O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

S.K.GANIEV, A.A.GANIEV, Z.T.XUDOYQULOV

KIBERXAVFSIZLIK ASOSLARI

O‘zbekiston Respublikasi Oliy va O‘rta maxsus ta’lim vazirligi tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan

professor S.K.Ganiev tahriri ostida

TOSHKENT 2020

UDK: 004
S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma. – T.: «Aloqachi», 2020, 221 bet.

O‘quv qo‘llanmada kiberxavfsizlik va uning asosiy tushunchalari, axborotning kriptografik himoyasi, foydalanishni nazoratlash, tarmoq xavfsizligi, foydalanuvchanlikni ta’minlash usullari, dasturiy vositalar xavfsizligi, axborot xavfsizligi siyosati va risklarni boshqarish, kiberjinoyatchilik, kiberhuquq, kiberetika hamda inson faoliyati xavfsizligining nazariy va amaliy asoslari muhokama etilgan.

O‘quv qo‘llanma 5330300 – “Axborot xavfsizligi”, 5330500 – “Kompyuter injiniringi (Kompyuter injiniringi, AT-servisi, Multimedia texnologiyalari)”, 5330600 – “Dasturiy injiniring”, 5350100 – “Telekommunikatsiya texnologiyalari (Telemommunikatsiya, teleradiouzatish, mobil tizimlar)”, 5350200 – “Televizion texnologiyalar (Audiovizual texnologiyalar, telestudiya tizimlari va ilovalari)”, 5350300– “Axborot-kommunikatsiya texnologiyalari sohasida iqtisodiyot va menejment”, 5350400 – “Axborot-kommunikatsiya texnologiyalari sohasida kasb ta’limi”, 5350500 – “Pochta aloqasi texnologiyasi” va 5350600 – “Axborotlashtirish va kutubxonashunoslik” yo‘nalishlari bo‘yicha ta’lim olayotgan talabalar uchun tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta’minlash bilan bog‘liq bo‘lgan mutaxassislarning keng doirasi uchun ham foydali bo‘lishi mumkin.

Taqrizchilar:

Tashev K.A. – texnika fanlari nomzodi, dotsent, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-ishlar va innovatsiyalar bo‘yicha prorektori.

Axmedova O.P. – texnika fanlari nomzodi, “UNICON.UZ” DUK – Fan-texnika va marketing tadqiqotlari markazi “Axborot xavfsizligi va kriptologiya ilmiy tadqiqot bo‘limi” boshlig‘i.

MUNDARIJA

MUQADDIMA

Yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat axborot-kommunikatsiya texnologiyalariga tobora koʻproq qaram boʻlib borayotganligi bois, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega.

Shu sababli, har bir tashkilotga, kiberxavfsizlikni ta’minlash maqsadida, mazkur soha bilan shugʻullanuvchi xodimlar jalb qilinmoqda va xodimlarni kiberxavfsizlikka oid bilimlar bilan muntazam tanishtirib borish uchun qator seminar-treyning mashgʻulotlari tashkil etilmoqda. Oliy ta’lim muassasalarida ham kiberxavfsizlikni fan sifatida oʻtilishi buning yaqqol misolidir.

Respublikamizda axborot texnologiyalarining rivojlanishi bilan bir qatorda xoʻjalik va davlat boshqaruvi organlarida axborot xavfsizligini, xususan, kompyuter bilan bogʻliq boʻlgan xavfsizlik muammolarini bartaraf etish yoʻnalishiga alohida e’tibor qaratilmoqda. 2017-2021 yillarda Oʻzbekiston Respublikasini yanada rivojlantirish boʻyicha Harakatlar strategiyasida vazifalar belgilab olindi, shular qatorida «...axborot xavfsizligini ta’minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga oʻz vaqtida va munosib qarshilik koʻrsatish» va kiberjinoyatchilikni fosh etish masalalariga alohida e’tibor qaratilgan. Bundan tashqari, “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yilida amalga oshirishga oid Davlat dasturi toʻgʻrisida”gi Oʻzbekiston Prezidenti Farmonida “2020 yil 1 sentyabrga qadar kiberxavfsizlikka doir milliy strategiya va qonun loyihasi ishlab chiqish” vazifalari belgilangan. Bu vazifalarni amalga oshirishda kiberxavfsizlik sohasiga oid oʻquv qoʻllanmalarini ishlab chiqish ham e’tibor berish kerak boʻlgan muhim jihatlardan hisoblanadi.

Qoʻllanmaning birinchi bobida kiberxavfsizlik asoslari fani sohasining vazifalari va asosiy tushunchalari, uning qoʻllanilish sohasi hamda kiberxavfsizlikda inson omili masalalari koʻrib chiqilgan. Kiberxavfsizlikning bilim sohalari, kiberxavfsizlik va axborot xavfsizligi tushunchalari oʻrtasidagi farq misollar asosida keltirilgan. Shuningdek, kiberjinoyatchilik, kiberhuquq va kiberetika masalalariga toʻxtalib oʻtilib, kiberjinoyatchilik uchun tayinlangan jazo turlari haqida ma’lumotlar keltirilgan.

Ikkinchi bob kiberxavfsizlikning fundamental masalalariga bag‘ishlangan, hamda kiberxavfsizlik arxitekturasi, strategiyasi va siyosatini amalga oshirish tartibi xususida ma’lumotlar keltirilgan.

Uchinchi bobda axborotning kriptografik himoyasi doirasidagi asosiy tushunchalar, simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, ma’lumotlar yaxlitligini ta’minlash usullari, disklarni va fayllarni shifrlash hamda ma’lumotlarni xavfsiz o‘chirish usullari ko‘rib chiqilgan.

Qo‘llanmaning to‘rtinchi bobi foydalanishlarni nazoratlashga bag‘ishlangan bo‘lib, autentifikatsiya usullari, ma’lumotlarni fizik va mantiqiy boshqarish usullari keltirilgan. Amalda keng qo‘llanilayotgan mantiqiy foydalanishlarni boshqarish modellari va ulardan foydalanish bo‘yicha tavsiyalar bayon etilgan.

Beshinchi bob tarmoq xavfsizligiga bag‘ishlangan bo‘lib, unda tarmoqda mavjud bo‘lgan xavfsizlik muammolari va ularni bartaraf etishda tarmoqlararo ekrandan, virtual himoyalangan tarmoqdan va boshqa vositalardan foydalanish masalalari keltirilgan. Bundan tashqari, simsiz tarmoqlarda xavfsizlik muammolari va risklarni boshqarish masalalariga to‘xtalib o‘tilgan.

Oltinchi bobda tizimning foydalanuvchanlik xususiyati va uning tizim uchun muhimligi, ma‘lumotlarni zaxira nusxalash va qayta tiklash usullari xususida ma’lumotlar keltirilgan. Tizim foydalanuvchanligi uchun audit muolajasi muhim hisoblangani bois, Windows OT uchun hodisalarni qaydlash tartibi bilan tanishib chiqiladi.

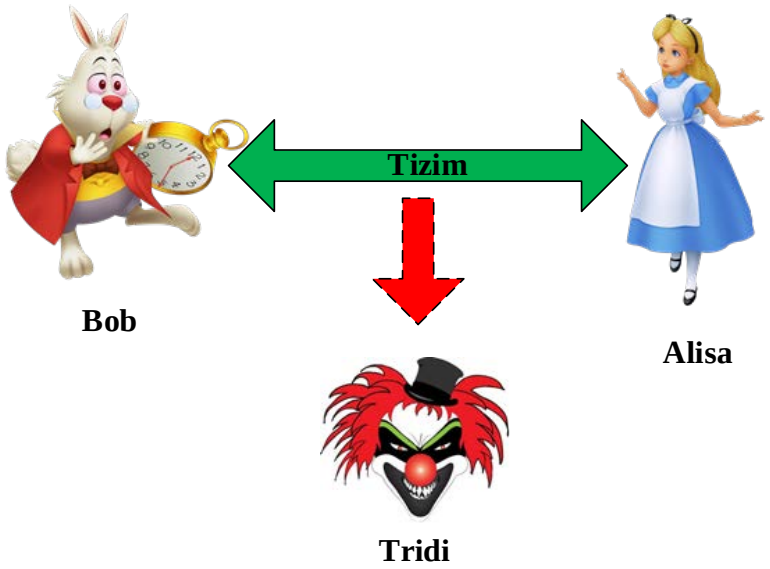
Yettinchi bob dasturiy vositalar xavfsizligiga bag‘ishlangan bo‘lib, dasturlardagi xavfsizlik muammolari va ularni oldini olishga qaratilgan fundamental prinsiplar bayon etilgan. Vazifasi tizimga ziyon yetkazish uchun yaratilgan zararli dasturiy vositalar, ularning tahlili va zamonaviy antivirus dasturiy vositalari haqida batafsil ma’lumotlar keltirilgan.

1 BOB. KIBERXAVFSIZLIK. UMUMIY MA’LUMOTLAR

1.1. Kiberxavfsizlikning asosiy tushunchalari

Axborotni ishlash, uzatish va to‘plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo‘qolishi, buzilishi va oshkor etilishi bilan bog‘liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash axborot texnologiyalari rivojining yetakchi yo‘nalishlaridan biri hisoblanadi.

Axborot xavfsizligi hayotda mavjud timsollarga asoslanadi. Hayotda qonuniy faoliyat olib boruvchi shaxslar mavjud, ular 1.1-rasmda *Alisa* va *Bob* timsolida akslantirilgan. Biroq, hayotda qonuniy faoliyat yurituvchi insonlarning faoliyatiga qiziquvchi, ularning ishlariga xalaqit beruvchi insonlar ham mavjud va ular 1.1-tasvirda *Tridi* timsolida tasvirlangan. Tridi timsoli barcha g‘arazli niyatlarni amalga oshiruvchi shaxslarni ifodalaydi.



1.1-rasm. Axborot xavfsizligining hayotdagi timsollari

O‘quv qo‘llanmaning keyingi bo‘limlarini yoritishda quyidagi hayotiy senariyni ko‘raylik. Ushbu hayotiy senariy *Alisaning onlayn banki (AOB)* deb ataladi. Bunga ko‘ra, Alisa onlayn bankning biznes faoliyatini amalga oshiradi. Mazkur senariyda Alisaning xavfsizlik muammosi nima? Alisaning mijozi bo‘lgan Bobning xavfsizlik muammosichi? Alisa va Bobning xavfsizlik muammolari bir xilmi? Tridi nuqtai nazaridan qaraganda qanday xavfsizlik muammolari mavjud? Ushbu savollarga keyingi qismlarda javob berib o‘tiladi.

Kompyuter tizimlari va tarmoqlarida axborotni himoyalash va axborot xavfsizligiga tegishli bo‘lgan ayrim tushunchalar bilan tanishib chiqaylik.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo‘lib, unga berilgan turlicha ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta’rif berilgan: *kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni to‘g‘ri bajarilishini kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi.*

Tarmoq sohasida faoliyat yuritayotgan *Cisco* tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: *Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.*

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilganidan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalarning va ularning vazifalarining himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga sabab bo‘ladi.

Hozirda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassisning kiberxavfsizlikning fundamental bilimlariga ega bo‘lishi talab etiladi. Kiberxavfsizlik fani sohasining tuzilishini quyidagicha tasvirlash mumkin (1.2-rasm).

1.2 – rasm. Kiberxavfsizlik fani sohasining tuzilishi

Kiberxavfsizlikni fundamental atamalarini aniqlashda turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida kiberxavfsizlikning quyidagi 6 ta atamasi keltirilgan:

Konfidensiallik – axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi. Konfidensiallik axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. AOB senariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o‘z balansida qancha pul borligini Tridining bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma’lumotlarning konfidensialligini ta’minlash muhim hisoblanadi.

Yaxlitlik - axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati. Yaxlitlik axborotni ruxsatsiz “yozish”dan (ya’ni, axborotni o‘zgartirishdan) himoyalash yoki kamida o‘zgartirilganligini aniqlash bilan shug‘ullanadi. AOB senariysida Alisaning banki qayd yozuvining yaxlitligini Tridan himoyalash shart. Masalan, Bob o‘zining akkauntida balansning o‘zgarishidan yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Shu o‘rinda konfidensiallik va yaxlitlik bir xil tushuncha emasligiga e’tibor berish kerak. Masalan, Tridi biror ma’lumotni o‘qiy olmagan taqdirda ham uni sezilmaydigan darajada o‘zgartirishi mumkin.

Foydalanuvchanlik - avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati. Foydalanuvchanlik axborotni (yoki tizimni) ruxsatsiz “bajarmaslik”dan himoyalash bilan shug‘ullanadi. AOB senariysida AOB web saytidan Bobning foydalana olmasligi Alisaning banki va Bob uchun foydalanuvchanlik muammosi hisoblanadi. Sababi, mazkur holda Alisa pul o‘tkazmalaridan daromad ola olmaydi va Bob esa o‘z biznesini amalga oshira olmaydi. Foydalanuvchanlikni buzishga qaratilgan hujumlardan eng keng tarqalgani – xizmat ko‘rsatishdan voz kechishga undovchi hujum (Denial of service, DOS).

Risk – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi. ISO “*risk* – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan.

Masalan, universitetga o‘qishga kirish jarayonini ko‘raylik. Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina abituriyent hujjatlarini va kirish imtihonlarini topshirganida, u o‘qishga kirishi yoki kira olmasligi mumkin. Bu o‘z navbatida qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga sabab bo‘ladi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda qaraladi.

Hujumchi kabi fikrlash - bo‘lishi mumkin bo‘lgan xavfni oldini olish maqsadida qonuniy foydalanuvchining hujumchi kabi fikrlash jarayoni.

Tizimli fikrlash - kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.

Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini o‘rganishda muhim hisoblanadi.

Axborot xavfsizligi - axborotning holati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo‘l qo‘yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.

Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo‘naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar, kerak bo‘lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

Aktiv - himoyalanuvchi axborot yoki resurslar. Yoki, tashkilot uchun qimmatli barcha narsalar.

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug‘diruvchi sharoit va omillar majmui. Tahdid tashkilotning aktivlariga qaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin.

Zaiflik – bir yoki bir nechta tahdidlarni amalga oshirishga imkon beruvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.

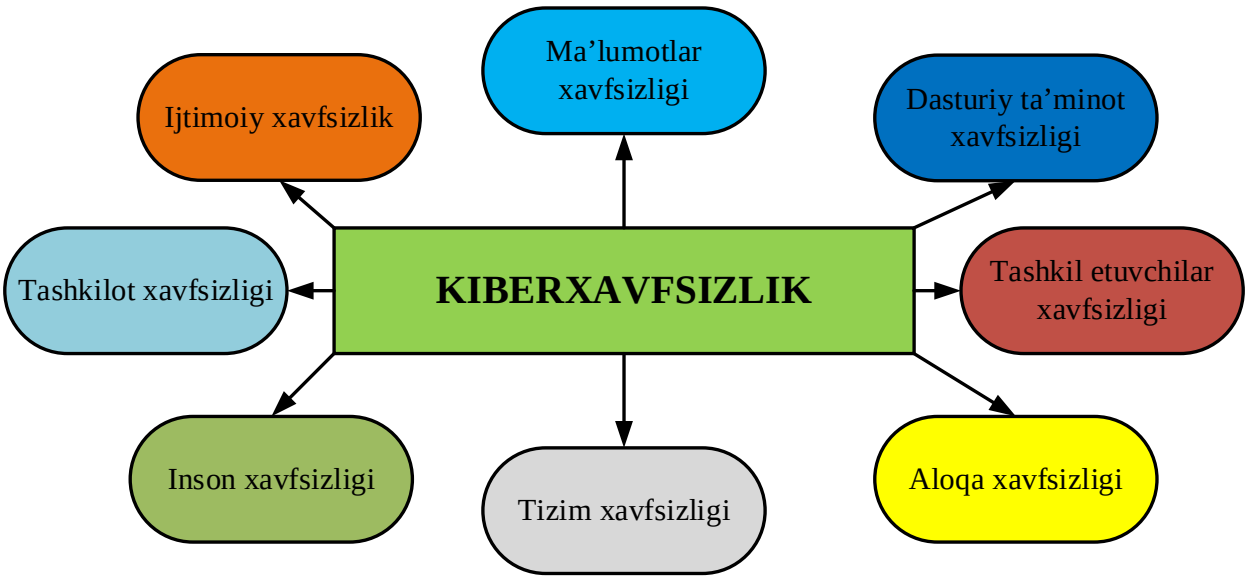
Boshqarish vositasi – riskni o‘zgartiradigan harakatlar bo‘lib, natijasi zaiflik yoki tahdidlarni o‘zgarishiga ta’sir qiladi. Bundan tashqari, boshqarish vositasining o‘zi turli tahdidlar foydalanishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin. Masalan, tashkilotda saqlanayotgan qog‘oz ko‘rinishidagi axborotni yong‘indan himoyalash uchun o‘chirish vositalari boshqarish vositasi sifatida ko‘rilishi mumkin. Yong‘in bo‘lganida xodimlarning xatti-xarakatlari va yong‘inni oldini olish bo‘yicha ko‘rilgan chora-tadbirlar ham boshqarish vositasi hisoblanishi mumkin. Yong‘inga qarshi kurashish tizimining ishlamay qolish holatiga esa boshqarish vositasidagi kamchilik sifatida qaraladi.

Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi farq. “Kiberxavfsizlik” va “axborot xavfsizligi” atamalaridan, ko‘pincha o‘rnilari almashgan holda, foydalanishadi. Ba’zilar kiberxavfsizlikka axborot xavfsizligi, axborot texnologiyalari xavfsizligi va (axborot) risklarni boshqarish tushunchalariga sinonim sifatida qarashsa, ayrimlar esa, xususan hukumat sohasidagilar, kompyuter jinoyatchiligi va muhim infrastrukturalar himoyasini o‘z ichiga olgan milliy xavfsizlik bilan bog‘liq texnik tushuncha sifatida qaraydilar. Turli soha xodimlari tomonidan o‘z maqsadlariga moslashtirish holatlari mavjud bo‘lsada, axborot xavfsizligi va kiberxavfsizlik tushunchalari orasida ba’zi muhim farqlar mavjud.

Axborot xavfsizligi sohasi, axborotning ifodalanishidan qat’iy nazar (qog‘oz ko‘rinishidagi, elektron va insonlar fikrlashida, og‘zaki va vizual) intelektual huquqlarni himoyalash bilan shug‘ullanadi. *Kiberxavfsizlik* esa elektron shakldagi axborotni (barcha holatdagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug‘ullanadi. Bundan tashqari, hukumatlar tomonidan moliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced

persistent threats, APT) ham aynan kiberxavfsizlikka tegishli. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo‘nalishi deb tushunish uni to‘g‘ri anglashga yordam beradi.

Kiberxavfsizlikning bilim sohalari. CSEC2017 JTF manbasiga ko‘ra kiberxavfsizlik 8 ta bilim sohasiga bo‘lingan, o‘z o‘rnida ularning har biri qismsohalarga bo‘linadi (1.3-rasm).



1.3-rasm. Kiberxavfsizlikning bilim sohalari

“*Ma’lumotlar xavfsizligi*” bilim sohasining maqsadi ma’lumotlarni saqlash, ishlash va uzatishda himoyani ta’minlash. Mazkur bilim sohasida himoyani to‘liq amalga oshirish uchun matematik va analitik algoritmlardan foydalaniladi.

“*Dasturiy ta’minot xavfsizligi*” bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy vositalarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.

“*Tashkil etuvchilar xavfsizligi*” bilim sohasi katta tizimlarda integrallashgan tashkil etuvchilarni loyihalashga, sotib olishga, testlashga, tahlillashga va texnik xizmat ko‘rsatishga e’tibor qaratadi. Tizim xavfsizligi gohida tashkil etuvchilar xavfsizligidan farq qiladi. Tashkil etuvchilar xavfsizligi tizimning qanday loyihalanganligiga, yaratilganligiga, sotib olinganligiga, boshqa tarkibiy qismlar bilan bog‘langanligiga, qanday ishlayotganligiga va saqlanayotganligiga bog‘liq bo‘ladi.

“*Aloqa xavfsizligi*” bilim sohasi tashkil etuvchilar o‘rtasidagi aloqani himoyalashga e’tibor qaratib, o‘zida fizik va mantiqiy ulanishni mujassamlashtiradi.

“*Tizim xavfsizligi*” bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat tizim xavfsizligining jihatlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun, nafaqat uning tarkibiy qismlari va ularning bog‘lanishlarini tushunish, balki yaxlitlikni ham hisobga olish talab etiladi. Ya’ni, tizimni to‘liqligicha ko‘rib chiqish talab etiladi. Mazkur bilim sohasi, “Tashkil etuvchilar xavfsizligi” va “Aloqa xavfsizligi” bilim sohalari bilan bir qatorda, tashkil etuvchilar bog‘lanishlarining xavfsizligi va undan yuqori tizimlarda foydalanish masalasini hal etadi.

“*Inson faoliyati xavfsizligi*” bilim sohasi kiberxavfsizlik bilan bog‘liq inson hatti-harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida ma’lumotlarni va shaxsiylikni himoya qilishga e’tibor qaratadi.

“*Tashkilot xavfsizligi*” bilim sohasi tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini madadlash uchun risklarni boshqarishga e’tibor qaratadi.

“*Ijtimoiy xavfsizlik*” bilim sohasi jamiyatda u yoki bu darajadagi ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. Kiberjinoyatchilik, qonunlar, axloqiy munosabatlar, siyosat, shaxsiy hayot va ularning bir-biri bilan munosabatlari ushbu bilim sohasidagi asosiy tushunchalar hisoblanadi.

Demak, aytish mumkinki, kiberxavfsizlik sohasi axborot texnologiyalari mutaxassislari uchun zarur soha hisoblanadi.

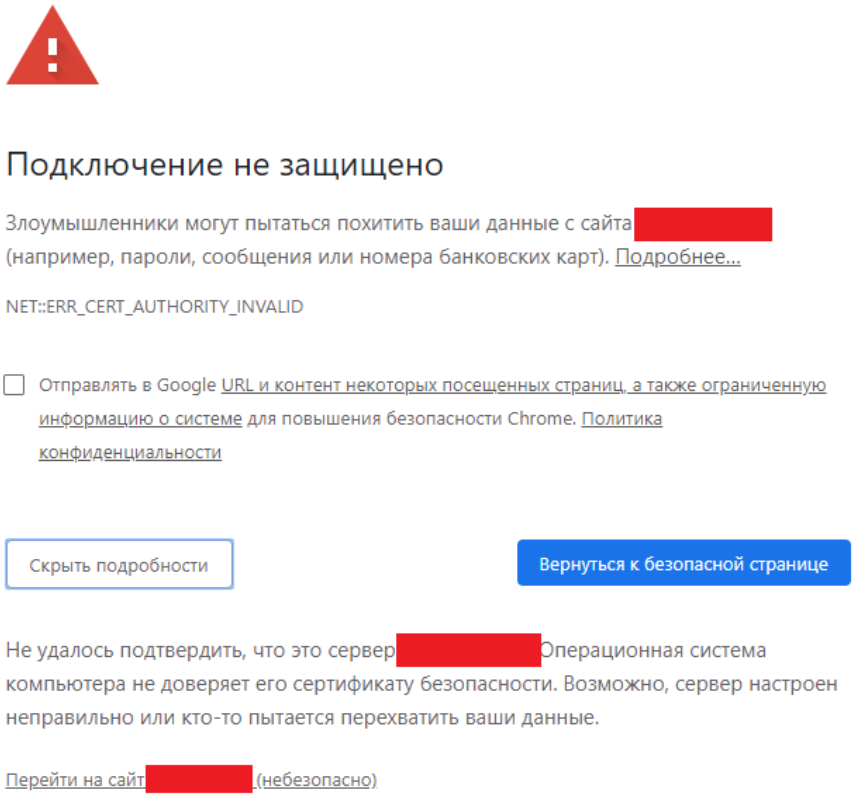
1.2. Kiberxavfsizlikda inson omili

Foydalanuvchilarga kiberxavfsizlik tizimidagi eng zaif nuqta sifatida qaraladi. Foydalanuvchilar tomonidan har qanday yuqori darajadagi xavfsizlik ham buzilishi mumkin. Masalan, Bob amazon.com onlayn do‘konidan biror narsani sotib olmoqchi, deylik. Buning uchun Bob turli kriptografik usullarga tayanadigan SSL (Secure Sockets Layer) protokoli yordamida Amazon bilan ishonchli bog‘lanish uchun web-brauzerdan foydalanishi mumkin. Ushbu protokol barcha zarur amallar to‘g‘ri bajarilganida kafolatli xavfsizlikni ta’minlaydi. Biroq, ushbu protokolga qaratilgan ba’zi hujum turlari (O‘rtada turgan odam hujumi, Man-in-the-middle attack) mavjudki, ularning amalga oshishi uchun foydalanuvchi “ishtiroki” talab etiladi (1.4-rasm). Agar foydalanuvchi

xavfsiz holatni tanlasa (*Вернуться к безопасной странице*) hujum amalga oshmaydi. Biroq, foydalanuvchi tomonidan xavfsiz bo‘lmagan tanlov (*Перейти на сайт .... (небезопасно)*) amalga oshirilganida hujum muvaffaqiyatli tugaydi. Boshqacha aytganda, yuqori xavfsizlik darajasiga ega protokoldan foydalanilganda ham foydalanuvchining noto‘g‘ri harakati sababli xavfsizlik buzilishi mumkin.

Odatda foydalanuvchilar esda saqlash oson bo‘lgan parollardan foydalanishga harakat qiladilar. Biroq, bunday yo‘l tutish buzg‘unchi uchun parollarni taxminlab topish imkoniyatini oshiradi. Boshqa tomondan, murakkab parollardan foydalanish va ularni turli eltuvchilarda saqlash (masalan, qog‘ozda qayd etish) esa, ushbu muammoni yanada kuchaytiradi.

Bu misollar inson omili tufayli turli joylar va holatlarda xavfsizlik muammolarining kelib chiqishi mumkinligini ko‘rsatadi. Inson omili tufayli yuzaga keladigan xavfsizlik muammolariga ko‘plab misollar keltirish mumkin. Biroq, keltirilgan holatlardagi eng muhim jihat shundaki, xavfsizlik nuqtai nazaridan “tenglamadan” inson omilini olib tashlash zarur. Boshqacha aytganda, inson omili ishtirok etmagan tizimlar ishtirok etgan tizimlarga nisbatan xavfsizroq bo‘ladi.



1.4-rasm. SSL protokolidagi xavfsizlik ogohlantirishi

Eng muhim inson omillariga quyidagilar taalluqli:

– *Kiberxavfsizlik sohasiga oid bilimlarni yetishmasligi* katta hajmdagi oshkor zaifliklarni paydo bo‘lishiga olib keladi. Kiberxavfsizlik sohasi an’anaviy xavfsizlikka aloqador bo‘lgani bois, zarur texnologik moslashishning tezkorligi ko‘p hollarda bo‘lishi mumkin bo‘lgan zaifliklar sonini oshiradi. Boshqa tomondan, insonning sohaga tegishli so‘nggi texnologik bilimlarni o‘zlashtirishi har doim ham yetarli bo‘lmaydi.

– *Risklarni bartaraf etishni va ular haqida xabar berishning yetarli bo‘lmasligi* kiberxavfsizlikda takrorlanuvchi va kutilmagan buzilishlarga sababchi bo‘ladi. Insonlar odatda tashkilotlariga jiddiy xavf soluvchi risk mavjudligini bilishsada, uni oshkor qilishmaydi. Buning asosiy sababi sifatida risk bevosita shaxsning o‘ziga, uni moliyaviy holatiga ta’sir etmasligini yoki oshkor qilinganida shaxsning obro‘si tushishini keltirishadi.

– *Madaniyat va munosabatlardagi muammolarga* tashkilotning o‘zi yoki tashkilot ichki ma’lumotlarini biluvchi norozi va e’tiborsiz xodimning paydo bo‘lishi sababchi bo‘lishi mumkin. Kiberxavfsizlik muammolarining aksariyati ichki hisoblanib, ular xodimlar orasidagi turli kelishmovchiliklar va tashkilot ichidagi muhitning yaxshi emasligi natijasida yuzaga keladi. Bu sabablar esa, xodimning tashkilot ichki strukturasini yaxshi bilgani bois, aksariyat hollarda jiddiy muammolarga olib keladi.

– *Xavfsizlik mashg‘ulotlariga kam mablag‘ sarflanishi* boshqarilayotgan xavfsizlik risklari to‘g‘risidagi ma’lumotning kamligi sababchi bo‘ladi. Odatda, soha korxonalaridagi xodimlar mustaqil ravishda kiberxavfsizlik qoidalarini o‘rganishmaydi. Shuning uchun kiberxavfsizlik qoidalarini xodimlarga maxsus mashg‘ulotlar shaklida yetkazish zarur bo‘ladi. Bu esa tashkilotdan xavfsizlik mashg‘ulotlariga yetarlicha mablag‘ sarflanishni talab qiladi.

– *Hisobga olish nuqtasining yagona emasligi* natijasida xavfsizlikning to‘laqonli amalga oshirilmasligi kuzatiladi. Amalda xavfsizlikni kafolatli ta’minlashda uning nazoratini bir nuqtada amalga oshirish muhim hisoblanadi. Yagona nuqtada amalga oshirilgan xavfsizlik nazorati taqsimlangan shakliga nisbatan ishonchli bo‘ladi. Biroq, tashkilotlardagi xavfsizlik nazoratining murakkabligi bois, nazorat odatda taqsimlangan holda boshqariladi.

– *Ijtimoiy injineriya* asosida xavfsizlik nazoratini aylanib o‘tishda foydalanuvchidan, an’anaviy josuslik texnikasi yordamida, ma’lumotlar qo‘lga kiritiladi. Eng yaxshi kiberxavfsizlik tizimiga ega bo‘lgan tashkilotga ham ijtimoiy injineriya tahdidi xavf solishi mumkin. Ayniqsa, foydalanuvchilarni turli ijtimoiy tarmoqlarda shaxsiy ma’lumotlarini e’tiborsizlik bilan qoldirishi bu xavfning keskin ortishiga sababchi bo‘lmoqda.

1.3. Kiberjinoyatchilik, kiberqonunlar va kiberetika

Kiberjinoyatchilik – g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Kiberhujumga duch kelgan tashkilot uchun kiberjinoyatlar ichki yoki tashqi bo‘lishi mumkin:

Ichki kiberjinoyatlar: tarmoqqa yoki kompyuter tizimiga, ular bilan tanish va ulardan qonuniy foydalanish huquqiga ega bo‘lgan shaxs tomonidan, amalga oshiriladi. Mazkur turdagi kiberjinoyatlar odatda tashkilotning xafa bo‘lgan va norozi xodimlari tomonidan amalga oshiriladi. Ushbu xodimlarning maqsadi esa tashkilot yoki uning rahbaridan o‘ch olish yoki ochko‘zlik bo‘lishi mumkin. Xafa bo‘lgan xodim, AT infrastrukturasi, xavfsizlik arxitekturasi va tizimi bilan yaqindan tanish bo‘lgani bois, mazkur turdagi jinoyatchilik tashkilotga jiddiy ziyon yetkazishi mumkin. Bundan tashqari, kiberjinoyatchi tashkilot tarmog‘idan foydalanish imkoniyatiga ega bo‘ladi. Shuning uchun, ichki kiberjinoyatchilik natijasida maxfiy axborotning sirqib chiqish imkoniyati yuqori bo‘ladi.

Tashqi kiberjinoyatlar: odatda tashqaridan yoki tashkilot ichkarisidan yollangan hujumchi tomonidan amalga oshiriladi. Mazkur kiberjinoyatchilik tashkilotning nafaqat moliyaviy yo‘qotishlariga, balki obro‘sining yo‘qolishiga ham sababchi bo‘ladi. Hujum tashqaridan amalga oshirilgani bois, hujumchi harakatni tashkilot AT infrastrukturasini skaner qilish va unga aloqador ma’lumotlarni to‘plashdan boshlaydi. Xususan, malakali buzg‘unchi dastlab tashkilotda foydalanilgan tarmoqlararo ekran vositasining log faylini tahlil qilishdan boshlaydi. Shu bois, tarmoq ma’muri mazkur imkoniyatni buzg‘unchiga taqdim etmasligi shart.

Kiberjinoyat amalga oshirilganida quyidagilar asosiy maqsad sifatida qaraladi:

- mablag‘, qimmatli qog‘ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko‘chmas mulk, yoqilg‘i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy o‘zlashtirish;
- soliq va boshqa yig‘imlarni to‘lashdan bosh tortish;
- jinoiy daromadlarni qonunlashtirish;
- qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuq chiptalarini qalbakilashtirish;
- shaxsiy yoki siyosiy maqsadlarda maxfiy ma’lumotlarni olish;
- ma’muriyatning yoki ishdagi hamkasblarning g‘arazli munosabatlari uchun qasos olish;
- shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish;
- mamlakatdagi vaziyatni, hududiy ma’muriy tuzilishni beqarorlashtirish;
- talonchilik, raqibni yo‘q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ish tartibini buzish;
- shaxsiy intelektual qobiliyatini yoki ustunligini namoyish qilish.

Kiberjinoyat turlarini qat’iy tasniflashning imkoni yo‘q. Quyida kriminologiya sohasiga nisbatan kiberjinoyatlarning turlari keltirilgan:

- iqtisodiy kompyuter jinoyatchiligi;
- inson va fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga qarshi qaratilgan kompyuter jinoyatchiligi;
- jamoat va davlat xavfsizligiga qarshi kompyuter jinoyatchiligi.

Iqtisodiy kompyuter jinoyatchiligi amalda ko‘p uchraydi. Ular jinoyatchilarga millionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik, asosan, bank hisob raqamlari va bank kartalari orqali amalga oshiriladi. Xalqaro amaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yoki o‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardan foydalanish, karta taqdim etmasdan bank hisob varag‘i ma’lumotlarini olish va noqonuniy foydalanish, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlariga va erkinliklariga qaratilgan jinoyatlar - “kompyuter qaroqchiligi”dir. Ushbu jinoyatlar dasturiy ta’minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi. Bu dasturiy ta’minot va ma’lumotlar bazasini yaratish bilan bog‘liq huquqiy munosabatlarga

(mualliflik huquqiga) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo‘qotishlarni olib keladi.

“Maykrosoft Armaniston” kompaniyasining direktori Grigor Barsegyanning ta’kidlashicha, “kompyuter qaroqchiligi”ning ishlab chiqaruvchilarga yetkazgan zarari yiliga 66 milliard dollarni tashkil etgan. Uning so‘zlariga ko‘ra Armanistonlik iste’molchilar, o‘zlarining moliyaviy resurslarini tejash maqsadida, viruslarni yuqtirish xavfi yuqori bo‘lgan dasturlardan ongli ravishda foydalanganlar.

Kompyuter jinoyatchiligining oxirgi turi - jamoat yoki davlat xavfsizligiga qarshi kompyuter jinoyatchiligi, ularga davlat yoki jamoat xavfsizligiga qaratilgan xavfli xatti - harakatlar taalluqli. Ular ko‘pincha ma’lumot uzatish qoidalarining, mamlakat mudofaa tizimining yoki uning tarkibiy qismlarining buzilishi bilan bog‘liq.

Kiberqonunlar. Qonun (huquq) — inson, jamiyat va davlat manfaatlari nuqtai nazaridan eng muhim hisoblanadigan ijtimoiy munosabatlarni mustahkamlash, rivojlantirish va tartibga solish vositasi. Qonunning nima maqsadga qaratilganini u yo‘naltirilgan munosabatga qarab aniqlash mumkin. Shu bois qonunlar turli sohaga oid maqsadlarga ega bo‘lishi mumkin. Umumiy nomda kiberjinoatchilikni tartibga solishni maqsad qilgan qonunlar kiberqonunlar deb ataladi.

