralari axlokiy-etikaga nisbatan zerikarli va mashaqqatli va apparat-dasturiga nisbatan aniqlikdan ayrilgan bo`lib ko`rinishi mumkin. Ammo ular axborotni noqonuniy ishlatish yo`lidagi kuchli to`siq va himoya qilishning boshqa darajalari uchun ishonchli baza ko`rinishiga egadirlar.

Axborotni himoya qilishni huquqiy usullarida huquqiy xarakterli masalalar ko`rib chiqiladi:

- kompyuter jinoyatchiligi uchun jazolash me’yorlarini ishlab chiqish;
- dasturlovchilarni mualliflik huquqlarini himoya qilish;
- jinoiy va fuqarolik qonunchiligini, hamda kompyuter jinoyatchiligi sohasida sud ishini mukammallashtirish;
- kompyuter tizimlari ishlab chiquvchilar ustidan jamoat nazorati masalalari;
- bu masalalar bo`yicha mos xalqaro shartnomalarni qabul qilish va h.k.

Axborotni himoya qilishning modellari

Xulosa qilib, axborotning himoya qilishning tizimini shakllan-tirishni asosiy mezonlarini kompyuter tarmoqlaridagi axborotni himoya qilish modellarida umumlashtiramiz.

Tarmoqlarning axborot va apparat resurslarini xavfsizligini ta’minlaydigan ikkita model keng ishlatiladi:

1) parol’ orqali himoya qilish,

2) murojaat qilish huquqi orqali himoya qilish.

Bu modellarni yana birgalikda ishlatiladigan resurslar (resoursce level - parol’ orqali himoya qilish) darajasida himoya qilish va foydalanuvchi (user level - murojaat qilish huquqi orqali himoya qilish) darajasida himoya qilish deb ham ataladi.

3. Identifikatsiya va autentifikatsiya, kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlari

Identifikatsiyalash va auntetifikatsiyalash tizimlari ob'ektga murojaat qilishda qismining tizimlari yoki axborotni anglash va murojaat qilishni cheklash qismining tizimlari hisoblanadi. Ma'lumki, KT da axborotlar jamlanib, uni ishlatishga huquqlar, shaxsiy tashabbuskorlik tartibida yoki mansab vazifalariga mos ravishda harakat qiladigan ma'lum bir shaxslarga yoki shaxslar guruhlariga tegishlidir. Resurslarni axborot xavfsizligini taminlash, taqiqlangan murojaat qilish imkoniyatini bartaraf etish, maxfiy axborotga yoki sirli axborotga ruxsat etilgan murojaat qilishni nazoratini kuchaytirish uchun turli xil murojaat qilishni anglash, ob'ektni (sub'ektni) haqiqiyligini o`rnatish va cheklash tizimlari tatbiq qilinadi. Bunday tizimlarni qurish asosida ruxsat etilgan texnologiyalarning mos belgilari mavjud bo`lgan axborotga faqatgina shunday murojaat qilishlarning printsiplari va bajarilishi yotadi.

Ob'ektga murojaat qilishni tashkil etishda echiladigan asosiy masalalardan bittasi ob'ektga qo`yiladigan shaxslarni (murojaat qilish sub'ektlarini) identifikatsiyalash va autentifikatsiyalash hisoblanadi.

Identifikatsiyalash - murojaat qilish sub'ektlariga identifikatorlarni taqdim etish va (yoki) ko`rsatilgan identifikatorlarni, egalari (tashuvchilari) ob'ektga kirishga ruxsat etilgan, oldindan taqdim etilgan identifikatorlar ro`yxati bilan taqqoslanadi.

Autentifikatsiyalash - murojaat qilish ob'ektlarini ular ko`rsatgan identifikatorlarga to`g`ri kelishligini tekshirish, haqiqiyligini tasdiqlashdir.

Insonlarni identifikatsiyalashni atributiv va biometrik usullari mavjuddir.

Atributiv usul murojaat qilish sub'ektiga yoki noyob predmetni, yoki parolni (kodni), yoki kodni o`z ichiga olgan predmetni berishni ko`zda tutadi. Identifikatorlar murojaat qilish jarayonini avtomatlashtirish imkonini bermaydi, shaxsiyatni identifikatsiyalash va autentifikatsiyalash sub'ektiv xarakterga egadir.

