14-Ma'ruza

14-Mavzu. Qurilish va arxitektura soxasida axborot xavfsizligi va axborotlarni himoyalash usullari.

Reja:

1. Axborot xavfsizligiga kirish
2. Predmetning asosiy tushunchalari va maqsadi
3. Axborotlarga nisbatan xavf-xatarlar tasnifi
4. Tarmoq xavfsizligini nazorat qilish vositalari

Tayanch so‘zlar: *maxfiylik, konfidentsiallik, yaxlitlik, autentifikatsiya, apellyatsiya qilishlik, ishonchlilik, aniqlilik, tizimga kirishni nazorat qilish, identifikatsiyalashni nazorat qilish, qasddan buzilishlarga to‘sqinlik.*

1. Axborot xavfsizligiga kirish.

Mamlakatimiz milliy iqtisodining hech bir tarmog‘i samarali va mo‘tadil tashkil qilingan axborot infratuzilmasisiz faoliyat ko‘rsatishi mumkin emas. Hozirgi kunda milliy axborot resurslari har bir davlatning iqtisodiy va harbiy salohiyatini tashkil qiluvchi omillaridan biri bo‘lib xizmat qilmoqda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta’minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha ilg‘or axborot – kommunikatsiyalar texnologiyalarini qo‘llash kengayadi. Turli xildagi axborotlar hududiy joylashishidan qat’iy nazar bizning kundalik hayotimizga Internet halqaro kompyuter tarmog‘i orqali kirib keldi. Axborotlashgan jamiyat shu kompyuter tarmog‘i orqali tezlik bilan shakllanib bormoqda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo‘qolib bormoqda. Jahon kompyuter tarmog‘i davlat boshqaruvini tubdan o‘zgartirmoqda, ya’ni davlat axborotlarning tarqalishi mexanizmini boshqara olmay qolmoqda. Shuning uchun ham mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va yo‘qotish kabi muammolar dolzarb bo‘lib qoldi. Bularning bari shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib kelmoqda. Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborot himoyasi esa davlatning birlamchi masalalariga aylanmoqda.

Hozirgi kunda xavfsizlikning bir qancha yo‘nalishlarini qayd etish mumkin. (1- rasm)

2. Predmetning asosiy tushunchalari va maqsadi.

Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo‘llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o‘qiy olmagan. Asrlar davomida bu san’at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o‘n yil oldin hamma narsa tubdan o‘zgardi, ya’ni axborot o‘z qiymatiga ega bo‘ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o‘g‘irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug‘iladi. Axborotni qayta ishlash sanoatining paydo bo‘lishi axborotni himoyalash sanoatining paydo bo‘lishiga olib keladi.

***Information security**, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)*[1]

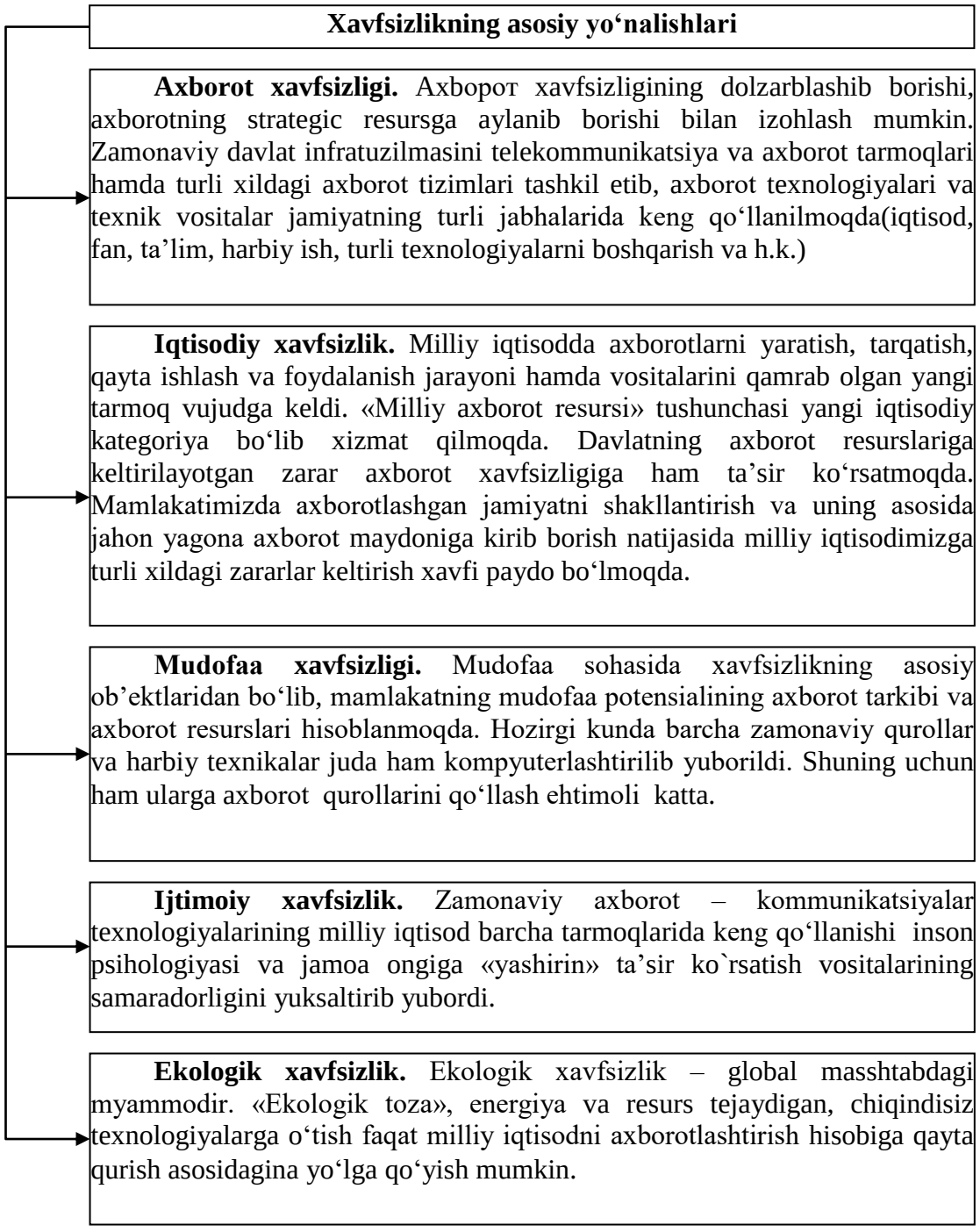
Avtomatlashtiriltan axborot tizimlarida axborotlar o‘zining hayotiy davriga ega bo‘ladi. Bu davr uni yaratish, undan foydalanish va kerak bo‘lmaganda yo‘qotishdan iboratdir (2-rasm).