Qonunni ishlab chiquvchilar va uni himoya qiluvchilar butun dunyo bo‘ylab kiberjinoyatchilikni aniq belgilaydigan va kiber dalillarni qabul qilishni to‘liq madadlovchi kiberqonunlar zarurligi haqida ogohlantirib keladilar. Mamlakatning biror xalqaro shartnomadagi ishtiroki bu shartnomani qonuniylashtiradigan ichki qonunlar ishlab chiqilgan va tasdiqlangan taqdirdagina kuchga kiradi. Masalan, Yevropada 2004 yilda Yevropa Kengashi butun dunyo mamlakatlariga taklif qilingan Kiberjinoyatchilik to‘g‘risidagi Shartnoma (Budapesht konvensiyasi deb ham ataladi) loyihasini qabul qildi. Mazkur Shartnomani ko‘pchilik davlatlar imzolagan bo‘lsada, ularning bir nechtasigina shartnomaga mos keladigan milliy qonunlarga ega.

2020 yil fevral oyiga kelib, Birlashgan millatlar tashkilotiga a’zo bo‘lgan 106 ta (yoki 55%) davlatlar Budapesht konvensiyasiga muvofiq milliy kiberjinoyatchilik to‘g‘risidagi qonunlarga ega bo‘ldilar. Bundan tashqari, hozirda rivojlanayotgan davlatlar kiberjinoyatchilarni tergov qilish va bu jarayon uchun kerakli ma’lumotlarni yig‘ish bo‘yicha ma’lum vakolatlarni qabul qildilar.

Xususan, Respublikamizda ham “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da amalga oshirishga oid davlat dasturi

to‘g‘risida”gi O‘zbekiston Respublikasi Prezidenti Farmoni loyihasi va 2020 yil Davlat dasturi loyihasida 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqish rejalashtirilgan.

Hujjatga asosan xavfsizlikni, millatlararo totuvlik va diniy bag‘rikenglikni ta’minlash, shuningdek, tashqi siyosat sohasida:

– 2020 yil 1 sentyabrga qadar kiberxavfsizlikning huquqiy asoslarini shakllantirish bo‘yicha choralar ko‘riladi, shu jumladan 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqiladi;

Loyihada:

– axborot kommunikatsiya texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo‘yicha zamonaviy mexanizmlarni joriy etish;

– kiberxavfsizlikni ta’minlash sohasida davlat organlari, korxona va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish;

– ushbu sohadagi normativ-huquqiy hujjatlarni unifikatsiyalash nazarda tutiladi.

Kiberqonunlar har bir davlatning milliy qonun me’yorlari asosida shakllantiriladi yoki ularning bir qismini tashkil qiladi. Quyida Respublikamizdagi qonun hujjatlarida kiberjinoyatni oldini olish va tartibga solishga aloqador bo‘lgan bandlar keltirilgan.

Milliy qonunlar. 2002 yil 12 dekabrda O‘zbekiston Respublikasining 439-II – sonli “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonuni qabul qilindi. Ushbu qonun 16 moddadan iborat bo‘lib, unda xususan, quyidagilar belgilangan:

1-modda. Ushbu Qonunning asosiy vazifalari

Ushbu Qonunning asosiy vazifalari axborot erkinligi prinsiplari va kafolatlariga rioya etilishini, har kimning axborotni erkin va moneliksiz izlash, olish, tekshirish, tarqatish, foydalanish va saqlash huquqlari ro‘yobga chiqarilishini, shuningdek axborotning muhofaza qilinishini hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlashdan iborat.

4-modda. Axborot erkinligi

O‘zbekiston Respublikasining Konstitutsiyasiga muvofiq har kim axborotni moneliksiz izlash, olish, tekshirish, tarqatish, undan foydalanish va uni saqlash huquqiga ega.

Axborot olish faqat qonunga muvofiq hamda inson huquq va erkinliklari, konstitutsiyaviy tuzum asoslari, jamiyatning axloqiy qadriyatlari, mamlakatning ma’naviy, madaniy va ilmiy salohiyatini muhofaza qilish, xavfsizligini ta’minlash maqsadida cheklanishi mumkin.

6-modda. Axborotning ochiqligi va oshkoraligi

Axborot ochiq va oshkora bo‘lishi kerak, maxfiy axborot bundan mustasno.

Maxfiy axborotga quyidagilar kirmaydi:

fuqarolarning huquq va erkinliklari, ularni ro‘yobga chiqarish tartibi to‘g‘risidagi, shuningdek davlat hokimiyati va boshqaruv organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining huquqiy maqomini belgilovchi qonun hujjatlari;

ekologik, meteorologik, demografik, sanitariya-epidemiologik, favqulodda vaziyatlar to‘g‘risidagi ma’lumotlar hamda aholining, aholi punktlarining, ishlab chiqarish obyektlari va kommunikatsiyalarning xavfsizligini ta’minlash uchun zarur bo‘lgan boshqa axborotlar;

axborot-kutubxona muassasalarining, arxivlarning, idoraviy arxivlarning va O‘zbekiston Respublikasi hududida faoliyat ko‘rsatayotgan yuridik shaxslarga tegishli axborot tizimlarining ochiq fondlaridagi mavjud ma’lumotlar.

Davlat hokimiyati va boshqaruv organlari, fuqarolarning o‘zini o‘zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlari jamiyat manfaatlariga taalluqli voqealar, faktlar, hodisalar va jarayonlar to‘g‘risida qonun hujjatlarida belgilangan tartibda ommaviy axborot vositalariga xabar berishi shart.

10-modda. Axborot berishni rad etish

Agar so‘ralayotgan axborot maxfiy bo‘lsa yoki uni oshkor etish natijasida shaxsning huquqlari va qonuniy manfaatlariga, jamiyat va davlat manfaatlariga zarar yetishi mumkin bo‘lsa, axborotni berish rad etilishi mumkin.

So‘ralayotgan axborotni berish rad etilganligi to‘g‘risidagi xabar so‘rov bilan murojaat etgan shaxsga so‘rov olingan sanadan e’tiboran besh kunlik muddat ichida yuboriladi.

Rad etish to‘g‘risidagi xabarda so‘ralayotgan axborotni berish mumkin emasligi sababi ko‘rsatilishi kerak.

Maxfiy axborot mulkdori, egasi axborotni so‘rayotgan shaxslarni bu axborotni olishning amaldagi cheklovlari to‘g‘risida xabardor etishi shart.

Axborot berilishi qonunga xilof ravishda rad etilgan shaxslar, shuningdek o‘z so‘roviga haqqoniy bo‘lmagan axborot olgan shaxslar o‘zlariga yetkazilgan moddiy zararning o‘rni qonunda belgilangan tartibda qoplanishi yoki ma’naviy ziyon kompensasiya qilinishi huquqiga ega.

11-modda. Axborotni muhofaza etish

Har qanday axborot, agar u bilan qonunga xilof ravishda muomalada bo‘lish axborot mulkdori, egasi, axborotdan foydalanuvchi va boshqa shaxsga zarar yetkazishi mumkin bo‘lsa, muhofaza etilmog‘i kerak.

Axborotni muhofaza etish:

shaxs, jamiyat va davlatning axborot sohasidagi xavfsizligiga tahdidlarning oldini olish;

axborotning maxfiyligini ta’minlash, tarqalishi, o‘g‘irlanishi, yo‘qotilishining oldini olish;

axborotning buzib talqin etilishi va soxtalashtirilishining oldini olish maqsadida amalga oshiriladi.

13-modda. Shaxsning axborot borasidagi xavfsizligi

Shaxsning axborot borasidagi xavfsizligi uning axborotdan erkin foydalanishi zarur sharoitlari va kafolatlarini yaratish, shaxsiy hayotiga taalluqli sirlarini saqlash, axborot vositasida qonunga xilof ravishda ruhiy ta’sir ko‘rsatilishidan himoya qilish yo‘li bilan ta’minlanadi.

Jismoniy shaxslarga taalluqli shaxsiy ma’lumotlar maxfiy axborot toifasiga kiradi.

Jismoniy shaxsning roziligisiz uning shaxsiy hayotiga taalluqli axborotni, xuddi shuningdek shaxsiy hayotiga taalluqli sirini, yozishmalar, telefondagi so‘zlashuvlar, pochta, telegraf va boshqa muloqot sirlarini buzuvchi axborotni to‘plashga, saqlashga, qayta ishlashga, tarqatishga va undan foydalanishga yo‘l qo‘yilmaydi, qonun hujjatlarida belgilangan hollar bundan mustasno.

Jismoniy shaxslar to‘g‘risidagi axborotdan ularga moddiy zarar va ma’naviy ziyon yetkazish, shuningdek ularning huquqlari, erkinliklari va qonuniy manfaatlari ro‘yobga chiqarilishiga to‘sqinlik qilish maqsadida foydalanish taqiqlanadi.

Fuqarolar to‘g‘risida axborot oluvchi, bunday axborotga egalik qiluvchi hamda undan foydalanuvchi yuridik va jismoniy shaxslar bu axborotdan foydalanish tartibini buzganlik uchun qonunda nazarda tutilgan tarzda javobgar bo‘ladilar.

Ommaviy axborot vositalari axborot manbaini yoki taxallusini qo‘ygan muallifni ularning roziligisiz oshkor etishga haqli emas. Axborot manbai yoki muallif nomi faqat sud qarori bilan oshkor etilishi mumkin.

14-modda. Jamiyatning axborot borasidagi xavfsizligi

Jamiyatning axborot borasidagi xavfsizligiga quyidagi yo‘llar bilan erishiladi:

demokratik fuqarolik jamiyati asoslari rivojlantirilishini, ommaviy axborot erkinligini ta’minlash;

qonunga xilof ravishda ijtimoiy ongga axborot vositasida ruhiy ta’sir ko‘rsatishga, uni chalg‘itishga yo‘l qo‘ymaslik;

jamiyatning ma’naviy, madaniy va tarixiy boyliklarini, mamlakatning ilmiy va ilmiy-texnikaviy salohiyatini asrash hamda rivojlantirish;

milliy o‘zlikni anglashni izdan chiqarishga, jamiyatni tarixiy va milliy an’analar hamda urf-odatlardan uzoqlashtirishga, ijtimoiy-siyosiy vaziyatni beqarorlashtirishga, millatlararo va konfessiyalararo totuvlikni buzishga qaratilgan axborot ekspansiyasiga qarshi harakat tizimini barpo etish.

15-modda. Davlatning axborot borasidagi xavfsizligi

Davlatning axborot borasidagi xavfsizligi quyidagi yo‘llar bilan ta’minlanadi:

axborot sohasidagi xavfsizlikka tahdidlarga qarshi harakatlar yuzasidan iqtisodiy, siyosiy, tashkiliy va boshqa tusdagi chora-tadbirlarni amalga oshirish;

davlat sirlarini saqlash va davlat axborot resurslarini ulardan ruxsatsiz tarzda foydalanilishidan muhofaza qilish;

O‘zbekiston Respublikasining jahon axborot makoniga va zamonaviy telekommunikatsiyalar tizimlariga integratsiyalashuvi;

O‘zbekiston Respublikasining konstitutsiyaviy tuzumini zo‘rlik bilan o‘zgartirishga, hududiy yaxlitligini, suverenitetini buzishga, hokimiyatni bosib olishga yoki qonuniy ravishda saylab qo‘yilgan yoxud tayinlangan hokimiyat vakillarini hokimiyatdan chetlatishga va davlat tuzumiga qarshi boshqacha tajovuz qilishga ochiqdan-ochiq da’vat etishni o‘z ichiga olgan axborot tarqatilishidan himoya qilish;

urushni va zo‘ravonlikni, shafqatsizlikni targ‘ib qilishni, ijtimoiy, milliy, irqiy va diniy adovat uyg‘otishga qaratilgan terrorizm va diniy ekstremizm g‘oyalarini yoyishni o‘z ichiga olgan axborot tarqatilishiga qarshi harakatlar qilish.

16-modda. Axborot erkinligi prinsiplari va kafolatlari to‘g‘risidagi qonun hujjatlarini buzganlik uchun javobgarlik

Axborot erkinligi prinsiplari va kafolatlari to‘g‘risidagi qonun hujjatlarini buzganlikda aybdor shaxslar belgilangan tartibda javobgar bo‘ladilar.

O‘zbekiston Respublikasida kiberjinoyatlarga qarshi javobgarliklar quyida keltirilgan.

O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeks:

155-modda. Axborotdan foydalanish qoidalarini buzish

- Axborot tizimidan foydalanish maqsadida unga ruxsatsiz kirib olishda ifodalangan axborot va axborot tizimlaridan foydalanish qoidalarini buzish —
    - fuqarolarga eng kam ish haqining uchdan bir qismidan bir baravarigacha, mansabdor shaxslarga esa — bir baravaridan uch baravarigacha miqdorda jarima solishga sabab bo‘ladi.
- Axborot tizimlarining ishini buzishga olib kelgan xuddi shunday huquqbuzarlik, xuddi shuningdek kirish cheklangan axborot tizimlarini axborot-hisoblash tarmoqlariga ulash chog‘ida tegishli himoya choralarini ko‘rmaganlik —
    - fuqarolarga eng kam ish haqining bir baravaridan uch baravarigacha, mansabdor shaxslarga esa — uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.
- Yuridik va jismoniy shaxslarning axborot tizimlarini xalqaro axborot tarmoqlariga qonunga xilof ravishda ulash, bu tarmoqlarga tegishli himoya choralarini ko‘rmasdan ulanish, xuddi shuningdek ulardan ma’lumotlarni qonunga xilof ravishda olish —
    - fuqarolarga eng kam ish haqining ikki baravaridan besh baravarigacha, mansabdor shaxslarga esa — besh baravaridan yetti baravarigacha miqdorda jarima solishga sabab bo‘ladi.
- O‘zganing elektron hisoblash mashinalari uchun yaratilgan dasturi yoki ma’lumotlar bazasini o‘z nomidan chiqarish yoxud qonunga xilof ravishda undan nusxa olish yoki bunday asarlarni tarqatish —
    - fuqarolarga eng kam ish haqining bir baravaridan uch baravarigacha, mansabdor shaxslarga esa — uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.

218-modda. Ommaviy axborot vositalari mahsulotlarini qonunga xilof ravishda tayyorlash va tarqatish

- Ommaviy axborot vositalarining mahsulotlarini belgilangan tartibda ro‘yxatdan o‘tkazmasdan yoki ularni chiqarishni yoxud nashr etishni to‘xtatish to‘g‘risida qaror qabul qilingandan keyin qonunga xilof ravishda tayyorlash va tarqatish —

  - bosma yoki boshqa mahsulotlarni musodara qilib, eng kam ish haqining uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.

O‘zbekiston Respublikasi jinoyat kodeksi:

143-modda. Xat-yozishmalar, telefonda so‘zlashuv, telegraf xabarlari yoki boshqa xabarlarning sir saqlanishi tartibini buzish

- Xat-yozishmalar, telefonda so‘zlashuv, telegraf xabarlari yoki boshqa xabarlarning sir saqlanishi tartibini qasddan buzish, shunday harakatlar uchun ma’muriy jazo qo‘llanilgandan keyin sodir etilgan bo‘lsa, eng kam oylik ish haqining yigirma besh baravarigacha miqdorda jarima yoki uch yilgacha muayyan huquqdan mahrum qilish yoki uch yuz oltmish soatgacha majburiy jamoat ishlari yoxud uch yilgacha axloq tuzatish ishlari bilan jazolanadi.

Kiberetika – kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi, umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi. Kiberetika masalalariga quyidagi misollarni keltirish mumkin:

- Internetda boshqa odamlar to‘g‘risidagi shaxsiy ma’lumotlarni (masalan, onlayn holatlar yoki GPS orqali joriy joylashuvni) uzatish joizmi?
- foydalanuvchilarni soxta ma’lumotlardan himoya qilish kerakmi?
- raqamli ma’lumotlarga kim egalik qiladi (musiqa, filmlar, kitoblar, web-sahifalar va boshqalar) va ularga nisbatan foydalanuvchilar qanday huquqlarga ega?;
- onlayn qimor va pornografiya tarmoqda qanday darajada bo‘lishi kerak?
- Internetdan foydalanish har bir kishi uchun mumkin bo‘lishi kerakmi?

Mulk. Axborotdan foydalanishdagi etikaga oid munozaralar uzoq vaqtdan beri mulkchilik tushunchasini tashvishga solmoqda va kiberetika sohasidagi ko‘plab to‘qnashuvlarga sabab bo‘lmoqda. Egalikka oid nizolar egalik huquqi buzilgan yoki noaniq bo‘lgan hollarda yuzaga keladi.

Intellektual mulk huquqlari. Internet tarmog‘ining doimiy ravishda o‘sib borishi va turli ma’lumotlarni zichlash texnologiyalarining (masalan, mp3 fayl formati) paydo bo‘lishi “peer-ro-peer” fayl almashinuviga katta yo‘l ochdi. Bu imkoniyat dastlab Napster kabi dasturlar yordamida amalga oshirilgan bo‘lsa, endilikda BitTorrent kabi ma’lumotlarni uzatish protokollarida foydalanilmoqda. Uzatilgan musiqalarning aksariyati mualliflik huquqi bilan himoyalangan bo‘lsada, mazkur fayl almashinuvi noqonuniy hisoblanadi.

Hozirgi kunda aksariyat elektron ko‘rinishdagi media fayllar (musiqa, audio va kinofilmlar) intelektual mulk huquqlariga rioya qilinmasdan ommaga tarqalmoqda. Masalan, aksariyat katta mablag‘ sarflangan kinofilmlarning “qaroqchilarcha (piratskiy)” versiyasining chiqishi bois o‘z sarf xarajatlarini qoplay olmaslik holatlari kuzatilmoqda.

Bu holatni dasturiy ta’minotlarda ham ko‘rish mumkin. Masalan, aksariyat dasturlar litsenziyaga ega hisoblansada, turli usullar yordamida ularning “darz ketgan (crack)” versiyalari amalda keng qo‘llaniladi. Masalan, litsenziyaga ega bo‘lmagan Windows 10 OT, antivirus dasturiy vositalari, ofis dasturiy vositalari va h.

Mualliflik huquqini himoyalashning texnik vositalari. Mualliflik huquqini ta’minlashda turli himoya usullaridan foydalaniladi. Ular CD/DVD disklardagi ma’lumotlarni ruxsatsiz ko‘chirishdan himoyalashdan tortib oddiy PDF fayllarni tahrirlash imkoniyatini cheklash kabi jarayonlarni o‘z ichiga olishi mumkin. Shu bilan birga, aksariyat insonlar litsenziyali CD diskni sotib olib, undan ko‘chirish imkoniyatiga ham ega bo‘lishim mumkin deb o‘ylaydilar.

Xavfsizlik. Internet tarmog‘idagi axborotdan xavfsiz foydalanish axloqiy munozaralar mavzusi bo‘lib kelmoqda. Bu birinchi navbatda jamoat faravonligini himoya qilish yoki shaxs huquqini himoya qilish masalasini o‘rtaga qo‘yadi. Internet tarmog‘idan foydalanuvchilar sonining ortishi, shaxsiy ma’lumotlarning ko‘payishi natijasida kiberjinoyatlar soni ortmoqda.

Ishonchlilik. Internetning mavjudligi va ba’zi bir shaxs yoki jamoalar tabiati tufayli ma’lumotlarning ishonchliligi bilan shug‘ullanish muammoga aylanmoqda. Boshqacha aytganda, Internetdagi ma’lumotlarning ishonchliligiga kim javob beradi? Bundan tashqari, Internetdagi ma’lumotlarni kim to‘ldirishi, undagi xatolar va kamchiliklar uchun kim javobgar bo‘lishi kerakligi to‘g‘risida ko‘plab tortishuvlar mavjud.

Foydalanuvchanlik, senzura va filtrlash. Foydalanuvchanlik, senzura va axborotni filtrlash mavzulari kiberetika bilan bog‘liq ko‘plab axloqiy masalalarni qamrab oladi. Ushbu masalalarning mavjudligi bizning maxfiylik va shaxsiylikni tushunishimizga va jamiyatdagi ishtirokimizga shubha tug‘diradi. Biror qonun qoidaga ko‘ra ma’lumotlardan foydalanishni cheklash yoki filtrlash asosida ushbu ma’lumotni tarqalishini oldini olish foydalanuvchanlikka ta’sir qilishi mumkin. Senzura ham past darajada (masalan, kompaniya o‘z xodimlari uchun) yoki yuqori darajada (hukumat tomonidan xavfsizlikni ta’minlash uchun amalga oshirilgan) bo‘lishi mumkin. Mamlakatga kiruvchi ma’lumotlarni boshqarishning eng yaxshi misollaridan biri - “Buyuk Xitoy Fayrvoli” loyihasi.

Axborot erkinligi. Axborot erkinligi, ya’ni, so‘z erkinligi, shu bilan birga ma’lumotni qidirish, olish va uzatish erkinligi kiberhujumda kimga va nimaga yordam beradi degan savol tug‘iladi. Axborot erkinligi huquqi, odatda, jamiyat yoki uning madaniyatiga ta’sir ko‘rsatadigan cheklovlarga bog‘liq. Cheklovlar turli ko‘rinishda bo‘lishi mumkin. Masalan, ayrim mamlakatlarda Internet ommaviy axborot vositalaridan foydalanishning bir shakli hisoblanib, undan barcha davlat rezidentlari foydalanadilar. Bundan tashqari, Internetdan foydalanish bo‘yicha cheklovlar ayrim davlatlarning turli shtatlarida farq qilishi mumkin.

Raqamli to‘siqlar. Axborot erkinligi bilan bog‘liq axloqiy masalalardan tashqari, *raqamli to‘siq* deb ataluvchi muammo turi mavjud bo‘lib, u kiberfazodan foydalanish imkoniyati cheklanganlar o‘rtasidagi ijtimoiy tafovutni anglatadi. Dunyo mamlakatlari yoki mintaqalari o‘rtasidagi bu tafovut global raqamli to‘siq deb ataladi.

Taqiqlangan kontentlar (pornografiya). Internet tarmog‘ida mavjud bo‘lgan taqiqlangan kontentlarni voyaga yetmaganlar tomonidan foydalanish doimo axloqiy munozaralarga sabab bo‘lgan. Ayrim davlatlarda bunday kontentlardan foydalanish qat’iy taqiqlansa, ayrim davlatlarda bunga ruxsat berilgan.

Qimor o‘yinlari. Bu muammo ham etik masaladagi munozaralardan biri, uni kimlardir zarar deb hisoblasa, yana kimlardir ularga qonun aralashuvini yoqtirmaydilar. O‘z navbatida tomonlar orasida “Qaysi turdagi o‘yinlarga ruxsat berish kerak? Ular qayerda o‘tkazilishi kerak?” degan savollar keng munozaralarga sabab bo‘lmoqda. Hozirda aksariyat davlatlarda bu turdagi o‘yinlarga qonuniy ruxsat berilgan bo‘lsa, qolganlarida qat’iy cheklovlar mavjud.

Kompyuterdan foydalanish etikasi. Kompyuterdan foydalanish etikasi instituti notijoriy tashkilot bo‘lib, vazifasi texnologiyani axloqiy nuqtai nazaridan targ‘ib qilish hisoblanadi. Ushbu tashkilot tomonidan quyidagi 10 ta etika qoidalari keltirib o‘tilgan:

- shaxsiy kompyuteringizdan boshqalarning zarariga foydalanmang;
- boshqa foydalanuvchilarning kompyuter ishlariga xalaqit bermang;
- boshqa foydalanuvchilarning kompyuter fayllariga qaramang;
- o‘g‘irlik maqsadida kompyuterdan foydalanmang;
- yomonlik maqsadida kompyuterdan foydalanmang;
- o‘z pulingizga sotib olmagan dasturdan foydalanmang va nusxa ko‘chirmang;
- birovning kompyuteridan ruxsatsiz foydalanmang;
- birovlarni intellektual mehnati samarasiga zarar yetkazmang;
- siz yaratgan dasturning ijtimoiy oqibati haqida o‘ylang;
- o‘z kompyuteringizdan boshqalarga nisbatan ongli va hurmat bilan foydalaning.

Axborotdan oqilona foydalinish kodeksi. Axborotdan oqilona foydalanish kodeksi buxgalteriya tizimiga qo‘yiladigan talablarni ta’kidlaydigan beshta prinsipga asoslanadi. Ushbu talablar AQSh sog‘liqni saqlash va insonlarga xizmat ko‘rsatish vazirligi tomonidan 1973 yilda kiritilgan:

- shaxsiy ma’lumotlarni to‘playdigan tizimlar bo‘lmasligi kerak;
- har bir kishi tizimda u to‘g‘risida qanday ma‘lumotlar saqlanishini va undan qanday foydalanilishini boshqarishi kerak;
- har bir kishi o‘zi to‘g‘risida to‘plangan ma’lumotlardan belgilangan maqsadda foydalanilishini nazoratlash imkoniyatiga ega bo‘lishi kerak;
- har kim o‘zi haqidagi ma’lumotlarni to‘g‘rilashi kerak;
- shaxsiy ma’lumotlar sirasiga kiruvchi ma’lumotlar to‘plamini yaratish, saqlash, ishlatish yoki tarqatish bilan shug‘ullanadigan har bir tashkilot ushbu ma’lumotlardan faqat belgilangan maqsadlar uchun foydalanilishni ta’minlash va boshqa maqsadlarda foydalanilishga qarshi choralar ko‘rishi kerak.

1.4. Inson faoliyati xavfsizligi

Ijtimoiy (sotsial) injineriya - turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish. Maxfiy ma’lumotlar - foydalanuvchi ismi/ parollari, shaxsiy ma’lumotlari, ayblov dalillari, bank karta raqamlari va moliyaviy yoki obro‘sini yo‘qotadigan har qanday ma’lumot.

Mazkur atama xakerlik sohasidan kirib kelgan, *xaker* - kompyuter tizimidagi zaifliklarni qidiradigan odam, boshqacha aytganda “buzg‘unchi”. Hozirgi vaqtda xakerlar har qanday tizimdagi asosiy zaiflik - mashina emas, balki shaxs ekanligini yaxshi tushunishadi. Inson, xuddi kompyuter singari, muayyan qonunlarga muvofiq ishlaydi. Psixologiya, hiyla-nayranglar va ta’sir mexanizmlari doirasida insoniyat tomonidan to‘plangan tajribadan foydalangan holda, xakerlar “odamlarga hujum qilishni” boshlaydilar. Gohida ularni “aql xakerlari” deb ham atashadi.

Masalan, xaker sizdan pul olmoqchi deb faraz qilaylik. Aytaylik, u sizning telefon raqamingiz va ijtimoiy tarmoqdagi akkauntingiz haqida ma’lumotga ega. Bundan tashqari, u izlanish natijasida sizning akangiz borligini ham aniqladi va akangiz haqida ham yetarlicha ma’lumot to‘pladi. U shuningdek, akangizning telefon raqamini ham biladi. Shundan so‘ng, ushbu ma’lumotlar asosida o‘z rejasini tuza boshladi.

Reja: Xaker sizga kechki vaqtda telefon qilib, sizga (sizni ismingiz o‘rniga faqat akangiz ataydigan biror “laqab” ham bo‘lishi mumkin) men akangman deb tanishtiradi va o‘zini ko‘chada bezorilarga duch kelganini, ular barcha narsalarini (telefon, pul, plastik kartochka va h.) olib qo‘yganini aytadi. Bundan tashqari, u o‘ziga bir qiz yordam berganini, biroq, uning yonida puli yo‘qligini aytadi. Shu bilan birga, ushbu qizni yonida plastik kartasi borligini va sizdan ushbu plastik kartaga kasalxonaga yetib borish uchun zarur bo‘lgan 20 000 so‘m pulni ko‘chirib berishni talab qiladi. Mazkur holatlarning 80% da xakerlar muvaffaqqiyatga erishganlar va bu ishlarni amalga oshirish malakali xaker uchun qiyinchilik tug‘dirmaydi.

Mazkur holda akangizni ovozini ajratish imkoniyati haqida gap borishi mumkin. Biroq, inson turli hayojon va shovqin bo‘lgan muhitda bo‘lishi mumkin. Bundan tashqari, agar siz uxlab yotgan vaqtingizda telefon bo‘lsa, ovozni aniqlashingiz yanada qiyinlashadi.

Ushbu holatda xaker tomonidan foydalanilgan fikrlarni ko‘rib chiqaylik:

1. Shaxsini yaxshi yashirgan va real misollarga asoslangan (masalan, sizning rasmlaringiz, faqat sizning yaqinlaringiz biladigan joylar va h.) va yaxshi afsona o‘ylab topdi.

2. Bularning barchasi yetarlicha tez va ishonchli tarzda aytilgan.

3. Ta’sirning juda ishonarli mexanizmidan foydalanilgan – achinishga majbur qilingan (hissiyotlarga murojaat qilish).

Sotsial injineriya bilan bog‘liq tahdidlarni quyidagicha tasniflash mumkin:

Telefon bilan bog‘liq tahdidlar. Telefon hanuzgacha tashkilotlar ichida va ular o‘rtasidagi aloqaning eng keng tarqalgan usullaridan biri hisoblanadi. Shuning uchun, u sotsial injineriya uchun samarali vosita bo‘lib qolmoqda. Telefonda gaplashayotganda, suhbatdoshining shaxsini tasdiqlashning imkoni yo‘q. Bu hujumchilarga xodimning, xo‘jayinning maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonishi mumkin bo‘lgan har qanday shaxsning o‘rnida bo‘lish imkonini beradi. Bunda, zo‘ravonlik qurbonining “yordam berishdan” boshqa imkoni qolmaydi. Hattoki, uyushtiriladigan suhbat ahamiyatsiz bo‘lib ko‘ringan taqdirda ham.

Uyali telefondan foydalanuvchilarni pul o‘g‘irlashga qaratilgan firibgarlikning turli usullari mavjud. Bunga qo‘ng‘iroqlar yoki lotereyalardagi yutuqlar, SMS-xabarlar, xatoliklar orqali pulni qaytarish to‘g‘risidagi so‘rovlar yoki jabrlanuvchining yaqin qarindoshlari muammoga duch kelganligi hamda ma’lum miqdordagi pulni zudlik bilan o‘tkazish kerakligi haqidagi xabarlarni keltirish mumkin.

Mazkur hollarda quyidagi xavfsizlik choralarini amalga oshirish talab etiladi:

- telefon qiluvchining shaxsini aniqlash;
- raqamni aniqlash xizmatidan foydalanish;
- SMS – xabardagi noma’lum havolalarga e’tibor bermaslik.

Elektron pochta bilan bog‘liq tahdidlar. Ko‘pgina xodimlar har kuni korporativ va shaxsiy pochta tizimlaridan o‘nlab, hatto yuzlab elektron pochta xabarlarini qabul qilishadi. Albatta, bunday yozishmalar oqimining har bir harfiga yetarlicha e’tibor berishning imkoni yo‘q. Bu esa hujumlarni amalga oshirishni sezilarli darajada osonlashtiradi. Elektron pochta tizimlarining ko‘plab foydalanuvchilari bunday holni bir papkadan ikkinchisiga qog‘ozlarni o‘tkazishning elektron analogi sifatida qabul qilishadi va xabarlarni qabul qilishda xotirjam bo‘lishadi. Tajovuzkor pochta orqali oddiy so‘rov yuborganida, uning qurboni ko‘pincha uning xatti-harakatlari haqida o‘ylamasdan ular so‘ragan ishni

bajaradi. Elektron pochtalarda xodimlarni korporativ atrof-muhit muhofazasini buzishga undaydigan giperhavolalar bo‘lishi mumkin. Bunday havolalar har doim ham da’vo qilingan sahifalarga murojaat qilmaydi.

Xavfsizlik choralarining aksariyati ruxsatsiz foydalanuvchilarning korporativ resurslardan foydalanishini oldini olish uchun ishlab chiqilgan. Buzg‘unchi tomonidan yuborilgan giperhavolaga murojaat orqali foydalanuvchining zararli dasturni korporativ tarmoqqa yuklashi ko‘plab himoya turlarini chetlab o‘tishga imkon beradi. Giperhavola, shuningdek, ma’lumot yoki yordamni talab qiladigan qalqib chiquvchi ilovalar bilan turli xostlarga murojaatni talab qilishi mumkin. Firibgarlikni va zararli hujumlarni oldini olishning eng samarali usuli - kutilmagan foydalanuvchining elektron pochtasi xabarlariga shubha bilan qarash. Ushbu yondashuvni butun tashkilotda tarqatish uchun xavfsizlik siyosatida belgilangan elektron pochtadan foydalanishning quyidagi elementlari kiritilishi kerak:

- hujjatlarga qo‘shimchalar;
- hujjatdagi giperhavolalar;
- shaxsiy yoki korporativ ma’lumotlarni kompaniya ichida so‘rash;
- shaxsiy yoki korporativ ma’lumotlarga kompaniya tashqarisidan keladigan so‘rovlar.

Tezkor xabarlardan foydalanishga asoslangan tahdidlar. Tezkor xabar almashish - ma’lumotlarni uzatishning nisbatan yangi usuli. Ammo, u korporativ foydalanuvchilar orasida allaqachon mashhurlikka erishgan. Foydalanishning tezligi va qulayligi tufayli ushbu aloqa usuli turli xil hujumlar uchun keng imkoniyatlarni ochib beradi. Foydalanuvchilar unga telefon kabi qarashadi va uni bo‘lishi mumkin bo‘lgan dasturiy tahdidlar sifatida baholashmaydi. Tezkor xabarlar xizmatidan foydalanishga asoslangan hujumlarning ikkita asosiy turi - zararli dasturga havola va dasturning o‘zi haqida xabarning ko‘rsatilishi hisoblanadi. Tezkor xabarlar xizmatlarining xususiyatlaridan biri - aloqaning norasmiyligi, unda har qanday nomlarni moslashtirish qobiliyati bilan bir qatorda, bu omil tajovuzkorni o‘zini boshqa odam bo‘lib ko‘rsatishiga imkon beradi. Bu esa muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada oshiradi. Agar kompaniya tezkor xabarlar sababli keladigan xarajatlarni kamaytirish maqsadida boshqa afzalliklardan foydalanmoqchi bo‘lsa, korporativ xavfsizlik siyosatida tegishli tahdidlardan himoya qilish mexanizmlarini ta’minlashi kerak. Korporativ muhitda tezkor xabar

almashish ustidan ishonchli boshqaruvga ega bo‘lish uchun quyidagi talablar bajarilishi shart:

- tezkor xabarlar uchun bitta platformani tanlash;
- tezkor xabar yuborish xizmatini o‘rnatishda xavfsizlik sozlamalarini aniqlash;
- yangi aloqalarni o‘rnatish prinsiplarini aniqlash;
- parol tanlash standartlarini o‘rnatish;
- tezkor xabarlardan foydalanish bo‘yicha tavsiyalar berish.

Sotsial injineriya mutaxassislari tashkilotlar uchun quyidagi asosiy himoya usullarini qo‘llashni tavsiya etishadi:

- muhim ma’lumotlar ko‘rinishida bo‘lgan, zararsiz ko‘rinadigan ma’lumot turlarini hisobga oladigan ishonchli ma’lumotlarni tasniflash siyosatini ishlab chiqish;
- ma’lumotlarni shifrlash yoki foydalanishni boshqarish yordamida mijoz ma’lumotlari xavfsizligini ta’minlash;
- xodimlarni sotsial injineriya ko‘nikmalariga o‘rgatish, ularni o‘zlari tanimaydigan odamlar bilan muloqotiga shubha bilan qarashni o‘rgatish;
- xodimlar orasida parollarni almashishni yoki umumiy foydalanishni taqiqlash;
- shaxsan tanish bo‘lmagan yoki biron-bir tarzda tasdiqlanmagan shaxsga korxonaga tegishli ma’lumotlarni berishni taqiqlash;
- maxfiy ma’lumotlardan foydalanishni so‘raganlar uchun maxsus tasdiqlash muolajalaridan foydalanish.