KT qurilmalariga murojaat qilishni cheklovchi tizimlarda parollar va kodlar ishlatiladi. Identifikatorlar eng istiqbolli hisoblanadi, ular murojaat qilish sub'ektini identifikatsiyali kodini, o`zida saqlagan axborotning material tashuvchili, masalan plastik kartali, ko`rinishga egadir. Kod faqatgina maxsus qurilma yordamida o`qiladi. Karta koddan tashqari fotosuratni, egasi to`g`risidagi ma'lumotlarni va h.k. o`zida saqlashi mumkin.

Atributiv identifikatorlarning kamchiligi - egasining shaxsiyati bilan kuchsiz aloqa yoki aloqaning yo`qligi. Bu kamchiliklardan biometrik identifikatsiyalash usullari xalosdir, ular insonning shaxsiy biologik xususiyatlarini ishlatishga asoslangandir: barmoqlarning kapilyar naqshlari, ko`z to`rining naqshlari, qo`l panjalarining shakli, nutq xususiyatlari, yuzning shakllari va o`lchamlari, imzo dinamikasi, klaviaturada ishlash ritmi, tana hidi, tananing termik tavsiflari.

Biometrik identifikatsiyalash usullarining asosiy afzalliklari taqiqlangan murojaat qilishga intilishlarni payqashni juda yuqori ehtimolligi hisoblanadi. Xatto eng yaxshi tizimlarda ham, murojaat qilish huquqiga ega bo`lgan sub'ektni murojaat qilishini noto`g`ri inkor qilishini ehtimoli 0,01 ni tashkil etadi. Murojaat qilishni biometrik usullarini taminlash harajatlari atributiv usullarni tashkil etish harajatlaridan sezilarli oshadi. SHuning uchun, aytish mumkinki, hozircha alohida biometrik usullar amaliy xarakterga nisbatan ko`proq reklama xarakteriga egadir.

Komp`yuterni virusdan ximoyalashni uchta chegarasi mavjud:

- Virusni kelishini to`xtatish,
- **Virus hujumini oldini olish.**
- Antivirus dasturlar yordamida yo`q qilish.

Viruslardan himoyalanishni uchta usuli bor:

- Himoyani dasturiy usullari,
- Himoyani apparat usullari,
- Himoyani tashkiliy usullari.

«Kasalni davolashdan ko`ra uni oldini olish yaxshi» iborasini qo`llab virusga qarshi kurashda samaraga erishiladi. Buning uchun aloqa vositalaridan kelayotgan fayl ko`rinishidagi ma`lumotlarni AVP Kasperskaya antivirus dastur aro yordamida nazoratdan o`tkazib so`ng xotiraga yoziladi.

Komp`yuter viruslariga qarshi kurashda DcWeb, Web32, Norton Antivir. AVP Kasperski va Noviskiy antivirus dasturlari ishlatib kelinmoqda. Bu dasturlarni oxirgi versiyalarini Internet tarmog``idan olish mumkin, chunki uning antivirus bazasi har doim yangilanib boriladi. Bu dasturlar yordamida fayllarni va jildlarni xususiyatlari va o`lchamlarini o`zgarishini operativ nazorat qilib borish ta`minlanadi va displey ekraniga tekshirish hisobotlari chiqariladi.

Jahon Komp`yuter tarmog`ida ishlayotganda shuni yodda tutish kerak, maxsus dasturiy vositalar tomonidan bajarilgan barcha qonuniy va noqonuniy amallar qayd etiladi va protokol yoziladi, albatta jamlanadi.

Hozirgi kunda 80000 dan ortiq kompyuter viruslari mavjud bo`lib, ular kompyuterda ma`lumotlarning ishonchli saqlanishiga xavf soladi va kompyuter ishlashi jarayonida turli muammolar kelib chiqishiga sabab bo`ladi. SHu bois, kompyuter viruslari, ularning turlari, etkazadigan zararlari hamda ulardan himoyalanish uchun ko`riladigan choralar bilan tanish bo`lish muhim.

