

REJA:

10.1 Axborot xavfsizligiga tahdidlarning asosiy turlari. Axborot xavfsizligini ta'minlash.

10.2 Kriptografik axborot himoyasi tamoyillari.

10.3 Internet tarmog'i orqali uzoqlashtirilgan hujumlardan himoya usullari va vositalari.

10.4 Elektron to'lov tizimlarida axborot xavfsizligi

10.1 Axborot xavfsizligiga tahdidlarning asosiy turlari. axborot xavfsizligini ta'minlash

Axborot tizimi tushunchasini kiritishdan oldin tizim (sistema) deganda nimani tushunishimizni aniqlab olaylik. Tizim (sistema) deganda, yagona maqsad yo'lida bir vaqtning o'zida ham yaxlit, ham o'zaro bog'langan tarzda faoliyat ko'rsatuvchi elementlar (ob'ektlar) majmuasi tushuniladi. Demak, har qanday tizim biror-bir aniq maqsad yo'lida xizmat qiladi. Masalan, sizga ma'lum bo'lgan shahar telefon tarmoqlari tizimi, insondagi yurak qon-tomir tizimi, asab tizimi va boshqalar sun'iy yaratilgan va tabiiy tizimlarga misol bo'la oladi. Ularning har biri tizimga qo'yiladigan barcha shartlarga javob beradi, ya'ni, har biri o'ziga xos yagona maqsad yo'lida faoliyat ko'rsatadi va tizimni tashkil etuvchi elementlardan iborat.

Quyidagi jadvalda elementlari va asosiy maqsadi ko'rsatilgan holda tizimlarga yana bir nechta misollar keltirilgan.

№	Tizim turi	Tizim elementlari	Tizimning asosiy maqsadi
1.	Korxona	Odamlar, qurilmalar, materiallar, bino va h.k.	Mahsulot ishlab chiqarish
2.	Kompyuter	Elektron va elektromexanik qurilmalar	Ma'lumotlarni qayta ishlash
3.	Telekommunikasion tizim	Kommunikasiya vositalari, elementlar, aloqa kanallari, qurilmalar	Aloqa kanallarini o'zaro bog'lash va ma'lumot almashinuvini ta'minlash
4.	Axborot tizimi	Kompyuterlar, kompyuter tarmoqlari, odamlar, axborot, dasturiy ta'minot va boshqalar.	Axborotlarni avtomatlashgan holda qayta ishlash

Informatikada «tizim» tushunchasi ko'proq texnik vositalar, asosan, kompyuterlar va murakkab ob'ektlarni boshqarishga nisbatan ishlatiladi. «Tizim» tushunchasiga «axborot» so'zining ko'shilishi uning belgilangan funksiyasini va yaratilish maqsadini aniq aks ettiradi.

Axborot tizimi — belgilangan maqsadga erishish yoʻlida axborotni yigʻish, saqlash, qayta ishlash va uzatish uchun qoʻllaniladigan usullar, vositalar va shaxslarning oʻzaro bogʻlangan majmuasidir.

Axborot tizimlari jamiyat paydo boʻlgan paytdan boshlab mavjud boʻlgan, chunki rivojlanishining turli bosqichida jamiyat oʻz boshqaruvi uchun tizimlashtirilgan, oldindan tayyorlangan axborotni talab etgan. Bu, ayniqsa, ishlab chiqarish jarayonlari — moddiy va nomoddiy neʼmatlarni ishlab chiqarish bilan bogʻliq jarayonlarga tegishlidir. Chunki ular jamiyat rivoji uchun xayotiy muhim ahamiyatga ega. Aynan ishlab chiqarish jarayonlari tezkor takomillashadi. Ularning rivojlanib borishi bilan boshqarish ham murakkablashadiki, oʻz navbatida, u axborot tizimlarini takomillashtirish va rivojlantirishni ragʻbatlantiradi. Shu sababli, avvalo, boshqaruv tizimi nima ekanligini bilib olaylik.

Kibernetik yondashuvga muvofiq boshqaruv tizimi boshqaruv ob'ekti (masalan, korxonalar, tashkilotlar va xokazo) va boshqaruv sub'ekti, boshqaruv apparati yigʻindisini oʻzida namoyon etadi. Boshqaruv apparati deganda maqsadlarni shakllantiruvchi, rejalarni ishlab chiquvchi, qabul qilingan qarorlarga talablarni moslashtiruvchi, shuningdek, ularning bajarilishini nazorat qiluvchi xodimlar tushuniladi. Boshqaruv ob'ekti vazifasiga esa boshqaruv apparati ishlab chiqqan rejalarni bajarish kiradi, yaʼni boshqaruv tizimining oʻzi muhim aynan mana shu ishlarni amalga oshirish uchun toʻzilgandir.

Boshqaruv tizimining ikkala komponenti toʻgʻri (T) va aks (A) aloqalar bilan bogʻlangan. Toʻgʻri muhim aloqa boshqaruv apparatidan boshqaruv ob'ektiga yoʻnaltiriladigan axborot oqimida ifodalanadi. Aks aloqa teskari yoʻnalishda yuboriluvchi qabul qilingan qarorlarning bajarilishi haqidagi hisobot axboroti oqimida oʻz aksini topadi.

Axborot oqimlari (T va A), qayta ishlash vositalari, maʼlumotlarni uzatish va saqlash, shuningdek, maʼlumotlarni qayta ishlash boʻyicha operatsiyalarni bajaruvchi boshqaruv apparati xodimlarining oʻzaro aloqasi ob'ektning axborot tizimini tashkil etadi.