Sotsial injineriya hujumlarini oldini olishda ko‘p hollarda kompaniyalar tomonidan murakkab, ko‘p darajali xavfsizlik tizimlari qo‘llaniladi. Bunday tizimlarning ba’zi xususiyatlari va majburiyatlari quyida keltirilgan:

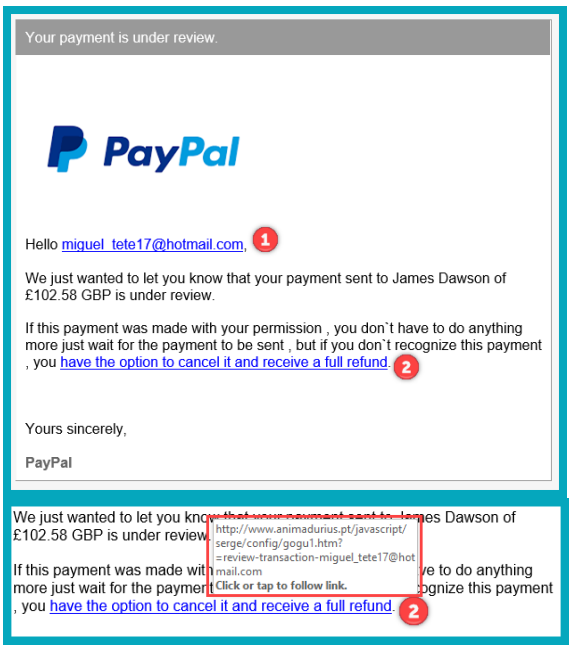
- *Fizik xavfsizlik.* Kompaniya binolari va korporativ resurslardan foydalanishni cheklaydigan to‘siqlar. Unutmaslik kerakki, kompaniyaning resurslari, masalan, kompaniya hududidan tashqarida joylashgan axlat konteynerlari fizik himoyalanmagan.
- *Ma’lumotlar*. Biznes ma’lumotlari: qayd yozuvlari, pochta va boshqalar bo‘lib, tahdidlarni tahlillash va ma’lumotlarni himoya qilish choralarini rejalashtirishda qog‘oz, elektron ma’lumot eltuvchilari bilan ishlash prinsiplarini aniqlash kerak.
- *Ilovalar* - foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofini himoya qilish uchun elektron pochta dasturlaridan,

tezkor xabarlar xizmati va boshqa dasturlardan tajovuzkorlar qanday foydalanishlari mumkinligini ko‘rib chiqish kerak.

- *Kompyuterlar*. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini ko‘rsatadigan qat’iy prinsiplarni belgilash, foydalanuvchilar kompyuterlariga to‘g‘ridan-to‘g‘ri hujumlardan himoya qilish.
- *Ichki tarmoq*. Korxona tizimlariga ta’sir qiladigan tarmoq, u mahalliy, global yoki simsiz bo‘lishi mumkin. So‘nggi yillarda masofadan ishlaydigan usullarning ommaviylashi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o‘zboshimchalik bilan kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari lozim.
- *Tarmoq perimetri.* Kompaniyaning ichki tarmoqlari va tashqi, masalan, Internet yoki hamkor tashkilotlar tarmoqlari o‘rtasidagi chegara.

Sotsial injineriyaga tegishli ko‘plab hujumlar mavjud, quyida ularning ayrimlari keltirilgan:

Fishing. Fishing (ing. Phishing – baliq ovlash) Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan (login/parol) foydalanish imkoniyatiga ega bo‘lish. Bu hozirda keng tarqalgan sotsial injineriya sxemalaridan biri hisoblanadi. Katta hajmdagi shaxsiy ma’lumotlarni keng tarqalishi, fishing “shamolisiz” amalga oshmaydi. Fishingning eng keng tarqalgan namunasi sifatida jabrlanuvchining elektron pochtasiga yuborilgan rasmiy ma’lumot ko‘rinishidagi bank yoki to‘lov tizimining soxta xabarini ko‘rsatish mumkin. Bunday elektron pochta xabarlari odatda rasmiy web-saytga o‘xshash va shaxsiy ma’lumotlarni talab qiladigan shakldagi qalbaki web sahifaga havolani o‘z ichiga oladi (1.5-rasm). Rasmda keltirilgan birinchi holatda mijozning yoki foydalanuvchining ismi va familiyasini yozish o‘rniga pochta manzili yozilgan bo‘lsa, ikkinchi holatda ko‘rsatilgan havola ustiga sichqoncha olib borilganida, haqiqiy manzilni (www.PayPal.com) emas, balki, boshqa manzilni ko‘rish mumkin.



1.5-rasm. Fishing hujumiga misol

Quyida keng tarqalgan fishing sxemalariga misollar keltirilgan.

Mavjud bo‘lmagan havola. Fishing hujumining mazkur turida biror web saytga o‘xshash web saytga murojaat amalga oshirilishi tavsiya etiladi. Masalan, www.PayPai.com manzilini www.PayPal.com manzili sifatida yuborish mumkin. Bu holda kamdan-kam holda foydalanuvchilar “l” harfini o‘riniga “i” harfi borligiga e’tibor berishadi. Havolaga murojaat qilinganida esa www.PayPal.com web saytga o‘xshash, biroq soxta web saytga tashrif buyuriladi va talab kiritilgan to‘lov kartasi ma’lumotlari kiritiladi. Natijada, kiritilgan ma’lumotlar xaker qo‘liga tushadi.

Bunga yaqqol misol sifatida, 2003 yilda eBay foydalanuvchilariga tarqalgan fishing xabarni keltirish mumkin. Mazkur xabarda foydalanuvchilarning akkauntlari blokirovkalangani va kredit karta ma’lumotlari blokirovkadan chiqarilishi kerakligi keltirilgan va unda rasmiy web-saytga o‘xshash soxta web saytga olib boruvchi havola mavjud bo‘lgan. Ushbu fishing hujumining keltirgan zarari bir necha yuz ming dollarga teng bo‘lgan.

Taniqli korporativ brendidan foydalanishga asoslangan firibgarlik. Firibgarlikning mazkur ko‘rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchiga xabar yuboriladi. Xabarda kompaniya tomonidan o‘tkazilgan biror tanlovda g‘alaba qozonilganligi haqidagi tabriklar bo‘lishi mumkin. Unda shuningdek, zudlik bilan qayd yozuvi ma’lumotlari va parolni o‘zgartirish kerakligi so‘raladi. Shunga o‘xshash

sxemalar texnik ko‘maklashish xizmati nomidan ham amalga oshirilishi mumkin.

Soxta lotareyalar. Mazkur fishing sxemasiga ko‘ra foydalanuvchi har qanday taniqli kompaniya tomonidan o‘tkazilgan lotereyada g‘olib bo‘lgani to‘g‘risidagi xabarni olishi mumkin. Tashqi tomondan, bu elektron xabar kompaniyaning yuqori lavozimli xodimlaridan biri nomidan yuborilganga o‘xshaydi.

Soxta antivirus va xavfsizlik dasturlari. Mazkur dasturlar firibgar dasturiy ta‘minoti yoki “chaqqon dastur” deb nomlanib, ular antivirus dasturlariga o‘xshasada, vazifasi boshqacha. Bu dasturiy ta’minot turli tahdidlar to‘g‘risidagi yolg‘on xabarnomalar asosida foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ulardan foydalanganida elektron pochtada, onlayn e’lonlarda, ijtimoiy tarmoqlarda, qidiruv tizimlari natijalarida va hatto foydalanuvchi kompyuterida turli qalqib chiquvchi oynalarga duch kelishi mumkin. Quyida keltirilgan misolda, aslida Microsoft Security Essentials bo‘lishi kerak bo‘lgan, biroq o‘ziga Security Essentials 2010 nomi berilgan soxta antivirus dasturining ko‘rinishi keltirilgan (1.6-rasm).

1.6-rasm. “Security Essentials 2010” antivirus dasturi

IVR (Interactive Voice Response) yoki telefon orqali fishing. Fishing sxemasining mazkur usuli oldindan yozib olingan xabarlar tizimidan foydalanishga asoslangan, ular bank va boshqa IVR tizimlarining “rasmiy qo‘ng‘iroqlari”ni qayta tiklash uchun ishlatiladi. Bu hujumda jabrlanuvchi bank bilan bog‘lanib, qandaydir ma’lumotlarni tasdiqlash yoki yangilash kerakligi haqidagi so‘ovni qabul qiladi. Tizim PIN kodni

yoki parolni kiritish orqali foydalanuvchi tasdig‘ini talab qiladi. Natijada, muhim ma’lumotlarni qo‘lgan kiritgan buzg‘unchi foydalanuvchi ma’lumotlaridan foydalanish imkoniyatiga ega bo‘ladi. Masalan, parolni almashtirish uchun “1” ni bosing va operator javobini olish uchun “2” ni bosing va h.

Pretekstinq. Mazkur fishing sxemasida xaker o‘zini boshqa shaxs sifatida ko‘rsatadi va oldindan tayyorlangan senariy (skript) bo‘yicha maxfiy axborotni olishni maqsad qiladi. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko‘riladi: tug‘ilgan kun, INN, pasport raqami yoki hisob raqamining oxirgi belgilari kabi ma’lumotlar topiladi. Ushbu fishing sxemasi odatda telefon yoki elektron pochta orqali amalga oshiriladi.

Kvid pro kvo (lotinchadan: Quid pro quo). Ushbu ibora ingliz tilida “*xizmat uchun xizmat*” degan ma’noni anglatib, sotsial injineriyaning mazkur turida xaker korporativ tarmoq yoki elektron pochta orqali kompaniyaga murojaatni amalga oshiradi. Ko‘pincha xaker o‘zini texnik xizmat ko‘rsatuvchi sifatida tanitib, texnik xodimning ish joyidagi muammolarni bartaraf etishda “yordam berishini” aytadi. Texnik muammoni “bartaraf” etish vaqtida nishondagi shaxsni buyruqlarni bajarishga yoki jabrlanuvchining kompyuteriga turli xil dasturlarni o‘rnatishga undash amalga oshiriladi. Masalan, 2003 yilda Axborot xavfsizligi dasturi doirasida o‘tkazilgan tadqiqot ofis xodimlarining 90% har qanday xizmat yoki to‘lov uchun maxfiy ma’lumotlarni, masalan, o‘zlarining parollarini, berishga tayyor bo‘lishini ko‘rsatdi.

Yo‘l-yo‘lakay olma. Sotsial injineriyaning mazkur usulida xaker maxsus zararli dastur yozilgan ma’lumot eltuvchilardan foydalanadi va zararli dasturlar yozilgan eltuvchilarni qurbonning ish joyi yaqinida, jamoat joylarida va boshqa joylarda qoldiradi. Bunda, ma’lumot eltuvchilari tashkilotga tegishli shaklda rasmiylashtiriladi. Masalan, xaker biror korporatsiya logotipi va rasmiy web-sayt manzili tushirilgan kompakt diskni qoldirib ketadi. Ushbu disk “Rahbarlar uchun ish haqlari” nomi bilan nomlanishi mumkin. Ushbu eltuvchini qo‘lga kiritgan qurbon uni o‘z kompyuteriga qo‘yib ko‘radi va shu orqali kompyuterini zararlaydi.

Ochiq ma’lumot to‘plash. Sotsial injineriya texnikasi nafaqat psixologik bilimlarni, balki, inson haqida kerakli ma’lumotlarni to‘plash qobilyatini ham talab etadi. Bunday ma’lumotlarni olishning nisbatan yangi usuli ochiq manbalardan, ijtimoiy tarmoqlardan to‘plash. Masalan, «Одноклассники», «ВКонтакте», «Facebook», «Instagram» kabi

saytlarda odamlar yashirishga harakat qilmaydigan juda ko‘p ma’lumotlar mavjud. Odatda, foydalanuvchilar xavfsizlik muammolariga yetarlicha e’tibor bermasdan, xaker tomonidan foydalanilishi mumkin bo‘lgan ma’lumotlar va xabarlarni qarovsiz qoldiradilar.

Bunga yaqqol misol sifatida Yevgeniy Kasperskiyning o‘g‘lini o‘g‘irlanganini keltirish mumkin. Mazkur holatda jinoyatchilar o‘smirning kun tartibini va marshrutini ijtimoiy tarmoq sahifalaridagi yozuvlardan bilgani aniqlangan.

Ijtimoiy tarmoqdagi o‘z sahifasidagi ma’lumotlardan foydalanishni cheklab qo‘ygan taqdirda ham, foydalanuvchining firibgarlik qurboni bo‘lmasligiga to‘liq kafolat yo‘q. Masalan, Braziliyaning kompyuter xavfsizligi bo‘yicha tadiqiqotchisi 24 soat ichida sotsial injineriya usullaridan foydalangan holda har qanday Facebook foydalanuvchisi bilan do‘stlashish mumkinligini ko‘rsatdi. Tajriba davomida Nelson Novayes Neto dastlab jabrlanuvchiga tanish bo‘lgan odam – uning xo‘jayini uchun soxta qayd yozuvini yaratadi. Avval Neto jabrlanuvchining xo‘jayinining do‘stlariga va undan keyin to‘g‘ridan-to‘g‘ri jabrlanuvchining do‘stiga do‘stlik so‘rovini yuboradi. 7,5 soatdan so‘ng esa tadqiqotchi jarblanuvchi bilan do‘stlashadi. Natijada tadqiqotchi foydalanuvchining shaxsiy ma’lumotlarini olish ikoniyatiga ega bo‘ladi.

Yelka orqali qarash. Ushbu hujumga ko‘ra buzg‘unchi jabrlanuvchiga tegishli ma’lumotlarini uning yelkasi orqali qarab qo‘lga kiritadi. Ushbu turdagi hujum jamoat joylarida, masalan, kafe, avtobus, savdo markazlari, aeroport va temir yo‘l stansiyalarida keng tarqalgan. Mazkur hujumga doir olib borilgan so‘rovnomalar quyidagilarni ko‘rsatgan:

- 85% ishtirokchilar o‘zlari bilishlari kerak bo‘lmagan maxfiy ma’lumotlarni ko‘rganliklarini tan olishgan;
- 82% ishtirokchilar ularning ekranidagi ma’lumotlarini ruxsatsiz shaxslar ko‘rishi mumkinligini tan olishgan;
- 82% ishtirokchilar tashkilotdagi xodimlar o‘z ekranini ruxsatsiz odamlardan himoya qilishiga ishonishmagan.

Teskari sotsial injineriya. Jabrlanuvchining o‘zi tajovuzkorga ma’lumotlarini taqdim qilishi teskari sotsial injineriyaga tegishli holat hisoblanadi. Bu bir qarashda ma’noga ega bo‘lmagan qarash hisoblansada, aksariyat hollarda jarblanuvchining o‘zi muammolarini hal qilish uchun tajovuzkorni yordamga jalb qiladi. Masalan, jabrlanuvchi bilan birga ishlovchi tajovuzkor jabrlanuvchi kompyuteridagi biror faylni

nomini o‘zgartiradi yoki boshqa katalogga ko‘chirib o‘tkazadi. Faylni yo‘‘q bo‘lganini bilgan qurbon esa ushbu muammoni tezda bartaraf etishni istab qoladi. Bu vaziyatda tajovuzkor o‘zini ushbu muammoni bartaraf etuvchi sifatida ko‘rsatadi va qurbonning muammosini bartaraf etish bilan birga unga tegishli login/ parolni ham qo‘lga kiritadi. Bundan tashqari, ushbu vazifasi bilan tajovuzkor tashkilot ichida obro‘ga ega bo‘ladi va o‘z qurbonlari sonini ortishiga erishadi. Bu holatni aniqlash esa ancha murakkab ish hisoblanadi.

Mashhur sotsial injinerlar. Kevin Mitnik tarixdagi eng mashhur sotsial injinerlardan biri, u dunyodagi mashhur kompyuter xakeri, xavfsizlik bo‘yicha mutaxassis va sotsial injineriyaga asoslangan kompyuter xavfsizligiga bag‘ishlangan ko‘plab kitoblarning ham muallifidir. Uning fikriga ko‘ra xavfsizlik tizimini buzishdan ko‘ra, aldash yo‘li orqali parolni olish osonroq.

Aka-uka Badirlar. Ko‘r bo‘lishlariga qaramasdan aka-uka Mushid va Shadi Badirlar 1990 yillarda Isroilda sotsial injineriya va ovozni soxtalashtirish usullaridan foydalangan holda bir nechta yirik firibgarlik sxemalarini amalga oshirishgan. Televideniyaga bergan intervyusida: “faqat telefon, elektr va noutbuklardan foydalanmaydiganlar uchun tarmoq xavfsizdir” deb aytishgan.

Sotsial injineriyadan himoyalanish choralari. Hujumlarni amalga oshirishda sotsial injineriya texnikasidan foydalangan tajovuzkorlar tez-tez muloyimlik, dangasalik, xushmuomilalik bilan foydalanuvchi va tashkilot xodimlarining qiziqishlaridan foydalanadilar. Hujumlarni oldini olish esa, xodimlarning aldanayotganliklarini bilmasliklari sababli, murakkab hisoblanadi.

Sotsial injineriya hujumlarini quyidagicha aniqlash mumkin:

- o‘zini do‘stingiz yoki yordam so‘rab murojaat qilgan yangi xodim sifatida tanishtirish;
- o‘zini yetkazib beruvchi, hamkor kompaniyaning xodimi yoki qonun vakili sifatida tanishtirish;
- o‘zini biror rahbar sifatida tanishtirish;
- biror zaiflikni bartaraf etuvchi yoki jabrlanuvchiga biror nimani yangilash imkoniyatini taqdim qiluvchi sotuvchi yoki ishlab chiqaruvchi sifatida tanishtirish;
- muammo yuzaga kelganida yordam beruvchi sifatida tanishtirish;
- ishonchni hosil qilish uchun ichki xotirjamlik va terminologiyadan foydalanish;

- “maktub”ga turli zararli dasturlarni qo‘shib yuborish;
- soxta ochilgan oynada login/ parolni qayta kiritishni so‘rash;
- foydalanuvchi nomi va paroli bilan saytga ro‘yxatdan o‘tish uchun biror sovg‘a taklif etish;
- jabrlanuvchi kompyuteriga yoki dasturiga kiritilgan kalitlarni yozib olish (keylogger dasturlari);
- turli xil zararli dasturiy vositaga ega ma’lumot eltuvchilarini foydalanuvchi stoliga tashlash;
- turli qo‘ng‘iroqlardagi ovozli xabarlar va h.

Hayotda ko‘plab jabhalarda sotsial injineriyaga tegishli muammolarni ko‘rish mumkin. Xususan, ommaviy madaniyatda (masalan, kinofilmlarda) sotsial injinerlikdan foydalanish holatlari tez-tez uchrab turadi. Masalan, quyidagi keltirilgan kinofilmlarda sotsial injineriyaga oid epizodlar mavjud:

- «Поймай меня, если сможешь»;
- «Поймай толстуху, если сможешь»;
- «Один дома»;
- «Хакеры»;
- «Афера Томаса Крауна»;
- «Бриллианты навсегда»;
- «Кто я».

Nazorat savollari

1. Axborot xavfsizligining hayotiy timsollari va ularning vazifalari.
2. Kiberxavfsizlik tushunchasiga izoh bering.
3. Kiberxavfsizlik fan sifatida qanday tuzilishga ega?
4. Kiberxavfsizlikning asosiy tushunchalari.
5. Axborotning konfidensialligini ta’minlash deganda nimani tushunasiz?
6. Axborotni yaxlitligini ta’minlash deganda nimani tushunasiz?
7. Axborot uchun foydalanuvchanlikning muhimligi.
8. Risk va uning kiberxavfsizlikdagi o‘rni.
9. Hujumchi kabi fikrlash nima uchun zarur?
10. Tizimli fikrlash nima va u nima uchun zarur?
11. Axborot xavfsizligi va axborotni himoyalash tushunchalarining bir-biridan farqi nimada?
12. Aktiv nima?

13. Tahdid va zaiflik tushunchalariga izoh bering.

14. Axborot xavfsizligi va kiberxavfsizlik tushunchalarining bir-biridan farqi nimada?

15. Kiberxavfsizlikning bilim sohalari va ularning asosiy xususiyatlari nimalardan iborat?

16. Kiberxavfsizlikda inson omilini misollar yordamida tushuntiring.

17. Kiberjinoyatchilik tushunchasiga izoh bering.

18. Kiberjinoyatni amalga oshirishdan ko‘zlangan maqsadlar.

19. Kiberjinoyatchilikning asosiy turlari.

20. Kiberetika tushunchasiga izoh bering va ularga misollar keltiring.

21. Kompterdan foydalanish davomida qanday etika qoidalarga e’tibor berish talab qilinadi?

22. Kiberjinoyatchilikni oldini olish usullari va kiberqonunlar haqida ma’lumot bering.

23. “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonunda axborotdan foydalanish tartiblari haqida nimalar deyilgan?

24. O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksida kiberjinoyatchilikka oid qanday bandlar mavjud?

25. O‘zbekiston Respublikasi jinoyat kodeksida kiberjinoyatchilikka oid qanday bandlar mavjud?

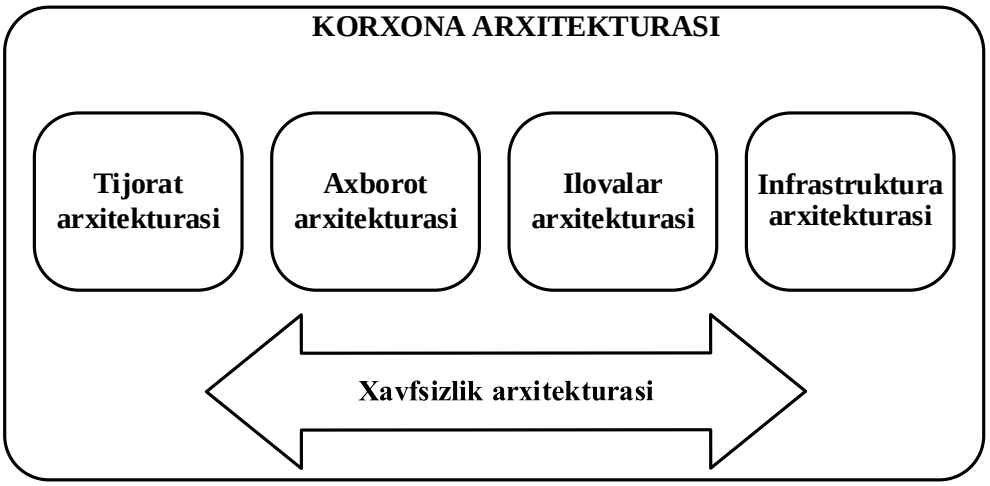
2 BOB. KIBERXAVFSIZLIK ARXITEKTURASI, STRATEGIYASI VA SIYOSATI

2.1. Kiberxavfsizlik arxitekturasi va strategiyasi

Zamonaviy tijorat oldida murakkab masalalar to‘plami ko‘ndalangki, beqaror iqtisodiy vaziyatda ularning dolzarbligi yanada oshadi. Bunday masalalarga quyidagilarni kiritish mumkin:

- daromadning oshishi;
- o‘zgaruvchi vaziyatlarga reaksiya tezligining oshishi;
- harajat va chiqimlarning pasayishi;
- innovatsiyaning tezlashishi;
- bozorga mahsulot va xizmatlarni taqdim etish vaqtining qisqarishi;
- buyurtmachilar va sheriklar xolisligining oshishi;
- raqobatlik qobiliyatining oshishi;
- me’yoriy talablarga moslikni ta’minlash.

Yuqorida keltirilgan barcha masalalarni yechishda korxona arxitekturasidan foydalaniladi (2.1-rasm). Korxona arxitekturasi prinsiplar, yondashishlar va texnologiyalar naborini shakllantirishga imkon beradiki, ular tashkilotning joriy holatini hisobga olgan holda uning kelgusi transformasiyasi, o‘sishi va rivojlanishi asosini belgilaydi.



2.1-rasm. Korxona arxitekturasi va uning boshqa arxitekturalar bilan bog‘liqligi

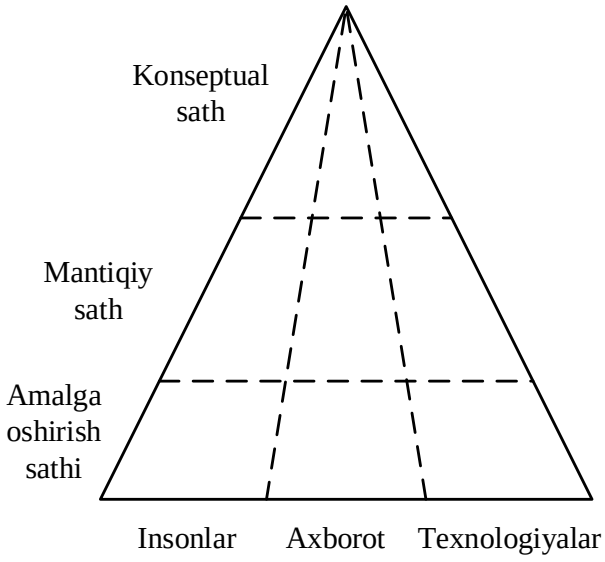
Hozirda bunday arxitekturalarni yaratishda bir necha yondashishlar mavjud, masalan TOGAF, Zachman Framework, FEAF, DoDAF va h.

Ammo, qaysi bir yondashish tanlanmasin, hozirgi sharoitda axborotdan va axborot tizimidan foydalanmay rivojlanish mumkin emas.

Axborot va axborot tizimlari nafaqat tijoratdagi har qanday o‘zgarishlarni madadlaydi, balki ularni oldindan sezadi, ularga oldindan tayyorlanadi, ba’zi xollarda esa yangi tijorat-imkoniyatlarining paydo bo‘lishiga yordam beradi. Biroq tijorat doimo istalgancha rivojlanmaydi. Bunda ma’lumotlarning sirqib chiqishi, axborot texnologiyalari infrastrukturasi elementlarining ishdan chiqishi va h. bilan bog‘liq axborot operatsion risklar anchagina rol o‘ynaydi. Hozirgi va kelajak risklarga tayyor bo‘lish uchun korxonaning boshqa arxitekturalari bilan uzviy bog‘langan axborot xavfsizligi arxitekturasi zarur.

Kiberxavfsizlik arxitekturasi jarayonlarni, inson rolini, texnologiyalarni va turli xil axborotni tavsiflaydi, hamda zamonaviy korxonaning murakkabligini va o‘zgaruvchanligini hisobga oladi. Boshqacha aytganda, kiberxavfsizlikning arxitekturasi tashkilotning va u bilan bog‘liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi xolatini tavsiflaydi. Bunda axborot xavfsiziligi arxitekturasi tijoratning joriy va eng muhimi, kelgusidagi ehtiyojini akslantiradi.

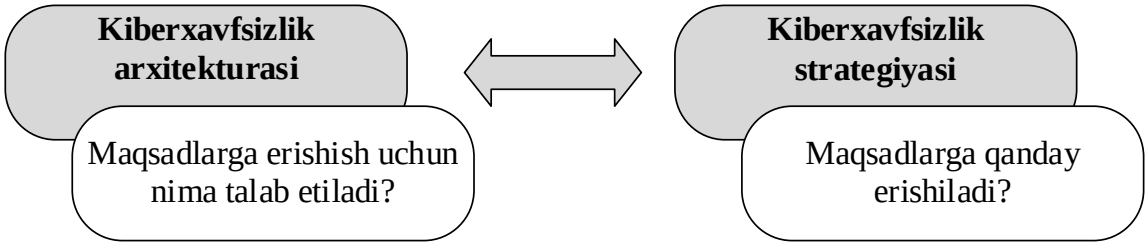
Odatda arxitekturaning 3 ta sathi ajratiladi – konseptual, mantiqiy va amalga oshirish (texnologik). 2.2-rasmda bunday arxitektura keltirilgan bo‘lib, odatda texnologiyalar jihatidagi qismi xavfsizlik xizmati nazoratidan chetda qoladi.



2.2-rasm. Kiberxavfsizlik arxitekturasi

Joriy holatdan qanday qilib yangi, mukammalroq va quyilgan maqsadlarga mos holatga o‘tish mumkin? Buning uchun strategiya, ya’ni quyilgan maqsadlarga erishish uchun harakat yo‘nalishi mavjud.

Strategiya – korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta’minlashga mo‘ljallangan strukturalangan va o‘zaro bog‘langan harakatlar to‘plami. 2.3-rasmda arxitektura bilan strategiyaning o‘zaro bog‘liqligi keltirilgan. Strategiya kiberxavfsizlik arxitekturasi ko‘rinishidagi maqsadga ega bo‘lgan holda unga erishishning optimal yo‘lini belgilaydi.



2.3-rasm. Arxitektura bilan strategiyaning o‘zaro bog‘liqligi

Ko‘pincha strategiya va arxitektura tushunchalarini farqlamay arxitektura tavsifini o‘z ichiga olgan kiberxavfsizlik strategiyasi ishlab chiqiladi. Bu unchalik to‘g‘ri emas, chunki arxitektura, ya’ni maqsadlar vaqt o‘tishi bilan o‘zgarmasligi, bu maqsadlarga erishishdagi strategiya esa tashqi va ichki omillarga bog‘liq holda jiddiy o‘zgarishi mumkin. Strategiya va arxitektura bitta hujjatda tavsiflansa, strategiya o‘zgarganida arxitekturani ham o‘zgartirishga to‘g‘ri keladi.

2.2. Kiberxavfsizlik siyosati va uni amalga oshirish

Axborot xavfsizligi siyosati (yoki xavfsizlik siyosati) – tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta’minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja. Siyosat xavfsizlikni umumlashgan atamalarda tavsiflaydi. U xavfsizlikni ta’minlashning barcha dasturlarini rejalashtiradi. Axborot xavfsizligi siyosati tashkilot masalalarini yechish jarayoni himoyasini yoki ish jarayoni himoyasini ta’minlashi shart.

Apparat vositalar va dasturiy ta’minot ish jarayonini ta’minlovchi vositalar hisoblanadi va ular xavfsizlik siyosati tomonidan qamrab olinishi shart. Shu sababli, asosiy vazifa sifatida tizimni (jumladan tarmoq xaritasini) to‘liq inventarizatsiyalashni ko‘zda tutish lozim. Tarmoq xaritasini tuzishda har bir tizimdagi axborot oqimini aniqlash lozim. Axborot oqimlari sxemasi axborot oqimlarining biznes-jarayonlarni qanchalik ta’minlayotganini, hamda axborotni himoyalash va yashovchanligini ta’minlash uchun qo‘shimcha choralarni ko‘rish muhim bo‘lgan soxani ko‘rsatishi mumkin. Undan tashqari, bu sxema yordamida

axborot ishlanadigan joyni, ushbu axborot qanday saqlanishi, qaydlanishi, joyini o‘zgartirishi va nazoratlanishi lozimligini aniqlash mumkin.

Inventarizatsiya apparat va dasturiy vositalardan tashqari dasturiy va apparatura hujjatlari, texnologik hujjat va h. kabi kompyuterga taalluqli bo‘lmagan resurslarni ham qamrab olishi shart. Ushbu hujjatlar tarkibida tijoratni tashkil etish xususiyatlari to‘g‘risidagi axborot bo‘lishi mumkin va bu hujjatlar buzg‘unchilar foydalanishi mumkin bo‘lgan joylarni ko‘rsatadi.

Xavfsizlik siyosatining zaruriyati:

- Tashkilot bo‘ylab foydalanilayotgan qurilmalar soni ortib borishi tarmoqda uzatilayotgan va saqlanadigan axborot hajmini ortishiga olib kelmoqda. Bu holat esa o‘z navbatida turli zaifliklar natijasida hosil bo‘lgan xavfsizlik tahdidlarini ortishiga ham sababchi bo‘ladi. Xavfsizlik siyosati tashkilotga ushbu tahdidlarga qarshi kurashish va unga axborotning yo‘qolishidan himoyalash imkonini beradi.
- Xavfsizlik siyosati tashkilotning barcha funksiyalarini xavfsiz tarzda amalga oshirish orqali xavfsizlik prinsiplarining kelishilgan vazifalarini ta’minlaydi. Xavfsizlik siyosati mijozlar bilan ishonchga asoslangan aloqani qurishda axborot xavfsizligi standartlarining mosligini ta’minlaydi. Xavfsizlik siyosati tashqi axborot tahdidlariga kompaniyaning duchor bo‘lishi xavfini pasaytirishga yordam beradi.
- Xavfsizlik siyosati tarmoqda qanday qoidalar foydalanishi kerakligini, konfidensial axborot qanday saqlanishi va tashkilot ma’lumotlarini oshkor bo‘lishi va majburiyatlarni kamaytirish uchun qanday shifrlash algoritmlari kerakligini aniqlash orqali qonuniy himoyani ta’minlaydi.
- Xavfsizlik siyosati tahdidlarning sodir bo‘lishidan oldin ularni bashoratlash va zaifliklarni aniqlash orqali xavfsizlik buzilishlari holatining ehtimolini kamaytiradi.
- U shuningdek, zaxira nusxalash va qayta tiklash amallarini joriy qilish orqali tashkilot ma’lumotlarining yo‘qolishi va sirqib chiqishi xavfini minimallashtiradi.

Xavfsizlik siyosatining afzalliklari:

- *Kuchaytirilgan ma’lumot va tarmoq xavfsizligi:* tashkilotlar o‘z ma’lumotlari xavfsizligini ta’minlovchi tarmoqqa asoslangan siyosatini amalga oshiradilar. Xavfsizlik siyosati tarmoqda boshqa tizimlardan ma’lumotlar uzatilishida himoyani ta’minlaydi.
- *Risklarni kamaytirish:* xavfsizlik siyosatini amalga oshirish orqali tashqi manbalardan bo‘lishi mumkin bo‘lgan risklar kamaytiriladi.

Agar xodimlar xavfsizlik siyosati asosida harakat qilsalar, ma’lumot va resurslarning yo‘qolishi holatlari deyarli kuzatilmaydi.

- *Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishi:* xavfsizlik siyosati xodimlar tomonidan amalga oshirilgani bois, ma’murlar tashkilotdagi trafikni va foydalanilgan tashqi qurilmalarni doimiy tarzda monitoringlashi zarur. Kiruvchi va chiquvchi trafikning monitoringi va auditi doimiy ravishda amalga oshirilishi shart.
- *Tarmoqning yuqori unumdorligi:* xavfsizlik siyosati to‘g‘ri amalga oshirilganida va tarmoq doimiy monitoring qilinganida ortiqcha yuklamalar mavjud bo‘lmaydi. Tarmoqda ma’lumotni uzatish tezligi ortadi va bu umumiy samaradorlikni ortishiga olib keladi.
- *Muammolarga darhol javob berish va harakatsiz vaqtning kamligi:* xavfsizlik siyosatini amalga oshirilishi tarmoq muammolari kuzatilganida darhol javob berish imkoniyatini taqdim etadi.
- *Boshqaruvdagi hayajon darajasining kamayishi:* xavfsizlik siyosati amalga oshirilganida boshqaruvchi kam hayajonga ega bo‘ladi. Xavfsizlik siyosatidagi bir vazifa tashkilotning biror xodimiga biriktirilishi shart. Agar ushbu holat amalga oshirilsa, tarmoqda biror nojo‘ya holat kuzatilsa ham, boshqaruvda hech qanday xavotir bo‘lmaydi.
- *Xarajatlarning kamayishi:* agar xodimlar siyosatga to‘g‘ri amal qilsalar, tashkilotga ta’sir qiluvchi turli xalaqitlar uchun ortiqcha harajat kamayadi.