Axborotlar hayotiy davrining har bir bosqichida ularning himoyalanganlik darajasi turlicha baholanadi.

IT security

[1] *Discovering Computers 2016. Tools, Apps, Devices,and the Impact of Texnology. 691 pg.*

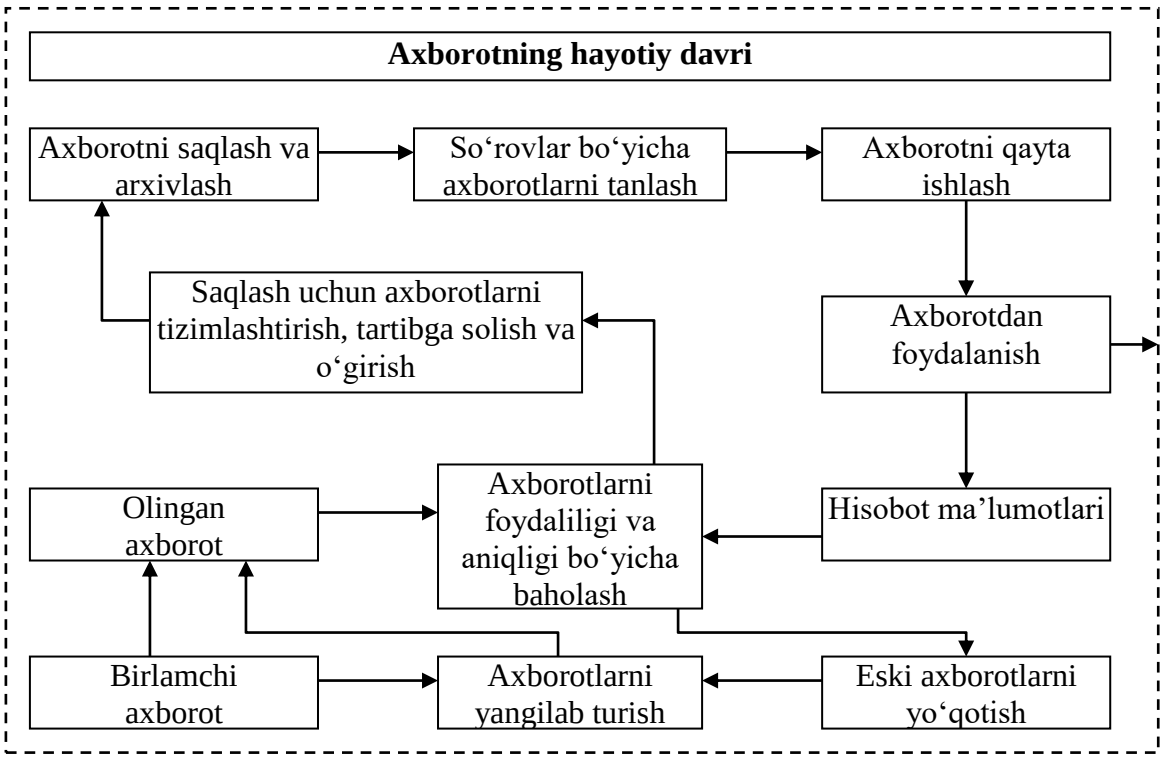
Sometimes referred to as computer security, information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.[2]



1-rasm.