Axborot tizimlari nafaqat axborotni qayta ishlash va saqlash, yozuv-chizuv ishlarini avtomatlashtirish, balki qarorlarni qabul qilish (sunʼiy intellekt usullari, ekspert tizimlari va xokazolar), zamonaviy telekommunikatsiya vositalari (elektron pochta, telekonferentsiyalar), yalpi va lokal hisoblash tarmoqlari va boshqaruvning yangi uslublaridan foydalanish hisobiga boshqaruv ob'ekti faoliyati samaradorligini oshiradi va shu maqsadda keng qoʻllaniladi.

Axborot tizimlarining avtomatlashtirilgan va avtomatik turlari maʼlum.

Avtomatlashtirilgan axborotlar tizimida boshqarish yoki maʼlumotlarni qayta ishlash funksiyalarining bir qismi avtomatik ravishda, qolgani esa inson tomonidan bajariladi.

Avtomatik axborotlar tizimida boshqarish va maʼlumotlarni qayta ishlashning barcha funksiyalari texnik vositalarda, inson ishtirokisiz amalga oshiriladi (masalan, texnologik jarayonlarni avtomatik boshqarish).

Qoʻllanish sohasiga qarab axborot tizimlarini quyidagi sinflarga ajratish mumkin:

ilmiy tadqiqotlarni avtomatlashtirish va boshqarish;

loyihalashtirishni avtomatlashtirish;

tashkiliy jarayonlarni boshqarish;

texnologik jarayonlarni boshqarish.

Ilmiy tadqiqotlarni avtomatlashtirish va boshqarishda axborot tizimlari ilmiy xodimlar faoliyatini avtomatlashtirish, statistik axborotni tahlil etish, tajribalarni boshqarish uchun mo'ljallangan.

Loyihalashtirishni avtomatlashtirishda axborot tizimlari yangi texnika (texnologiya) ishlab chiqaruvchilar va muxandis loyihachilar mehnatini avtomatlashtirish uchun mo'ljallangan.

Tashkiliy boshqaruvda axborot tizimlari — shaxslar funksiyalarini avtomatlashtirish uchun mo'ljallangan. Bu sinfga ham sanoat (korxonalar), ham nosanoat ob'ektlari (bank, birja, sug'urta kompaniyalari, mexmonxonalar va xokazolar) va ayrim ofislar (ofis tizimlari)ni boshqarishning axborot tizimlari kiradi.

Texnologik jarayonlarni boshqarishda axborot tizimi turli texnologik jarayonlarni avtomatlashtirish uchun mo'ljallangan (moslashuvchan ishlab chiqarish jarayonlari, metallurgiya, energetika va xokazolar).

Dastlabki axborot tizimlari 50-yillarda paydo bo'ldi. Bu yillarda ular maosh hisob-kitoblarini qayta ishlash uchun mo'ljallangan bo'lib, elektromexanik buxgalterlik hisoblash mashinalarida amalga oshirilgan. Bu qog'oz hujjatlarni tayyorlashda mehnat va vaqtni bir qadar qisqartirishga olib kelgan.

60-yillarda axborot tizimlariga munosabat butunlay o'zgardi. Bu tizimlardan olingan axborot davriy hisobot uchun ko'pgina parametrlar bo'yicha qo'llana boshlandi. Buning uchun tashkilotlarga ko'pgina funksiyalarga ega bo'lgan EHM lar talab etila boshlandi.

70—80-yillarda axborot tizimlari qarorlarni qo'llab-quvvatlovchi va tezlashtiruvchi jarayonga ega bo'lgan nazorat boshqaruvi vositalari sifatida keng foydalanila boshlandi.

80-yillar oxiridan boshlab, axborot tizimlaridan foydalanish kontseptsiyasi yanada o'zgarib bormoqda. Ular axborotning strategik manbai bo'lib qolmoqda va istalgan sohada tashkil etishning barcha darajalarida foydalanilmoqda. Bu davrning axborot tizimlari axborotni o'z vaqtida berib, tashkilot faoliyatida muvaffaqiyatga erishishga yordam bermoqda

Istalgan vazifalardagi axborot tizimi ishini ta'minlovchi jarayonlarni umumiy holda quyidagicha tasavvur etish mumkin:

- tashqi yoki ichki manbalardan axborotni kiritish;
- kiritilgan axborotni qayta ishlash va uni qulay ko'rinishda taqdim etish;
- iste'molchiga axborotni o'zatish;
- teskari aloqa, ya'ni kiritilayotgan axborotni tuzatish uchun foydalanuvchilar tomonidan qayta ishlangan axborot bilan ta'minlash.

Qo'llash sohasidan qat'iy nazar, axborot tizimlarining samarali faoliyat ko'rsatishi bir qator ta'minotlar bilan bog'liqdir. Ularni dasturiy, texnik, huquqiy, axborot, tashkiliy, matematik va lingvistik ta'minotlarga ajratilishi qabul qilingan.

Axborot ta'minoti — axborot tizimlarida ma'lumotlar omborini yaratish, hujjatlashtirishning bir hil tartibga keltirilgan tizimlarini ichiga olgan axborotni kodlashtirish, joylashtirish va tashkil qilish bo'yicha uslublar va vositalar yig'indisidir.