Xavfsizlik siyosatining iyerarxiyasi:

Tashkilotlarda xavfsizlik siyosatini ishlab chiqishda turli hujjatlardan foydalaniladi. Ushbu hujjatlarni ishlab chiqish xavfsizlik siyosatining iyerarxiyasining sathi va uning soniga bog‘liq.

- *Qonunlar*. Qonunlar iyerarxiyaning eng yuqori sathida joylashgan bo‘lib, ular tashkilotdagi har bir xodim amalga oshirishi kerak bo‘lgan vazifalarni o‘z ichiga oladi. Ushbu qonunlarga amal qilmagan har bir xodim uchun javobgarlik choralari ko‘rilishi shart bo‘ladi.
- *Normativ hujjatlar.* Normativ hujjatlar iyerarxiyadagi ikkinchi tashkil etuvchi bo‘lib, ular xodimlarning qonunlarga rioya qilishini kafolatlaydi. Normativ hujjatlar xavfsizlik siyosati qonuniga mos bo‘lgan yo‘l yo‘riq ko‘rsatuvchi hujjatlar to‘plami bo‘lib, ular hukumat yoki ijtimoiy normativ hujjatlardan tashkil topadi.
- *Siyosatlar.* Siyosatlar yordamida tashkilot shaxsiy tarmoq xavfsizligi uchun qonuniy ichki tarmoq talablarini yaratadi. Siyosat turli muolajalardan iborat bo‘lib, ular tashkilot uchun xavfsizlik arxitekturasini

koʻrsatadi. Ushbu siyosatlarning amalga oshirilishi tashkilotga standartlarni oʻrnatish va risklarni boshqarish kabi vazifalarni bajarishiga imkon yaratadi.

- *Standartlar*. Standartlar siyosatni amalga oshirish usullarini tavsiflaydi va tashkilotlar tomonidan amalga oshiriladi. Standartlar korxona siyosatiga ixtiyoriy va mandatli aloqador boʻlib, ishlab chiqilgan standartni maʼlum vaqtdan soʻng oʻzgartirish talab etilmasligi zarur. Shuningdek, standartlar texnologiya, qurilma va dasturiy vositaga bogʻliq holda xavfsizlik nazoratini oʻz ichiga oladi.
- *Yoʻriqnomalar*. Yoʻriqnomalar tashkilot siyosati va standartlarini amalga oshirish strategiyasini aniqlab, tashkilotning tahdidlarga qarshi tura olishida yordam beradi. Shuning uchun, tashkilot xodimlari yoʻriqnomalarni bajarish uchun, maxsus oʻqitiladi.
- *Muolajalar*. Muoalajalar tashkilot siyosatini amalga oshiruvchi ketma-ket bosqichlar toʻplami boʻlib, ularni amalga oshirishda imtiyozga ega subyektdan tasdiq talab etiladi. Muolajalar quyidagi savollar asosida ishlaydi:
  - kim nimani bajaradi?;
  - ular qanday bosqichlarga ega?;
  - ular qaysi shakl va hujjatlardan foydalanadilar?
- *Umumiy qoidalar*. Umumiy qoidalar tanlovga koʻra maslahatlar bilan taʼminlovchi hujjat boʻlib, ulardan biror maxsus standartlar boʻlmagan holda foydalaniladi. Umumiy qoidalar tavsiyalar sifatida boʻladi va tashkilotlar ularni rad eta olmaydi. Umumiy qoidalarni amalga oshirish risklarni kamaytirsada, biznes talablari oʻzgarganida umumiy qoidalarni ham oʻzgartirish tavsiya etiladi.

Xavfsizlik siyosati quyidagi xususiyatlarga ega boʻlishi shart:

- *Qisqa va aniq:* xavfsizlik siyosati infrastrukturada joriy qilishda qisqa va aniq boʻlishi shart. Murakkab xavfsizlik siyosati tushunish uchun qiyin boʻlib, xodimlar tomonidan kutilgani kabi amalga oshirilmaydi.
- *Foydalanuvchan boʻlishi:* siyosat tashkilotning turli sektorlari boʻylab oson foydalanishli yozilishi va loyihalanishi shart. Yaxshi yozilgan siyosatlar boshqarishga va amalga oshirishga oson boʻladi.
- *Iqtisodiy asoslangan boʻlishi:* tashkilotlar tejamkor va oʻz xavfsizligini kuchaytiruvchi siyosatni amalga oshirishlari shart.
- *Amaliy boʻlishi:* siyosatlar reallikka asoslangan amaliy boʻlishi kerak. Real boʻlmagan siyosatning amalga oshirilishi tashkilotga muammo tugʻdiradi.

- *Barqaror bo‘lishi:* tashkilot o‘zining siyosatini amalga oshirishda barqarorlikga ega bo‘lishi kerak.
- *Mulojaviy bardoshli bo‘lishi:* siyosat muolajalari amalga oshirilganida, ular ish beruvchi va ishlovchiga mos bo‘lishi kerak.
- *Kiber va yuridik qonunlarga, standartlarga, qoidalarga va yo‘riqnomalarga mos bo‘lishi:* amalga oshiriluvchi ixtiyoriy siyosat kiber qonunlar asosida ishlab chiqilgan qoidalar va yo‘riqnomalarga mos bo‘lishi zarur.

Axborot xavfsizligi siyosatining turlari. Tashkilotda axborot xavfsizligini rejalashtirish, loyihalash va amalga oshirishda siyosat muhim hisoblanib, ular foydalanuvchilarga xavfsizlik maqsadlariga erishishda mavjud muammolarni bartaraf etish choralarini taqdim etadi. Bundan tashqari, xavfsizlik siyosati tashkilotdagi dasturiy ta’minot va jihozlar vazifasini tavsiflaydi.

Axborot texnologiyalari sohasidagi korxonalarda quyidagi xavfsizlik siyosatlari qo‘llaniladi:

- *Tashkilot axborot xavfsizligi siyosati (Enterprise Information Security Policies, EISP):* mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi.
- *Muammoga qaratilgan xavfsizlik siyosatlari (Issue-Specific Security Policies, ISSP):* bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profilaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi.
- *Tizimga qaratilgan xavfsizlik siyosatlari (System-Specific Security Policies, SSSP):* mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini ta’minlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga olgan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi. Bu siyosat texnologiyani amalga oshirish, sozlash va foydalanuvchilar harakatlarini hisobga olishi mumkin.

Tashkilotlarda turli maqsadlarga qaratilgan ko‘plab xavfsizlik siyosatlari mavjud bo‘lishi mumkin. Quyida ularning ayrimlari keltirilgan.

Internetdan foydalanish siyosati. Mazkur siyosat Internetdan foydalanishdagi cheklanishlarni aniqlab, xodimlar uchun Internet tarmog‘idan foydalanish tartibini belgilaydi. Internetdan foydalanish siyosati o‘z ichiga Internetdan foydalanish ruxsati, tizim xavfsizligi, tarmoqni o‘rnatish, AT xizmati va boshqa yo‘riqnomalarni qamrab oladi.

Internetdan foydalanish siyosatini quyidagi to‘rtta kategoriyaga ajratish mumkin:

1. *Tartibsiz siyosat (Promiscuous Policy):* ushbu siyosat tizim resurslaridan foydalanishda hech qanday cheklovlarni amalga oshirmaydi. Masalan, bu siyosatga ko‘ra foydalanuvchi istalgan saytga kirishi, istalgan dasturni yuklab olishi, masofadagi kompyuterdan yoki tarmoqdan foydalanishi mumkin. Bu siyosat korporativ tashkilotlarning ofislarida ishlovchi yoki tashkilotga kelgan mehmonlar uchun foydali hisoblansada, kompyuterni zararli dasturlar asosidagi tahdidlarga zaif qilib qo‘yishi mumkin. Ya’ni, Internetdan foydalanishda cheklanishlar mavjud bo‘lmagani bois, foydalanuvchilar bilimsizligi natijasida zararli dasturlar kirib kelishi mumkin.
2. *Ruxsat berishga asoslangan siyosat (Permissive Policy):* Bu siyosatga ko‘ra faqat xavfli xizmatlar/ hujumlar yoki harakatlar blokirovkalanadi. Masalan, ruxsat berishga asoslangan Internet siyosatida qator keng tarqalgan zararli xizmatlar/ hujumlardan tashqari Internet trafigining asosiy qismi ochiq bo‘ladi. Faqat keng tarqalgan hujumlar va zararli dasturlar blokirovkalanganligi tufayli, ma’mur joriy holatdagi zararli harakatlarga qarshi himoyani ta’minlay oladi. Bu siyosatda har doim yangi hujumlarni va zararli dasturiy ta’minotlarni tutish va bazaga kiritib borish talab etiladi.
3. *Paranoid siyosati (Paranoid Policy):* Paranoid siyosatga ko‘ra barcha narsa blokirovkalanadi va tizim yoki tarmoqdan foydalanuvchi tashkilot kompyuterlarida qat’iy cheklovlar mavjud bo‘ladi. Bu siyosatga ko‘ra foydalanuvchi Internetga umuman ulanmagan yoki qat’iy cheklovlar bilan ulangan bo‘lishi mumkin. Bunday hollarda, foydalanuvchilar odatda siyosatdagi qoidalarni aylanib o‘tishga harakat qiladilar.
4. *Ehtiyotkorlik siyosati (Prudent Policy):* Ehtiyotkorlik siyosati barcha xizmatlar blokirovkalanganidan so‘ng amalga oshirilib, unda xavfsiz va zarur xizmatlarga ma’mur tomonidan individual ravishda

ruxsat beriladi. Bu maksimal xavfsizlikni ta’minlab, tizim/ tarmoq faoliyatiga oid barcha hodisalarni qaydlaydi.

Maqbul foydalanish siyosati. Maqbul foydalanish siyosati tarmoq va web sayt egalari tomonidan qaror qilingan qoidalardan iborat va u hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi. Ushbu siyosatda foydalanuvchilarning o‘z akkauntlarida mavjud bo‘lgan ma’lumotlarni himoya qilish majburiyati ko‘rsatilgan bo‘lib, foydalanuvchidan tarmoqdan yoki Internetdagi kompyuterdan foydalanishida siyosat cheklovlarini qabul qilishi talab etiladi. Ehtiyotkorlik siyosati prinsiplar, taqiqlar, qayta ko‘rib chiqish va jazo choralarini o‘z ichiga olib, foydalanuvchini, shaxsiy sabablarga ko‘ra, korporativ resurslardan foydalanishini taqiqlaydi.

Maqbul foydalanish siyosati axborot xavfsizligi siyosatining ajralmas qismi hisoblanadi. Bunda, tashkilotlar, o‘zlarining yangi xodimlariga axborot resurlaridan foydalanishga ruxsat berishdan oldin, maqbul foydalanish siyosati bo‘yicha tanishganligi xususida kafolat imzosi olinadi. Maqbul foydalanish siyosati foydalanuvchilarni axborot texnologiyalari infrastrukturasida nimalarni bajarish kerak va nimalarni bajarmaslik kerakligi haqidagi asosiy jihatlarni o‘z ichiga oladi.

Maqbul foydalanish siyosati to‘g‘ri amalga oshirilganiga ishonch hosil qilish uchun ma’mur doimiy ravishda xavfsizlik auditini olib borishi kerak. Masalan, aksariyat tashkilotlar o‘z saytlarida va pochtalarida siyosatga aloqador va diniy mavzularda muzokaralar olib borilishini taqiqlaydi. Maqbul foydalanish siyosatlarining aksariyatida siyosatni buzganlik uchun jazolar tayinlanadi. Bunday jazolar foydalanuvchi akkauntini vaqtincha yopib qo‘yishdan tortib qonuniy jazo choralarigacha bo‘lishi mumkin.

Nazorat savollari

1. Axborot xavfsizligi arxitekturasi va uning sathlari mohiyati.
2. Axborot xavfsizligi strategiyasi tushunchasi.
3. Korxona arxitekturasini tuzishda xavfsizlik strategiyasi va arxitekturasining o‘rni.
4. Axborot xavfsizligi siyosati va uning asosiy vazifasi nimadan iborat?
5. Xavfsizlik siyosati nima uchun zarur?
6. Xavfsizlik siyosatining tarkibi va tuzilishi.
7. Xavfsizlik siyosatining asosiy turlari.
8. Internetdan foydalanish siyosati.

3 BOB. AXBOROTNING KRIPTOGRAFIK HIMOYASI

3.1. Kriptografiyaning asosiy tushunchalari

Muhim axborotni muayyan adresatga, boshqalarga bildirmasdan, uzatish masalasini uchta usul yordamida hal etish mumkin:

– adresatlar orasida axborotni uzatishning mutlaqo ishonchli yashirin kanalini yaratish evaziga. Ammo, buni real sharoitlarda amalga oshirish murakkab;

– uzatish kanalini yoki trafikni niqoblash orqali uzatish faktining o‘zini berkitish evaziga;

– axborotni shunday o‘zgartirish lozimki, uni faqat qonuniy qabul qiluvchi tiklay olishi mumkinligi evaziga.

Aynan uchinchi variant kriptografiyani o‘rganish predmetini tashkil etadi. Hozirda kriptografiya doirasida yechiladigan masalalarga quyidagilar taalluqli:

- axborotning konfidensialligini ta’minlash;
- axborotning yaxlitligini ta’minlash;
- autentifikatsiya usullarini amalga oshirish;
- harakatni rad qila olmaslikni ta’minlash.

Konfidensiallik xususiyati simmetrik va ochiq kalitli (asimmetrik) kriptotizimlar evaziga ta’minlanadi. Yaxlitlik xususiyati kriptografik xesh funksiyalar va raqamli imzolardan foydalanib amalga oshiriladi. Autentifikatsiya qismtizimi turli kriptografik primitivlar (cryptographic primitives) asosida amalga oshirilishi mumkin. Harakatni rad qilaolmaslik xususiyati xabar oluvchining, xabar jo‘natuvchisining oldin jo‘natgan xabar muallifligidan tonishiga urinishidan, himoyalanishini tavsiflaydi. Ushbu xususiyat faqat ochiq kalitli kriptografiya vositalari yordamida ta’minlanadi.

Kriptografiyaning yuqorida qayd etilgan masalalari qator kriptografik primitivlardan foydalanib amalga oshiriladi:

- simmetrik kriptotizimlar;
- ochiq kalitli kriptotizimlar;
- kriptografik xesh funksiyalar;
- raqamli imzolar;
- raqamli sertifikatlar.

Quyida keyingi bayonlarda ishlatiluvchi asosiy atamalarga oydinlik kiritiladi.

Alfavit deganda axborotni ifodalashda ishlatiluvchi bilgilarning chekli to‘plami tushuniladi. Zamonaviy kriptotizimlarda ko‘pincha atigi

ikkita simvoldan (0, 1) iborat ikkili alfavit ishlatiladi. Shuningdek, o‘ttiz oltita belgidan (harfdan) iborat o‘zbek tili alfavitini, o‘ttiz ikkita belgidan (harfdan) iborat rus tili alfavitini, yigirma sakkizta belgidan (harfdan) iborat lotin alfavitini, ikki yuzi ellik oltita belgidan iborat ASSII kompyuter belgilarining alfavitini ham misol sifatida keltirish mumkin.

Matn yoki xabar – alfavit elementlaridan tartiblangan nabor. *Ochiq matn* (plaintext) – shifrlashga atalgan dastlabki xabar. *Shifrmatn* (cipher text) – ochiq matnni shifrlash natijasi.

Shifrlash (encryption, enciphering) – ochiq matnni shifrmatnga o‘zgartirish jarayoni.

Rasshifrovkalash (decryption, deciphering) – shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayon.

Deshifrlash (breaking) – kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni.

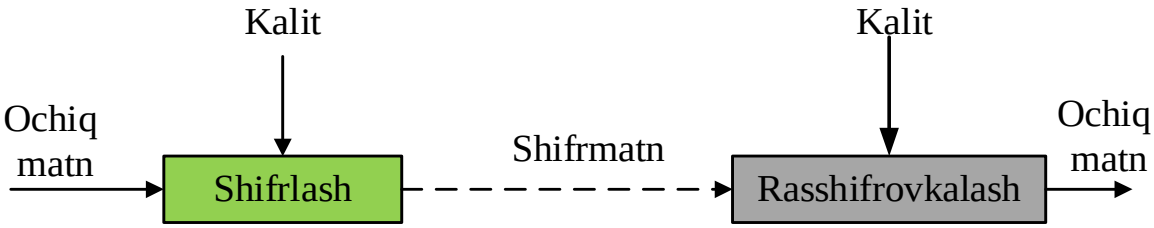
Rasshifrovkalash bilan deshifrlash orasidagi tafovutga e’tibor qarataylik: agar rasshifrovkalash kriptografik algoritmdan foydalanilganda standart shtatli muolaja hisoblansa, deshifrlash, ko‘proq kriptotahlilga taalluqli, kriptotizimni buzishdir. “Shifrlash” umumiy atamasi shifrlash va rasshifrovkalash jarayonini bildiradi.

Kriptotizimlarni buzish usullari *kriptotahlil* (cryptanalysis)ni o‘rganish predmeti hisoblanadi. Kriptografiya va kriptotahlil uzviy bog‘langanliklari sababli, ularni ko‘pincha birgalikda yagona fan – *kriptologiya* (cryptology) (*kryptos* - mahfiy, *logos*- ilm) sifatida qabul qilinadi.

Kriptotizim (cryptosystem) – ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi.

Kalit (key), yoki kriptoo‘zgaruvchi (cryptovariable) – o‘zgartirishlar oilasidan birini tanlashni ta’minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati.

Kriptotizimning “qora quti” sifatidagi ko‘rinishi 3.1 – rasmda keltirilgan.



3.1-rasm. Kriptotizimning “qora quti” sifatidagi ko‘rinishi

Kriptotizimni ikki tarkibli algoritm va kalitdan iborat ekanligiga asoslangan holda *Kerkgoff prinsipini* eslatib o‘tish lozim. Ushbu prinsipga binoan faqat kalit sir saqlanishi, shifrlash algoritmi esa ochiq bo‘lishi lozim. Bu degani, agar niyati buzuq algoritmni bilgan taqdirda ham tizim obro‘sizlanmaydi. Kalitni esa almashtirish mumkin. Klod Shennon ushbu prinsipni “Dushman tizimni biladi” deb ta’riflagan.

Aksariyat hollarda foydalanuvchilar ma’lumotni *shifrlash* va *kodlash* tushunchalarini bir xil deb tushunishadi. Aslida ular turlicha tushunchalardir. *Kodlash* – ma’lumotlarni osongina asliga qaytarish uchun hammaga (hattoki hujumchiga ham) ochiq bo‘lgan sxema yordamida ma’lumotlarni boshqa formatga o‘zgartirish. Kodlash ma’lumotlardan foydalanish qulayligini ta’minlash uchun amalga oshiriladi va hamma uchun ochiq bo‘lgan sxemalardan foydalanadi.

Shifrlash jarayonida ham ma’lumot boshqa formatga o‘zgartiriladi. Biroq, uni faqat ma’lum shaxslar (rasshifrovkalash kalitiga ega bo‘lgan shaxslar) qayta o‘zgartirishi mumkin bo‘ladi. Shifrlashdan asosiy maqsad ma’lumotni maxfiyligini ta’minlash bo‘lib, uni qayta o‘zgartirish ba’zi shaxslar (rasshifrovkalash kalitiga ega bo‘lmagan shaxslar) uchun cheklangan bo‘ladi.

Kriptografiya va *steganografiya* fan sohalari o‘xshashlikga ega bo‘lganligi sababli, aksariyat hollarda ularni chalkashtirish kuzatiladi. *Steganografiya* – bu maxfiy xabarni sohta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi. Boshqacha aytganda, steganografiyaning asosiy g‘oyasi – maxfiy ma’lumotlarning mavjudligi haqidagi shubhani oldini olish.

*Kriptografiya*da jo‘natuvchi faqat ochiq matn ko‘rinishidagi xabar yuborishi mumkin. Bunda u xabarni ochiq tarmoq (masalan, Internet) orqali uzatishdan oldin shifrlangan matnga o‘zgartiradi. Ushbu shifrlangan xabar qabul qiluvchiga kelganida yana oddiy matn ko‘rinishiga qaytariladi. Umumiy holda ma’lumotni *shifrlashdan asosiy maqsad* (simmetrik yoki ochiq kalitli kriptografik tizimlar asosida - farqi yo‘q) – ma’lumotni maxfiyligini qolganlardan sir tutish.

Kriptografiyaning tarixi. Ma’lumotlarni shifrlashning dastlabki ko‘rinishlaridan ming yillar avval foydalanib kelingan. Yaqin o‘n yilliklarga qadar foydalanilgan shifrlar *klassik* shifrlar deb atalgan. Kriptografiyani fan sifatida taraqqiy etishini aksariyat adabiyotlarda bir necha davrlarga ajratib, turli yondashuvlarga asoslanib o‘rganilgan. Masalan, ba’zi manbalarda hisoblash qurilmalari yaratilgunga qadar foydalanilgan shifrlar – *klassik shifrlar* davriga tegishli deb olingan.

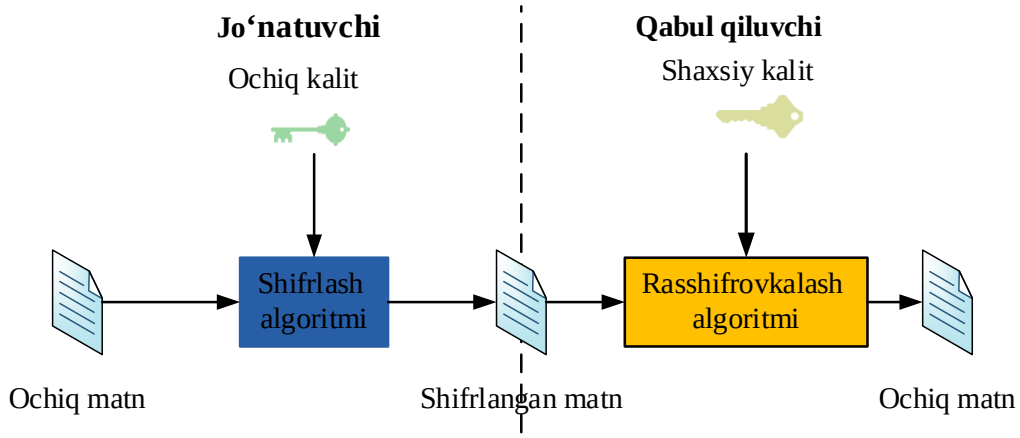
Undan keyingi davr esa *zamonaviy shifrlar* davri deb yuritiladi. Biroq, hisoblash qurilmalari yaratilgunga qadar bo‘lgan davr juda uzoq bo‘lgani bois, ularni ham qismdavrlarga ajratish muhim ahamiyat kasb etgan. Shuning uchun, kriptologiyani fan sifatida shakllanishini quyidagi davrlarga ajratish mumkin:

1. *Qadimiy davr (qadimiy davr klassik shifrlari).* Ushbu davrda klassik shifrlar asosan bir alfavitli o‘rniga qo‘yish va o‘rin almashtirish akslantirishlariga asoslangan. Masalan, Sezar, Polibiya kvadrati usullari.
2. *O‘rta davr (o‘rta davr klassik shifrlari).* Ushbu davrda shifrlar asosan ko‘p alfavitli o‘rniga qo‘yishga asoslangan bo‘lib, ularga Vijiner, Atbash usullarini misol sifatida keltirish mumkin. Ushbu davrdagi shifrlarning, birinchi davr shifrlariga qaraganda, bardoshligi yuqori bo‘lgan.
3. *1 va 2 – jaxon urushlari davri (1 va 2- jaxon urushlari davridagi klassik shifrlar).* Ushbu davr kriptotizimlari asosan elektromexanikaga asoslangan bo‘lib, radioto‘lqin orqali shifrmatnni uzatish (Morze alifbosi) amalga oshirilgan. Mazkur davrga oid shifrlash usullariga Zimmermann telegrammi, Enigma shifri, SIGABA mashinalarini misol sifatida keltirish mumkin.
4. *Kompyuter davri (zamonaviy shifrlar).* Ushbu davr shifrlari hisoblash qurilmalariga mo‘ljallangan bo‘lib, yuqori xavfsizlik darajasiga ega. Zamonaviy shifrlarga misol sifatida DES, AES, ГОСТ Р 28147-89, IDEA, A5/1, RC4 (barchasi simmetrik) va RSA, El-Gamal (ochiq kalitli) larni keltirish mumkin.

Kriptografiyaning asosiy bo‘limlari. Kriptografiyani quyidagi bo‘limlarga ajratish mumkin:

1. *Simmetrik kalitli kriptografiya.* Simmetrik kalitli kriptografiyaning umumiy ko‘rinishi 3.1-rasmdagi kabi bo‘lib, ma’lumotni shifrlash va rasshifrovkalashda yagona kalitdan (simmetrik kalitdan) foydalaniladi. Shuning uchun simmetrik kalitli kriptotizimlarni – *bir kalitli* kriptotizimlar deb ham yuritishadi. Demak, simmetrik kalitli shifrlash algoritmlaridan foydalanish uchun har ikkala tomonda bir xil kalit mavjud bo‘lishi zarur. Simmetrik kalit odatda bir tomonda hosil qilinadi va maxsus usullar asosida ikkinchi tomonga xavfsiz tarzda yetkaziladi.
2. *Ochiq kalitli kriptografiya.* Ochiq kalitli kriptografiyada (yoki asimmetrik kriptografiya deb ham ataladi) ma’lumotni shifrlash qabul qiluvchining *ochiq kaliti* bilan amalga oshirilsa, uni rasshifrovkalash qabul qiluvchining *shaxsiy kaliti* bilan amalga oshiriladi. Shuning uchun

ham ochiq kalitli kriptotizimlarni *ikki kalitli* kriptotizimlar deb ham yuritishadi. Ochiq kalitli kriptografiyaning umumiy ko‘rinishi 3.2-rasmda keltirilgan.



3.2-rasm. Ochiq kalitli shifrlashning umumiy ko‘rinishi

Ochiq kalitli kriptografik algoritmlar asosida ma’lumot almashinish uchun dastlab, jo‘natuvchi qabul qiluvchining ochiq kalitiga ega bo‘lishi kerak. Qabul qiluvchining ochiq kalitidan faqat ma’lumotni shifrlash uchun foydalaniladi va u bilan shifrmatnni rasshifrovkalashning imkoni mavjud emas. Xuddi shuningdek, shaxsiy kalit bilan ma’lumotni shifrlash imkoni ham mavjud emas. Shifrmatnni rasshifrovkalash esa faqat shaxsiy kalit egasiga joiz. Demak, shaxsiy kalit egasi tomonidan xavfsiz saqlanishi va o‘zidan boshqa hech kimga ma’lum bo‘lmasligi kerak.

3. *Xesh funksiyalar*. Ma’lumotni xeshlash uning yaxlitligini kafolatlash maqsadida amalga oshirilib, agar ma’lumot uzatilishi davomida o‘zgarishga uchrasa, uni aniqlash imkoni mavjud bo‘ladi. Xesh-funksiyalarda odatda kiruvchi ma’lumotning uzunligi o‘zgaruvchan, chiqishda esa o‘zgarmas uzunlikdagi qiymatni qaytaradi. Zamonaviy xesh funksiyalarga MD5, SHA1, SHA256, O‘z DSt 1106:2009 larni misol sifatida keltirish mumkin.

Odatda kriptografiyada ma’lumotlarni shifrlashda (rasshifrovkalashda) ikki turdagi *akslantirish*lardan foydalaniladi. Ulardan biri *o‘rniga qo‘yish (substitution)* akslantirishi, ikkinchisi *o‘rin almashtirish (permutation)* akslantirishi.

O‘rniga qo‘yish akslantirishi. Ushbu akslantirish sodda va zamonaviy simmetrik kriptografik algoritmlarning asosi hisoblanadi. O‘rniga qo‘yish akslantirishida, ochiq matn simvollari bir alfavitdan olinib, unga mos shifrmatn simvollari boshqa bir alfavitdan olinadi.

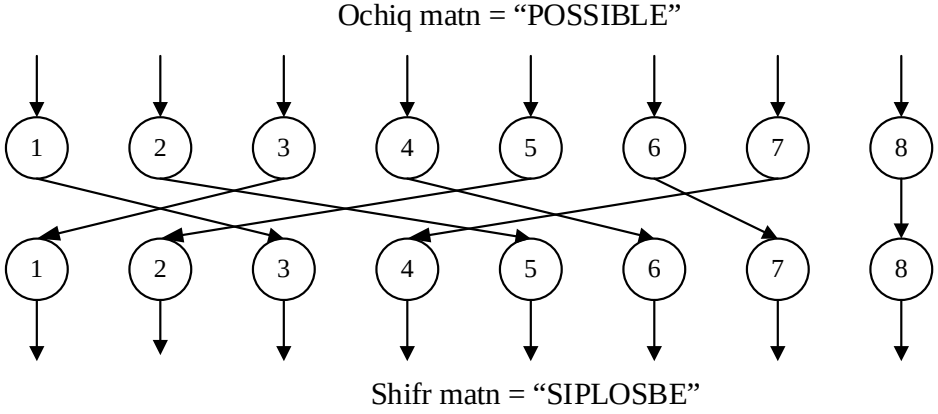
Sodda ko‘rinishda olingan o‘rniga qo‘yish akslantirish amali asosida shifrlash uchun olingan matn quyida keltirilgan. Ushbu sodda shifrlash usuli Sezar nomi bilan mashhur. Masalan, agar ochiq matn “HELLO” ga teng bo‘lsa, unga mos holda shifrmatn “KHOOR” ga teng bo‘ladi. Mazkur holda shifrmatn alfaviti ochiq matn alfavitidan 3 ta pozisiyaga surish natijasida hosil qilingan va shuning uchun shifrlash kalitini 3 ga teng deb hisoblash mumkin (3.1-jadval). Rasshifrovkalash jarayonida esa shifrmatn simvollari shifrmatn alfavitidan olinib, unga mos ochiq matn alfavitidagi simvollarga almashtiriladi. Masalan, shifrmatn “ILUVW” ga teng bo‘lsa, unga mos ochiq matn “FIRST” ga teng bo‘ladi.

3.1-jadval

O‘rniga qo‘yish akslantirishiga misol

Ochiq matn	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shifr matn	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

O‘rin almashtirish akslantirishi. Ushbu akslantirishga ko‘ra, ochiq matn simvollarining o‘rni biror qoidaga ko‘ra o‘zaro almashtiriladi. Bunda ochiq matnda ishtirok etgan simvollar shifrmatnda ham ishtirok etib, faqat ularning o‘rni almashgan bo‘ladi (3.3-rasm).



3.3-rasm. Sodda o‘rin almashtirish usuliga misol

Bir martali bloknot. Bir martali bloknot (one time pad) yoki “Vernam shifri” nomi bilan tanilgan kriptotizim *bardoshli* shifrlash algoritmi hisoblanib, tarixda keng foydalanilgan bo‘lsada, ko‘p hollarda amalga oshirishning imkoniyati mavjud bo‘lmagan. Uning bir martali deb

atalishiga asosiy sabab, undagi *kalitning (bloknotning)* bir marta foydalanilishi bo‘lib, uni aksariyat hollarda amalga oshirishning imkoni bo‘lmaydi. Masalan, ushbu shifrlash algoritmi 8 ta simvoldan iborat bo‘lgan alfavit bo‘lsin. Olingan alfavit simvollari va unga mos bo‘lgan binar qiymatlar 3.2 - jadvalda keltirilgan. Alfavit simvollari va ularga mos bit qiymatlari barcha uchun ochiq va sir saqlanmaydi.

3.2-jadval

Ochiq matn chun tanlangan alfavit

Simvollar	B	E	I	L	O	P	S	T
Binar qiymat	000	001	010	011	100	101	110	111

Faraz qilaylik, biror qonuniy foydalanuvchi A bir martali bloknotdan foydalangan holda “POSSIBLE” matnini shifrlab, o‘z sherigi B tomonga jo‘natishi talab etilsin. Ushbu ochiq matnning binar qiymatdagi ko‘rinishi quyidagicha bo‘ladi:

P	O	S	S	I	B	L	E
101	100	110	110	010	000	011	001

Bir martali bloknot usulida shifrlashda ochiq matn uzunligiga teng bo‘lgan tasodifiy tanlangan kalitdan foydalaniladi. Shifrmatn ochiq matn va kalitga XOR amalini qo‘llab hosil qilinadi (*P – ochiq matn, K – kalit* va *C – shifrmatn*): $C = P \oplus K$. XOR amali ($\oplus$) quyida keltirilgan:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Jadvaldan, $x \oplus y \oplus y = x$ tenglik o‘rinligini ko‘rish mumkin. Bu esa bir martali parol bilan rasshifrovkalashda shifrmatnga kalitni XOR amalida bajarilishining o‘zi yetarligini ko‘rsatadi: $P = C \oplus K$.

Faraz qilaylik, A tomon 3.2-jadvaldagi ochiq matn uzunligiga teng bo‘lgan quyidagi kalitga ega bo‘lsin:

111 101 110 101 111 100 000 101

A tomon ushbu kalit asosida shifrmatnni quyidagicha hisoblaydi:

	P	O	S	S	I	B	L	E
Ochiq matn:	101	100	110	110	010	000	011	001
Kalit:	111	101	110	101	111	100	000	101
Shifrmatn:	010	001	000	011	101	100	011	100
	I	E	B	L	P	O	L	O

A tomonidan jo‘natilgan shifrmatn B tomonda bir xil kalitdan foydalanib osongina rasshifrovkalanadi:

	I	E	B	L	P	O	L	O
Shifrmatn:	010	001	000	011	101	100	011	100
Kalit:	111	101	110	101	111	100	000	101
Ochiq matn:	101	100	110	110	010	000	011	001
	P	O	S	S	I	B	L	E

3.2. Simmetrik kriptografik algoritmlar

Quyida simmetrik kriptotizimlar, shuningdek ularning ikki turi: *oqimli* va *blokli* simmetrik shifrlash algoritmlariga to‘xtalib o‘tiladi. Simmetrik shifrlash algoritmlarida ma’lumotlarni shifrlash va rasshifrovkalashda yagona kalitdan foydalaniladi. Ma’lumotlarni shifrlash va rasshifrovkalash jarayonlarini amalga oshirish tartibi foydalanilayotgan tizim xususiyatiga asosan tanlanadi.

Simmetrik kriptotizimlarning ishlashi bilan tanishishda quyidagi belgilashlar kiritiladi:

– ochiq matn P ni simmetrik kalit K bilan shifrlash: $C = E(P, K)$;

– shifrmatn C ni simmetrik kalit K bilan rasshifrovkalash: $M = D(C, K)$.

Bu yerda, $E()$ va $D()$ lar mos ravishda simmetrik kriptotizimdagi shifrlash va rasshifrovkalash funksiyalari.

Oqimli simmetrik shifrlash algoritmlari. Oqimli simmetrik shifrlash algoritmlari bir martali bloknotga asoslangan, farqli jihati – bardoshligi yetarlicha pastligi va boshqariladigan kalitning mavjudligi. Ya’ni, kichik uzunlikdagi kalitdan ochiq matn uzunligiga teng bo‘lgan

ketma-ketlik hosil qilinadi va undan bir martali bloknot sifatida foydalaniladi.

Oqimli shifr n bitli kalit K ni qabul qiladi va uni ochiq matnni uzunligiga teng bo‘lgan ketma-ketlik S ga uzaytiradi. Shifrmatn C ketma – ketlik S ochiq matn P bilan XOR amali yordamida hosil qilinadi. Bunda ketma-ketlikni qo‘shish bir martali bloknotni qo‘shish kabi amalga oshiriladi.