Kompyuter viruslari va ularni davolash.

Kompyuter virusi o`lchami bo`yicha katta bo`lmagan, maxsus yozilgan dasturdan iborat bo`lib, u o`zini boshqa dasturlarga "yozib qo`yishi", shuningdek, kompyuterda turli noxush amallarni bajara olishi mumkin. Bunday dastur ishlashni boshlaganda dastlab boshqaruvini virus oladi. Virus boshqa dasturlarni topadi va unga "yuqadi", shuningdek, qandaydir zararli amallarni (masalan, diskdagi fayl yoki fayllarning joylashish jadvalini buzadi, tezkor xotirani "ifloslaydi" va h.k.) bajaradi. Virus o`ziga tegishli amallarni bajarib bo`lgandan so`ng boshqaruvini o`zi joylashgan dasturga uzatadi. Virus joylashgan dastur odatdagidek ishini davom etgiradi. Tashqaridan dasturning "kasallanganligi" bilinmaydi.

Ko`p turdagi viruslar shunday tuzilganki, kasallangan dasturni ishga tushirganda virus kompyuter xotirasida doimiy qoladiva vaqt-vaqti bilan dasturlarni kasallaydi va kompyuterda zararli amallarni bajaradi. Virusning barcha amallari etarlicha tez va hech qanday ma`lumot eolon qilmasdan bajariladi. SHuning uchun foydalanuvchi kompyuterda qanday jarayonlar amalga oshayotganligini bilishi qiyin.

Komp`yuter ishini nazoratga olish deganda nima tushuniladi? Unga quyidagilar kiradi:

1. litsenziyasiz dasturiy taominotdan foydalanmaslik;
2. tashqaridan kiritiladigan viruslarning oldini olish;
3. tizimga sanktsiyasiz kiruvchi xakerlarga imkon bermaslik.

Axborot va dasturlar xavfsizligini taominlash uchun quyidagilar zarur bo`ladi: birinchidan, litsenziyalangan dasturiy taominotni ishlatish; ikkinchidan, tashqi tarmoqlarga ulanishda filtr cheklovchilar o`rnatish (viruslardan himoyalanish va sanktsiyasiz foydalanishni cheklash).

Albatta, bunday himoya vositalari uzluksiz rivojlanib takomillashib bormoqda.

Komp`yuter viruslarini quyidagi guruhlarga ajratish mumkin:

- Diskning yuklanish sektorlarini buzadigan yuklanish viruslari;
- Bajariladigan fayllar - com, exe, sys, bat fayllarini buzuvchi fayl viruslari;
- Diskning yuklanish sektori va bajariladigan fayllarni buzadigan yuklanish fayli viruslari;
- Stels - ko`rinmas viruslar;
- Microsoft Word muharriri yordamida hosil qilingan ma`lumotli fayllarni yozuvchi makrobuyruq viruslari.

Bundan tashqari, boshqa turdagi viruslar ham mavjud. Viruslardan himoyalanishda axborotni himoya qilishning umumiy vositalaridan foydalanish kifoya qilmaydi. Buning uchun maxsus dasturlardan foydalanish zarur bo`ladi. Bu dasturlarni bir necha turga ajratish mumkin: detektorlar, vaktsinalar (immunizatorlar), doktorlar, revizorlar (fayl va disklarning tizimli sohalaridagi o`zgarishlarni nazorat qiluvchi dasturlar), doktor - revizorlar va filtrlar (virusdan himoyalanish uchun mo`ljallangan rezident dasturlar). Ularning xususiyatlarini ko`rib chiqamiz

Virusdan ko`riladigan zararlarga quyidagilarni misol qilib ko`rsatish mumkin:

- Komp`yuter qattiq diski yoki tezkor xotirasining ifloslanishi - virusli dastur ko`payishi jarayonida butun qattiq diskni o`zining nuqtalari yoki boshqa belgilari bilan to`ldirishi mumkin. Bularni u tezkor xotiraga ham yozishi va shu bilan uning hajmini kamaytirishi mumkin;
- Fayllar joylashish jadvalining buzilishi. U buzilsa, diskdan kerakli fayl va katalogni o`qish mumkin bo`lmaydi;
- Yuklanish sektoridagi ma`lumotlarning buzilishi. Yuklanish sektori diskdagi maxsus dastur bo`lib, uning buzilishi disk ishini to`xtatib qo`yadi;
- Diskni qayta formatlash - diskdagi barcha axborot butunlay yooqoladi
- Diskka biror xabar chiharishi yoki biror kuyni ijro etishi mumkin. Ko`p hollarda bu xabar tushunarsiz bo`ladi;
- Komp`yuterning o`z-o`zidan qayta yuklanishi;
- Tugmachalar majmui ishini to`xtatib qo`yishi;
- Dasturli va ma`lumotli fayllar mazmunining o`zgarishi. Virus ma`lumotlarni ixtiyoriy ravishda aralashtirib qo`yadi va hokazo.

Oddiy virusdan zararlanishni virusga qarshi dasturlar yordamida oson aniqlashi mumkin. Polimorf (murakkab tuzilishga ega) viruslarni bu usul bilan aniqlashi qiyin chunki ular o`z-o`zini nusxalashda ko`rinishini o`zgartiradi.

Hozirgi vaqtda viruslarni yo`qotish uchun ko`pgina usullar ishlab chiqilgan va bu usullar bilan ishlaydigan dasturlarni **antiviruslar** deb atashadi. Antiviruslarni, kullanish usuliga ko`ra, quyidagilarga ajratishimiz mumkin: ***detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar.***

Fil'tr dasturlar komp`yuter ishlash jarayonida viruslarga xos bo`lgan shubhali harakatlarni topish uchun ishlatiladi.

Bu xarakatlar quyidagicha bo`lishi mumkin:

- fayllar atributlarining o`zgarishi;
- disklarga doimiy manzillarda ma`lumotlarni yozish;
- diskning ishga yuklovchi sektorlariga ma`lumotlarni yozib yuborish.

Komp`yuterni viruslar bilan zararlanishidan saklash va axborotlarni ishonchli saqlash uchun quyidagi qoidalarga amal qilish lozim:

- komp`yuterni zamonaviy antivirus dasturlar bilan ta`minlash;
- disketalarni ishlatishdan oldin har doim virusga qarshi tekshirish;
- qimmatli axborotlarning nusxasini har doim arxiv fayl ko`rinishida saqlash.

Komp`yuter viruslariga karshi kurashning quyidagi turlari mavjud:

- viruslar komp`yuterga kirib buzgan fayllarni o`z holiga qaytaruvchi dasturlarning mavjudligi;
- komp`yuterga parol' bilan kirish, disk yurituvchilarning yopiq turishi;
- disklarni yozishdan ximoyalash;
- litsenzion dasturiy ta`minotlardan foydalanish va o`g`irlangan dasturlarni qo`llamaslik;
- antivirus dasturlaridan keng foydalanish;
- davriy ravishda komp`yuterlarni antivirus dasturlari yordamida viruslarga qarshi tekshirish.

Antivirus dasturlaridan DrWeb, Adinf, AVP, VootCHK va Norton Antivirus, Kaspersky Security kabilar keng foylalaniladi.

4. Axborotni himoyalashda tarmoqlararo ekranlarning o'rni, operatsion tizim himoyasi, axborot sirqib chiqish kanallari va ularni aniqlash hamda ob'ektlarni injener himoyalash va texnik qo'riqlash masalalari

Tarmoqlararo zkranlarni amalga oshirish siyosatiga mos ravishda ichki tarmoqning resurslariga murojaat qilish qoidalari aniqlanadi. Eng avvalo himoya qilish tizimini qanchalik darajada "ishonchli" yoki "shubhali" ekanligini o`rnatish kerakdir. Boshqacha aytganda, ichki resurslarga murojaat qilish qoidalari quyidagi printsiplardan bittasiga asoslanishi kerak:

1) ochiq shaklda taqiqlangan barcha narsalarga ruxsat bermaslik;
2) ochiq shaklda ta'qiqlanmagan barcha narsalarga ruxsat berish.