Qabul qilinadigan boshqaruv qarorlarining ishonchliligi va sifati ko'p jixatdan ishlab chikilgan axborot ta'minoti sifatiga bog'liq.



Dasturiy ta'minot — kompyuter texnikasi vositasida ma'lumotlarni qayta ishlash tizimi (MKIT)ni yaratish va foydalanish dasturiy vositalari yig'indisidir. Dasturiy ta'minot tarkibiga bazaviy (umumtizimli) va amaliy (maxsus) dasturiy maxsulotlar kiradi.

Bazaviy dasturiy vositalar inson va kompyuterning o'zaro harakatlarini avtomatlashtirish, ma'lumotlarni qayta ishlash, namunaviy protseduralarni tashkil etish, MKIT texnik vositalari ishlashi nazorati va diagnostikasi uchun xizmat qiladi.

Amaliy dasturiy ta'minot axborot tizimi funksional vazifalarni hal etishni avtomatlashtirish uchun mo'ljallangan dasturiy maxsulotlar yig'indisini o'zida namoyon etadi. Ular universal vositalar (matn muharrirlari, elektron jadvallar, ma'lumotlar bazasini bosqaruv tizimlari) va maxsus vositalar — funksional kichik tizimlarni amalga oshiruvchi turli hil ob'ektlar (iqtisodiy, muxandislik, texnik va boshqalar) sifatida ishlab chiqilishi mumkin.

Texnik ta'minot ma'lumotlarni qayta ishlash tizimining faoliyat ko'rsatishi uchun qo'llaniluvchi texnik vositalar kompleksidir. Ushbu ta'minot ma'lumotlarni qayta ishlovchi, namunaviy operatsiyalarni amalga oshiruvchi qurilmalarni o'z ichiga oladi. Bunday qurilmalarga kompyuterlardan tashqari, atrof (periferiya) texnik vositalari, turli hil tashkiliy texnika, telekommunikatsiya va aloqa vositalari ham kiradi.

Huquqiy ta'minot axborot tizimini yaratish va faoliyat ko'rsatishini tartibga soluvchi huquqiy me'yorlar yig'indisini o'zida namoyon etadi.

Lingvistik ta'minot inson va kompyuter muloqotini ishlab chiqish va ta'minlash samaradorligini oshirish uchun MKITni yaratish va foydalanishning turli bosqichlarida ishlatilgan til vositalari yig'indisidan iborat.

Ta'sir etish maqsadi bo'yicha xavfsizlik xavfini uchta asosiy turga farqlanadi:

1. Axborot maxfiyligining buzilish xavfi;
2. Axborot butunligining buzilish xavfi;
3. Tizimning ishlash layoqatligining buzilish xavfi (xizmat ko'rsatishdagi inkor (rad) etishlar).

Axborot maxfiyligining buzilish xavfi maxfiy yoki sirli axborotni xavfni amalga oshirishda axborot unga murojaat qilishi mumkin bo'lmagan shaxslarga ma'lum bo'lib qoladi. Kompyuter tizimida, bir tizimdan boshqasiga uzatilayotgan yoki kompyuter

tizimida saqlanayotgan biror yopiq axborotga ruxsat etilmagan murojaat qilish bo'lganda har safar axborot maxfiylikni buzilishi havfi sodir bo'ladi.

Axborot butunligining buzilishi xavfi uning sifati va ishonchligi buzilishiga yoki to'liq yo'qotilishiga olib keladigan xalaqitlarga yoki axborotning o'zgarishiga yo'naltirilgandir. Axborotning butunligi niyati yomon odam tomonidan ko'ra bila turib hamda tizimni o'rab turgan muhit tomonidan ob'yetiv ta'sirlar natijasida buzilishi mumkin. Bu havf ayniqsa, axborotni uzatish tizimlari, kompyuter tarmoqlari va radiotexnika tizimlari uchun dolzarbdir.

Tizimning ishlash layoqatligini buzilish xavfi (xizmat ko'rsatishdagi inkor etishlar) ma'lum bir oldindan mo'ljallangan ta'sirlar yoki tizimning ishlash layoqatligini susaytiradigan yoki uning ba'zi bir resurslariga murojaat qilishni blokirovkalaydigan xolatlarni yaratishga yo'naltirilgandir.

Axborot xavfsizligini buzish bo'yicha sabablar tasodifiy va yomon niyatli (oldindan mo'ljallangan) bo'lishi mumkin. Birinchi holda buzuvchi, xalaqit beruvchi va boshqa jarayonlarning manbalari bo'lishi mumkin:

- tasodifiy holatlar (yer qimirlashi, yongin, dovul va b.);
- tizimning tarkibiy elementlarini izdan chiqishi (texnik buzilishlar);
- foydalanuvchilar va xizmat ko'rsatish xodimlarini xato xarakatlari;
- dastur ta'minotidagi xatoliklar;
- tashqi muhit ta'siri natijasida aloqa yo'lidagi xalaqitlar va boshqalar.