[2] *Discovering Computers 2016. Tools, Apps, Devices,and the Impact of Texnology. 691 pg*

Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muhim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulki huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshqa moddiy hamda nomoddiy zararlar keltirishi mumkin bo‘lgan turli kirishlar va o‘g‘irlashlardan himoyalashdir.



2-rasm

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

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va hujjatlarni o‘g‘irlash yoki nusxa olishdan iborat bo‘lsa, hozirgi paytdagi xavf esa kompyuter ma’lumotlari to‘plami, elektron ma’lumotlar, elektron massivlardan ularning egasidan ruxsat so‘ramasdan foydalanishdir. Bulardan tashqari, bu harakatlardan 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 boshqa shaxsga zarar etkazmoqchi bo‘lgan nohuquqiy muomaladan har qanday h**ujjatlashtirilgan,** ya’ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo‘yilgan holda moddiy jismda qayd etilgan **axborot** himoyalanishi kerak.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

• **maxfiylik** — aniq bir axborotga faqat tegishli shaxslar doirasigina kirishi mumkinligi, ya’ni foydalanilishi qonuniy hujjatlarga muvofiq cheklab qo‘yilib, hujjatlashtirilganligi kafolati. Bu bandning buzilishi **o‘g‘irlik** yoki **axborotni oshkor qilish,** deyiladi;

• **konfidentsiallik** — inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

• **yaxlitlik** — axborot boshlang‘ich ko‘rinishda ekanligi, ya’ni uni saqlash va uzatishda ruxsat etilmagan o‘zgarishlar qilinmaganligi kafolati; bu bandning buzilishi **axborotni soxtalashtirish** deyiladi;

• **autentifikatsiya** — axborot zahirasi egasi deb e’lon qilingan shaxs haqiqatan ham axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi **xabar muallifini soxtalashtirish** deyiladi;

• **apellyatsiya qilishlik** — etarlicha murakkab kategoriya, lekin elektron biznesda keng qo‘llaniladi. Kerak bo‘lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yuqoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin:

• **ishonchlilik** — tizim me’yoriy va g‘ayri tabiiy hollarda rejalashtirilganidek o‘zini tutishlik kafolati;

• **aniqlilik** — hamma buyruqlarni aniq va to‘liq bajarish kafolati;

• **tizimga kirishni nazorat qilish —** turli shaxs guruxlari axborot manbalariga har xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati;

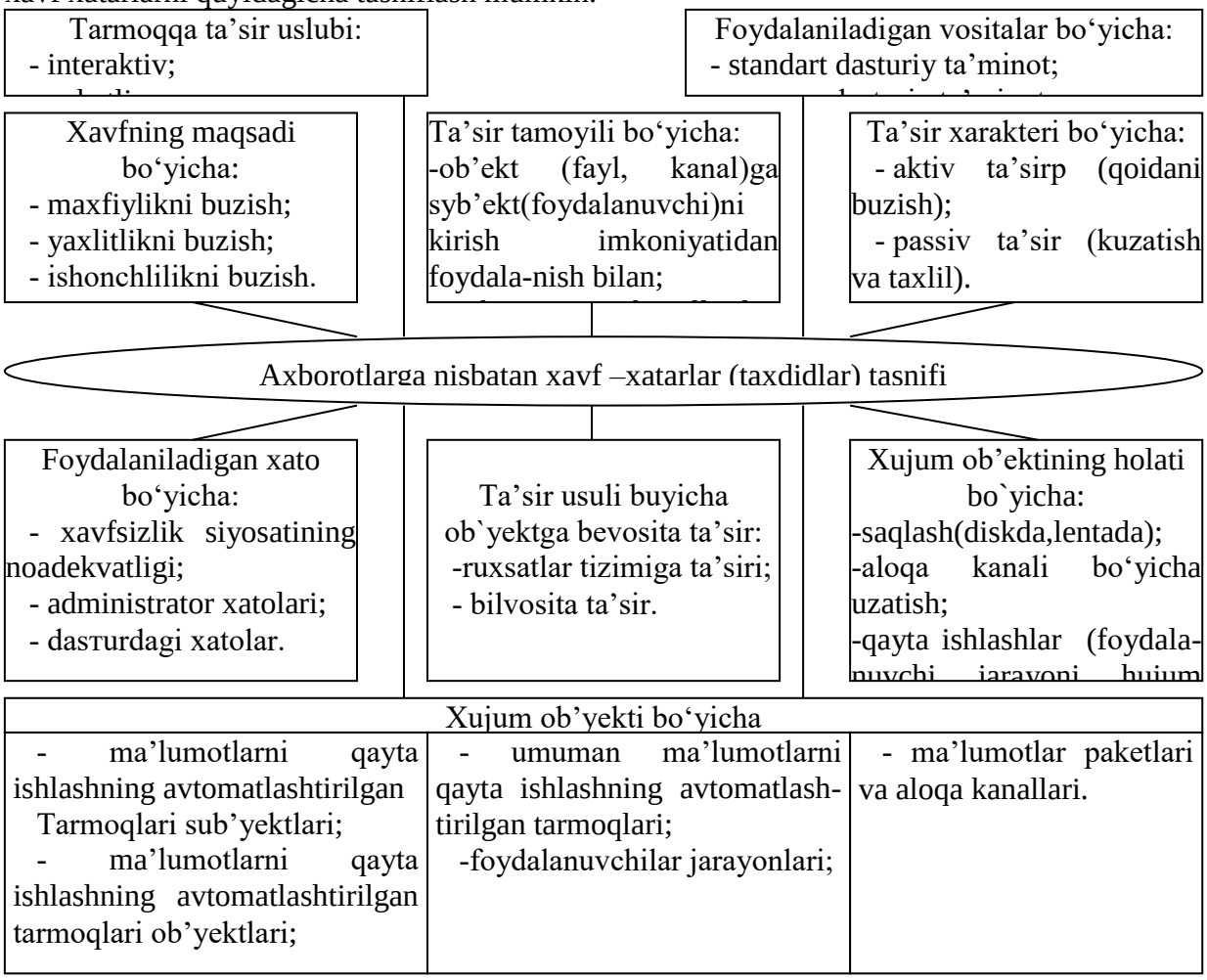
• **nazorat qilinishi** — istalgan paytda dastur majmuasining xoxlagan kismini to‘liq tekshirish mumkinligi kafolati;