Oqimli shifrni quyidagicha sodda ko‘rinishda yozish mumkin:

$$StreamCipher(K) = S$$

Bu yerda K kalit, S esa natijaviy ketma-ketlik. Esda saqlash lozimki, bu yerdagi ketma-ketlik shifrmatn emas, balki bir martali bloknotga o‘xshash oddiy qator.

Agar berilgan ketma-ketlik $S = s_0, s_1, s_2, ...$, va ochiq matn $P = p_0, p_1, p_2, ...$, berilgan bo‘lsa, XOR amali yordamida shifrmatnning mos bitlari $C = c_0, c_1, c_2, ...$, ni quyidagicha hosil qilish mumkin.

$$c_0 = p_0 \oplus s_0, c_1 = p_1 \oplus s_1, c_2 = p_2 \oplus s_2 , ...$$

Shifrmatn C ni rasshifrovkalash uchun, yana ketma-ketlik C dan foydalaniladi:

$$p_0 = c_0 \oplus s_0, p_1 = c_1 \oplus s_1, p_2 = c_2 \oplus s_2 , ...$$

Jo‘natuvchi va qabul qiluvchini bir xil oqimli shifrlash algoritmi va kalit K bilan ta’minlash orqali, ikkala tomonda bir xil ketma-ketliklarni hosil qilish mumkin. Biroq, natijaviy shifr kafolatli xavfsizlikka ega bo‘lmaydi va asosiy e’tibor amaliy jihatdan qo‘llashga qaratiladi.

A5/1 oqimli shifrlash algoritmi. Ushbu oqimli shifrlash algoritmidan GSM mobil aloqa tizimlarida ma’lumotlarni konfidensialligini ta’minlashda foydalaniladi. Mazkur algoritm algebraik tuzilishga ega bo‘lsada, uni sodda diagramma ko‘rinishda ham tasvirlash imkoniyati mavjud.

A5/1 shifrlash algoritmi uchta *chiziqli siljitish registr*laridan iborat, ular mos holda X, Y va Z kabi belgilanadi. X registr o‘zida 19 bit $(x_0, x_1, \dots, x_{18})$, Y registr 22 bit $(y_0, y_1, \dots, y_{21})$ va Z registr 23 bit $(z_0, z_1, \dots, z_{22})$ ma’lumotni saqlaydi. Uchta registrning bunday

o‘lchamdagi bitlarni saqlashi bejiz emas. Sababi, chiziqli siljitish registrlari o‘zida jami bo‘lib 64 bitni saqlaydi. A5/1 shifrlash algoritmida foydalaniluvchi kalit K ning uzunligi 64 bitga teng va ushbu kalitdan registrlarni dastlabki to‘ldirish uchun foydalaniladi. So‘ngra oqimli shifrlash algoritmi asosida talab etilgan uzunlikdagi (ochiq matn uzunligiga teng bo‘lgan) ketma-ketliklar generasiyalanadi. Ketma-ketliklarni generatsiyalash tartibini o‘rganishdan oldin, registrlar xususidagi ba’zi ma’lumotlar quyida keltirilgan.

X siljitish registrida quyidagi amallar ketma-ketligi bajariladi:

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$$
$$i = 18,17,16, \dots ,1 \; uchun \; x_i = x_{i-1}$$
$$x_0 = t$$

Shunga o‘xshash, $Y \; va \; Z$ registrlar uchun ham quyidagilarni yozish mumkin:

$$t = y_{20} \oplus y_{21}$$
$$i = 21,20,19, \dots ,1 \; uchun \; y_i = y_{i-1}$$
$$y_0 = t$$

va

$$t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$$
$$i = 22,21,20, \dots ,1 \; uchun \; z_i = z_{i-1}$$
$$z_0 = t$$

Berilgan uchta bit x, y va z uchun $maj(x, y, z)$ funksiya qiymati eng ko‘p bitga teng bo‘ladi. Masalan, agar $x, y \; va \; z$ bitlar 0 ga teng bo‘lsa, u holda funksiyaning qiymati 0 ga teng bo‘ladi. Funksiyaga kiruvchi bitlar toq bo‘lgani uchun, funksiya har doim 0 ni yoki 1 ni qaytaradi. Boshqa holatlar bo‘lmaydi.

A5/1 shifrida, ketma-ketlikning har bir bitini generatsiyalash uchun quyidagilar bajariladi. Dastlab, $m = maj(x_8, y_{10}, z_{10})$ funksiya qiymati hisoblanadi. So‘ngra X, Y va Z registrlar quyidagicha sijitiladi (yoki siljitilmaydi):

- agar $x_8 = m$ ga teng bo‘lsa, X siljitiladi;
- agar $y_{10} = m$ ga teng bo‘lsa, Y siljitiladi;
- agar $z_{10} = m$ ga teng bo‘lsa, Z siljitiladi.

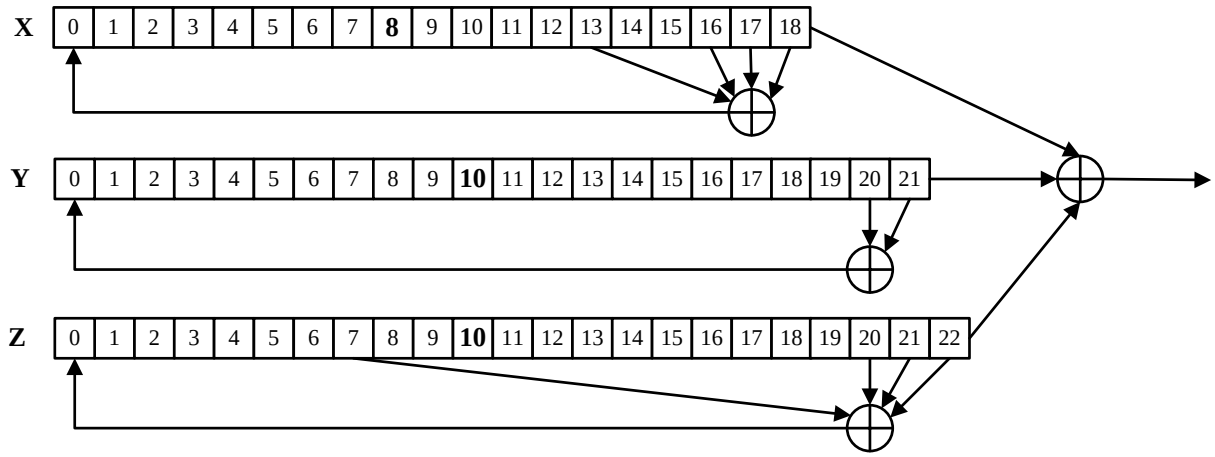
Ketma-ketlikning bir biti s quyidagicha generatsiyalanadi:

$$s = x_{18} \oplus y_{21} \oplus z_{22}$$

Yuqorida keltirilgan ketma-ketlik amallari talab etilguncha takrorlanadi (ochiq matn yoki shifrmatn uzunligiga teng).

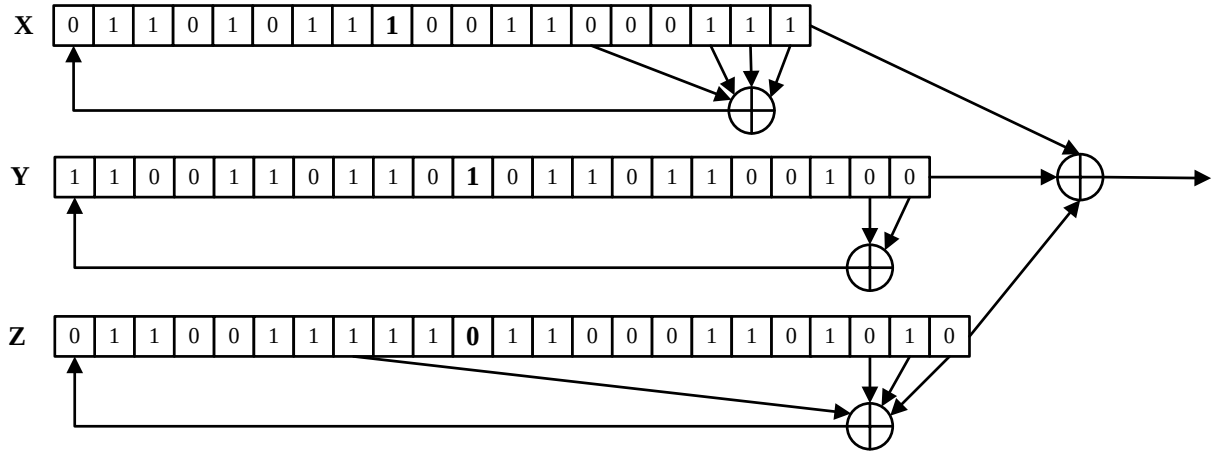
Agar biror registr siljitilsa, uning to‘liq holati o‘zgaradi. Ketma-ketlikning bir bitini hosil qilishda uchta registrdan kamida ikkitasi siljiydi va shuning uchun yuqoridagi ketma-ketlikni davom ettirgan holda yangi bitlar ketma-ketligini hosil qilish mumkin.

A5/1 oqimli shifrlash algoritmi murakkab ko‘rinsada, qurilmada amalga oshirilganida yuqori tezlik qayd etiladi. Umumiy holda A5/1 oqimli shifrni 3.4 - rasmdagi kabi ifodalash mumkin.



3.4 -rasm. A5/1 ketma-ketlik generatorining umumiy ko‘rinishi

Misol. Faraz qilaylik, 64 bitli kalit K ni X, Y va Z registrlariga bo‘lib yozish natijasi quyidagicha bo‘lsin (3.5 - rasm).



3.5 - rasm. X, Y va Z registrlarining dastlabki holati

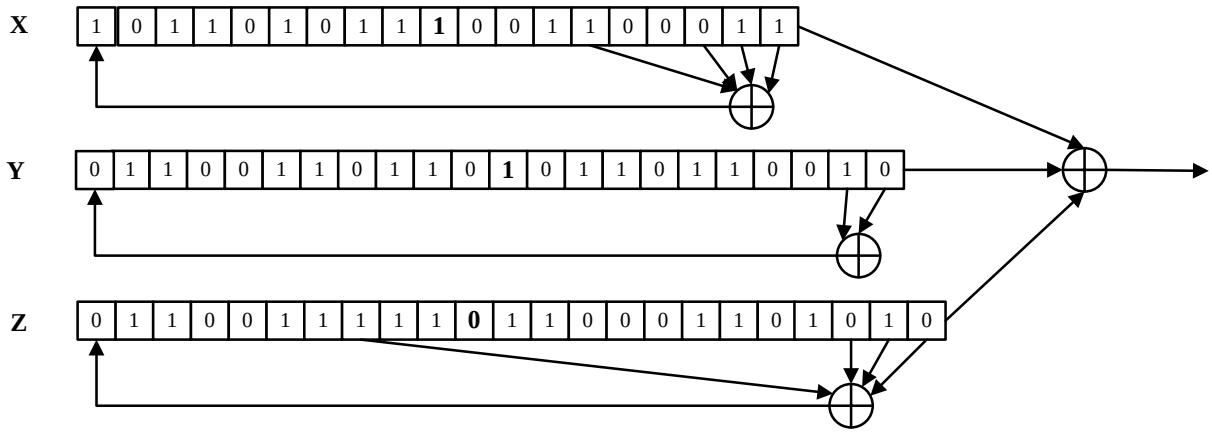
Mazkur holda $maj(x_8, y_{10}, z_{10}) = maj(1,1,0) = 1$ va bu $X\ va\ Y$ registrlar siljishini ko‘rsatadi. Shuning uchun,

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18} = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$
$$i = 18,17,16, \dots ,1\ uchun\ x_i = x_{i-1}$$
$$x_0 = 1$$

Shunga o‘xshash, Y registr uchun ham quyidagilarni yozish mumkin:

$$t = y_{20} \oplus y_{21} = 0 \oplus 0 = 0$$
$$i = 21,20,19, \dots ,1\ uchun\ y_i = y_{i-1}$$
$$y_0 = 0$$

$X\ va\ Y$ registrlar siljiganidan keyingi holat quyidagicha (3.6 - rasm):



3.6 - rasm. X, Y va Z registrlarining siljiganidan keyingi holati

Siljigan holatdan so‘nggi registrlar holatidan generatsiyalangan bir bit $s = x_{18} \oplus y_{21} \oplus z_{22} = 1 \oplus 0 \oplus 0 = 1$. Shu tartibda talab etilgan bitlar ketma-ketligi generatsiyalanadi.

Hisoblash qurilmalari hozirgi kundagi kabi rivojlanmagan vaqtlarda oqimli shifrlash algoritmlari juda ham mashhur bo‘lgan, hozirgi kunda esa ularning o‘rnini simmetrik blokli shifrlar egallamoqda. Biroq, shunday holatlar mavjudki, oqimli shifrlar shubhasiz zarur bo‘ladi. Masalan, real vaqt tizimlaridan biri GSM tarmog‘ida ma’lumotlarni shifrlashda blokli simmetrik shifrlarni qo‘llashning imkoni yo‘q. Sababi, shifrlash uchun zarur bo‘lgan bir blokni (blok uzunligi kamida 64 bit bo‘ladi) ma’lum vaqtda to‘plash talab etiladi. Bu esa so‘zlashuvda to‘xtalishlarga olib keladi. Bundan tashqari, ma’lumotni shifrlab uzatish jarayonida

shifrmatnda bo‘lgan o‘zgarishga (tashqi ta’sirlar natijasida) simmetrik oqimli shifrlash bardoshli sanaladi. Masalan, oqimli shifrlashda shifrmatndagi bir bitning o‘zgarishi ochiq matnning ham bir bitining o‘zgarishiga olib keladi. Simmetrik blokli shifrlarda esa bir bitning o‘zgarishi bir blokning (masalan, 64 bit) o‘zgarishiga olib keladi. Bundan tashqari, simmetrik oqimli shifrlash, blokli shifrlarga qaraganda, kichik qurilmalarda amalga oshirilishi mumkin.

Blokli simmetrik shifrlash algoritmlari. Takroriy amalga oshiriluvchi blokli shifrlash ochiq matnni cheklangan uzunlikdagi bloklarga ajratadi. Aksariyat blokli simmetrik shifrlarda, shifrmatn ochiq matnni funksiya F ning biror miqdordagi *raund*lar soni davomida takroran bajarilishi natijasida olinadi. Oldingi raunddan chiqqan natija va kalit K ga asoslangan F funksiya – *raund funksiyasi* deb nomlanadi. Bunday nomlanishiga asosiy sabab, uni ko‘plab raundlar davomida bajarilishidir.

Blokli simmetrik shifrlarni yaratishdan asosiy maqsad – xavfsizlik va samaradorlikga erishish. Xavfsiz yoki samarali bo‘lgan blokli shifrlarni yaratish murakkab muammo emas. Biroq, ham xavfsiz ham samarali bo‘lgan simmetrik blokli shifrlarni yaratish – *san’at*.

Simmetrik blokli shifrlarni yaratishda ko‘plab *tarmoqlardan* foydalaniladi. Quyidagi tarmoqlar amalda keng qo‘llaniladi:

1. Feystel tarmog‘i.
2. SP (Substitution – Permutation network) tarmoq.
3. Lai-Messey tarmog‘i.

Feystel tarmog‘i - aynan bir blokli shifr hisoblanmay, simmetrik blokli shifrlashning umumiy prinsipi. Feystel tarmog‘iga ko‘ra ochiq matn bloki P ikkita teng chap va o‘ng qismlarga bo‘linadi:

$$P = (L_0, R_0),$$

va har bir raund $i = 1,2, \dots, n,$ uchun yangi chap va o‘ng tomonlar quyidagi qoidaga ko‘ra hisoblanadi:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Bu yerda, K_i kalit i – raund uchun *qismkalit* (raund kaliti) hisoblanadi. Qismkalitlar esa o‘z navbatida kalit K dan biror *kalitni generatsiyalash* algoritmi yordamida hisoblanadi. Yakuniy, shifrmatn bloki C oxirgi raund natijasiga teng bo‘ladi, ya’ni:

$$C = (L_n, R_n).$$

Feystel tarmog‘ida rasshifrovkalash XOR amalining “sehrgarligi”ga asoslanadi. Ya’ni, $i = n, n-1, \dots, 1$ lar uchun quyidagi tenglik amalga oshiriladi:

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus F(R_{i-1}, K_i)$$

Oxirgi raund natijasi, rasshifrovkalangan matnni beradi: $P = (L_0, R_0)$.

Feystel tarmog‘ida har bir raundda foydalaniluvchi F funksiyasining qaytariluvchi (teskari funksiyasiga ega) bo‘lishi talab etilmaydi. Biroq, olingan har qanday F funksiya to‘liq xavfsiz bo‘la olmaydi. Simmetrik blokli shifrlarga AES, DES, GOST R 28147-89, O‘z Dst 1105:2009, IDEA, Blowfish va h. misol bo‘la oladi.

Simmetrik kriptotizimlardagi muammolar. Simmetrik shifrlash tizimlari ma’lumotni shifrlashda va rasshifrovkalashda aynan bir kalitdan foydalanadi. Bu esa tarmoq bo‘ylab shifrlangan ma’lumotni uzatishdan oldin shifrlash kalitini uzatishni taqozo etadi. Boshqacha aytganda, *kalitlarni tomonlar orasida xavfsiz uzatish* simmetrik kriptotizimlar oldidagi asosiy muammo sanaladi.

Bundan tashqari, bir foydalanuvchining, qolganlari bilan ma’lumot almashishida, ularning har biri bilan alohida kalitlarga ega bo‘lishi talab etiladi. Bu esa foydalanuvchiga ko‘p sonli kalitlarni xavfsiz saqlash zaruriyatini keltirib chiqaradi.

Simmetrik kriptotizimlarda kalit uzunligi. Amalda kriptografik tizimlarning kalit uzunligiga qat’iy talablar qo‘yiladi. Ushbu talablar vaqt o‘tishi bilan hisoblash qurilmalari imkoniyatining o‘zgarishiga bog‘liq holda o‘zgarib boradi. Kriptotizimlarda foydalanilgan kalitni joriy vaqtdagi hisoblash qurilmalari orqali hisoblab topishning imkoniyati bo‘lmasligi zarur. Bu yerda kalitni topish deganda biror uzunlikdagi kalitni bo‘lishi mumkin bo‘lgan barcha variantlarini hisoblab chiqish nazarda tutiladi. Masalan, kalit uzunligi 4 bitga teng bo‘lsa, u holda bo‘lishi mumkin bo‘lgan variantlar soni $2^4 = 16$ ga teng bo‘ladi yoki, umumiy qilib aytganda, n bitli kalitlarni bo‘lishi mumkin bo‘lgan variantlari 2^n ga teng bo‘ladi.

Hozirgi kunda simmetrik kriptotizimlarda foydalaniluvchi kalitlarning uzunligi kamida 128 bitli bo‘lishi zarur. 3.3-jadvalda turli uzunlikdagi kalitlarning bo‘lishi mumkin bo‘lgan barcha variantlarini

hisoblash uchun turli qiymatli qurilmalardan foydalanilganida sarflanadigan vaqt ko‘rsatilgan. Ko‘rsatilgan natijalar 2005 yildagi narx asosida keltirilgan.

3.3-jadval

Turli uzunlikdagi kalitlarning barcha variantlarini hisoblash vaqtlari

Kalit uzunligi / **Qurilma narxi**	**80 bit**	**112 bit**	**128 bit**
10 000 $	7 000 yil	10^{13} yil	10^{18} yil
100 000 $	700 yil	10^{12} yil	10^{17} yil
1 000 000 $	70 yil	10^{11} yil	10^{16} yil
10 000 000 $	7 yil	10^{10} yil	10^{15} yil
100 000 000 $	245 kun	10^{9} yil	10^{14} yil

3.3. Ochiq kalitli kriptotizimlar

Simmetrik kriptotizimlardagi mavjud muammolardan biri – maxfiy kalitni xavfsiz uzatish va saqlash. Quyida kalitlarni uzatish va xavfsiz saqlash bilan bog‘liq muammolar bartaraf etilgan, asimmetrik yoki ochiq kalitli deb ataluvchi kriptotizimlar xususida so‘z boradi.

Ochiq kalitli kriptotizimlarda ma’lumotlarni shifrlash bir kalit bilan amalga oshirilsa (ochiq kalit deb ataladi), uni rasshifrovkalash boshqa bir kalit (shaxsiy kalit deb ataladi) bilan amalga oshiriladi. Shuning uchun, ochiq kalitli kriptotizimlarda simmetrik kriptotizimlarda mavjud bo‘lgan kalitlarni taqsimlash muammosi bartaraf etilgan. Biroq, ochiq kalitli kriptografik tizimlarning ham o‘ziga xos muammolari mavjud.

Ochiq kalitli kriptotizimlarni yaratishda *“qopqonli” bir tomonlama funksiyalarga* asoslaniladi. Bu o‘rinda “bir tomonlama” iborasining ma’nosi – funksiya bir tomonlama osonlik bilan hisoblanadi. Biroq, ushbu funksiyani teskarisini hisoblash juda ham murakkab (ya’ni, hisoblash mumkin emas). Bu yerda “qopqonli” deyilishiga asosiy sabab, hujumchi ochiq axborotdan (masalan, ochiq kalit) shaxsiy axborotni (masalan, shaxsiy kalitni) tiklashda foydalana olmaydi. Mazkur bir tomonlama funksiyalarga misol sifatida *faktorlash* amalini ko‘rsatish mumkin. Ya’ni, tub bo‘lgan ikkita p va q sonlarni generatsiyalash va $N = p * q$ ni hisoblash oson. Biroq, N soni yetarlicha katta bo‘lganida uni ikkita tub sonning ko‘paytmasi shaklida ifodalash murakkab vazifa va u yuqori hisoblash imkoniyatini talab etadi.

Simmetrik kalitli shifrlarda ochiq matn P shifrlansa, shifrmatn C hosil bo‘ladi degan shartli belgilash kiritilgan edi. Ochiq kalitli shifrlash tizimlarida esa xabar M shifrlansa, shifrmatn C hosil bo‘ladi deb shartli belgilash kiritiladi.

Ochiq kalitli kriptografik tizimlardan foydalanish uchun, B tomon *ochiq kalit* va unga mos bo‘lgan *shaxsiy kalit* juftiga ega bo‘lishi talab etiladi. B tomonning ochiq kaliti kimga ma’lum bo‘lsa, u ma’lumotni shifrlashi mumkin. Shifrlangan xabarni ochish faqat shaxsiy kalit egasi bo‘lgan B tomonga joiz.

Modul arifmetikasi. Ochiq kalitli kriptotizimlar, asosan modul arifmetikasiga asoslangani bois, dastlab unga to‘xtalib o‘tiladi.

Har qanday butun sonni $m \in z$ ga bo‘lsak, bu songa tayin bir qoldiq to‘g‘ri keladi. Masalan, $\frac{5}{2} = 2 * 2 + 1$ bo‘lib, unda qoldiq 1 ga va butun qism 2 ga teng bo‘ladi. Kriptografiyada a sonni b songa bo‘lgandagi qoldiq r ga teng bo‘lsa, u quyidagicha belgilanadi: $amodb \equiv r$. Dasturlash tillarida esa $a\%b$ kabi belgilanadi.

Quyida qoldiq arifmetikasiga oid bir qancha misollar keltirilgan:

- $7mod3 \equiv (3 * 2)mod3 + 1mod3 \equiv 0 + 1 \equiv 1;$
- $14mod3 \equiv (3 * 4)mod3 + 2mod3 \equiv 0 + 2 \equiv 2;$
- $2mod3 \equiv (0 * 3)mod3 + 2mod3 \equiv 2;$
- $5mod7 \equiv 5;$
- $-2mod5 \equiv (-2 + 5)mod5 \equiv 3mod5 \equiv 3;$
- $-7mod3 \equiv (-7 + 3)mod3 \equiv -4mod3 \equiv (-4 + 3)mod3 \equiv -1mod3 \equiv (-1 + 3)mod3 \equiv 2.$

Bundan tashqari ochiq kalitli kriptografiyada sonning modul bo‘yicha teskarisini hisoblash muhim hisoblanadi. Masalan, odatiy matematikada a sonining teskarisi $\frac{1}{a}$ ga teng bo‘lsa, modul arifmetikasida esa a sonining n modul bo‘yicha teskarisi $a^{-1}modn$ ko‘rinishida belgilanadi. Odatiy matematikada sonni uning teskarisiga ko‘paytmasi birga teng bo‘lgani kabi, modul arifmetikasida ham soning uning teskarisiga moduldagi ko‘paytmasi birga teng bo‘ladi. Ya’ni, $a^{-1}modn \equiv b$ bo‘lsa, u holda $(a * b)modn \equiv 1$ tenglik o‘rinli bo‘ladi.

Izoh. Kriptografiyada modul sifatida (ya’ni, bo‘luvchi) faqat tub sonlardan foydalanish talab etiladi. Ya’ni, amodn tenglikdagi n har doim tub bo‘lishi lozim.

Aytaylik, 3 sonining 7 moduldagi teskarisini topish talab etilsin. Ya'ni, x ni topish talab etilsin: $3^{-1} mod 7 \equiv x$. Yuqoridagi tenglik $(3 * x) mod 7 \equiv 1$ dan foydalanib, x ning o'rniga son qo'yib natijani hisoblash mumkin. Lekin ushbu jarayon ko'p vaqt talab etadi (ayniqsa katta sonlarda).

RSA algoritmi. RSA nomi algoritmni yaratuvchilari familiyalarining birinchi harflaridan olingan (Rivest, Shamir va Adleman). RSA algoritmi modul arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan.

RSA algoritmida ochiq va shaxsiy kalitlar juftini generatsiyalash uchun ikkita katta uzunlikdagi p va q sonlari tanlanadi va ularning ko'paytmasi hisoblanadi: $N = p * q$. Shundan so'ng $\varphi(N) = (p-1) * (q-1)$ bilan o'zaro tub bo'lgan, e soni tanlanadi ($\varphi(N)$ funksiya ma'nosi quyida keltirilgan). Shundan so'ng $\varphi(N)$ modulda e sonining teskarisi hisoblanadi va u d ga teng bo'ladi. Shundan so'ng, ikkita tub sonning ($p\ va\ q$) ko'paytmasi N va $ed = 1\ mod\ \varphi(N)$ shartni qanoatlantiruvchi e va d sonlari mavjud. Shundan so'ng, $p\ va\ q$ lar esdan chiqariladi (o'chirib tashlanadi).

Bu yerda, N modul hisoblanib, (N, e) ochiq kalit juftini va d maxfiy kalitni tashkil etadi. RSA algoritmida shifrlash va rasshifrovkalash modul bo'yicha darajaga oshirish asosida bajariladi. RSA algoritmida shifrlash uchun M xabarni son ko'rinishida ifodalash talab etiladi va N modul bo'yicha e darajaga ko'tariladi, ya'ni

$$C = M^e\ mod\ N.$$

C ni rasshifrovkalash uchun uni N modul bo'yicha shaxsiy kalit d darajaga ko'tarish talab etiladi:

$$M = C^d\ mod\ N.$$

Boshqacha aytganda, RSA algoritmida xabar ochiq kalit bilan shifrlansa va shaxsiy kalit bilan rasshifrovkalansa, $M = C^d\ mod\ N = M^{ed}\ mod\ N$ tenglikning to'g'riligini isbotlash zarur.

Aytaylik, RSA algoritmida ma'lumotni shifrlash va rasshifrovkalash amallarini tanlab olingan ($p = 11\ va\ q = 3$) "katta" sonlar ustida amalga oshirish talab qilinsin. Mazkur holda modul $N = p * q = 33$ ga teng bo'ladi va $\varphi(N) = (p-1)(q-1) = 20$ ga

teng bo‘ladi. U holda shifrlash uchun zarur bo‘lgan daraja e ni (3) ga teng deb olish mumkin. Sababi, 3 soni $\varphi(N) = 20$ bilan o‘zaro tubdir. Shundan so‘ng, Evklidning kengaytirilgan algoritmi asosida rasshifrovkalash kaliti $d = 7$ aniqlanadi. Ya’ni, $ed = 3 * 7 = 1\ mod\ 20$. U holda A tomonning ochiq kalit jufti $N, e = 33, 3$ va shaxsiy kaliti d esa 7 ga teng bo‘ladi.

Shundan so‘ng, A tomon o‘zining ochiq kalitini barchaga uzatadi. Biroq, shaxsiy kalitini maxfiy saqlaydi.

Faraz qilaylik, B tomon A tomonga $M = 15$ ma’lumotni shifrlab yubormoqchi. Buning uchun B tomon A tomonning ochiq kaliti juftini $N, e = 33{,}3$ oladi va shifrmatnni quyidagicha hisoblaydi:

$$C = M^e\ mod\ N = \ 15^3 = 3375 = 9\ mod\ 33$$

va uni A tomonga yuboradi.

A tomon $C = 9$ shifrmatnni rasshifrovkalash uchun shaxsiy kalit $d = 7$ dan foydalanadi:

$$M = C^d\ mod\ N = 9^7 = 4782969 = 144938 * 33 + 15 = 15\ mod\ 33$$

Agar RSA algoritmida kichik tub sonlardan ($p\ va\ q\ uchun$) foydalanilgan taqdirda, hujumchi ochik bo‘lgan N ni osonlik bilan ikkita tub sonning ko‘paytmasi ko‘rinishida yozishi mumkin. Shundan so‘ng, ochiq kalitning ikkinchi qism e dan foydalangan holda, shaxsiy kalit d ni hisoblay oladi. Shuning uchun RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida 2048 bit bo‘lishi talab etiladi. Bundan tashqari, RSA algoritmini buzish faqat faktorlash muammosiga bog‘liqligi isbotlanmagan.

Ochiq kalitli kriptotizimlardan foydalanish. Ochiq kalitli kriptografik tizimlardan foydalanish masalasini ko‘rib chiqishda quyidagi belgilashlar kiritiladi:

A tomonning ochiq kaliti bilan xabar M ni shifrlash: $C = \{M\}_A$.

A tomonning shaxsiy kaliti bilan shifrmatnni rasshifrovkalash: $M = [C]_A$.

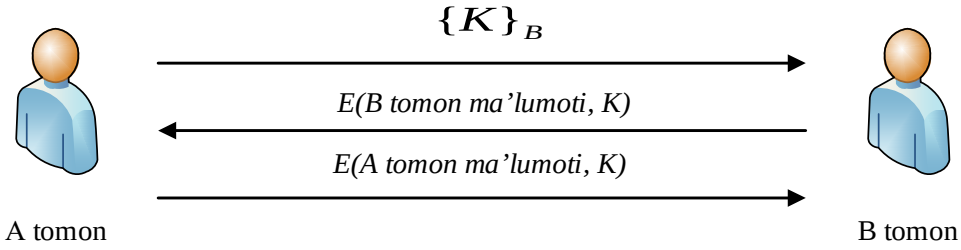
Bundan quyidagi tenglikni osongina yozish mumkin: $[\{M\}_A]_A = M$. Boshqacha aytganda, M xabarni A tomonning ochiq kaliti bilan shifrlab, keyin aynan shu tomonning shaxsiy kaliti bilan rasshifrovkalash amalga oshirilsa, yana dastlabki xabar hosil bo‘ladi.

Simmetrik shifrlar bilan bajarilgan ixtiyoriy amalni, ochiq kalitli shifrlash algoritmlari bilan ham amalga oshirish mumkin. Masalan, tarmoqda ma’lumotlarni uzatishda va xavfsiz bo‘lmagan muhitda axborot konfidensialligini ta’minlashda simmetrik shifrlash algoritmlarining o‘rniga ochiq kalitli kriptografik tizimlardan foydalanish mumkin. Biroq, jarayon ko‘proq vaqt talab etadi.

Bundan tashqari, simmetrik kriptotizimlar kabi ochiq kalitli kriptotizimlardan ham ma’lumotlarning yaxlitligini ta’minlashda foydalanish mumkin.

Ochiq kalitli kriptotizimlar simmetrik kriptotizimlarda mavjud kalitni taqsimlash muammosini o‘zida bartaraf etgan. O‘z o‘rnida simmetrik kriptotizimlar ochiq kalitli kriptotizimlarga qaraganda samaradorligi bilan ajralib turadi. Boshqacha aytganda, shifrlash va rasshifrovkalash amallari simmetrik kriptotizimlarda, ochiq kalitli shifrlash algoritmlariga nisbatan, tezroq amalga oshiriladi.

Har ikkala kriptotizimning afzalliklarini birlashtirish imkoniyati mavjudmi? Ya’ni, ma’lumotni shifrlashda yuqori samaradorlikka ega va kalitlarni taqsimlash muammosi bo‘lmagan kriptotizimni yaratish mumkinmi? Albatta, buning imkoniyati mavjud va bunday tizimlar *gibrid* kriptotizimlar deb ataladi. Gibrid kriptotizimlarda simmetrik shifrlash algoritmining kaliti ochiq kalitni shifrlash orqali yetkazilsa, ma’lumotlarning o‘zi esa simmetrik shifrlash orqali himoyalanadi. Gibrid kriptotizim sxemasi 3.7-rasmda aks ettirilgan.



3.7-rasm. Gibrid kriptotizim

Ochiq kalitli kriptotizimlarda kalit uzunligi. Simmetrik kalitli kriptotizimlarda bo‘lgani kabi ochiq kalitli kriptotizimlarda ham real hayotda foydalanish uchun kalit uzunligiga talablar qo‘yiladi. Yuqorida simmetrik kriptotizimlar uchun ushbu masala bilan tanishib o‘tilgan edi. Simmetrik va ochiq kalitli kriptotizimlarning matematik asosi turlicha bo‘lgani bois, ular bir xil bardoshlik darajasida bo‘lganida turli kalit uzunliklariga ega bo‘ladilar (3.4-jadval).

3.4-jadval

Bir xil bardoshlikka ega simmetrik va ochiq kalitli kriptotizimlar kalitlarining uzunligi

Simmetrik shifrlash algoritmi	**RSA algoritmi (*p va q sonlari*)**
56 bit	512 bit
80 bit	1024 bit
112 bit	2048 bit
128 bit	3072 bit
192 bit	7680 bit
256 bit	15360 bit

Simmetrik kriptotizimlarda bo‘lgani kabi ochiq kalitli kriptotizimlarda ham kalitlarni barcha variantlarini hisoblash qurilmalar imkoniyatiga bog‘liq. Ya’ni, hozirgi kunda yetarli deb qaralgan kalit uzunligi, 10 yildan keyin tavsiya etilmasligi mumkin. Chunki, 10 yil davomida hisoblash qurilmalarining imkoniyatlari hozirgi kundagi kabi bo‘lmaydi.

3.5-jadvalda RSA algoritmidagi N modulning turli uzunligida faktorlash uchun talab etilgan vaqt qiymatlari ko‘rsatilgan. Bunda natijalar bir sekundda million amal bajaruvchi (*one-million-instruction-per-second*, *mips*) kompyuter yoki yiliga 10^{13} amal bajarilishi hisobida olingan. Faktorlash algoritmi sifatida GNFS (general number field sieve) dan foydalanilgan.

3.5-jadval

RSA algoritmidagi N modulning turli uzunligida faktorlash uchun talab etiladigan vaqt qiymatlari

N ning bitdagi uzunligi	**Talab etiluvchi yillar**
512	30 000
768	$2*10^8$
1024	$3*10^{11}$
1280	10^{14}
1536	$3*10^{16}$
2048	$3*10^{20}$

Yuqorida keltirilgan ma’lumotlardan ko‘rish mumkinki, hisoblash qurilmalari imkoniyatining ortishi kriptografik algoritmlarning bardoshligini kamayishiga olib keladi. Bu har ikkala simmetrik va ochiq kalitli kriptotizimlarga taalluqli.