Hozir jahonda moliya – bank kompyuter tarmoqlari oldindan mo'ljallangan xavflarga eng yuqori darajada ta'qib etiladi? bunday xavflarga quyidagilar tegishlidir:

- bank xizmatchilari soniga tegishli bo'lmagan begona shaxslarning ruxsat etilmagan murojaat qilishi va saqlanayotgan maxfiy axborot bilan tanishishi;
- bank xizmatchilarining ular murojaat qilishi mumkin bo'lmagan axborot bilan tanishib chiqishi;
- dasturlarni va berilganlarni ruxsatsiz nusxalash;
- maxfiy axborotni o'z ichiga olgan magnit tashuvchilarni o'g'irlash;
- chop qilingan bank xujjatlarini o'g'irlash;
 - axborotni ataylab yo'qotish;
- bank xodimlari tomonidan moliyaviy hujjatlarni, hisobot va ma'lumot bazasini ruxsatsiz o'zgarish;
- aloqa kanallari bo'yicha uzatilayotgan ma'lumotlarni qalbakilashtirish;
- aloqa kanallari bo'yicha uzatilayotgan ma'lumotlar mualliflarini rad etish;
- ma'lumotlar (axborotni) olish dalilini rad etish;
- oldin uzatilgan ma'lumotlarni to'xtatib qo'yish;
- virusli harakatlar keltirib chiqargan axborotning buzilishi;
- magnit tashuvchilarda saqlanayotgan arxivdagi bank axborotlarini buzilishi;
- tizim tashkil etuvchilari va tugunlarini o'g'irlanishi.



Ruxsatsiz kirishning mumkin bo'lgan asosiy usullari

Kompyuter tizimlari va tarmoqlarida (KT va T) axborotni ishonchli himoya qilish, agar havf paydo bo'lishi mumkin bo'lgan tizimning barcha ob'yektlari va elementlarida ishonchli bo'lsagina, samarali bo'lishi mumkin. Shu munosabat bilan himoya qilish vositalarini yaratish uchun havf tabiatini, shakllarini va ularning mumkin bo'lgan paydo bo'lish va amalga oshirish yo'llari, ob'yektlar va elementlar ro'yxatini aniqlash muhimdir. Ular, bir tomondan, axborotning himoyalanganligini buzish maqsadida havflarga duch kelishi mumkin, boshqa tomondan esa, axborotni samarali himoya qilishni tashkil etishi mumkin.

Himoya qilish ob'yekti deganda, tizimning shunday tashkil etuvchisi tushuniladiki, unda himoya qilinishi mumkin bo'lgan axborot joylashgan yoki joylashishi mumkin.

Kompyuter tizimlarini axborotni himoya qilish ob'yektlari sifatida quyidagilarni ajratish mumkin:

- foydalanuvchilarning terminallari (shaxsiy kompyuterlar tarmoqning ishchi stansiyalari);
- tarmoq majburiyatining terminali yoki guruhli abonentlik tuguni;
- aloqa tuguni;
- axborotni aks ettirish vositalari;
- mashina vali (kompyuterli yoki displeyli) va axborot tashuvchilari omborxonasi;
- tashqi aloqa kanallari va tarmoqdagi jihozlar;

- axborotni yig'uvchilar va tashuvchilar.

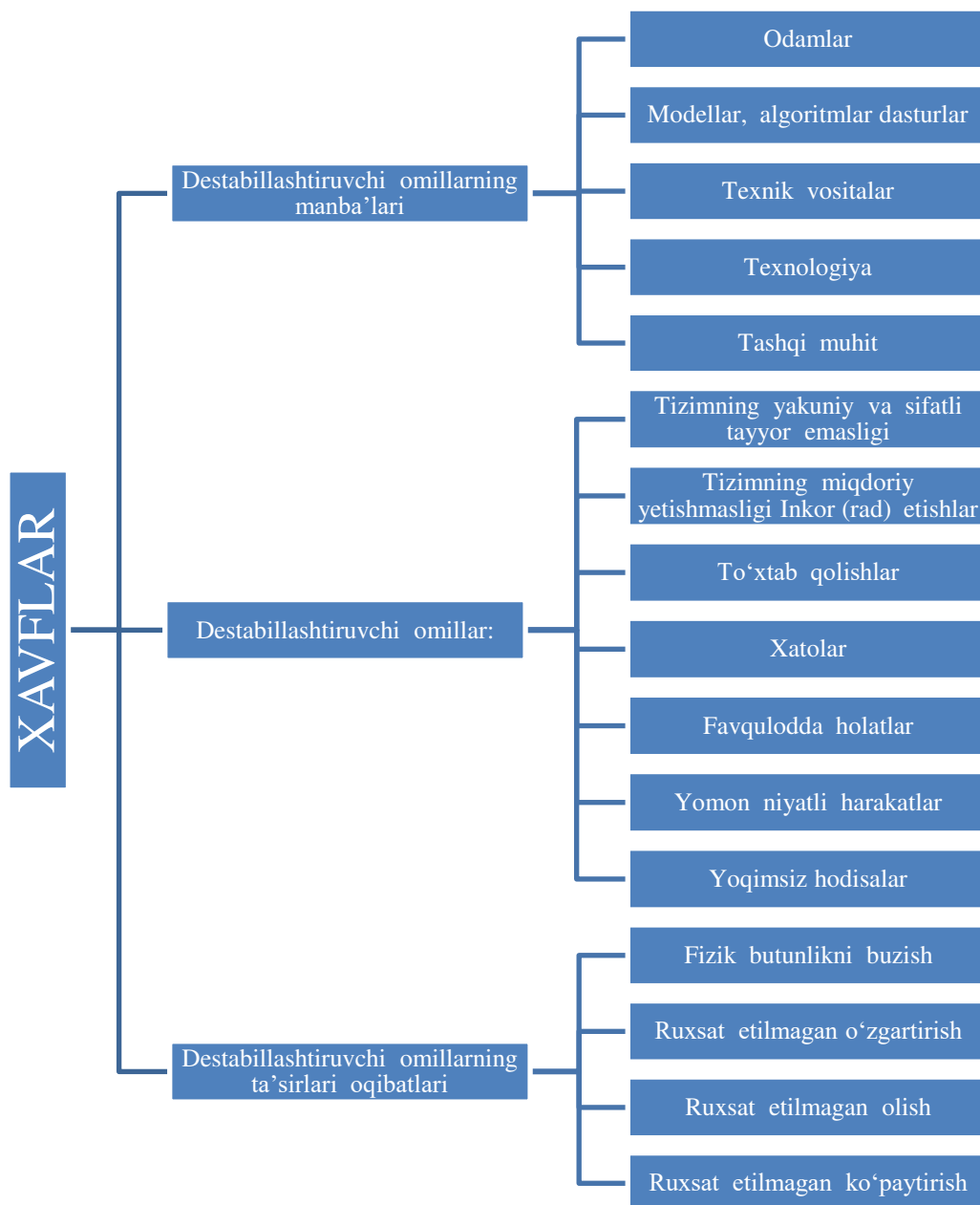
Himoya qilish elementi deganda esa, himoya qilinishi kerak bo'lgan ma'lumotlarni o'z ichiga olgan berilganlar to'plami tushuniladi.