• **identifikatsiyalashni nazorat qilish** — hozir tizimga ulangan mijoz aniq o‘zini kim deb atagan bo‘lsa, aniq o‘sha ekanligining kafolati;

• q**asddan buzilishlarga to‘sqinlik** — oldindan kelishilgan me’yorlar chegarasida qasddan xato kiritilgan ma’lumotlarga nisbatan tizimning oldindan kelishilgan holda o‘zini tutishi.

Axborotlarga nisbatan xavf-xatarlar tasnifi

Ilmiy va Amaliy tekshirishlar natijalarini umumlashtirish natijasida axborotlarga nisbatan xavf xatarlarni quyidagicha tasniflash mumkin.



Xavfsizlik siyosatining eng asosiy vazifalaridan biri himoya tizimida potentsial xavfli joylarni qidirib topish va ularni bartaraf etish hisoblanadi.

Tekshirishlar shuni ko‘rsatadiki, tarmoqdagi eng katta xavflar — bu ruxsatsiz kirishga mo‘ljallangan maxsus dasturlar, kompyuter viruslari va dasturning ichiga joylashtirilgan maxsus kodlar bo‘lib, ular kompyuter tarmoqlarining barcha ob’ektlari uchun katta xavf tug‘diradi.

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment

or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.[3]

Tarmoq xavfsizligini nazorat qilish vositalari

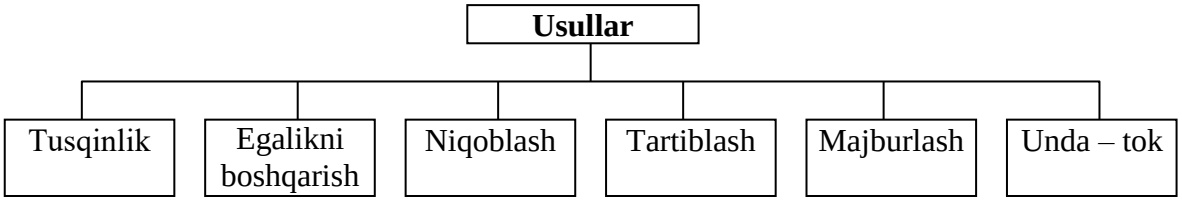
Zamonaviy axborot - kommunikatsiyalar texnologiyalarining yutuqlari himoya uslublarining bir qator zaruriy instrumental vositalarini yaratish imkonini berdi.

Axborotlarni himoyalovchi instrumental vositalar deganda dasturlash, dasturiy - apparatli va apparatli vositalar tushuniladi. Ularning funksional to‘ldirilishi xavfsizlik xizmatlari oldiga qo‘yilgan axborotlarni himoyalash masalalarini echishda samaralidir. Hozirgi kunda tarmoq xavfsizligini nazorat qilish texnik vositalarining juda keng spektri ishlab chiqarilgan.

Kompyuter tarmoqlarida himoyani ta’minlash usullari

Kompyuter tarmoqlarida axborotni himoyalash deb foydalanuvchilarni ruxsatsiz tarmoq, elementlari va zaxiralariga egalik qilishni man etishdagi texnik, dasturiy va kriptografik usul va vositalar, hamda tashkiliy tadbirlarga aytiladi.

Bevosita telekommunikatsiya kanallarida axborot xavfsizligini ta’minlash usul va vositalarini quyidagicha tasniflash mumkin:



Yuqorida keltirilgan usullarni quyidagicha ta’riflash qabul qilingan.

To’sqinlik apparatlarga, ma’lumot tashuvchilarga va boshqalarga kirishga fizikaviy usullar bilan qarshilik ko‘rsatish deb aytiladi.