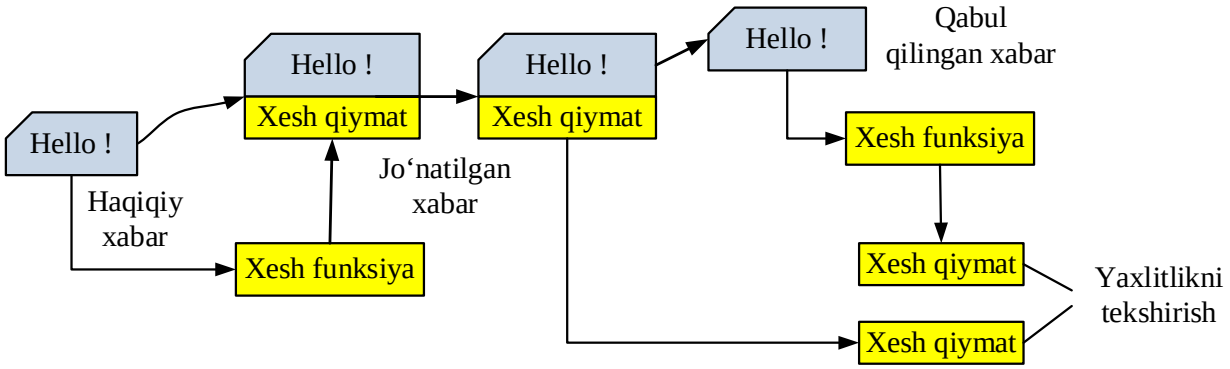
3.4. Ma’lumotlar yaxlitligini ta’minlash usullari

Yuqorida keltirilgan har ikkala shifrlash algoritmidan (simmetrik va ochiq kalitli) faqat ma’lumotlarning konfidensialligini ta’minlashda foydalanish xususida aytib o‘tildi. Quyida esa ulardan ma’lumotlarning yaxlitligini tekshirishda foydalanish masalasi bilan tanishib o‘tiladi.

Xesh funksiya. Xesh funksiya chekli alfavitdagi uzunligi chekli kirish yo‘li so‘zini berilgan, odatda qat’iy uzunlikdagi, so‘zga akslantiruvchi funksiya. Xesh funksiya quyidagi xususiyatlarga ega:

1. Ixtiyoriy uzunlikdagi matnga qo‘llash mumkin.
2. Chiqishda tayinlangan uzunlikdagi qiymat shakllanadi.
3. Berilgan ixtiyoriy x bo‘yicha $h(x)$ oson hisoblanadi.
4. Berilgan ixtiyoriy H bo‘yicha $h\,(x) = N$ tenglikdan x ni hisoblab topib bo‘lmaydi (bir tomonlilik xossasi).
5. Olingan x va $y \neq x$ matnlar uchun $h(x) \neq h(y)$ bo‘ladi (kolliziyaga bardoshlilik xossasi).

Xesh funksiya yordamida uzatilayotgan ma’lumotlar yaxlitligini tekshirishning sodda ko‘rinishi 3.8-rasmda keltirilgan. Jo‘natuvchi xabarning xesh qiymatini hisoblaydi va uni qabul qiluvchiga xabar bilan birgalikda yuboradi. Qabul qiluvchi dastlab xabarning xesh qiymatini hisoblaydi va qabul qilingan xesh qiymat bilan taqqoslaydi. Agar har ikkala xesh qiymat teng bo‘lsa, ma’lumotning yaxlitligi o‘zgarmagan, aks holda o‘zgargan deb topiladi. Odatda xesh funksiya kirishda ma’lumotdan tashqari xech qanday qiymatni talab etmagani bois, *kalitsiz kriptografik funksiyalar* deb ham ataladi (kalit talab qiluvchi ma’lumotlarning yaxlitligini ta’minlash usullari ham mavjud).

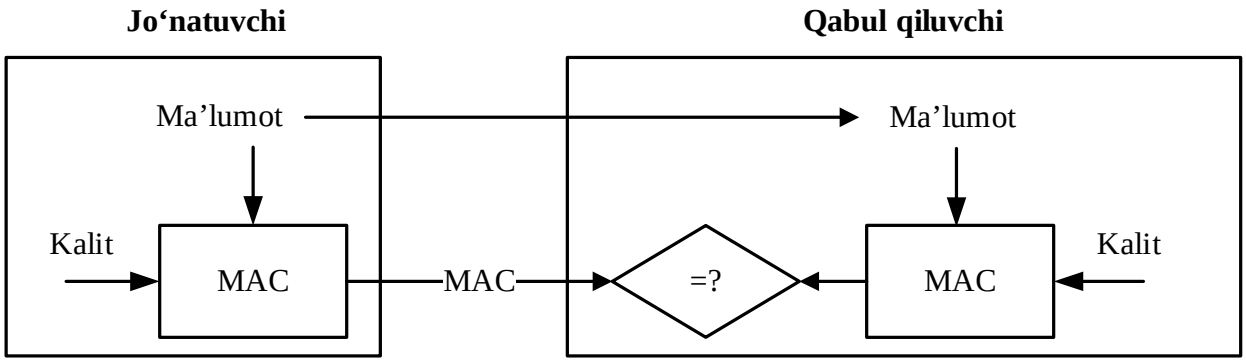


3.8-rasm. Xesh funksiya asosida ma’lumotlar yaxlitligini tekshirish

Yuqorida keltirilgan usulda xavfsizlik muammosi jiddiy bo‘lgani bois, undan amalda foydalanilmaydi. Ya’ni, hujumchi tomonidan faqat ma’lumot o‘zgartirilgan holda yaxlitlikni tekshirish imkoniyati mavjud.

Biroq, hujumchi ma’lumotning xesh qiymatini almashtirish orqali foydalanuvchini osonlik bilan ma’lumot yaxlitligiga ishontirishi mumkin.

Ushbu muammoni bartaraf etuvchi – *xabarlarni autentifikatsiyalash kodi (message authentication code, MAC)* tizimlari mavjud bo‘lib, unga ko‘ra biror maxfiy kalit asosida ma’lumotning xesh qiymati hisoblanadi (3.9-rasm).



3.9-rasm. MAC tizimi

MAC tizimini ishlab chiqishda blokli shifrlardan ham foydalanish mumkin. Buning uchun blokli shifrni CBC (Cipher Block Chaining – shifr bloklar zanjiri) rejimida foydalanish va eng oxirgi shifrmatn blokini olishning o‘zi yetarli (qolganlari tashlab yuboriladi).

Albatta, mazkur usul MAC tizimini yaratishning yagona usuli emas. Quyida xesh funsiyalar asosida MAC tizimini yaratish bilan tanishib chiqiladi.

Xesh – funksiyalar asosida ma’lumot yaxlitligini tekshirish. Yuqorida M ma’lumot yaxlitligini tekshirishda $h(M)$ ni hisoblash va qabul qiluvchiga $M, h(M)$ ni yuborish orqali amalga oshirishning kamchiligi haqida aytib o‘tilgan edi. Shuning uchun, amalda xesh funksiyalardan ma’lumot yaxlitligini ta’minlashda bevosita foydalanilmaydi. Boshqacha aytganda, xesh funksiyalar asosida ma’lumot yaxlitligini ta’minlashda hisoblangan xesh qiymatni o‘zgartira olmaslikni kafolatlash maqsad qilinadi. Buni amalga oshirish uchun balki xesh qiymatni simmetrik kalitli shifrlar asosida shifrlash zarurdir (ya’ni, $E(h(M), K)$). Biroq, buni amalga oshirishning soddaroq usuli – *xeshlangan MAC* (hashed MAC yoki HMAC) usuli mavjud. Bu usulga ko‘ra, xesh qiymatni shifrlashning o‘rniga, xesh qiymatni hisoblash jarayonida kalitni bevosita ma’lumotga biriktirish amalga oshiriladi. HMAC tizimida kalitlar qanday biriktiriladi? Umumiy holda ikki usul: kalitni matnni oldidan qo‘yish ($h(K, M)$) yoki kalitni matndan keyin

qo‘yish ($h(M,K)$) mavjud bo‘lsada, ularning har ikkalasida jiddiy xavfsizlik muammosi mavjud.

Xesh funksiyalar ham simmetrik kriptotizim hisoblanadi va simmetrik blokli shifrlash kabi ma’lumotlarni xeshlashda bloklarga ajratiladi. Odatda aksariyat xesh funksiyalar uchun (masalan, MD5, SHA1, Tiger) blok uzunligi 64 baytga yoki 512 bitga teng.

HMAC tizimida kalit ma’lumotga quyidagicha biriktiriladi. Dastlab xesh funksiyadagi blokning uzunligi baytlarda aniqlanadi. Masalan. MD5 xesh fuknsiyasida blok uzunligi $B = 64$ baytga teng bo‘lsin. Olingan kalit (K) uzunligi ham blok uzunligiga keltiriladi. Bunda 3 ta holat bo‘lishi mumkin: (1) agar kalitning uzunligi 64 baytga teng bo‘lsa, hech qanday o‘zgarish amalga oshirilmaydi, (2) agar kalitning uzunligi 64 dan kichik bo‘lsa, u holda yetmagan baytlar o‘rni nollar bilan to‘ldiriladi, (3) agar kalit uzunligi blok uzunligidan katta bo‘lsa, kalit dastlab xeshlanadi va hosil bo‘lgan xesh qiymatning o‘ng tomoni blok uzunligiga yetguncha nollar bilan to‘ldiriladi. Shu tariqa, kalit uzunligi blok uzunligiga moslashtiriladi.

Shunday qilib, ma’lumot va moslashtirilgan kalit asosida HMAC qiymati quyidagicha hisoblanadi:

$$HMAC(M,K) = H\big(K \oplus opad, H(K \oplus ipad, M)\big).$$

Bu yerda, $ipad$ va $opad$ o‘zgaruvchilar quyidagicha hosil qilinadi:

$$ipad = 0x36 \; ni \; B \; marta \; takrorlash \; natijasida$$
$$opad = 0x5c \; ni \; B \; marta \; takrorlash \; natijasida$$

Tenglikdan ko‘rinib turibdiki, HMAC da ikki marta xeshlash amalga oshirilmoqda. Kalit K faqat ikki tomonga (jo‘natuvchi va qabul qiluvchiga) ma’lum bo‘lgani uchun, hujumchi mos xesh qiymatni qayta hisoblay olmaydi. A tomondan yuborilgan ($M, HMAC(M,K)$) ma’lumot juftlaridan hujumchi faqat ma’lumotni o‘zgartirishi mumkin bo‘ladi va bu holat qabul qiluvchi tomonidan osonlik bilan aniqlanadi.

Ochiq kalitli shifrlash algoritmlari asosida ma’lumot yaxlitligini tekshirish va rad-etishdan himoyalash. Quyida ochiq kalitli kriptotizimlar va xesh funksiyalar asosida ishlovchi – *elektron raqamli imzo* tizimi bilan tanishib o‘tiladi. O‘zbekiston Respublikasining Elektron raqamli imzo to‘g‘risidagi qonunida elektron raqamli imzoga quyidagicha ta’rif berilgan:

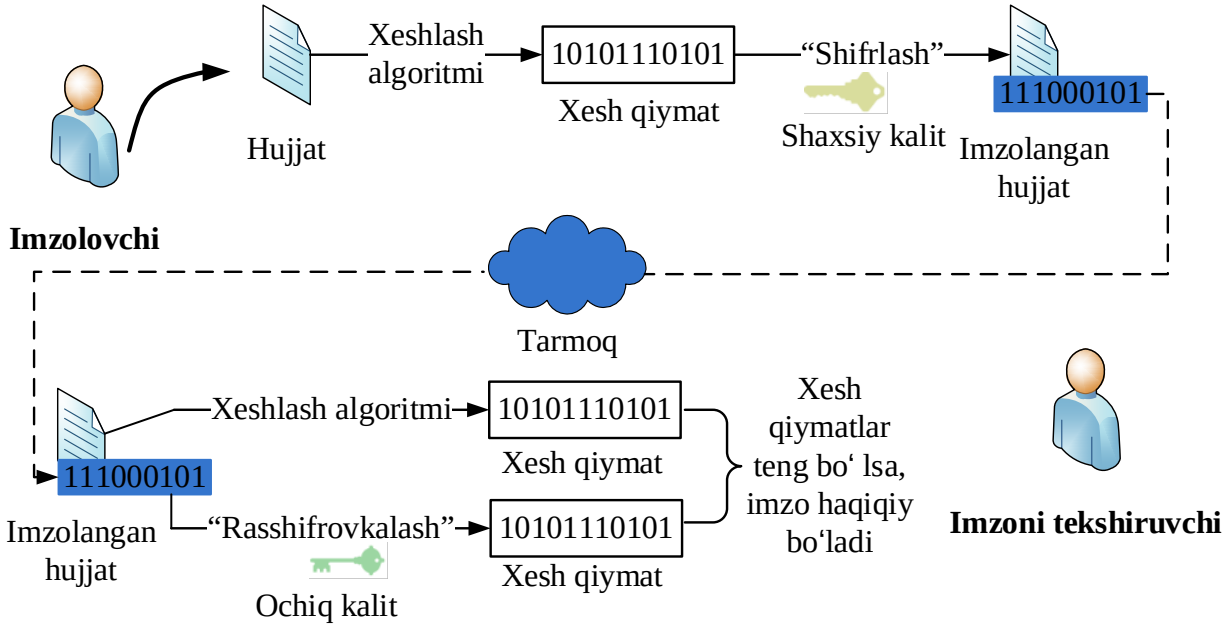
“*Elektron raqamli imzo (ERI)* — elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda, maxsus o‘zgartirish natijasida hosil qilingan, hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo”.

Elektron raqamli imzo oddiy qo‘lda qo‘yiluvchi imzo kabi, faqat elektron hujjatlarda qo‘yiladi va imzo qo‘yilgan ma’lumotning yaxlitligini ta’minlaydi va imzolovchining qo‘yilgan imzodan bosh tortmasligini (rad etmasligini) kafolatlaydi. Axborot xavfsizligida *rad etish* muammosi mavjud, unga ko‘ra foydalanuvchi hujjatni imzolaganini rad etadi (ya’ni, men imzolamadim deb turib oladi). Mazkur muammoni oldini olishda aynan elektron raqamli imzo tizimlaridan foydalaniladi.

Shunday qilib, ERI tizimlari nafaqat ma’lumot yaxlitligini ta’minlaydi, balki imzolovchining majburiyatlardan tonishiga yo‘l qo‘ymaydi (yoki rad etishni oldini oladi). Shu sababli, ERI tizimlari ma’lumotlar yaxlitligini ta’minlovchi simmetrik kriptotizimlarga asoslangan MAC tizimlaridan ajralib turadi.

MAC tizimlarida xesh qiymatni qayta hisoblay olmaslik uchun, matnga kalit biriktirilgan bo‘lsa, ERI tizimlarida ma’lumotning xesh qiymati shaxsiy kaliti bilan “shifrlash” amalga oshiriladi va ERI hosil qilinadi. Ushbu xabarni “rasshifrovkalash” uchun esa tomonning ochiq kalitini bilishning o‘zi yetarli. Demak, oddiy imzo tizimiga o‘xshash (oddiy imzo tizimida bir kishi imzo qo‘yadi va qolganlardan uning haqiqiyligini tekshirish talab etiladi). ERI tizimida ham shaxsiy kalit egasi xabarni imzolaydi, qolganlar esa, uning ochiq kalitidan foydalanib, imzoni haqiqiyligini tekshiradi.

Agar A tomon xabar M ga imzo qo‘ygan bo‘lsa, u holda imzo $S = [M]_A$ shaklida ifodalanadi (xuddi ochiq kalitli kriptografiyada shaxsiy kalit bilan rasshifrovkalash kabi). ERI tizimlarini yaratish ikkita muolajadan iborat: *ERIni shakllantirish* va *ERIni tekshirish* (3.10-rasm).



3.10-rasm. Elektron raqamli imzo sxemasi

ERIni shakllantirish jarayoni. Faraz qilaylik, A tomondan M xabarni imzolash talab etilsin. Buning uchun xabar M ning xesh qiymati hisoblanadi: $H = h(M)$. So‘ngra, xabarning xesh qiymati H foydalanuvchining shaxsiy kaliti bilan “shifrlanadi” (bu haqiqiy shifrlash emas, shunchaki shaxsiy kalit bilan H ustida biror amal bajarishdan iborat) va imzo $S = [H]_A$ hosil qilinadi. Hosil qilingan imzo ma’lumotga biriktirilib $\{M, S\}$ qabul qiluvchiga uzatiladi.

ERIni tekshirish jarayoni. Faraz qilaylik, B tomondan M' xabarga qo‘yilgan imzo S ni tekshirish talab etilsin. Buning uchun B tomon dastlab xabar M' ni xesh qiymatini hisoblaydi: $H' = h(M')$. A tomonning ochiq kaliti bilan S ni “rasshifrovkalaydi” (bu haqiqiy rasshifrovkalash emas, shunchaki ochiq kalit bilan S ustida biror amal bajarishdan iborat) va H ni hosil qiladi. Agar ikkala xesh qiymatlar (H va H') o‘zaro teng bo‘lsa, ERI to‘g‘ri deb topiladi (demak xabar yaxlit).

Rad etishdan himoyalashni tushunishdan oldin, MAC asosida yaxlitlikni ta’minlashga biror sodda misol keltiraylik. Faraz qilaylik, A tomon o‘zining dilleriga B tomondan 100 ta aksiyani olishga buyurtma berdi. Berilgan buyurtmani yaxlitligini ta’minlash uchun A tomon B tomon bilan taqsimlangan kalit K_{AB} yordamida MAC ni hisoblaydi. Ma’lum vaqt o‘tganidan so‘ng, buyurtmalar tayyor bo‘ladi. Biroq, A tomon to‘lovni amalga oshirishdan oldin aksiyalarning narxi tushib ketadi. Bu vaqtda, A tomon buyurtmani men bermadim deb turib oladi va

uni rad etadi. Bunga yaxlitlikni ta’minlash uchun hisoblangan MAC ni har ikkala tomon ham hosil qilishi sabab bo‘ladi.

Mazkur holat ERI bilan amalga oshirilsachi? Bunda, A tomon buyurtmani o‘zining shaxsiy kaliti bilan imzolab B tomonga yuboradi. Bu yerda A tomon buyurtmani men bermadim deb rad eta olmaydi. Sababi, buyurtmani imzolash faqat shaxsiy kalit bilan amalga oshiriladi. Shaxsiy kalit esa, faqat A tomonga ma’lum.

Ochiq kalitlar infrastrukturasi (Public key infrastructure, PKI). Ochiq kalitli kriptografiya bilan bog‘liq bo‘lgan muammolardan yana biri - ochiq kalitning kimga tegishli ekanligini aniqlash. Faraz qilaylik, A tomon biror maxfiy xabar M ni B tomonga yubormoqchi. Buning uchun A tomon B tomonning ochiq kalitidan foydalanadi. Biroq, g‘arazli niyatda bo‘lgan C tomon o‘zining ochiq kalitini A tomonga B tomonni ochiq kaliti sifatida taqdim etadi. A tomonni mazkur holatni tekshirish imkoniyati bo‘lmagani bois, unga ishonadi va maxfiy xabarni C tomonning ochiq kaliti bilan shifrlaydi.

Ushbu muammoni oldini olish uchun ochiq kalitli kriptografik tizimlarda *ochiq kalitlar infrastrukturasi*dan foydalaniladi.

Ochiq kalitlar infrastrukturasi yoki PKI real hayotda ochiq kalitli kriptotizimlardan xavfsiz foydalanish uchun talab etiluvchi barcha narsani o‘z ichiga oladi. PKI tarkibidagi barcha narsalarning birgalikda ishlashi juda ham murakkab jarayon, quyida ularning ayrim tashkil etuvchilari va PKI ning asosiy vazifalari bayon etilgan.

Raqamli sertifikat (yoki ochiq kalit sertifikati yoki qisqacha sertifikat) foydalanuvchining ismi va uning ochiq kalitidan iborat (amalda foydalanuvchiga va sertifikatga tegishli ma’lumotlar ham bo‘ladi) va u *sertifikat markazi (certificate authority* yoki *CA)* tomonidan imzolanadi. Masalan, A tomonning sertifikati quyidagidan iborat bo‘ladi:

$$M = (\text{A tomon nomi}, A\ tomonning\ ochiq\ kaliti) \text{ va } S = [M]_{CA}.$$

Ushbu sertifikatni tekshirish uchun B tomon $\{S\}_{CA}$ ni hisoblaydi va M ga tengligini tekshiradi.

CA tomoniga, odatda, *ishonchli uchinchi tomon (trusted third party* yoki *TTP)* sifatida qaraladi. Ya’ni, odatda A tomon foydalanuvchi uchun shaxsiy va ochiq kalitlar juftini generatsiyalaydi. Shaxsiy kalit A tomonga taqdim etilganidan so‘ng, CA dan o‘chirib tashlanadi. Ochiq kalit esa sertifikat shaklida taqdim etiladi. Agar B tomon A tomonga biror

ma’lumotni shifrlab yubormoqchi bo‘lsa, uning sertifikatidan foydalanadi. Buning uchun sertifikatdagi imzoni tekshirish talab etiladi. Bu esa o‘z navbatida B tomonga CA ning ochiq kalitini (ya’ni, unga teng bo‘lgan sertifikatni) bilishi talab etadi. Demak, CA tomonning ochiq kaliti (yoki sertifikati) oldindan foydalanilayotgan tizimda mavjud va bu haqida barcha ma’lumotga ega bo‘ladi.

3.5. Disklarni va fayllarni shifrlash

Axborotni kriptografik himoyasi, xususan, shifrlash algoritmlari amalda keng qo‘llaniladi. Masalan, saqlash qurilmalarida ma’lumotlarni shifrlash yoki tarmoq bo‘ylab uzatiladigan axborotni shifrlab uzatishni misol sifatida keltirish mumkin. Umuman, ma’lumotni shifrlashda ma’lum algoritmdan foydalaniladi. Ushbu algoritm biror bir operatsion tizim (OT) uchun (masalan, Windows OT, Linux OT, Android OT) mo‘ljallangan dastur ko‘rinishida yoki maxsus qurilma ko‘rinishida (masalan, maxsus prosessorlar, USB token, smart karta va h.) bo‘lishi mumkin.

Kriptografik algoritmlar amalda quyidagi ko‘rinishdagi vositalar sifatida qo‘llaniladi:

- apparat-dasturiy ko‘rinishdagi vositalar;
- apparat ko‘rinishdagi vositalar;
- dasturiy ko‘rinishdagi vositalar.

Apparat-dasturiy shifrlash – shifrlash jarayoni bo‘lib, maxsus ishlab chiqilgan hisoblash qurilmasidan foydalaniladi. Unga misol sifatida, ruToken USB shifrator qurilmasini ko‘rsatish mumkin (3.11 - rasm).

3.11-rasm. Turli ko‘rinishdagi ruToken USB shifrator qurilmasi

ruToken USB shifrator qurilmasi – Rossiya Federatsiyasida ishlab chiqariluvchi qurilma bo‘lib, undan asosan Rossiya Federatsiyasining

kriptografik algoritmlarida amalga oshirilgan. Masalan, ishlab chiqarilgan Rutoken S qurilmasining umumiy xarakteristikalari quyidagicha:

- shifrlash kalitlari, ERI kalitlari va turli sertifikatlarni xavfsiz saqlash uchun foydalaniladi;
- ushbu tokendan foydalanish uchun PIN kodni kiritish talab etiladi;
- diskdagi ma’lumotlarni shifrlash uchun qo‘llaniladi;
- tokenda mehmon, foydalanuvchi va ma’mur darajalari mavjud;
- Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/ Vista/2008/XP/2003, GNU/Linux, Apple macOS/OSX muhitlarida foydalanish mumkin;
- 32, 64 va 128 KB xotiraga ega EEPROM;
- USB 1.1 va undan yuqori interfeysga ega;
- 58x16x8mm (mikro-token 17,8x15,4x5,8mm) o‘lchamga ega;
- 6,3g (mikro-token 1,6g) og‘irlikka ega.

Apparat shifrlash o‘ziga xos quyidagi xususiyatlarga ega:

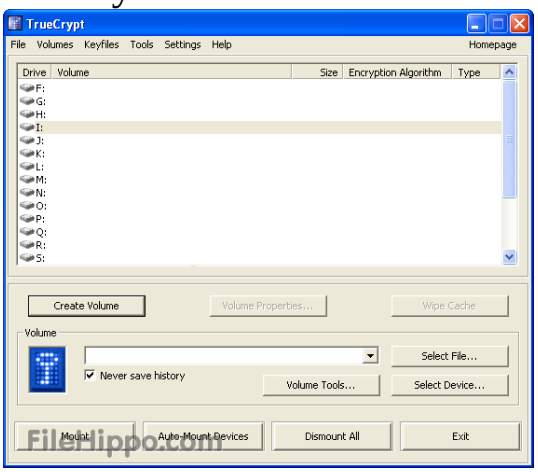
- saqlagichda (qurilmada) joylashgan maxsus prosessordan foydalaniladi;
- prosessorda shifrlash kalitini generatsiyalash uchun maxsus kalit generatori mavjud bo‘lib, foydalanuvchi kiritgan parol asosida qulf yechiladi;
- asosiy tizimdan (qurilma ulangan tizim, masalan, kompyuterdan) shifrlash uchun foydalanmaslik orqali, samaradorlikka erishiladi;
- kalitlar va boshqa maxfiy kattaliklar apparatda shifrlash orqali himoyalangan;
- autentifikatsiya apparat qurilmaga nisbatan amalga oshiriladi;
- o‘rta va katta hajmdagi tashkilotlar sharoitida yuqori iqtisodiy samaradorlik beradi va madadlanishining oddiyligi;
- qurilmada amalga oshiriluvchi doimiy mavjud shifrlash funksiyasi;
- qo‘shimcha drayver yoki dasturlarni o‘rnatishning zaruriyati yo‘q;
- ma’lumotlar keng tarqalgan hujum usullaridan, parolni to‘liq tanlash usuli, zararli dasturni kiritish asosidagi hujumlar va kalitni topishga qaratilgan hujumlardan himoyalangan;
- amalga oshirish, dasturiy vositaga qaraganda, yuqori narx talab etadi.

Dasturiy shifrlash kompyuter vositasi yordamida disklarni, fayllarni, kataloglarni va turli ma’lumot saqlash vositalaridagi axborotni shifrlash va rasshifrovkalash jarayonini amalga oshiradi. Umumiy holda, dasturiy shifrlash vositalarini quyidagi guruhlarga ajratish mumkin:

- diskni shifrlash dasturiy vositalari (Disk encryption software);
- fayl/ katalogni shifrlash dasturiy vositalari (File/folder encryption);
- ma’lumotlar bazasini shifrlash dasturiy vositalari (Database encryption);
- aloqani shifrlash dasturiy vositalari (Communication encryption software).

3.12-rasmda diskni shifrlashda foydalaniluvchi TrueCrypt dasturiy vositasining ko‘rinishi keltirilgan. Ushbu dasturlash vositasi quyidagi xususiyatlarga ega:

- C, C++, Assembly dasturlash tillaridan foydalanib yozilgan;
- Windows, macOS va Linux OTlarida foydalanish mumkin;
- 3.30 MB hajmga ega;
- ushbu dasturiy vositada AES, Serpent va Twofish blokli shifrlash algoritmlaridan foydalaniladi.



3.12-rasm. TrueCrypt dasturiy vositasi

Dasturiy shifrlash o‘ziga xos bo‘lgan quyidagi xususiyatlarga ega:

- shifrlash uchun boshqa dasturlar bilan bir vaqtning o‘zida kompyuter resursidan foydalanadi;
- kompyuterning himoyalanganlik darajasi saqlagichning himoyalanganlik darajasini belgilaydi;
- foydalanuvchi tomonidan kiritilgan paroldan ma’lumotni shifrlash kaliti sifatida foydalaniladi;
- dasturni yangilab turish talab etilishi mumkin;

- katta bo‘lmagan tashkilotlar uchun foydalanish yuqori iqtisodiy samaradorlik beradi;
- ixtiyoriy ma’lumotni saqlash usullari uchun shifrlashni amalga oshirish imkoniyati mavjud;
- parolni to‘liq tanlash hujumiga yoki parolni topishga qaratilgan boshqa hujumlarga bardoshsiz;
- apparat shifrlashga qaraganda kam sarf xarajat talab etadi.

Disk va fayl tizim sathida shifrlash. *Diskni shifrlash.* Bu jarayon turli ma’lumotlarni saqlash vositalarida (qattiq disk, yumshoq disk, USB disk va bosh.) saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi. Bunda diskni shifrlashning apparat-dasturiy yoki dasturiy vositasidan foydalanilib, butun diskdagi yoki uning bir qismidagi (masalan, D disk) har bir bit shifrlanadi. Ushbu jarayonning maqsadi ruxsat etilmagan foydalanishdan nazoratlash.

Butun diskni shifrlash (Full disk encryption (FDE) yoki *whole disk encryption)* deb nomlanuvchi vositalar diskdagi barcha ma’lumotlarni shifrlaydi va bunda faqat operatsion tizimning yuklanishi uchun zarur bo‘lgan sektorlar *(master boot record, (MBR))* shifrlanmaydi. Ba’zi qurilmaga asoslangan diskni shifrlash vositalari (Hardware-based full disk encryption, FDE) esa MBR ni ham shifrlaydi. Bular quyidagi disk ishlab chiqaruvchilar mahsulotlarida mavjud:

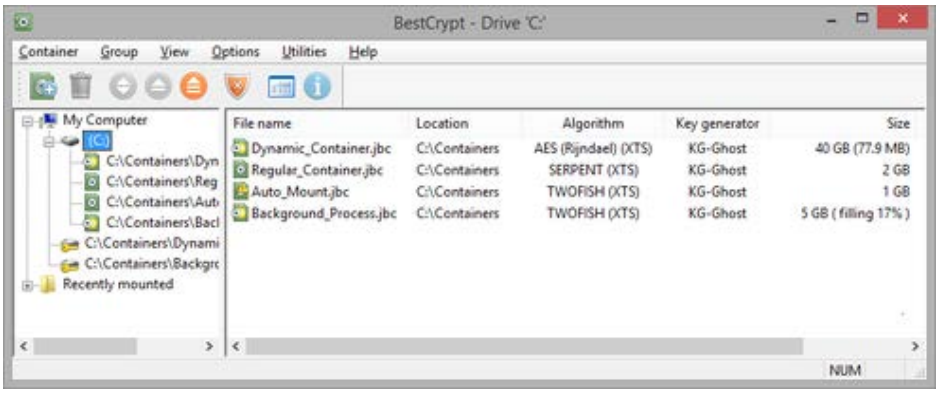
- *qattiq disk ishlab chiqaruvchilar:* iStorage Limited, Seagate Technology, Hitachi, Western Digital, Samsung, Toshiba;
- *SSD turidagi disk ishlab chiqaruvchilar:* OCZ, SanDisk, Samsung, Micron, Integral Memory;
- *USB disk ishlab chiqaruvchilar:* Yubikey yoki iStorage Limited.

Qurilmaga asoslangan FDE ikkita tashkil etuvchidan: qurilmaga asoslangan shifrlash vositasidan va ma’lumotlarni saqlash qismidan iborat. Qurilmaga asoslangan FDE ning hozirda uchta ko‘rinishi amalda keng qo‘llaniladi:

1. Hard disk drive (HDD) FDE.
2. Enclosed hard disk drive FDE.
3. Bridge and Chipset (BC) FDE.

HDD FDElar odatda HDD ishlab chiqaruvchilar tomonidan ishlab chiqariladi. Bunda ishlab chiqaruvchilar *Opal Storage Specification* texnologiyasidan foydalanadilar. Hitachi, Micron, Seagate, Samsung va Toshiba tomonidan esa TCG OPAL SATA drayveridan foydalanish orqali diskni shifrlash amalga oshiriladi.

Ba’zi diskni shifrlovchi dasturiy vositalar tomonidan *shaffof shifrlash (Transparent encryption)* usuli foydalaniladi. Bu usulga ko‘ra shifrlash kaliti taqdim etilganidan so‘ng avtomatik tarzda diskning barcha sektorlari (fayl nomini, katalog nomini, fayl kontentini va boshqa meta ma’lumotlarni o‘z ichiga olgan holda) shifrlanadi. Dasturiy vosita ko‘rinishidagi diskni shifrlash vositalariga *Aloaha Crypt Disk, BestCrypt Volume Encryption, BitArmor DataControl*, *BitLocker*, *Bloombase Keyparc, Cryptic Disk, USBCrypt* va boshqalarni misol sifatida keltirish mumkin (3.13-rasm).



3.13-rasm. Windows OTda BestCrypt dasturiy vositasining ko‘rinishi

Diskni to‘liq shifrlash usuli alohida fayl/ katalogni shifrlash usuliga qaraganda quyidagi afzalliklarga ega:

- Deyarli barcha narsa, almashtirish maydoni (swap space) va vaqtinchalik fayllar shifrlanadi. Ushbu fayllarni shifrlash juda zarur, chunki odatda ular muhim axborotni oshkor qilishi mumkin. Dasturiy vosita ko‘rinishidagi diskni shifrlovchilar dastlabki yuklash kodini (bootstrapping code) shifrlamaydi. Masalan, BitLocker Drive Encryption dasturiy vositasini ishga tushirish uchun shifrlanmagan soha qoldiradi va qolgan sohalarni to‘liq shifrlaydi.
- Ushbu usul foydalanuvchi shaxsiy xabarlarini alohida shifrlashni unutgan vaqtlarda juda qo‘l keladi.
- Zudlik bilan ma’lumotlarni yo‘q qilish, masalan, kriptografik kalitni yo‘q qilish mavjud ma’lumotni foydasiz holatga keltiradi. Kelajakda bo‘lishi mumkin bo‘lgan ma’lumotlarni tiklash usullariga bardoshli bo‘lishi uchun diskni fizik yo‘q qilish tavsiya etiladi.

Faylni shifrlash (Filesystem-level encryption yoki *file-based encryption (FBE)* yoki *file/folder encryption)* deb nomlanuvchi shifrlash usuli diskni shifrlashning bir ko‘rinishi bo‘lib, fayl tizimi orqali fayllar yoki kataloglar shifrlanadi. FBE shifrlash o‘z ichiga quyidagilarni oladi:

- asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalanish (masalan, ZFS, EncFS);
- shifrlashni amalga oshiruvchi yagona umumiy maqsadli fayl tizimi.

Fayl/ katalogni shifrlash usuli quyidagi afzalliklarga ega:

- faylga asoslangan holda kalitlarni boshqarish, ya’ni, har bir fayl uchun turli kalitlardan foydalanish;
- shifrlangan fayllarni alohida boshqarish butun shifrlangan diskni boshqarishdan ko‘ra osonroq;
- foydalanishni boshqarish ochiq kalitli kriptografik tizimlar yordamida amalga oshirilishi mumkin;
- faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi.

3.6. Ma’lumotlarni xavfsiz o‘chirish usullari

Axborot xavfsizligida ma’lumotlarni xavfsiz saqlash qanchalik muhim hisoblansa, ularni xavfsiz yo‘q qilish ham shunchalik muhim. Sababi, konfidensial axborot to‘liq yo‘q qilinmagan taqdirda uni tiklash imkoniyati saqlanib qoladi. Hozirgi kunda foydalanilayotgan barcha ma’lumotlarni yo‘q qilish usullarini ishonchli deb aytib bo‘lmaydi. Quyida qog‘oz ko‘rinishidagi va elektron ko‘rinishdagi hujjatlarni yo‘q qilish usullari va ularning xususiyatlari bilan tanishib chiqiladi.

Qog‘oz ko‘rinishdagi hujjatlarni yo‘q qilish usullari. Odatda qog‘oz ko‘rinishdagi hujjatlarni yo‘q qilishda quyidagi usullardan foydalaniladi:

- maydalash (shreder);
- yoqish;
- ko‘mish;
- kimyoviy ishlov berish.