Yuqorida keltirilgan ta'rifga mos ravishda himoya qilish elementlari sifatida himoya qilish ob'yektlaridagi axborot bloklari (miqdorlar, to'plamlar, oqimlar, bazalar va boshqa) qatnashishi mumkin, xususan:

- kompyuterning asosiy xotirasidagi berilganlar va dasturlar;
- tashqi mashina tashuvchisidagi (qattiq yoki egiluvchan diskardagi) berilganlar va dasturlar;
- shaxsiy kompyuterlar avtonom yoki tarmoqda ishlatilganda printerga chiqarilayotgan ma'lumotlar;
- monitor ekranida aks ettirilayotgan ma'lumotlar;
- aloqa kanallari bo'yicha uzatilayotgan ma'lumotlar paketlari;
- nusxa olish – ko'paytirish jihozlari yordamida ko'paytirilayotgan ma'lumotlar;
- foydalanuvchi tomonidan ro'yhatga olingan parol va prioritetlar vazifalarining jurnallari;
- masalalar to'plami bilan ishlash bo'yicha xizmatga doir yo'riqnomalar;
- berilganlar va dastur ta'minoti arxivlari;
- tarmoqli operasion tizimlar;
- tarmoqli ishchi tugunlar va qism stansiyalar.

Buzg'unchilar modeli

Barcha ta'sirlarning sababi turli omillar bo'lishi mumkin. 1-rasmda KT va T larida axborot himoyalanganligini buzadigan omillarining kelib chiqishi keltirilgan. Ushbu rasmdan ko'rinib turibdiki, informasion xavfsizlikni xavfini yaratishga destabillashtiruvchi omillarning manbalari ham, destabillashtiruvchi omillarning o'zlari ham to'g'ridan-to'g'ri ta'sir ko'rsatadi.



1. Rasm. Axborotning ximoyalanganligini buzuvchi omillar va ularning ta'sirlari oqibatlari

Destabillashtiruvchi omillarning asosiy manbalariga quyidagilar tegishlidir:

- **insonlar.** Kompyuter tizimiga murojaat qilish huquqiga va amaliy jihatdan faqatgina ikki toifadagi shaxslar egadirlar. Hususiy mutaxassis foydalanuvchilar va begonalar. Yomon niyatli axborotni buzuvchilarni mutlaq ko'pchiligini begona odamlar amalga oshiradi. Bu esa jiddiy va havfli oqibatlarga olib keladi. Yomon niyatli odam sifatida KT va T ning o'zini odamlari bo'lishi ehtimoli xam e'tibordan chetda emas. Har qanday holda ham axborotga ruxsat etilmagan murojaat qilish (AREMK) odamlar tomonidan kompyuterdagi bu qonun buzilishlarning manba'lari hisoblanadi.
- **modellar, algoritmlar, dasturlar.** Ular axborotni himoya qilish xavfiga olib keladigan kuchli manba' bo'lishlari mumkin, negaki axborotni qayta ishlash dasturlarini, modellarni va algoritmlarni mukammal emasligi oqibatlari hisoblash jarayonini to'xtashiga, ko'ngilsiz natijalarga, axborotni o'zgarishi va chiqib ketishiga olib keladi.
- **texnik qurilmalar.** Ular hozir KT va T larida katta va o'ta katta integral optik tolali va lazerli chizmalarni keng yo'llanishiga asoslanadi. Bunday chizmalarni ishlashida

kuchlanishlar, impuls va toklarning darajalarini yuqori chastotali o'zgarishlari bo'lib o'tadi. Bu, o'z navbatida, ozuqa zanjirlarida, efirda, yaqinda joylashgan apparaturada va shunga o'xshash turli hil elektromagnit maydonlarni va yo'naltirishlarning paydo bo'lishiga olib keladi, ular esa maxsus vositalar yordamida qayta ishlanadigan axborotga aylantirish mumkindir.

Tashqi muhit ham informasion xavfsizlik havfini paydo bo'lishiga ta'sir etadigan negativ omillarning manba'si bo'lishi mumkin.