Egalikni boshqarish — tizim zaxiralari bilan ishlashni tartibga solish usulidir. Ushbu usul quyidagi funksiyalardan iborat:

• tizimning har bir ob’ektini, elementini ndentifikatsiyalash, masalan, foydalanuvchilarni;

• identifikatsiya buyicha ob’ektni yoki sub’ektni xakikiy, asl ekanligini aniqlash;

• vakolatlarni tekshirish, ya’ni tanlangan ish tartibi buyicha (reglament) xafga kunini, kunlik soatni, talab kilinadigan zaxiralarni qo‘llash mumkinligini tekshirish;

• kabul kilingan reglament buyicha ishlash sharoitlarini yaratish va ishlashga ruxsat berish;

• himoyalangan zaxiralarga kilingan murojaatlarni kayd qilish;

• ruxsatsiz harakatlarga javob berish, masalan, signal berish, uchirib kuyish surovnomani bajarishdan voz kechish va boshqalar.

Niqoblash – ma’lumotlarni o‘qib olishni qiyinlashtirish maqsadida ularni kriptografiya orqali kodlash.

---

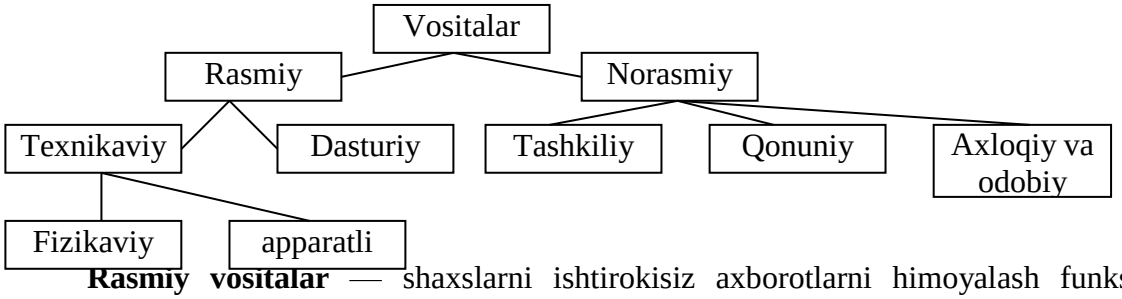
[3] Discovering Computers 2016. Tools, Apps, Devices,and the Impact of Texnology. 691 page.

Tartiblash — ma’lumotlar bilan ishlashda shunday shart-sharoitlar yaratiladiki, ruxsatsiz tizimga kirib olish ehtimoli kamaytiriladi.

Majburlash – kabul kilingan qoidalarga asosan ma’lumotlarni kayta ishlash, aks holda foydalanuvchilar moddiy, ma’muriy va jinoiy jazolanadilar.

Undamoq — axlokiy va odobiy qoidalarga binoan kabul kilingan tartiblarni bajarishga yunaltirilgan.

Yuqorida keltirilgan usullarni amalga oshirishda quyidagicha tasniflangan vositalarni tadbik etishadi.



Rasmiy vositalar — shaxslarni ishtirokisiz axborotlarni himoyalash funksiyalarini bajaradigan vositalardir.

Norasmiy vositilar — bevosita shaxslarni faoliyati yoki uning faoliyatini aniklab beruvchi reglamentlardir.

Texnikavny vositalar sifatida elektr, elektromexanik va elektron qurilmalar tushuniladi. Texnikaviy vositalar uz navbatida, fizikaviy va apparatli bo‘lishi mumkin.

Apparat-texnik vositalari deb telekommunikatsiya qurilmalariga kiritilgan yoki u bilan interfeys orqali ulangan qurilmalarga aytiladi. Masalan, ma’lumotlarni nazorat qilishning juftlik chizmasi, ya’ni junatiladigan ma’lumot yulda buzib talkin etilishini aniqlashda kullaniladigan nazorat bo‘lib, avtomatik ravishda ish sonining juftligini (nazorat razryadi bilan birgalikda) tekshiradi.

Fizikaviy texnik vositalar — bu avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, oddiy eshik kulflari, derazada urnatilgan temir panjaralar, kuriklash elektr uskunalari fizikaviy texnik vositalarga kiradi.

Dasturiy vositalar – bu axborotlarni himoyalash funksiyalarini bajarish uchun muljallangan maxsus dasturiy ta’minotdir.

Axborotlarni himoyalashda birinchi navbatda eng keng kullanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parol’ tizimini keltirish mumkin.

Tashkiliy himoyalash vositalari — bu talekommunikatsiya uskunalarining yaratilishi va kullanishi jarayonida kabul kilingan tashkiliy-texnikaviy va tashkiliy-huquqiy tadbirlardir. Bunga bevosita misol sifatida quyidagi jarayonlarni keltirish mumkin: binolarning kurilishi, tizimni loyixalash, qurilmalarni urnatish, tekshirish va ishga tushirish.

Axloqiy va odobiy himoyalash vositalari — bu hisoblash texnikasini rivojlanishi oqibatida paydo buladigan tartib va kelishuvlardir. Ushbu tartiblar qonun darajasida bulmasada, uni tan olmaslik foydalanuvchilarni obro‘siga ziyon etkazishi mumkin.