Tarmoqlararo ekranni birinchi printsip asosida amalga oshirish sezilarli himoya qilinganlikni ta’minlaydi. Lekin bu printsipga mos ravishda shakllantirilgan murojaat qilish qoidalari foydalanuvchilarga katta noqulayliklar keltirib chiqarishi mumkin, bundan tashqari esa ularni amalga oshirish etarlicha qimmatga tushadi. Ikkinchi printsipni amalga oshirishda ichki tarmoq xakerlarning hujumlaridan kamroq himoyalangan bo`ladi. Lekin undan foydalanish qulayroqdir va kam harajatlarni talab qiladi.

Ichki tarmoqni tarmoqlararo ekranlar yordamida himoya qilish samaradorligi nafaqatgina tarmoq servislariga va ichki tarmoqning resurslariga murojaat qilishning tanlangan siyosatiga emas, balki tarmoqlararo ekranni asosiy tashkil etuvchilarini oqilona tanlash va ishlatishga ham bog`liqdir.

Tarmoqlararo ekranlarga funktsional talablar o`z ichiga oladi:

- tarmoq ekranida filtrlashga talablar;
- amaliy darajada filtrlashga talablar;
- filtrlash va ma’muriylashtirish qoidalarini sozlash bo`yicha talablar;
- tarmoqli autentifikatsiyalash vositalariga talablar;
- jurnallarni va hisobga olishlarni tatbiq qilish bo`yicha talablar.

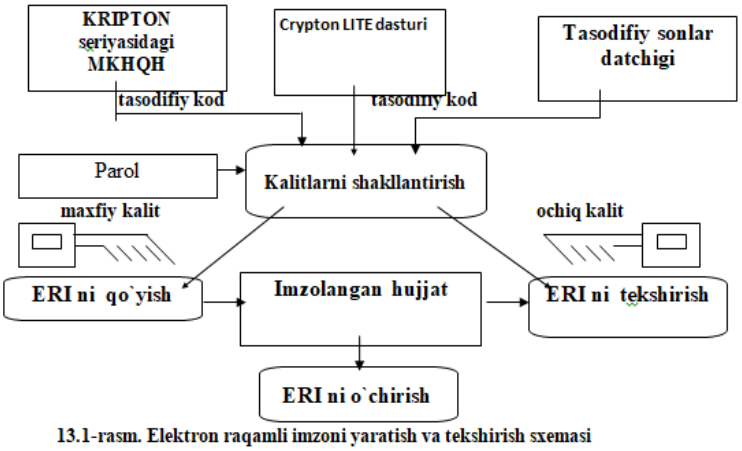
Elektron raqamli imzo (ERI) imzolanayotgan hujjat oxiriga yoki alohida faylga joylashtiriladigan baytlar ketma-ketligi ko`rinishiga egadir. ERI hujjat mazmuni, maxfiy kalit va hujjatni imzolayotgan shaxsning paroli asosida shakllantiriladi. Har bir maxfiy kalitning imzosini tekshirish uchun ochiq kalit yaratiladi.

Elektron raqamli imzo - elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o’zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo’qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo;

elektron raqamli imzoning yopiq kaliti - elektron raqamli imzo vositalaridan foydalangan holda xosil qilingan, faqat imzo qo’yuvchi shaxsning o’ziga ma’lum bo’lgan va elektron hujjatda elektron raqamli imzoni yaratish uchun mo’ljallangan belgilar ketma-ketligi;

elektron raqamli imzoning ochiq kaliti - elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, elektron raqamli imzoning yopiq kalitiga mos keluvchi, axborot tizimining har qanday foydalanuvchisi foydalana oladigan va elektron hujjatdagi elektron raqamli imzoning haqiqiyligini tasdiqlash uchun mo’ljallangan belgilar ketma-ketligi;

elektron hujjat - elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan hamda elektron hujjatning uni identifikatsiya qilish imkonini beradigan boshka rekvizitlariga ega bo’lgan axborot.



13.1-rasm. Elektron raqamli imzoni yaratish va tekshirish sxemasi