O'z navbatida yuqorida sanab o'tilgan destabillashtiruvchi omillarning manba'lari informasion xavfsizlik havfini bevosita yaratadigan bir qator ob'yektiv, sub'yektiv omillarni paydo bo'lishini oldindan aniqlaydi. Ularga quyidagilar tegishlidir:

1. **Ishlashga tizimning yakuniy va sifatli tayyor emasligi**, loyihalash va sinab ko'rish bosqichlarida qandaydir xatolarning oqibati. Bu dastur-algoritmik ta'minlaydigan ishlarning oxiriga yetmaganligi, axborotli berilganlar bazasini rivojlanmaganligi, texnologik birika olmaslik, alohida amallarning o'zaro to'g'ri kelmasligi va x.k. bo'lishi mumkin.
2. **Mikdoriy yetishmaslik**-bu bir xil vositalarning boshqalariga zarar keltirgan holda to'liq komplektlanmaganligi yoki ortiqcha komplektlashganligi, ularning o'zaro bir-biri bilan to'g'ri kelmasligi tashqaridan murojaat qilish ochiqligi va x.k.
3. **Inkor etilishlar, to'xtab qolishlar va xatoliklar** ular KT va T larini ishlash jarayonini qisman kuzatadilar, tizimga xizmat ko'rsatadigan mutaxassislarning kasbiy malakasini pastligi, o'zlarining vazifalariga va ishlariga nisbatan intizomsizligi, loqaydligi tufayli kelib chiqadi. Tabiiyki, ana shu negativ omillar moddiy va fizik eskirgan jihozlar va vositalar ularning ortiqcha yuklanishi va hakoza oqibatida ham paydo bo'lishi mumkin.
4. **Favkulodda xolatlar** (yong'in, suv toshqini, yer qimirlashi, elektrozuqani izdan chiqishi va b.) ular halokatli holatlarni yaratadi va kompyuter tarmoqlarini va tizimlarini havfsiz ishlashida salbiy ta'sir ko'rsatadi.
5. **Yomon niyatli xarakatlar**- tizimning ob'yektlarga va elementlariga hamda undagi bo'lib o'tayotgan jarayonlariga turli sabablar (moddiy qiziqish, zarar o'tkazish istagi, qiziqish, o'zinikini ma'qullash va h.k) bo'yicha insonning faol aralashishini natijasidir.
6. **Yokimsiz xodisalar** – bu tizimni va hizmat ko'rsatish xodimlarini ishlashi bilan bevosita bog'liq bo'lmagan omillar.

10.2 Kriptografik axborot himoyasi tamoyillari.

Jamiyatni kompyuterlashtirish, bir qator foydalardan tashqari, o'zi bilan bir qator muammolarni olib keldi. Juda ham murakkab bo'lgan bunday muammolardan bittasi axborotni qayta ishlash va uzatish tizimlarida maxfiy axborot xavfsizligini ta'minlashdadir.

Bu muammoni hal qilish uchun axborotni himoya qilishning kriptografik usullari keng ishlatilmoqda, bunda boshlang'ich axborot shunday o'zgartiriladiki, buning natijasida axborot kerakli vakolatlarga ega bo'lmagan shaxslarga tanishish va ishlatish uchun mumkin bo'lmay qoladi.

Boshlang'ich axborotga ta'sir ko'rinishi bo'yicha kriptografik o'zgartirishni quyidagi usullari mavjud: **shifrlash, stenografiya, kodlash, zichlashtirish.**

Shifrlash jarayoni boshlang'ich axborot ustida orqaga qaytadigan matematik, mantiqiy, kombinatorlik va boshqa o'zgartrishlarni o'tkazishdir, buning natijasida

shifrlangan axborot harflarning, raqamlarning, boshqa belgilar va ikkilik kodlarning tartibsiz to'plami ko'rinishiga egadir.

Axborotni shifrlash uchun o'zgartirish algoritmi va kalit ishlatiladi. Odatda, ma'lum bir shifrlash algoritmi uchun o'zgartirish algoritmi o'zgarmas hisoblanadi. Shifrlash algoritmi uchun boshlang'ich qiymatlar bo'lib shifrlash uchun axborot va shifrlash kaliti xizmat qiladi. Kalit boshqaruvchi axborotni o'z ichiga oladi, u shifrlash algoritmini amalga oshirishda ishlatiladigan operandlar kattaliklarini va algoritmnining ma'lum qadamlarida o'zgartirishlarni tashlashni aniqlaydi.

Stenografiya usullari nafahatgina saqlanayotgan yoki uzatilayotgan axborotni ma'nosini berkitib qolmasdan, balki yopiq axborotni saqlash yoki uzatish omilini xam yashirish imkonini xam beradi. Stenografiya usullarining barchasi asosida yopiq axborotni ochiq fayllar ichida niqoblash yotadi. Stenografiya vositalari yordamida matn, tasvir, nutq, raqamli imzo, shifrlangan xabar niqoblanishi mumkin. Stenografiyani va shifrlashni kompleks ishlatish maxfiy axborotni payqash va ochish masalasini yechishning murakkabligini oshiradi.