Qonuniy himoyalash vositalari — bu davlat tomonidan ishlab chikilgan huquqiy hujjatlar sanaladi. Ular bevosita axborotlardan foydalanish, kayta ishlash va uzatishni tartiblashtiradi va ushbu qoidalarni buzuvchilarning mas’uliyatlarini aniklab beradi.

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The

policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- *In the business sector, labels such as:* ***Public, Sensitive, Private, Confidential****.*
- *In the government sector, labels such as:* ***Unclassified****,* ***Unofficial****,* ***Protected****,* ***Confidential****,* ***Secret****,* ***Top Secret*** *and their non-English equivalents.*
- *In cross-sectoral formations, the Traffic Light Protocol, which consists of:* ***White, Green, Amber****, and* ***Red****.*

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place and are followed in their right procedures.[4]

Masalan, O'zbekiston Respublikasi Markaziy banki tomonidan ishlab chiqilgan qoidalarida axborotni himoyalash guruzlarini tashkil qilish, ularning vakolatlari, majburiyatlari va javobgarliklari anik yoritib berilgan.

Xavfsizlikni ta'minlash usullari va vositalarining rivojlanishini uch bosqichga ajratish mumkin: 1) dasturiy vositalarni rivojlantirish; 2) barcha yo'nalishlar buyicha rivojlanishi; 3) ushbu bosqichda quyidagi yo'nalishlar buyicha rivojlanishlar kuzatilmokda:

- himoyalash funksiyalarini apparatli amalga oshirish;
- bir necha himoyalash funksiyalarini kamrab olgan vositalarni yaratish;
- algoritm va texnikaviy vositalarni umumlashtirish va standartlash.

Hozirgi kunda ma'lumotlarni ruxsatsiz chetga chiqib ketish yo'llari quyidagilardan iborat:

• elektron nurlarni chetdan turib o'qib olish;
• aloqa kabellarini elektromagnit tulkinlar bilan nurlatish;
• yashirin tinglash qurilmalarini qo'llash;
• masofadan rasmga tushirish;
• printerdan chikadigan akustik tulkinlarni o'qib olish;
• ma'lumot tashuvchilarni va ishlab chikarish chikindilarini ugirlash;
• tizim xotirasida saklanib kolgan ma'lumotlarni o'qib olish;
• himoyani engib ma'lumotlarni nusxalash;
• qayd qilingan foydalanuvchi niqobida tizimga kirshi;
• dasturiy tuzoklarni qo'llash;
• dasturlash tillari va operatsion tizimlarning kamchiliklaridan foylalanish;

[4] *Discovering Computers 2016. Tools, Apps, Devices,and the Impact of Texnology. 691 page*

• dasturlarda maxsus belgilangan sharoitlarda ishga tushishi mumkin bo‘lgan qism dasturlarning mavjud bo‘lishi;

• aloqa va apparatlarga noqonuniy ulanish;

• himoyalash vositalarini kasddan ishdan chikarish;

• kompyuter viruslarini tizimga kiritish va undan foydalanish.

Ushbu yullardan deyarli barchasining oldini olish mumkin, lekin kompyuter viruslaridan hozirgacha konikarli himoya vositalari ishlab chikilmagan.

Bevosita tarmoq buyicha uzatiladigan ma’lumotlarni himoyalash maqsadida quyidagi tadbirlarni bajarish lozim buladi:

- uzatiladigan ma’lumotlarni ochib ukishdan saklanish;

- uzatiladigan ma’lumotlarni taxtil kiliшdan saklanish;

- uzatiladigan ma’lumotlarni uzgartirishga yul kuymaslik va uzgartirishga urinishlarni aniqlash;

- ma’lumotlarni uzatish maqsadida kullaniladigan dasturiy uzilishlarni aniqlashga yul kuymaslik;

- firibgar ulanishlarning oldini olish.

Ushbu tadbirlarni amalga oshirishda asosan kriptografik usullar kullaniladi.

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.[5]

EHM himoyasini ta’minlashning texnik vositalari

Kompyuter orqali sodir etidadigan jinoyatlar oqibatida faqatgina AQSH har yili 100 mlrd. dollar zarar ko’radi. O‘rtacha har bir jinoyatda 430 ming dollar o’girlanadi va jinoyatchini qidirib topish ehtimoli 0,004% ni tashkil etadi.

Mutaxassislarning fikricha ushbu jinoyatlarni 80%i bevosita korxonada ishlaydigan xodimlar tomonidan amalga oshiriladi.

Sodir etiladigan jinoyatlarning taxlili quyidagi xulosalarni beradi:

• ko‘pgina hisoblash tarmoqlarida foydalanuvchi istalgan ishchi urindan tarmoqda ulanib faoliyat kursatishi mumkin. Natijada jinoyatchi bajargan ishlarni kaysi kompyuterdan amalga oshirilganini aniqlash qiyin buladi.