Maydalash. Tashkilotda rahbariyat ruxsati bilan xodimlar qo‘lida bo‘lgan qog‘oz ko‘rinishidagi hujjatlar vaqt o‘tib o‘z kuchini yo‘qotadi yoki ularda arzimas ma’lumotlar saqlangani bois ularni yo‘q qilish zaruriyati tug‘iladi. Biroq, mazkur holda qimmat ma’lumotlar bo‘lsa ularni to‘liq yo‘q qilish talab etiladi. Maydalash jarayoni ushbu vazifani bajarishda keng qo‘llaniladigan usullardan biri hisoblanadi. Bunda ofis maydalagichi qog‘ozni kesish orqali juda kichik bo‘laklarga ajratadi (3.14-rasm).

3.14-rasm. Shreder Rexel Auto+ 90X

Maydalash usulining afzalligi quyidagilardan iborat:

- bir marta sotib olish bilan uzoq vaqt foydalanish mumkin;
- materiallarni yo‘q qilish uchun qo‘shimcha joy talab qilinmaydi;
- maxfiy ma’lumotlarni ham maydalay oladi.

Yoqish. Yoqish orqali katta hajmdagi hujjatlarni tezda yo‘q qilish mumkin. Ma’lumotlarni yo‘q qilishning mazkur usuli ekologik jixatdan ma’qullanmaydi. Bundan tashqari yoqish usuli quyidagi kamchiliklarga ega:

- tashkilot ichida yoki tashqarisida qog‘ozlarni yoqish uchun maxsus joy bo‘lishi talab etiladi;
- agar yonish yuqori sharoitda maxsus qozonxonalarda amalga oshirilmasa, qattiq bosilgan papkalarni to‘liq yonmaslik ehtimoli mavjud;
- olovni yoqish, qog‘ozlarni yuklash va tushirish ortiqcha xarajat talab etadi.

Ko‘mish. Ushbu usul avvallari keng foydalanilgan usul hisoblansada, hozirda kamdan-kam hollarda foydalaniladi. Ushbu usul qog‘ozdagi ma’lumotlarni to‘liq yo‘q qilish imkoniyatini bermaydi. Iqlimi quruq hududlarda qozog‘dagi ma’lumotlarni yo‘q bo‘lishi uchun uzoq vaqt talab etiladi.

Kimyoviy ishlov berish. Yuqori maxfiylik darajasiga ega hujjatlarni yo‘q qilishda yuqorida keltirilgan usullar to‘liq kafolatni ta’minlamaydi. Kimyoviy usul esa qog‘oz ko‘rinishidagi axborotni 100% ishonchlik bilan yo‘q qilish imkonini beradi. Buning uchun maxsus kimyoviy modda va suvdan foydalaniladi. Hosil qilingan massani tiklashning umuman imkoni mavjud emas. Ushbu usulning yagona kamchiligi narxining yuqoriligi va maxsus joy talab etilishi.

Elektron hujjatlarni yo‘q qilish. Elektron shaklda saqlanadigan shaxsiy va tashkilotga tegishli ma’lumotlardan noqonuniy foydalanish usullarining ko‘payishi sababli elektron ommaviy axborot vositalariga ishonish muammosining dolzarbligi oshmoqda. Misol sifatida, markaziy

razvedka boshqarmasi va AQSh milliy xavfsizlik agenti Edvard Snoudenga tegishli yangiliklarni olish mumkin. Xususan, 2013 yil iyun oyining boshida u NSA tashkilotiga tegishli hujjatlarni oshkor qildi. Bunga ko‘ra G20 sammitining chet ellik mehmonlari, shu jumladan Dmitriy Medvedovni Amerika va Buyuk Britaniya razvedka idoralari tomonidan kuzatilayotgani aytilgan. Maxfiy agentlar PRISM dasturi yordamida noutbuk va telefonlarda saqlanayotgan shaxsiy ma’lumotlardan foydalanishni uddasidan chiqishgan. Buyuk Britaniya hukumati aloqa markazining xodimlari BlackBerry kodini buzib, qo‘ng‘iroqlarni tinglash va sammit ishtirokchilarining yozishmalarini o‘qish imkoniyatiga ega bo‘lishgan.

Elektron vositalardagi ma’lumotlardan xalos bo‘lishning eng oson yo‘li uni *Korzinka*ga yuborish yoki, yanada radikal usuli, *formatlash.* Bu usul aksariyat foydalanuvchilar tomonidan ishonchli usul deb qaralsada, aslida bunday emas. Bu usul ma’lumotlarni fizik yo‘qolishini ta’minlamaydi. Bu holda maxsus dasturlar (Recuva, Wise Data Recovery, PC Inspector File Recovery, EaseUS Data Recovery Wizard Free, TestDisk and PhotoRec, Stellar Data Recovery) yordamida ularni qayta tiklash imkoniyati mavjud.

Hozirgi kunda amalda elektron hujjatlarning saqlagichlari sifatida quyidagi vositalardan foydalanilmoqda:

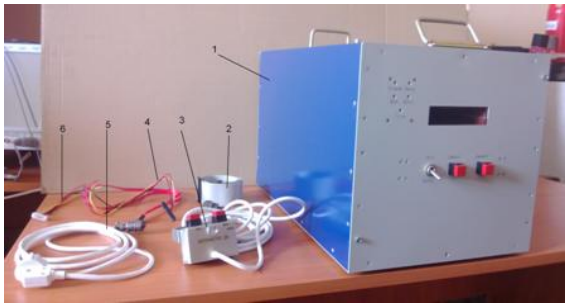
- qattiq disklar: noutbuk va kompyuterdagi qattiq disklar;
- magnit lentalar (zaxira nusxalashdagi);
- floppi-disk: 3.5 va 5.25 dyumli va boshqa;
- ZIP disklar;
- optik disklar: CD, DVD, Blue Ray va HD DVD;
- flesh xotiralar va h.

AQSh hukumati tomonidan konfidensial axborotni saqlash va o‘chirib tashlash bo‘yicha qator normativ hujjatlar ishlab chiqilgan (Code of Federal Regulations). Masalan, AQShning markaziy arxiv markazlarida elektron saqlagichdagi ma’lumotlarni yo‘q qilishning quyidagi uchta usulidan foydalaniladi:

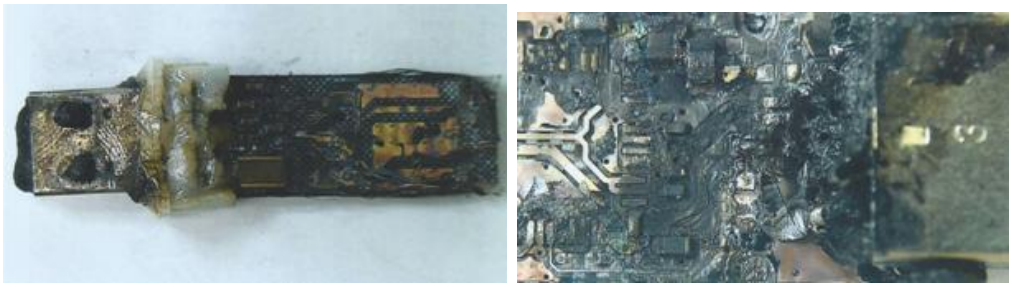
Shrederlash. Kuchli sanoat maydalagichlari deyarli barcha ko‘chma saqlaguvchilarni: CD, DVD, disket, magnit lentalar va h. maydalash natijasida ularni 25 mm. li qismlarga bo‘lib tashlaydi (3.15-rasm).

3.15-rasm. Shrederlash jarayoni

Magnitsizlantirish. Maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o‘zgartiriladi va shu bilan o‘qib bo‘lmaslik ta‘minlanadi. Agar kuchli magnitsizlantirish amalga oshirilsa ma’lumotlar saqlagichdan o‘chiriladi va saqlagichning o‘zi neytral magnit holatiga kiradi. Ushbu ma’lumotni yo‘q qilish usuli dattiq disklar va ba’zi ko‘chma qurilmalarda qo‘llaniladi (3.16-rasm).



3.16-rasm. a) UE-02 qurilmasi



3.16-rasm. b) Kuchli magnit maydoni ta’siri natijasida USB flesh saqlagichining o‘zgarishi

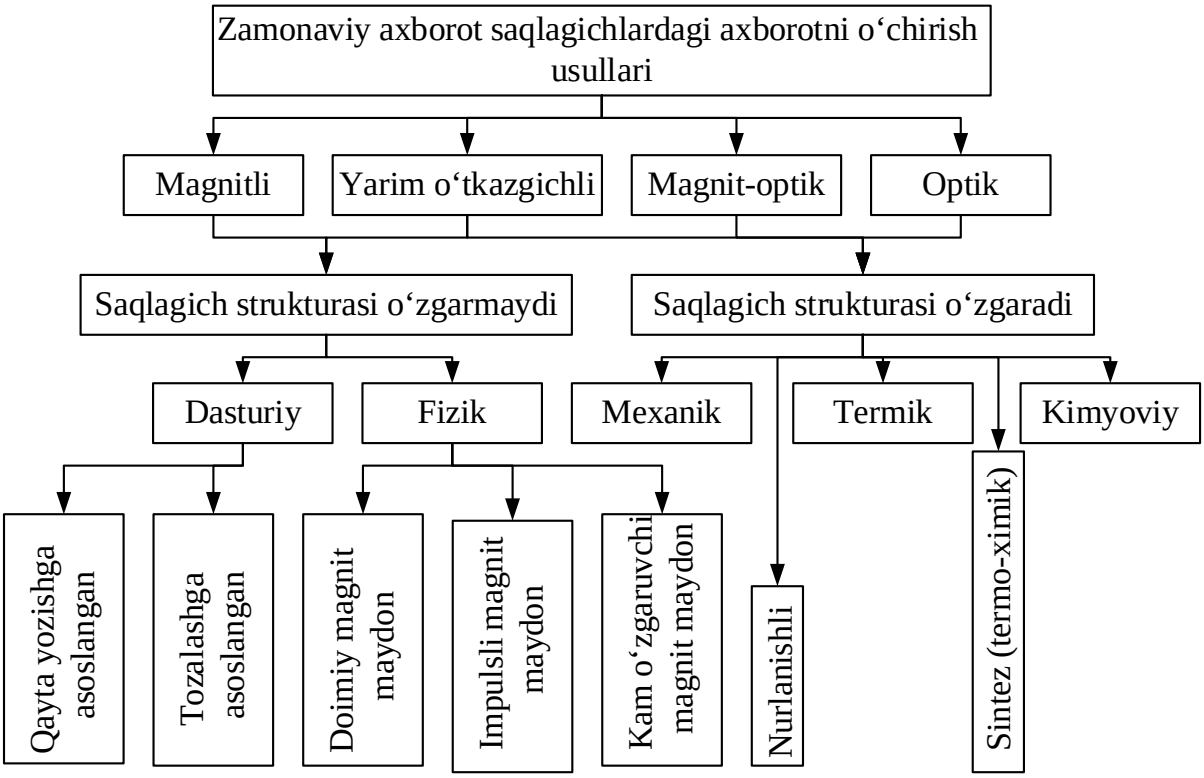
Yanchish. Shrederlash jarayonidan tashqari AQSh federal arxiv markazlari tomonidan qattiq diskni yanchish orqali uni jismonan yo‘q qilish usuli ham mavjud. 5.5 tonna og‘irlikdagi tosh ostida kompyuter va noutbuklarning qattiq disklari tamomila yo‘q qilinadi. Ushbu mexanizm maksimal hajmi 2.5×10×15 sm. bo‘lgan, 3.5, 2.5 va 1 dyumli disklar (SATA, PATA, SCSI) ni maydalash uchun mo‘ljallangan.

Yuqorida keltirilgan usullarning maqsadi aksariyat ma’lumot eltuvchilarini fizik yo‘q qilish. TOP SECRET bo‘lmagan axborot saqlangan holda esa saqlagichlardan qayta foydalanish talab etiladi. Buning uchun quyidagi usullardan foydalaniladi:

- saqlagich xotirasiga takroran yozish;
- maxsus dasturlar yordamida saqlagichni tozalash (formatlashdan oldin ma’lumotni o‘chirish).

Ushbu usul ma’lumotni kafolatli yo‘q qilish imkonini bermasada, amaliyotdagi aksariyat holatlar uchun yetarli hisoblanadi.

Umumiy holda elektron saqlagichlardagi axborotni yo‘q qilishda quyidagi 3.17-rasmda keltirilgan usullardan foydalaniladi.



3.19-rasm. Elektron saqlagichlardan ma’lumotlarni yo‘q qilish usullari

AQShning Cornell kompaniyasi tomonidan elektron axborotni saqlagichlardan qayta foydalanishda va ularni yo‘q qilish uchun quyidagi tavsiyalar beriladi (3.6-jadval).

3.6-jadval

Elektron saqlagichlardan qayta foydalanish va yo‘q qilish uchun tavsiyalar

Elektron saqlagichlar	**Qayta foydalanish uchun**	**Yo‘q qilish**
Qattiq disk	DoD 5220.22 algoritmi yordamida formatlashdan oldin o‘chirish.	Fizik yo‘q qilish yoki magnitsizlantirish.
Floppi disk	Magnitsizlantirish yoki formatlashdan oldin o‘chirish.	Fizik yo‘q qilish, magnitsizlantirish.
Optik disklar	Odatda qo‘llanilmaydi.	Fizik yo‘q qilish: yanchish, ishqalash orqali sirtni bir xil holatga keltirish.
ZIP disklar	DoD 5220.22 algoritmi yordamida o‘chirish.	Fizik yo‘q qilish, magnitsizlantirish.
Flesh-saqlagichlar	Formatlashdan oldin ma’lumotni o‘chirish.	Fiziq yo‘q qilish.
Magnit lentalar	Magnitsizlantirish.	Fizik yo‘q qilish, magnitsizlantirish.

Izoh: DoD 5220.22 algoritmi AQSh mudofaa vazirligida qo‘llaniluvchi ma’lumotlarni yo‘q qilishga asoslangan va 4-7 martagacha takror yozish orqali ma’lumotlarning tiklanishini oldini oladi.

Nazorat savollari

1. Kriptografiyaning asosiy tushunchalarig.
2. Rasshifrovkalashning deshifrlashdan farqi nimada?
3. Axborotni simmetrik va ochiq kalitli shifrlash algoritmlari yordamida shifrlashdagi afzallik va kamchiliklari.
4. Kerkgoff prinsipining mohiyatini tushuntiring.
5. Kodlash va shifrlash tushunchalarining bir – biridan farqi nimada?
6. Kriptologiya va steganografiya fan sohalari va ularning o‘zaro farqi.
7. Simmetrik kriptografiyaning axborotni himoyalashdagi o‘rni.

8. Ochiq kalitli kriptografiyaning axborotni himoyalashdagi o‘rni.

9. Xesh funksiya, unga qo‘yilgan talablar va uning axborot himoyalashdagi o‘rni.

10. Kriptografik akslantirishlar: o‘rniga qo‘yish va o‘rin almashtirish nima?

11. Bir martali bloknot yordamida ma’lumotlarni shifrlash va uning xavfsizligi.

12. Simmetrik kriptotizimlar: kodlar kitobi, A5/1 va TEA shifrlash algoritmlari.

13. Simmetrik blokli shifrlash rejimlari va ular nima uchun zarur?

14. Modul arifmetrikasidagi asosiy amallar.

15. RSA algoritmi va u asoslangan matematik muammo.

16. Ma’lumotlarning yaxlitligini ta’minlash usullari.

17. Elektron raqamli imzo va xabarlarni autentifikatsiyalash kodlarining bir-biridan farqi hamda o‘xshash tomonlari nimada?

18. Axborotni kriptografik himoyalash vositalarining ko‘rinishlari va ularning afzallik va kamchiliklari.

19. Diskni va faylni shifrlash usullarining bir-biridan farqi nimadan iborat?

20. Qog‘ozdagi ma’lumotlarni yo‘q qilish usullari va ularning xususiyatlari.

21. Elektron saqlagichlaridagi ma’lumotlarni yo‘q qilish usullari va ularning xususiyatlari.

4 BOB. FOYDALANISHNI NAZORATLASH

4.1. Identifikatsiya va autentifikatsiya vositalari

Tizim resurslaridan foydalanishni boshqarish bilan bog‘liq har qanday xavfsizlik muammosi uchun *foydalanishni nazoratlash* tushunchasidan “soyabon” sifatida foydalanish mumkin. Bunda 3 ta asosiy tushuncha farqlanadi: *identifikatsiya, autentifikatsiya* va *avtorizatsiya.*

Identifikatsiya – shaxsni kimdir deb da’vo qilish jarayoni. Masalan, siz telefonda o‘zingizni tanishtirishingizni identifikatsiyadan o‘tish deb aytish mumkin. Bunda siz o‘zingizni, masalan, “Men Bahodirman” deb tanitasiz. Bu o‘rinda “Bohodir” sizning *identifikatoringiz* bo‘lib xizmat qiladi. *Identifikatsiya* – subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni. Elektron pochta tizimida pochta manzilini *identifikator*, manzilini taqdim etish jarayonini esa *identifikatsiyalash* deb ataladi. Elektron pochta tizimida pochta manzili takrorlanmas va noyob. Demak, foydalanuvchining identifikatori tizim ichida noyob va takrorlanmasdir.

Autentifikatsiya – foydalanuvchining (yoki uning nomidan ish ko‘ruvchi vositaning) tizimdan foydalanish huquqiga egaligini tekshirish jarayoni. Masalan, foydalanuvchining shaxsiy kompyuterdan foydalanish jarayonini ko‘raylik. Dastlab foydalanuvchi o‘z identifikatorini (ya’ni, foydalanuvchi nomini) taqdim etib, tizimga o‘zini tanitadi (identifikatsiya jarayonidan o‘tadi). So‘ngra, tizim foydalanuvchidan, taqdim etilgan identifikatorni haqiqiyligini tekshirish uchun, parol talab qiladi. Agar identifikatorga mos parol kiritilsa (ya‘ni, autentifikatsiyadan o‘tilsa), foydalanuvchi kompyuterdan foydalanish imkoniyatiga ega bo‘ladi. Umuman olganda, autentifikatsiya foydalanuvchining yoki subyektning haqiqiyligini tekshirish jarayoni deb yuritiladi.

Foydalanuvchi autentifikatsiyadan o‘tganidan so‘ng, tizim resurslaridan foydalanish imkoniyatiga ega bo‘ladi. Biroq, autentifikatsiyadan o‘tgan foydalanuvchi tizimda faqatgina ruxsat berilgan amallarni bajarishi mumkin. Masalan, autentifikatsiyadan o‘tgan – imtiyozga ega foydalanuvchi uchun dasturlarni o‘rnatish imkoniyatini berilishi talab etilsin. Bunda autentifikatsiyadan o‘tgan foydalanuvchining foydalanish huquqlari qanday cheklanadi? Bu masala avtorizatsiyalash orqali yechiladi.

Avtorizatsiya – identifikatsiya va autentifikatsiya jarayonlaridan muvaffaqiyatli o‘tgan foydalanuvchiga tizimda amallarni bajarish

huquqini berish jarayoni. Umumiy holda, autentifikatsiya binar qaror hisoblanadi - ya’ni, ruxsat beriladi yoki yo‘q. Avtorizatsiya esa tizimning turli resurslaridan foydalanishni cheklash uchun foydalaniluvchi qoidalar to‘plami.

Xavfsizlik sohasida aksariyat atamalar standart ma’nolaridan boshqa hollarda ham qo‘llaniladi. Xususan, foydalanishlarni nazoratlash ko‘p hollarda avtorizatsiyaga sinonim sifatida ishlatiladi. Biroq, mazkur o‘quv qo‘llanmada foydalanishlarni nazoratlash biroz kengroq qaralgan. Ya’ni, autentifikatsiya va avtorizasiya jarayonlari foydalanishlarni nazoratlashning alohida qismlari sifatida ko‘riladi.

Yuqorida keltirilgan atamalarga berilgan ta’riflarni umumlashtirgan holda quyidagicha xulosa qilish mumkin:

Identifikatsiya – siz kimsiz?

Autentifikatsiya – siz haqiqatan ham sizmisiz?

Avtorizatsiya – sizga buni bajarishga ruxsat bormi?

Bir tomonlama va ikki tomonlama autentifikatsiya. Agar tomonlardan biri ikkinchisini autentifikatsiyadan o‘tkazsa - *bir tomonlama*, agar har ikkala tomon bir-birini autentifikatsiyadan o‘tkazsa, u holda *ikki tomonlama autentifikatsiya* deb ataladi. Masalan, elektron pochtadan foydalanishda faqat server foydalanuvchini haqiqiyligini (parol orqali) tekshirsa, uni *bir tomonlama autentifikatsiyalash* deb ataladi. Elektron to‘lov tizimlarida server foydalanuvchini, foydalanuvchi esa serverni autentifikatsiyadan o‘tkazadi. Shuning uchun mazkur holat *ikki tomonlama autentifikatsiyalash* deb yuritiladi.

Ko‘p omilli autentifikatsiya. Yuqorida keltirilgan barcha autentifikatsiya senariylarida foydalanuvchilarni faqat bitta omil bo‘yicha haqiqiyligi tekshiriladi. Masalan, elektron pochtaga kirishda faqat parolni bilishning o‘zi yetarli bo‘lsa, binoga kirishda barmoq izini to‘g‘ri kiritishning o‘zi eshikning ochilishi uchun yetarli bo‘ladi. Ya’ni, server faqat foydalanuvchidan parolni yoki barmoq izi tasvirini to‘g‘ri bo‘lishini talab qiladi. Bir omilli autentifikatsiyada tekshirish faqat bitta omil bo‘yicha (masalan, parol) amalga oshirilsa, bunday autentifikatsiya *bir omilli autentifikatsiya* deb yuritiladi.

Identifikatsiya va autentifikatsiya foydalanishni boshqarish jarayonida dastlabki chegara hisoblanadi. Tizimning turli variantlarda amalga oshirilishida ba’zi qurilmalar va mexanizmlar ham identifikatsiya, ham autentifikatsiya qismtizimi komponentlari bo‘lishi mumkin. Shu sababli, identifikatsiya va autentifikatsiya vositalarini birlashgan holda baholash lozim.

Identifikatsiya va autentifikatsiya vositalarini, odatda, autentifikatsiya omillari bo‘yicha uchta turga ajratishadi.

1-tur. Qandaydir yashirin axborotni (masalan, parolni, maxfiy PIN-kodni, klavishalar va iboralar kombinatsiyalarini) bilishga asoslangan vositalar (something you know).

2-tur. Noyob qurilmadan, usuldan yoki ma’lumotlar naboridan (masalan, smart kartalardan, raqamli sertifikatlardan) foydalanishga asoslangan vositalar (something you have).

3-tur. Tirik organizmning fiziologik atributlariga (something you are) masalan, ko‘z yoyi to‘rpardasiga yoki odatiy atributlarga (something you do) masalan, imzoga asoslangan biometrik vositalar.

Ba’zi tasniflarda foydalanuvchi o‘rnashgan joyi (some where you are), bilan bog‘liq axborotga asoslangan yana bir vositalar turini uchratish mumkin. Bunda autentifikatsiya omili sifatida telefon nomeri (mamlakat, shahar, tuman kodi) ishtirok etganligi sababli, bunday vositalarni, ko‘pincha, 2-turga (something you have) tegishli deb hisoblashadi.

Agar tizimda turli tur autentifikatsiya omillarini birgalikda ishlatuvchi vositalardan foydalanilsa, ko‘p omilli autentifikatsiya xususida gapirish mumkin. Bunday tizimlarni ko‘p sathli himoyalash (defence in depth) kategoriyasiga tegishli deb hisoblashadi. Shu sababli, bunday tizimlar faqat bitta tip qurilmalardan foydalanuvchi tizimlarga nisbatan yuqori bardoshlikka ega. Hozirda ikki omilli autentifikatsiya (two-factor authentication) keng tarqalgan. Masalan, zamonaviy operatsion tizimlarni maxfiy PIN-kod va cmart-kartadan foydalanib sozlash mumkin.

Parol tizimlari. Maxfiy identifikatorlarga-parollarga (password) asoslangan tizimlar autentifikatsiyaning an’anaviy vositalari hisoblanadi. Afsuski, parol tizimlari, obyektiv va subyektiv sabablarga ko‘ra, zaif.

Birinchidan, parol tizimlari tizim buzg‘unchilarining jiddiy e’tibori ostida. Buzg‘unchi parol himoyasini buzib, tizim nuqtai nazaridan, ruxsatga ega foydalanuvchiga aylanishi mumkin. Masalan, axborot xavfsizligi sohasidagi 80%dan ortiq insidentlar parol himoyasini buzish bilan bog‘liq. Aksariyat kompyuter xujumlari aynan ma’mur parolini qo‘lga kiritishni ko‘zda tutadi. Ta’kidlash lozimki, ko‘pgina autentifikatsiya tizimlarining zaifligi ularning noto‘g‘ri amalga oshirilishi bilan bog‘liq. Masalan, ba’zi tizimlarda parol ochiq holda uzatiladi va saqlanadi (PAP protokoli, parol bo‘yicha autentifikatsiyalash protokoli yordamida). Parol axborotini shifrlash protokollari va vositalari esa yetarlicha kriptobardoshlikka ega emas.

Ikkinchidan, parollarni ko‘pincha oddiygina aniqlash mumkin. Gap shundaki, parol tizim yordamida (tasodifiy sonlar datchiklari yordamida) generatsiyalash mumkin va, demak, uni esda saqlash qiyin. Bu holda, foydlanuvchilar bunday psevdotasodifiy parollarni ko‘pincha qog‘oz parchasiga, kompyuterning tashqi qurilmasiga, “Ish stolidagi” fayllarga, uyali telefonlarning “xotirasiga” va h. yozishadi. Bu esa buzg‘unchilar uchun yoqimli holat.

Boshqa tomondan, oson esda saqlanuvchi parol, odatda, oddiy va foydalanuvchining shaxsiy hayoti va yaqinlari bilan assosatsiyalangan bo‘ladi. Demak, parol osongina topilishi mumkin.

Parol himoyasining bardoshligini qanday oshirish mumkin? Bir necha usullar mavjud:

– doimiy (static) parollar o‘rniga bir martali parollardan foydalanish;

– parol va qayd yozuvlari himoyasi siyosatini kuchaytirish.

Ta’siri yo‘qolgan parollardan foydalanish xavfini istisno qilish maqsadida dinamik tarzda o‘zgaruvchi (dinamic) parollardan foydalaniladi. Dinamik parollar vaqtning qandaydir oralig‘idan so‘ng yangi parolning generatsiyalanishini va ishlatilishini ta’minlaydi. Masalan, parollarni generatsiyalash funksiyasida parametrlarning biri sifatida kun ko‘zda tutilgan bo‘lsa, ravshanki, har kuni parol yangilanadi. Amalda, dinamik tarzda o‘zgaruvchi parollar sifatida subyekt ishining bitta seansida qo‘llaniluvchi bir martali (one-time, single -use) parollar keng tarqalgan.

Dinamik tarzda o‘zgaruvchi parollarga asoslangan autentifikatsiya tizimlarida mijoz va server parollarni generatsiyalashning bir xil algoritmidan foydalanishadi. Bir martali parol ta’sirining vaqt oralig‘ini nazoratlash uchun tizim vaqti serverda va mijozda “sinxronlanishi” lozim. Parolni nazoratlashda tizim vaqti ishlatilmay, hodisaning boshlanishi prinsipi ishlatilsa, bunday tizimlar “asinxron tizimlar” deb ataladi.

Parolli himoyalash xavfsizligi siyosatini kuchaytirish parolni tanlashda uning oshkor bo‘lishini qiyinlashtiruvchi talablarga hamda parolni saqlash va tarmoq orqali uzatish talablariga rioya qilish ko‘zda tutiladi, masalan:

– parol tarkibida ko‘p uchraydigan ismlar, so‘zlar, qisqartirishlar, kunlar, telefon nomerlari bo‘lmasligi, autentifikator bilan bir xil bo‘lmasligi va h. lozim;

– parol tarkibida bosh harflar, raqamlar, tinish belgilari va maxsus simvollar (-@#;%^&*) bo‘lishi lozim;

– paroldagi simvollar soni 8 dan kam bo‘lmasligi va parolni 90 kundan so‘ng almashtirish lozim;

– hisob yozuvidan foydalanishga cheklashlar (kun, sutka vaqti, ulanish manzili, ulanish soni bo‘yicha) o‘rnatililishi lozim;

– parolni muvaffaqiyatsiz kiritish va urinish sonini cheklash - 3 dan 5 gacha;

– parol axborotini saqlash va tarmoq bo‘yicha uzatishning kriptohimoya rejimlari o‘rnatilishi lozim.

Parol himoyasini kuchaytirishning o‘ziga hos variantlari – parol iboralaridan (pass phrase) va kognitiv (cognitive - anglab bo‘ladigan) parollardan foydalanish. Uzun, ammo xotirlash uchun oson parol iborasi parolning oshkor qilinishini qiyinlashtiradi. Kognitiv parol odatda, tasodifiy tanlangan, ammo maxfiy ravishda oldindan aniqlangan savollarga javoblar qismto‘plamidan iborat.

Avtomatlashtirilgan tizimlarda parollar bardoshligini baholashda matematik ko‘rsatkichlar ishlatilishi mumkin. Klod Shennon tomonidan taklif etilgan axborot entropiyasi keng tarqalgan ko‘rsatkich sifatida ishlatiladi:

$$H = n * \log_2|A|,$$

Bu yerda, $|A|$- A alfavitning quvvati (bo‘lishi mumkin bo‘lgan simvollar soni), n esa paroldagi simvollar soni.

Entropiya qanchalik katta bo‘lsa, parolning tasodifiy tarzda oshkor qilinishi shunchalik qiyinlashadi. Agar parol parollarni tanlash lug‘atida bo‘lsa, uning entropiyasi nulga teng deb hisoblash qabul qilingan.

Xulosa sifatida ta’kidlash lozimki, parol himoyasini kuchaytirishning radikal usuli - noyob elektron qurilmadan qo‘shimcha tarzda foydalanib, ikki omilli autentifikatsiyaga o‘tish.

Elektron qurilmalar. Identifikatsiya va autentifikatsiya vositalarining 2-turiga, tarkibida subyekt xususida qandaydir noyob axborot mavjud elektron qurilmalar taalluqli. Bunday qurilmalar foydalanuvchilar bilan birga bo‘lishi lozim. 4.1-rasmda maxsus maqsadli smartkarta va uni o‘quvchi qurilma (smartkarta o‘quvchi qurilma) aks ettirilgan.

4.1-rasm. Smartkarta va smartkarta o‘quvchi (ACR39U) qurilma

Elektron qurilmalarni quyidagicha tasniflash mumkin:

- amalga oshirilishi bo‘yicha passiv (faqat xotirali) va aktiv (mikroprosessorli) elektron qurilmalar farqlanadi;
- o‘qish qurilmalarining mavjudligi bo‘yicha alohida o‘qish qurilmasili (reader), kalit bilan integrallangan o‘qish qurilmasili (masalan USB- portga ulanadi) va kompyuterning kiritish qurilmasidan va asosiy xotirasidan foydalanuvchi elektron qurilmalar farqlanadi;
- funksional belgilanishi bo‘yicha statik, sinxron dinamik va asinxron dinamik elektron qurilmalar farqlanadi.

Statik qurilmalar doimiy noyob axborotni saqlashni ta’minlaydi va subyektni autentifikatsiyalash yoki identifikatsiyalash uchun ishlatiladi. Oddiygina statik qurilmalarga disketa, xotira kartasi, magnit tasmali, qog‘oz karta, tarkibida identifikator, parol, sertifikat va h. bo‘lgan ATM-karta misol bo‘la oladi.

Zamonaviy statik qurilmalarga quyidagilar taalluqli:

– smart kartalar – mikroprosessor o‘rnatilgan kredit karta o‘lchamidagi karta;

– USB kalitlar – kompyuterning USB-portiga to‘g‘ridan-to‘g‘ri ulanuvchi qurilma bo‘lib, tarkibida mikroprosessor o‘rnatilgan kalit va o‘qish qurilmasi mavjud;

– iButton elektron tabletkalari. Ba’zida, Touch Memory deb ham ataladi;

– kontaktsiz radiochastota identifikatorlari – RFID–radiometkalar.

Sinxron dinamik qurilmalar vaqtning o‘zgarmas oralig‘ida parol generatsiyalaydi. Serverdagi va tokendagi tizim vaqtlari sinxronlanishi lozim.

Asinxron dinamik qurilmalar qandaydir hodisa (masalan, serverdagi va tokendagi tugmalar bosilganida) sodir bo‘lganida navbatdagi parolni generatsiyalaydi. Sinxron va asinxron qurilmalar generatsiyalovchi parol identifikatsiyani, kiritiluvchi PIN-kod yoki parol esa autentifikatsiyani ta’minlashi mumkin. Undan tashqari, bunday tizimlar, foydalanuvchi ismidan foydalanib, ikki omilli autentifikatsiyani tashkil etishi mumkin.

So‘rov-javobli kurilmalar autentifikatsiyaning nomdosh mexanizmini amalga oshiradi. Mijoz (kalit) so‘rovni boshlaydi, autentifikatsiya vazifasini bajaruvchi server javob sifatida qandaydir psevdotasodifiy kodni yoki iborani generatsiyalaydi va kalitga uzatadi. Olingan ma’lumotlar asosida elektron qurilma o‘rnatilgan algoritm bo‘yicha javobni hisoblaydi va serverga qayta jo‘natadi. Server kalitda amalga oshirilgan algoritmni biladi va mijozdan kelgan javobning to‘g‘riligini tekshiruvchi autentifikatsiya amalini bajaradi.

Elektron qurilmalar qator kamchiliklarga ega:

– qurilmani bilmasdan sindirish mumkin, qurilma energiya iste’mol qilsa uning energiya ta’minoti holatini kuzatish lozim;

– qurilma o‘g‘irlanishi, yo‘qotilishi, olib qo‘yilishi yoki kimdir undan foydalanishi holati tug‘ilishi mumkin;

– oddiy qurilmalar klonlashtirilishi mumkin;

– USB-tokenlardan tashqari, aksariyat qurilmalar qo‘shimcha o‘qish qurilmalarining mavjudligi talab etiladi.

Biletlar. Identifikatsiya va autentifikatsiyani nafaqat elektron qurilmalar, balki mustaqil noyob ma’lumotlarning kriptografik nabori yordamida tasavvur etish mumkin. Tarmoqda autentifikatsiya jarayonida ishtirokchilarga taqdim etiladigan seans biletlari yoki mandatlar keng tarqalgan. Biletlardan foydalanib autentifikatsiya mexanizmini amalga oshiruvchi tizimlarga Kerberos misol bo‘la oladi.

Tarmoq autentifikatsiyasini markazlashtirilmagan (har bir stansiyada) yoki markazlashtirilgan tarzda amalga oshirish mumkin. Markazlashtirilgan tarzda amalga oshirishda autentifikatsiyaning ajratilgan serveridan foydalaniladi. Markazlashtirilgan autentifikatsiyaning mashhur serveri – Kerberos. Uning asosiy xususiyatlari quyidagilar:

– barqaror autentifikatsiyani amalga oshirishda seans biletlaridan foydalaniladi. Bilet tarkibida shifrlangan yashirin kalit, so‘rov xarakteristikasi, almashishning vaqtiy oralig‘i va h. mavjud;

– autentifikatsiya axborotini yashirish uchun simmetrik algoritmdan foydalaniladi;

– tarmoq komponentlari orasida aloqani o‘rnatishdan oldin ikkita stansiyaning (mijoz va server) o‘zaro autentifikatsiya mexanizmlari ishlatiladi;

– tizimda yagona kirish texnologiyasi amalga oshiriladi. Bunda sessiya doirasida turli tarmoq so‘rovlarini bajarishda avtorizatsiyalangan foydalanuvchining foydalanuvchi parolini qaytadan kiritishiga hojat qolmaydi;

– har bir stansiya Kerberos serverida saqlanuvchi uzoq muddatli maxfiy kalitga ega.