Axborotni kodlash jarayonining mazmunini boshlang'ich axborot (gaplar, so'zlar) ma'nosiga ko'ra tuzilishlarini kodlar bilan almashtirish hisoblanadi. Kodlar sifatida harflar, raqamlar, raqamlar va xarflarning birlashmalari ishlatilishi mumkin. Kodlashda va teskari o'zgartirishda maxsus jadval yoki lug'atlar ishlatiladi. Kamchiligi kodlaydigan jadvallarni saqlash va tarqatishning zarurligidir, ularni, ushlab olingan xabarlarni qayta ishlashning statistik usullari bilan kodlarni ochishdan saqlanish uchun, tez-tez almashtirish kerakdir. Kodlash usulini ma'nosiga ko'ra tuzilishlari cheklangan to'plamli tizimlarda qo'llash maqsadga muvofiqdir.

Zichlashtirish axborot xajmini qisqartirishdir. Zichlashtirilgan axborot teskari o'zgartirishsiz o'qilishi yoki ishlatilishi mumkin emas. Zichlashtirish va qayta o'zgartirish vositalariga murojaat qila olishlikni inobatga olib, maxfiy axborotni zichlashtirilgan fayllari keyinchalik shifrlanadi. Vaqtni qisqartirish uchun axborotni zichlashtirish uchun axborotni zichlashtirish va shifrlash jarayonini birgalikda ishlatish maqsadga muvofiqdir.

10.3 Internet tarmog'i orqali uzoqlashtirilgan hujumlardan himoya usullari va vositalari.

Shifr va kalit, shifrlash va qayta shifrlash to'g'risida tushunchalar

Shifrlash kriptografik o'zgartirishning asosiy ko'rinishidir. Bu ochiq axborotni shifrlangan axborotga (shifrmtn) o'zgartirish yoki shifrlangan axborotni ochiq axborotga teskari o'zgartirish jarayonlaridir.

Ochiq axborotni yopiq axborotga o'zgartirish jarayoni shifrlash, teskarisi esa - qayta shifrlash deyiladi.

Shifrlash usullarining va shifrlarning ko'plab turlari mavjud. Bu shifrlash algoritmiga mos ravishda ochiq axborotni yopiq axborotga orqaga qaytmaydigan o'zgartirishlar to'plamidir. EHM va KT larining paydo bo'lishi axborotni shifrlash qayta shifrlash uchun xam, shifrga xujum qilish uchun ham EHM ni ishlatish imkoniyatlarini inobatga oladigan yangi shifrlarni ishlab chiqish jarayonini keltirib chiqardi.

Zamonaviy shifrlash usullariga quyidagi talablar qo'yiladi:

- Kriptochidamlilik (kriptotaxlil qilishga qarshi turish) shunday bo'lishi kerakki, shifrnı ochish kalitlarini to'liq tanlab olish masalasini yechish yo'li bilan amalga oshirilishi kerak;
- Kriptochidamlilik shifrlash algoritmining maxfiyligi bilan emas, balki kalitning maxfiyligi bilan ta'minlanadi;

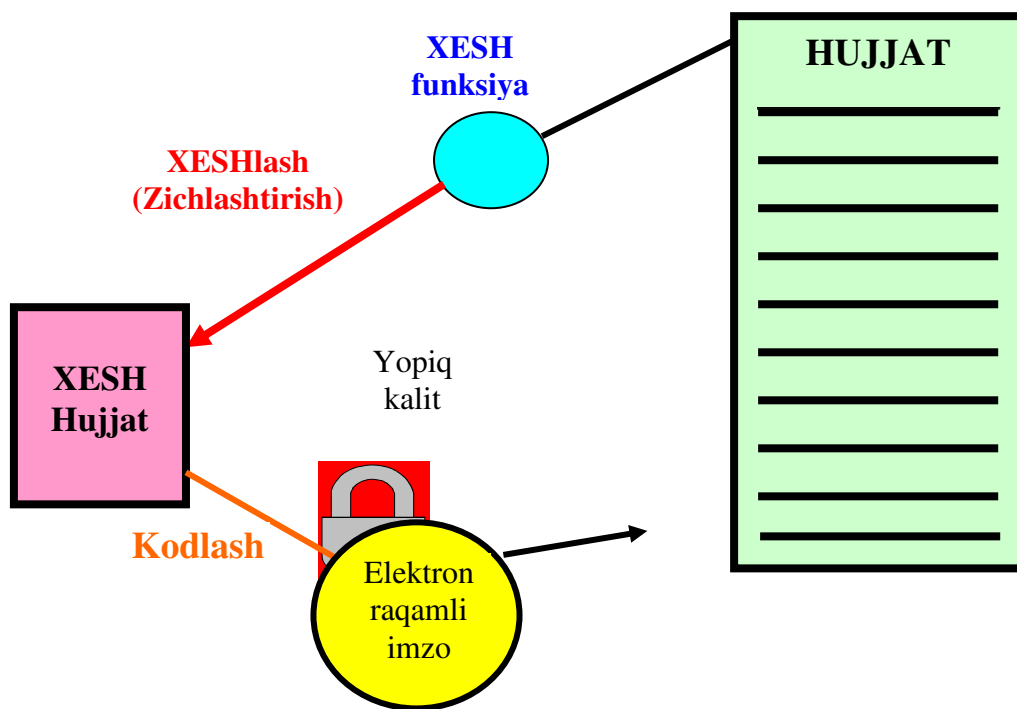
- Shifratn o'zi hajmi bo'yicha boshlang'ich axborotdan ko'payib ketmasligi kerak;
- Shifr xatoliklari axborotni xalaqitlarga uchrashiga va yo'qolishlariga olib kelmasligi kerak;
- Shifrlash vaqti katta bo'lmasligi kerak;
- Narxi berkitiladigan axborotning narxi bilan moslashtirilishi kerak.