[5] *Discovering Computers 2016. Tools, Apps, Devices,and the Impact of Texnology. 691 page.*

• ugirlash natijasida xech nima yukolmaydi, shu bois ko‘pincha jinoiy ish yuritilmaydi;

• ma’lumotlarga nisbatan mulkchilik xususiyati yukligi;

• ma’lumotlarni kayta ishlash jarayonida yul kuyilgan xatolik uz vaktida kuzatilmaydi va tuzatilmaydi, natijada kelgusida sodir buladigan xatolarning oldini olib bulmaydi;

• sodir etiladigan kompyuter jinoyatlari uz vaktida e’lon kilinmaydi, buning sababi hisoblash tarmoqlarida kamchiliklar mavjudligini boshqa xodimlardan yashirish hisoblanadi.

Ushbu kamchiliklarni bartaraf qilishda va kompyuter jinoyatlarini kamaytirishda quyidagi chora-tadbirlarni o‘tkazish kerak buladi:

• personal mas’uliyatini oshirish:

• ishga kabul kilinadigan xodimlarni tekshiruvdan o‘tkazish;

• muhim vazifani bajaruvchi xodimlarni almashtirib turish;

• parol’ va foydalanuvchilarni kayd qilishni yaxshi yulga kuyish;

• ma’lumotlarga egalik kiilishni cheklash;

• ma’lumotlarni shifrlash.

Axborot-kommunikatsiyalar texnologiyalarining rivojlanishi oqibatida ko‘pgina axborotni himoyalash instrumental vositalari ishlab chikilgan. Ular dasturiy, dasturiy-texnik va texnik vositalardir.

Hozirgi kunda tarmoq xavfsizligini ta’minlash maqsadida ishlab chikilgan texnikaviy vositalarni quyidagicha tasniflash mumkin:

Fizikaviy himoyalash vositalari — maxsus elektron qurilmalar yordamida ma’lumotlarga egalik qilishni taqiqlash vositalaridir.

Mantikiy himoyalash — dasturiy vositalar bilan ma’lumotlarga egalik qilishni taqiqlash uchun kullaniladi.

Tarmoqlararo ekranlar va shlyuzlar — tizimga keladigan hamda undan chikadigan ma’lumotlarni ma’lum hujumlar bilan tekshirib boradi va protokollashtiradi.

Xavfsizlikni auditlash tizimlari — joriy etilgan operatsion tizimdan urnatilgan parametrlarni zaifligini kidirishda kullaniladigan tizimdir.

Real vaktda ishlaydigan xavfsizlik tizimi — doimiy ravishda tarmoqning xavfsizligini taxlillash va auditlashni ta’minlaydi.

Stoxastik testlarni tashkillashtirish vositalari — axborot tizimlarining sifati va ishonchliligini tekshirishda kullaniladigan vositadir.

Anik yunaltirilgan testlar — axborot-kommunikatsiyalar texnologiyalarining sifati va ishonchliligini tekshirishda kullaniladi.

Xavflarni imitatsiya qilish — axborot tizimlariga nisbatan xavflar yaratiladi va himoyaning samaradorligi aniklanadi.

Statistik taxlilgichlar — dasturlarning tuzilish tarkibidagi kamchiliklarni aniqlash, dasturlar kodida aniklanmagan kirish va chikish nuktalarini topish, dasturdagi uzgaruvchilarni tugri aniqlanganligini va kuzda tutilmagan ishlarni bajaruvchi qism dasturlarini aniqlashda foydalaniladi.

Dinamik taxlilgichlar — bajariladigan dasturlarni kuzatib borish va tizimda sodir buladigan uzgarishlarni aniqlashda kullaniladi.

Tarmoqning zaifligini aniqlash — tarmoq zaxiralariga sun’iy hujumlarni tashkil qilish bilan mavjud zaifliklarni aniqlashda kullaniladi.

Misol sifitida quyidagi vositalarni keltirish mumkin:

• Dallas Lock for Administrator — mavjud elektron Proximity uskunasi asosida yaratilgan dasturiy-texnik vosita bo‘lib, bevosita ma’lumotlarga ruxsatsiz kirishni nazorat qilishda kullaniladi;

• Security Administrator Tool for ANALYZING Networks (SATAN) — dasturiy ta’minot bo‘lib, bevosita tarmoqning zaif tomonlarini aniklaydi va ularni bartaraf etish yullarini kursatib beradi. Ushbu yo’nalish buyicha bir necha dasturlar ishlab chikilgan, masalan: Internet Security Scanner, Net Scanner, Internet Scanner va boshqalar.

• NBS tizimi — dasturiy-texnik vosita bo‘lib, aloqa kanallaridagi ma’lumotlarni himoyalashda kullaniladi;

• Free Space Communication System — tarmoqda ma’lumotlarning har xil nurlar orqali, masalan lazerli nurlar orqali almashuvini ta’minlaydi;

• SDS tizimi — ushbu dasturiy tizim ma’lumotlarini nazorat kiladi va kaydnomada aks ettiradi. Asosiy vazifasi ma’lumotlarni uzatish vositalariga ruxsatsiz kirishni nazorat qilishdir;

• Timekey — dasturiy-texnik uskunadir, bevosita EXMning parallel portiga urnatiladi va dasturlarni belgilangan vaktda keng kullalilishini taqiqlaydi;

• IDX — dasturiy-texnik vosita, foydalanuvchining barmok, izlarini «o‘qib olish» va uni taxlil qiluvchi texnikalardan iborat bo‘lib, yukori sifatli axborot xavfsizligini ta’minlaydi. Barmok izlarini o‘qib olish va xotirada saqlash uchun 1 minutgacha, uni takkoslash uchun esa 6 sekundgacha vakt talab qilinadi.