10.4 Elektron to'lov tizimlarida axborot xavfsizligi

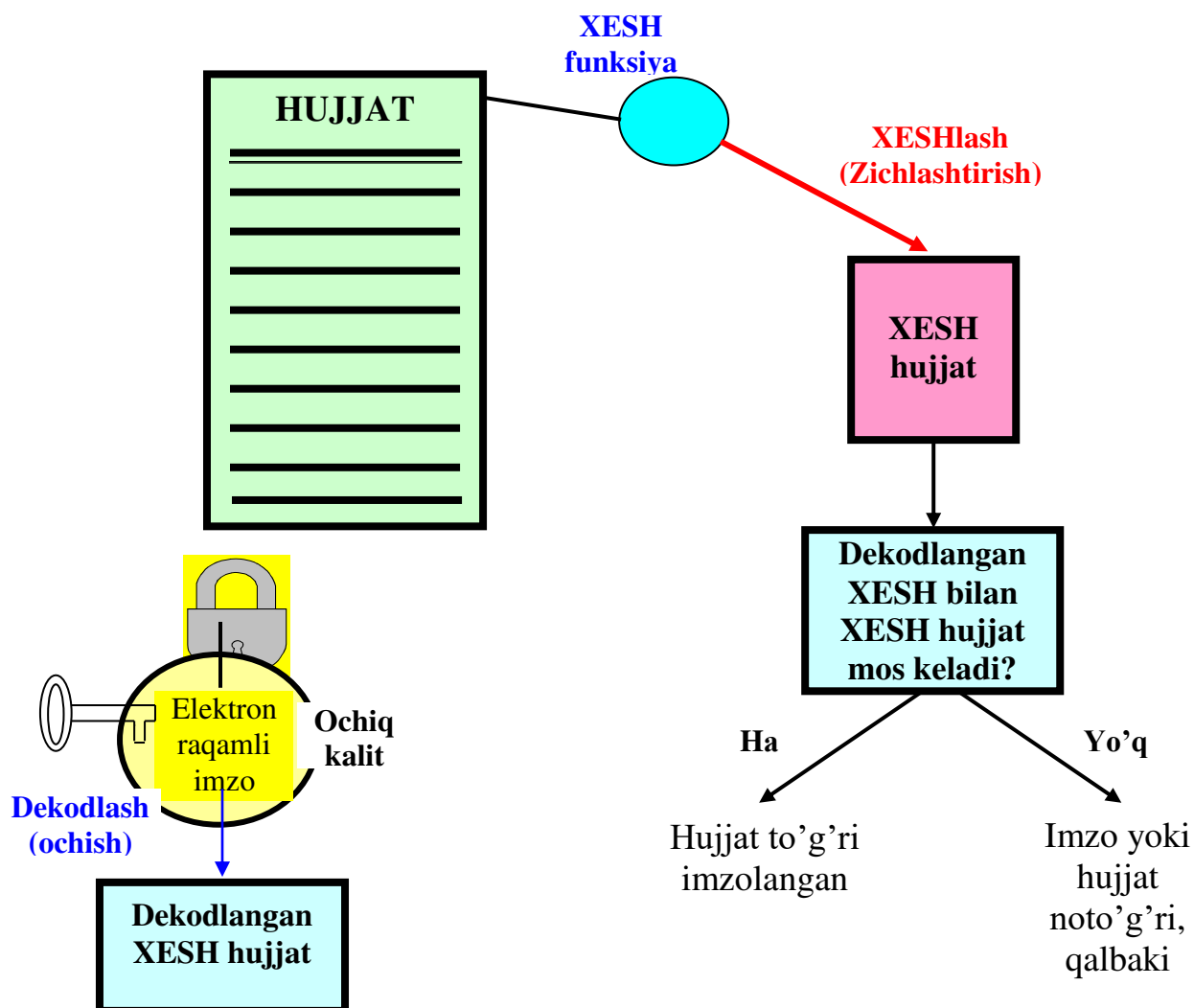
Elektron raqamli imzo va uning zamonaviy turlari

Telekommunikasiya tizimlarning rivojlanishi natijasida hozirgi kunda axborot almashuvini qog'ozli texnologiyasidan elektron xujjat ko'rinishdagi axborot almashinuviga o'tish jarayoni yuz bermoqda. Axborot almashinuvini elektron xujjat ko'rinishdagi texnologiyasiga o'tish natijasida telekommunikasiya tarmoqlari orqali uzatiladigan axborotlarni muallifini aniqlash, uning to'liqliligi ta'minlash kabi muammolar vujudga keladi. Ushbu muammoni to'la-to'kis «Elektron raqamli imzo» yordamida xal qilish mumkin. "Elektron raqamli imzo" bu telekommunikasiya tarmoqlari orqali uzatishga mo'ljallangan elektron xujjatni o'zini ma'lum bir algoritmlar yordamida zichlashtirib so'ng shifrlangan diskret ko'rinishdagi ifodasi xisoblanadi.

"Elektron raqamli imzo"ni xosil qilish uchun turli davlatlarda turli xil shifrlash algoritmlari ishlatiladi masalan, RSA, El-Gamelya kabi shifrlash algoritmlari. Bu algoritmlarda mustaxkamlik darajasi turli xil.



Asimmetrik shifrlash asosida elektron raqamli imzo ishlab chiqish sxemasi



Asimmetrik shifrlash asosida elektron raqamli imzoni tekshirish sxemasi