Kompyuter tarmoqlarida ma’lumotlarni himoyalashning asosiy yo’nalishlari

Axborotlarni himoyalashning mavjud usul va vositalari hamda kompyuter tarmoqlari kanallaridagi aloqaning xavfsizligini ta’minlash texnologiyasi evolyutsiyasini solishtirish shuni kursatmokdaki, bu texnologiya rivojlanishining birinchi bosqichida dasturiy vositalar afzal topildi va rivojlanishga ega buldi, ikkinchi bosqichida himoyaning hamma asosiy usullari va vositalari intensiv rivojlanishi bilan harakterlandi, uchinchi bosqichida esa quyidagi tendentsiyalar ravshan bulmokda:

- axborotlarni himoyalash asosiy funksiyalarining texnik jixatdan amalga oshirilishi;

- bir nechta xavfsizlik funksiyalarini bajaruvchi himoyalashning birgalikdagi vositalarini yaratish:

- algoritm va texnik vositalarni unifikatsiya qilish va standartlashtirish.

Kompyuter tarmoqlarida xavfsizlikni ta’minlashda hujumlar yukori darajada malakaga ega bo‘lgan mutaxassislar tomonidan amalga oshirilishini doim esda tutish lozim. Bunda ularning harakat modellaridan doimo ustun turuvchi modellar yaratish talab etiladi. Bundan tashkari, avtomatlashtirilgan axborot tizimlarida personal eng ta’sirchan qismlardan biridir. SHuning uchun, yovuz niyatli shaxsga axborot tizimi personalidan foydalana olmaslik chora-tadbirlarini utkazib turish ham katta ahamiyatga ega.

Network security *consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.[citation needed] Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.*[6]

Internet mapmogida mavjud aloqaning himoyasini (xavfsizligini) ta’minlash asoslari

Ma’lumotlarni uzatish tizimlarining rivojlanishi va ular asosida yaratilgan telekommunikatsiya xizmat kursatish vositalarining yaratilishi bevosita foydalanuvchilarga tarmoq zaxiralaridan foydalanish tartiblarini ishlab chikarish zaruriyatini paydo qildi:

• foydalanuvchining anonimligini ta’minlovchi vositalar;

• serverga kirishni ta’minlash. Server faqatgina bitta foydalanuvchiga emas, balki keng mikyosdagi foydalanuvchilarga uz zaxiralaridan foydalanishga ruxsat berishi kerak;

• ruxsatsiz kirishdan tarmoqni himoyalash vositalari.

---

[6] *Discovering Computers 2016. Tools, Apps, Devices,and the Impact of Texnology. 691 page.*

Internet tarmogida ruxsatsiz kirishni taqiqlovchi tarmoqlararo ekran — Fire Wall vositalari keng tarkalgan. Ushbu vosita asosan UNIX operatsion tizimlarida kuldanilib, bevosita tarmoqlar orasida aloqa urnatish jarayonida xavfsizlikni ta’minlaydi. Bundan tashkari, Fire Wall tizimlari tashki muxit, masalan, Internet uchun, asosiy ma’lumotlarni va MBlarini xotirasida saklab, bevosita ma’lumot almashuvini ta’minlashi va korxona tizimiga kirishini taqiqlashi mumkin.

Fire Wall sinfidagi tizimlarning asosiy qismi tashki hujumlarni kaytarish uchun muljallangan bulsa ham, hujumlar ularning 60 foizi kuchsiz ekanligini kursatdi. Bundan tashkari, Fire Wall zabt etilgan serverning ishlashiga karshilik kursata olmaydi.

SHu bois, Internet tizimida xavfsizlikni ta’minlash buiicha quyidagi uzgarishlar kutilmokda:

• Fire Wall tizimlarining bevosita xavfsizlik tizimlariga kiritilishi;

• tarmoq protokollari bevosita foydalanuvchilarni huquqlarini aniqlovchi, xabarlarning yaxlitligini ta’minlovchi va ma’lumotlarni shifrlovchi dasturiy imkoniyatlaridan iborat bo‘lishlari. Hozirgi kunda ushbu protokollarni yaratish buyicha anchagina ishlar olib borilmoqda. SKIP protokoli (Simple Key management for Internet Protocol — Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi) shunga misol bo‘la oladi.

Nazorat savollari

1. Kompyuter tarmoqlarida himoyani ta’minlash usullari.
2. EHM himoyasini ta’minlashning texnik vositalari.
3. Kompyuter tarmoqlarida ma’lumotlarni himoyalashning asosiy yo‘nalishlari.