Kerberos serveri ishtirokidagi mijoz va server orasidagi dastlabki autentifikatsiya algoritmi quyidagi ko‘rinishga ega:

- mijoz Kerberos serveriga, tarkibida mijoz identifikatori va so‘raluvchi server servisi bo‘lgan so‘rovni jo‘natadi;
- Kerberos, serverning maxfiy kaliti bilan shifrlangan shakllantirilgan biletni va mijozning maxfiy kaliti bilan shifrlangan biletdagi axborot qismi nusxasini mijozga qaytarib jo‘natadi;
- mijoz biletdagi axborotning ikkinchi qismini rasshifrovkalab, uni bilet bilan birga serverga jo‘natadi;
- server biletni rasshifrovkalab, uning tarkibini mijoz jo‘natgan axborot bilan taqqoslaydi. Mos kelishi mijoz va serverning o‘zaro muloqotning vakolatli abonentlari ekanligini tasdiqlaydi.

Odatda biletni shifrlash DES, 3DES, AES (Kerberos v5) simmetrik algoritmlari bo‘yicha bajariladi.

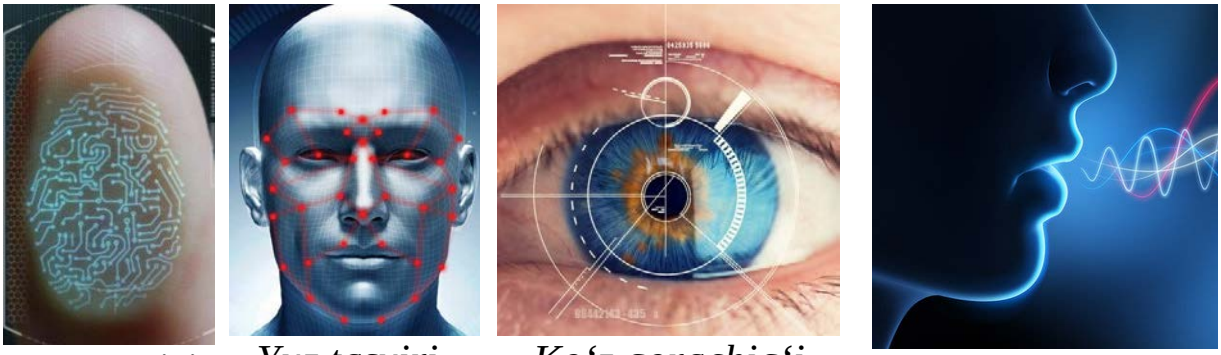
Kerberos tizimining asosiy kamchiligini aksariyat markazlashtirilgan tizimlar kamchiliklari bilan, xususan, kalitlarni taqsimlash markazida (Key Destribution Center, KDCda) maxfiy kalitlarning markazlashgan holda saqlanishi bilan bog‘lashadi.

Ta’kidlash lozimki, autentifikatsiya protokollarida asimmetrik shifrlash va elektron raqamli imzodan ham foydalanish mumkin.

Biometrik tizimlar. Biometrik qurilmalar tirik organizmning fiziologik yoki odatiy (g‘ayri-ixtiyoriy) xarakateristikalariga asoslangan.

Keng tarqalgan biometrik usullarga quyidagilar taalluqli (4.2-rasm):

- barmoq izlari bo‘yicha. Barmoq izlarini skanerlash usuli har bir inson barmoqlarining kapilyar shakllarining noyobligiga asoslangan. Barmoq izi skanerlarining o‘lchami kichik, ular universal, arzon va keng qo‘llaniladi;
- qo‘l kaftining biometrik shakli bo‘yicha. Ushbu usul qo‘l panjasining shakliga asoslangan. Kaftni skanerlash vositalarining samaradorligi barmoq skanerlari samaradorligi bilan taqqoslana oladi;
- ko‘z to‘rpardasi bo‘yicha. Bunda ko‘z qorachig‘i orqali uning orqa devori qon tomirlariga yorug‘likning infraqizil nuri yo‘naltiriladi. Shu tariqa yoritilgan ko‘z tubi maxsus kamera yordamida skanerlanadi;
- ko‘zning rangdor pardasi bo‘yicha. Rangdor pardadagi dog‘ insonning eng noyob xarakteristikasi hisoblanadi. Usulning afzalligi shundaki, masofadan skanerlash mumkin. Bu skanerlarni kuzatuv kameralari bilan integrallashga imkon beradi;
- yuzning shakli bo‘yicha. Usul inson yuzining ko‘p o‘lchamli qiyofasini qurishga asoslangan;
- qo‘lyozma dastxat bo‘yicha. Usul imzoning yoki maxsus iboraning grafik identifikatsiyasiga asoslangan;
- klaviatura dastxati bo‘yicha. Usul, odatda, oldindan belgilangan matnni klaviuaturada terishning o‘ziga xos xususiyatlariga asoslangan;
- ovoz bo‘yicha. Usul inson nutqining chastotasi yoki statistik xarakteristikalari profiliga asoslangan. Afsuski, usul inson holatiga bog‘liq.



Barmoq izi *Yuz tasviri* *Ko‘z qorachig‘i* *Ovoz*

4.2-rasm. Biometrik namunalarga misollar

Autentifikatsiya sohasida foydalanish uchun ideal biometrik parametr quyidagi xususiyatlarga ega bo‘lishi shart:

- *universal bo‘lishi* – biometrik parametrlar barcha foydalanuvchilarda bo‘lishi;
- *farqli bo‘lishi* – barcha insonlarning tanlangan biometrik parametri bir-biridan farqlanishi;
- *o‘zgarmaslik* – tanlangan biometrik parametr vaqt o‘tishi bilan o‘zgarmay qolishi;
- *to‘planuvchanlik* – fizik xususiyat osonlik bilan to‘planuvchan bo‘lishi. Amalda fizik xususiyatni to‘planuvchanligi, insonning autentifikatsiya jarayonga e’tibor berishiga ham bog‘liq bo‘ladi.

Biometrik tizimlarning eng ishonchligi – ko‘zning rangdor pardasi yoki ko‘z to‘rpardasi bo‘yicha skanerlash. Hozirda beshta barmoq skaneri va bir vaqtda barmoq izi va ko‘zning rangdor pardasidan foydalanuvchi kombinatsiyalangan qurilmalar eng yuqori aniqlikni ta’minlaydi.

Biometrik atributlar bo‘yicha autentifikatsiyalashning o‘ziga xos xususiyatlari va kamchiliklari mavjud:

- biometrika faqat tirik organizmga mo‘ljallangan;
- ehtimollik xarakterga ega bo‘lganligi sababli, asboblarning ta’sirchanligini hisobga olish lozim;
- aksariyat vositalar atrof-muhitga hamda insonning yoshi va sog‘lig‘iga bog‘liq;
- hozirda barmoq izlari skanerlaridan tashqari barcha vositalar yetarlicha qimmat;
- davlat tomonidan total nazorat tahdidi xususida foydalanuvchilarda ishonchsizlikning mavjudligi.

Iste’molchi nuqtai nazaridan biometrik autentifikatsiyalash tizimi quyidagi ikkita parametr orqali xarakterlanadi:

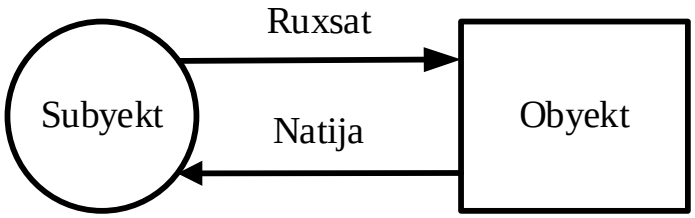
- FAR (False Acceptance Rate) – foydalanishga yolg‘on ruxsatlar chastotasi;
- FRR (False Rejection Rate) – foydalanishga yolg‘on inkorlar chastotasi.

1- va 2-xil xatoliklar (FAR va FRR ko‘rsatkichlari) o‘zaro bog‘langan: bir parametr qanchalik yaxshi bo‘lsa, ikkinchisi shunchalik yomon bo‘ladi, ya’ni, bu yerda teskari mutanosiblik mavjud. Mukammal biometrik tizimda xatolikning ikkala parametri nolga teng bo‘lishi shart. Afsuski, biometrik tizim ideal emas. Shu sababli nimanidur qurbon qilishga to‘g‘ri keladi.

4.2. Ma’lumotlardan foydalanishni mantiqiy boshqarish

Foydalanishni boshqarish. Avtorizatsiya foydalanishlarni nazoratlashning autentifikatsiyadan o‘tgan foydalanuvchilar harakatlarini cheklash qismi bo‘lib, aksariyat hollarda foydalanishni boshqarish modellari yordamida amalga oshiriladi.

Foydalanishni boshqarish subyektning obyektga yo‘naltirilgan faollik manbai imkoniyatini aniqlashdir. Umumiy holda foydalanishni boshqarish quyidagi sxema orqali tavsiflanadi (4.3-rasm):



4.3-rasm. Foydalanishni boshqarish sxemasi

Hozirda tizimlarda obyektlardan foydalanishni boshqarishning quyidagi usullari keng tarqalgan:

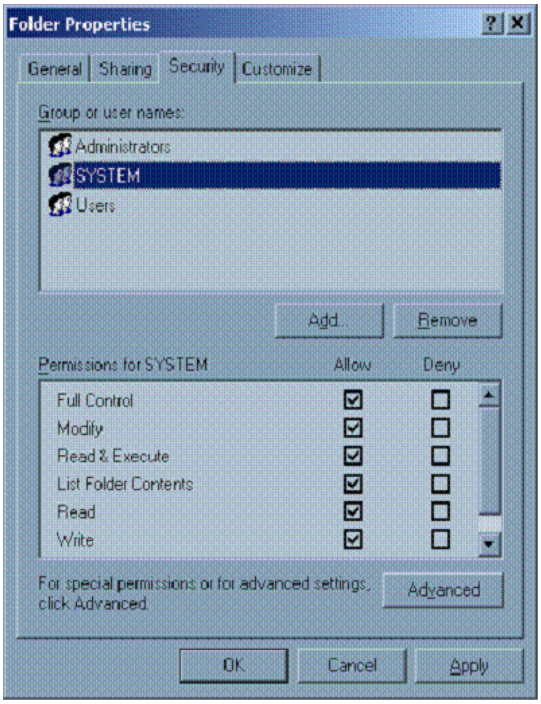
- foydalanishni diskretsion boshqarish usuli (Discretionary access control, DAC);
- foydalanishni mandatli boshqarish usuli (Mandatory access control, MAC);
- foydalanishni rollarga asoslangan boshqarish usuli (Role-based access control, RBAC);
- foydalanishni atributlarga asoslangan boshqarish usuli (Attribute-based access control, ABAC).

Tizimda ushbu usullarning bir-biridan alohida-alohida foydalanilishi talab etilmaydi, ya’ni ularning kombinatsiyasidan ham foydalanish mumkin.

Foydalanishni boshqarishning DAC usuli. Foydalanishni boshqarishning mazkur usuli tizimdagi shaxsiy aktivlarni himoyalash uchun qo‘llaniladi. Bunga ko‘ra obyekt egasining o‘zi undan foydalanish huquqi va foydalanish turini belgilaydi.

DAC da subyektlar tomonidan obyektlarni boshqarish subyektlarning identifikatsiya axborotiga asoslanadi. Masalan, UNIX operatsion tizimida fayllarni himoyalashda, fayl egasi qolganlarga *o‘qish (read, r), yozish (write, w)* va *bajarish (execute, x)* amallaridan bir yoki bir nechtasini berishi mumkin. Umumiy holda DAC usuli aksariyat operatsion tizimlarda foydalanishlarni boshqarishda foydalaniladi.

Masalan, 4.4-rasmda DAC usulini Windows NT/2k/XP OTlarida foydalanish holati keltirilgan.



4.4-rasm. Windows XP da DACdan foydalanish

Biroq, DACning jiddiy xavfsizlik muammosi - ma’lumotlardan foydalanish huquqiga ega bo‘lmagan subyektlar tomonidan foydalanilmasligi to‘liq kafolatlanmaganligi. Bu holat ma’lumotlardan foydalanish huquqiga ega bo‘lgan biror bir foydalanuvchining ma’lumot egasining ruxsatisiz foydalanish huquqiga ega bo‘lmagan foydalanuvchilarga yuborish imkoniyati mavjudligida namoyon bo‘ladi. Bundan tashqari, DACning yana bir kamchiligi tizimdagi barcha obyektlar ulardan foydalanishni belgilaydigan suyektlarga tegishli ekanligi. Amalda esa, tizimdagi barcha ma’lumotlar shaxslarga tegishli bo‘lmay, balki butun tizimga tegishli bo‘ladi. Bularga yaqqol misol sifatida axborot tizimini keltirish mumkin.

DACning klassik tizimida, dastlab obyekt hech kimga biriktirilmagan bo‘lsa, “yopiq” obyekt deb ataladi. Agar obyekt foydalanuvchiga biriktirilgan va ulardan foydalanish bo‘yicha cheklovlar o‘rnatilgan bo‘lsa, “ochiq” obyekt deb ataladi.

Foydalanishni boshqarishning MAC usuli. MAC usuli bo‘yicha foydalanishni boshqarish xavfsizlik siyosati ma’muriga markazlashgan holda boshqarishni amalga oshirish imkoniyatini beradi. Bunda foydalanuvchi xavfsizlik siyosatini o‘zgartira olmaydi. DAC usulida esa

obyektning egasi xavfsizlik siyosatini quradi va kimga foydalanish uchun ruxsat berilishini belgilaydi.

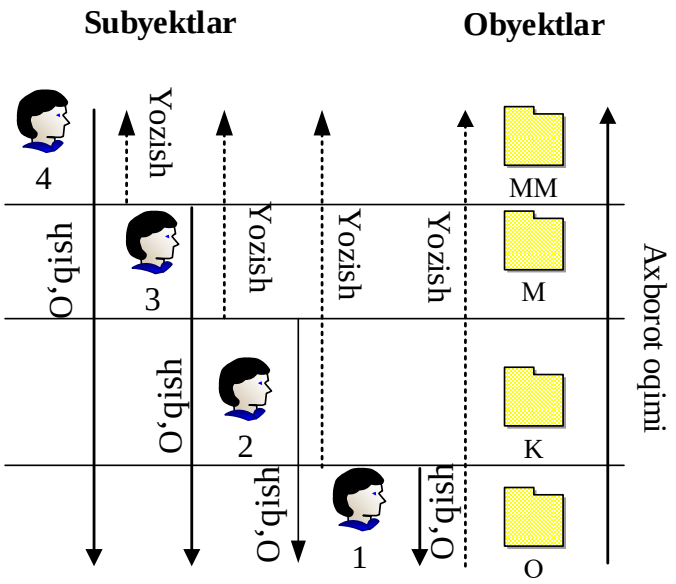
Foydalanishni boshqarishning MAC usuli xavfsizlik siyosati ma’muriga tashkilot bo‘ylab xavfsizlik siyosatini amalga oshirish imkoniyatini beradi. MAC usulida foydalanuvchilar tasodifan yoki atayin ushbu siyosatni bekor qila olmaydilar. Bu esa xavfsizlik ma’muriga barcha foydalanuvchilar uchun bajarilishi kafolatlangan markazlashgan siyosatni belgilashga imkon beradi.

MAC usulida foydalanishni boshqarish subyektlar va obyektlarni tasniflashga asoslanadi. Tizimning har bir subyekti va obyekti bir nechta xavfsizlik darajasiga ega bo‘ladi. Obyektning xavfsizlik darajasi tashkilotda obyektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi. Subyektning xavfsizlik darajasi esa unga ishonish darajasi bilan belgilanadi. Oddiy holda xavfsizlik darajasi uchun: “*mutlaqo maxfiy” (MM)*, “*maxfiy” (M)*, *“konfidensial” (K)* va “*ochiq” (O)* belgilar tayinlanadi. Bu yerda, *MM>M>K>O.*

MAC asosida axborot maxfiyligini ta’minlash. Agar obyekt va subyektning xavfsizlik darajalari orasidagi bir qancha bog‘liqlik shartlari bajarilsa, u holda subyekt obyektdan foydalanish huquqiga ega bo‘ladi. Xususan, quyidagi shartlar bajarilish kerak (4.5-rasm):

- agar subyektning xavfsizlik darajasida obyektning xavfsizlik darajasi mavjud bo‘lsa, o‘qish uchun ruxsat beriladi;
- agar subyektning xavfsizlik darajasi obyektning xavfsizlik darajasida mavjud bo‘lsa, yozishga ruxsat beriladi.

Ushbu modelda foydalanuvchi va subyekt tushunchalari bir – biridan farqlanadi. Xususan, xavfsizlik darajasi subyektga berilsa, foydalanuvchi esa u yoki bu vaqtda subyekt nomidan ish qilishi mumkin bo‘ladi. Shuning uchun, turli hollarda bir foydalanuvchi turli subyekt nomidan ish ko‘rishi mumkin bo‘ladi. Biroq, biror aniq vaqtda foydalanuvchi faqat bitta subyekt nomidan ish qilishi muhim hisoblanadi. Bu axborotni yuqori sathdan quyi sathga uzatilmasligini ta’minlaydi.



4.5-rasm. Axborot xavfsizligini ta’minlash uchun axborot oqimini boshqarish sxemasi

Yuqorida keltirilgan modelni muvofiqligini shubha ostiga qo‘yadigan ikkita noaniq fikr mavjud:

1. Quyi sathli foydalanuvchi barcha yuqori sathli obyektlarga yozishi mumkin. Bu holda u o‘zining mavjud obyektini ham qayta yozishi mumkin va bu o‘chirishga teng bo‘ladi. Ushbu kamchilikni yuqori darajadagi yozishni taqiqlash orqali bartaraf etish mumkin. Ushbu sxema uchun qoidalar quyidagicha bo‘ladi:

- agar subyektning xavfsizlik darajasi o‘zida obyektning xavfsizlik darajasini qamragan bo‘lsa, o‘qish uchun ruxsat beriladi;
- agar subyektning xavfsizlik darajasi obyektning xavfsizlik darajasiga teng bo‘lsa, yozishga ruxsat beriladi.

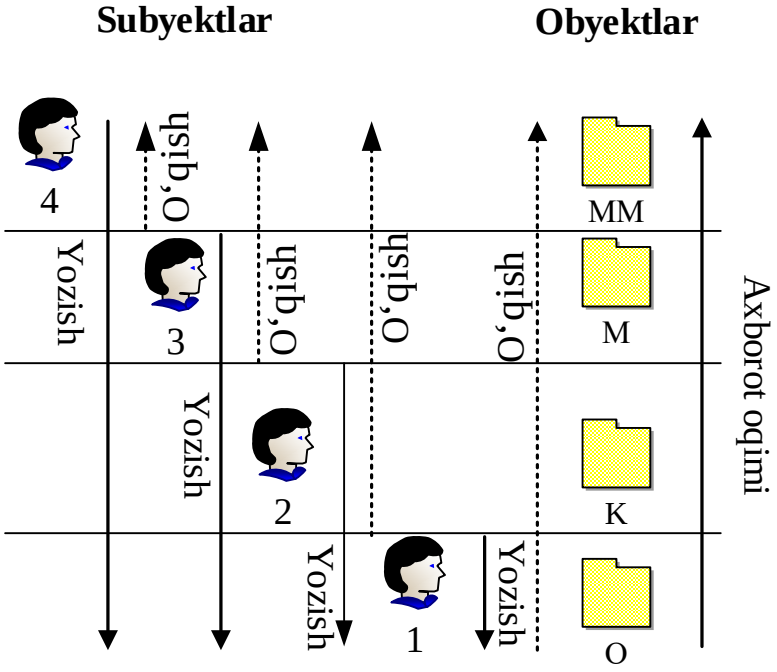
2. Sxemadan ko‘rinib turibdiki, yuqori darajali ishonchga ega foydalanuvchilar xavfsizlik darajasi past bo‘lgan obyektlarni o‘zgartira olmaydi. Ushbu muammoni bartaraf etishda foydalanuvchi turli hujjatlardan foydalanish uchun turli darajadagi ishonchga ega bo‘lgan subyektlar nomidan ish ko‘rishi mumkin. Ya’ni, “M” darajasiga ega foydalanuvchi o‘zi, “K” va “O” ishonch darajasidagi subyektlar nomidan ish ko‘rishi mumkin.

Axborot ishonchligini ta’minlash. Axborot konfidensialligini ta’minlashdan tashqari, ba’zida axborot ishonchligini ta’minlash ham talab etiladi. Ya’ni, obyektning ishonchlik darajasi qanchalik yuqori bo‘lsa, subyektning ishonchligi ham shunchalik yuqori va subyektning xavfsizlik darajasi qanchalik yuqori bo‘lsa, u tizimga shuncha ishonchli

ma’lumotlarni kiritishi mumkin. Mazkur model uchun yuqorida keltirilgan qoidalarni quyidagicha o‘zgartirish mumkin:

- agar subyektning xavfsizlik darajasida obyektning xavfsizlik darajasi mavjud bo‘lsa, yozish uchun ruxsat beriladi;
- agar subyektning xavfsizlik darajasi obyektning xavfsizlik darajasida bo‘lsa, o‘qishga ruxsat beriladi.

Ko‘rinib turibdiki, 4.5-rasmda keltirilgan holatlarning o‘rni almashgan (4.6-rasm). MAC usulida xavfsizlik darajalaridan foydalanish bilan bir qatorda obyekt va subyektlarning kategoriyalaridan ham foydalanish mumkin. Bu holda xavfsizlik darajasidan tashqari har bir obyekt va subyektga tegishli bo‘lgan toifalar ro‘yxati berilishi mumkin. Obyektning kategoriyalari ushbu obyekt ishlatiladigan joylarni tavsiflash uchun ishlatilsa, subyektning kategoriyasi esa uning qaysi sohada ishlashini tavsiflaydi. Bunday tizim foydalanishlarni yanada batafsil boshqarish imkoniyatini beradi.



4.6-rasm. Ma’lumotlar ishonchligini ta’minlash uchun axborot oqimini boshqarish sxemasi

Foydalanishni boshqarishning RBAC usuli. RBAC usulida foydalanishni boshqarishning asosiy g‘oyasi tizimning ishlash prinsipini tashkilotdagi kadrlar vazifasini haqiqiy ajratilishiga maksimal darajada yaqinlashtirishdir.

RBAC usulida foydalanuvchini axborotdan foydalanilishini boshqarish uning tizimdagi harakat xiliga asoslanadi. Ushbu usuldan

foydalanish tizimdagi rollarni aniqlashni nazarda tutadi. Rol tushunchasini muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida qarash mumkin. Shunday qilib, har bir obyekt uchun har bir foydalanuvchining foydalanish ruxsatini belgilash o‘rniga, rol uchun obyektlardan foydalanish ruxsatini ko‘rsatish yetarli. Bunda, foydalanuvchilar o‘z navbatida o‘zlarining rollarini ko‘rsatishadi. Biror rolni bajaruvchi foydalanuvchi rol uchun belgilangan foydalanish huquqiga ega bo‘ladi.

Umuman olganda, foydalanuvchi turli vaziyatlarda turli rollarni bajarishi mumkin. Xuddi shu rolni ba’zida bir nechta foydalanuvchilar bir vaqtning o‘zida ishlatishlari mumkin. Ba’zi tizimlarda foydalanuvchiga bir vaqtning o‘zida bir nechta rollarni bajarishga ruxsat berilsa, boshqalarida har qanday vaqtda bir-biriga zid bo‘lmagan bir yoki bir nechta rollarga cheklov mavjud bo‘lishi mumkin.

RBAC usulining asosiy afzalliklari quyidagilar:

1. Ma’murlashning osonligi. Foydalanishlarni boshqarishning klassik modellarida obyekt bo‘yicha muayyan amallarni bajarish huquqlari har bir foydalanuvchi yoki foydalanuvchilar guruhi uchun ro‘yxatga olingan bo‘ladi. Rolli modelda rol va foydalanuvchi tushunchalarini ajratish vazifasini ikki qismga ajratish imkonini beradi: foydalanuvchi rolini aniqlash va rol uchun obyektga bo‘lgan ruxsatni aniqlash. Ushbu yondashuv, foydalanuvchi javobgarlik sohasini o‘zgartirganida undan eski rolni olib tashlash va yangi vazifasiga mos keladigan rolni berishning o‘zi boshqaruv jarayonini sezilarli darajada soddalashtiradi. Agar foydalanish huquqi bevosita foydalanuvchi va obyektlar o‘rtasida aniqlansa, foydalanuvchining yangi huquqlarini qayta tayinlash muolajasi ko‘p harakatlarni talab etar edi.

2. Rollar iyerarxiyasi. Rollarning haqiqiy iyerarxiyasini yaratish orqali real biznes jarayonlarini aks ettiruvchi rollar tizimini yaratish mumkin. Har bir rol o‘z imtiyozlari bilan bir qatorda boshqa rollarning imtiyozlariga ega bo‘lishi mumkin. Ushbu yondashuv tizimni boshqarishni sezilarli darajada osonlashtiradi.

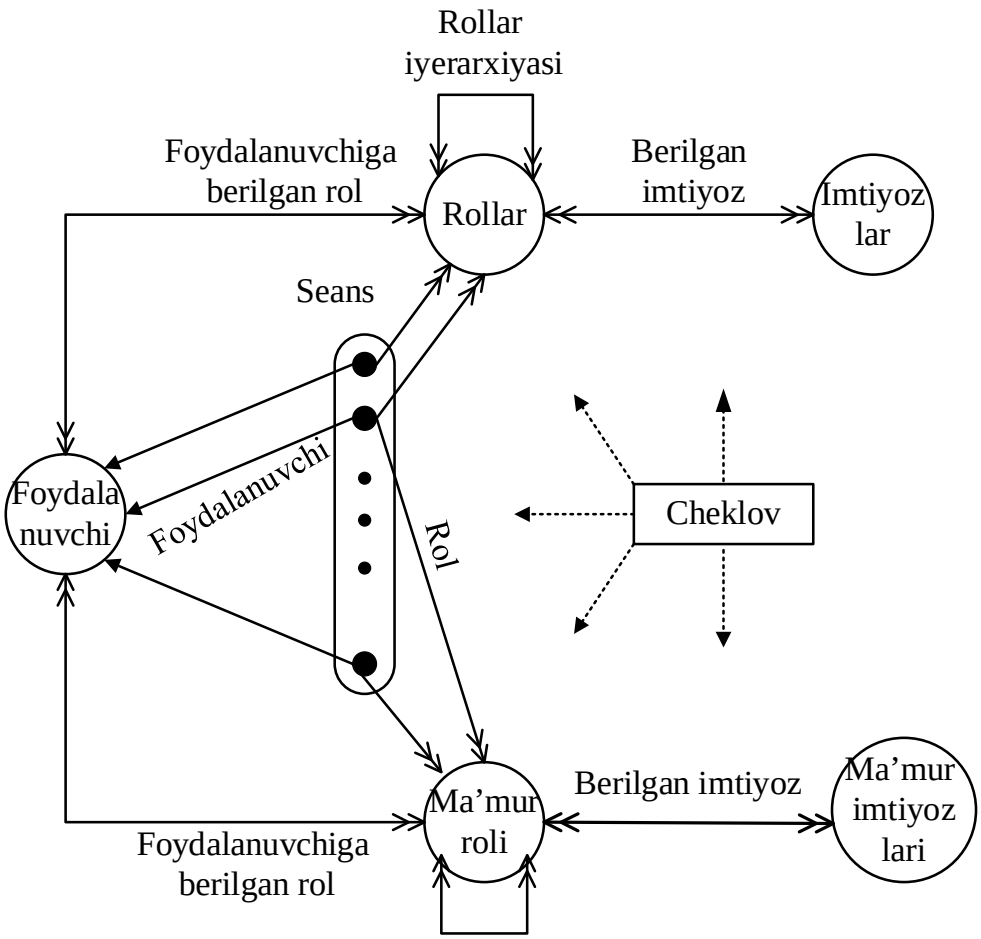
3. Eng kam imtiyoz prinsipi. Rolli model foydalanuvchiga tizimda kerakli vazifalarni bajarishga imkon beruvchi eng kichik rol bilan ro‘yxatdan o‘tish imkonini beradi. Ko‘plab rollarga ega foydalanuvchilar aniq bir vazifani bajarishi uchun o‘zining barcha imtiyozlaridan foydalanishi har doim ham talab etilmaydi.

Eng kam imtiyoz prinsipi tizimdagi ma’lumotlarning ishonchligini ta’minlash uchun juda muhimdir. Bu foydalanuvchiga imkoniyatlari

orasidan faqat muayyan vazifani bajarishi uchun kerak bo‘lganini berilishini talab etadi. Buning uchun rol maqsadini aniqlash, uni bajarish uchun zarur bo‘lgan imtiyozlarni to‘plash va bu asosida foydalanuvchi imtiyozlarini cheklash talab etiladi. Joriy vazifani bajarish uchun talab qilinmaydigan foydalanuvchi imtiyozlarini rad etish tizimni xavfsizlik siyosatini buzilishidan saqlaydi.

4. Majburiyatlarni ajratish. Tizimda foydalanishlarni boshqarishning yana bir muhim prinsiplaridan biri – vazifalarni taqsimlashdir. Firibgarlikni oldini olish uchun bir shaxs tomonidan ko‘plab vazifalarni bajarish talab etilmaydigan holatlar amalda yetarlicha mavjud. Bunga misol sifatida bir kishi tomonidan to‘lov ma’lumotini yaratish va uni tasdiqlashni keltirish mumkin. Shubhasiz, bu amallarni bir shaxs bajara olmaydi. Rollarga asoslangan usul esa ushbu muammoni maksimal darajada osonlik bilan hal qilishga yordam beradi.

Rasman RBAC modelini quyidagicha tasvirlash mumkin (4.7-rasm):



4.7-rasm. RBAC modelining tasviri

Model quyidagi tarkibga ega: foydalanuvchilar, rollar va imtiyozlar. Foydalanuvchi inson yoki uning nomidan ish ko‘ruvchi dastur bo‘lishi mumkin. Rol foydalanuvchining tashkilotdagi faoliyati turi bo‘lsa, imtiyoz tizimning bir yoki bir nechta obyektlaridan foydalanishi uchun aniqlangan ruxsat. Tasvirdagi “rollarni foydalanuvchilarga tayinlash” va “imtiyozlarni tayinlash” munosabati ko‘pgina turga tegishli. Ya’ni, foydalanuvchi bir nechta rollarga ega bo‘lishi va bir nechta foydalanuvchi bir rolda bo‘lishi mumkin. Shunga o‘xshash, bir qancha imtiyozlar bitta rolga tegishli yoki bir nechta rollar bitta imtiyozga ega bo‘lishi mumkin.

Foydalanishni boshqarishning ABAC usuli. Atributlarga asoslangan foydalanishlarni boshqarish usuli (ABAC) - obyektlar va subyektlarning atributlari, ular bilan mumkin bo‘lgan amallar va so‘rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. Undagi qoidada har qanday turdagi attributlardan (foydalanuvchi atributlari, resurs atributlari, obyekt va muhit atributlari va h.) foydalanish mumkin. Ushbu model so‘rovni, resursni va harakatni kim bajarayotgani to‘g‘risidagi holatlar “AGAR, U HOLDA” dan tashkil topgan qoidalarga asoslanadi. Masalan, AGAR talabgor boshqaruvchi bo‘lsa, U HOLDA maxfiy ma’lumotni o‘qish/ yozish huquqi berilsin.

Atributga asoslangan siyosat normativ talablar murakkabligini kamaytirish orqali foydalanishni boshqarishni yanada samarali amalga oshiradi. Xuddi shu atributlarga asoslangan siyosat turli tizimlarda ishlatilishi bir tashkilotda yoki hamkorlikdagi tashkilotlarda resurslardan foydalanishda muvofiqlikni boshqarishga yordam berishi mumkin. Bunday markazlashgan foydalanishni boshqarish yagona vakolatli manbani o‘z ichiga olgani bois, har bir aniq tizim talablariga o‘z siyosati bilan moslikni tekshirishni talab etmaydi.

Atributlarga asoslangan foydalanishni boshqarishdagi asosiy standartlardan biri bu - XACML (*eXtensible Access Control Markup Language*) bo‘lib, 2001 yilda OASIS (*Organization for the Advancement of Structured Information Standards*) tomonidan ishlab chiqilgan.

XACML standartida quyidagi asosiy tushunchalar mavjud: qoidalar (rules), siyosat (policy), qoidalar va siyosatni mujassamlashtirgan algoritmlar (rule-combing algorithms), atributlar (attributes) (subyekt, obyekt, harakat va muhit shartlari), majburiyatlar (obligations) va maslahatlar (advices). Qoida markaziy element bo‘lib, maqsad, ta’sir, shart, majburiyat va maslahatlarni o‘z ichiga oladi. Maqsad – subyektning obyekt ustida qanday harakatlarni amalga oshirishi (o‘qish, yozish, o‘chirish va h.). Ta’sir mantiqiy ifodalarga asoslangan va tizimdan

foydalanish uchun *ruxsat, taqiq, mumkin emas, aniqlanmagan* holatlaridan biriga asoslangan ruxsatni berishi mumkin. *Mumkin emas* buyrug‘ining mantiqiy shart noto‘g‘ri bo‘lganida qaytarilishi, ifodani hisoblash vaqtida yuzaga kelgan xatoliklar uchun *aniqlanmagan* ta’sirning mavjudligini ko‘rsatadi. Quyida ABAC usuliga misol keltirilgan.

Maqsad	Bemorni tibbiy kartasidan qon guruhini bilish
Harakat	Ruxsat
Shart	Subyekt.lavozimi=Vrach & muhit.vaqt >= 8:00 & muhit.vaqt <=18:00
Majburiyat	Tibbiy yozuvini ko‘rish sanasini (muhit.vaqt) ro‘yxatga olish jurnalida ko‘rsatish.

Foydalanishni boshqarishning mazkur usulidan Cisco Enterprise Policy Manager mahsulotlarida, Amazon Web Service, OpenStack kabilarda foydalanib kelinmoqda.

Foydalanishni boshqarish matritsasi. Avtorizatsiyaning klassik ko‘rinishi Lampsonning foydalanishni boshqarish matritsasidan boshlanadi. Ushbu matrisa operatsion tizimni barcha foydalanuvchilar uchun turli ma’lumotlarni boshqarishi xususidagi qarorni qabul qilishida zarur bo‘lgan barcha axborotni o‘z ichiga oladi. Bunda, operatsion tizimdagi foydalanuvchilar *subyekt* sifatida va tizim resurslari *obyekt* sifatida qaraladi. Avtorizatsiya sohasidagi ikkita asosiy tushuncha: *foydalanishni boshqarish ro‘yxati (Access control list, ACL)* va *imtiyozlar ro‘yxati (Capability list, C-list)* hisoblanib, har ikkalasi ham Lampsonning foydalanishni boshqarish matrisasidan olingan. Ya’ni, matrisaning satrlari subyektlarni, ustunlari esa obyektlarni ifodalaydi. Biror subyekt S va obyekt O uchun berilgan imtiyozlar ularning matrisadagi indekslari kesishgan nuqtada saqlanadi. 4.1-jadvalda foydalanishni boshqarish matrisasi keltirilgan, unda imtiyozlar UNIX operatsion tizimidagi imtiyozlar shaklida, ya’ni, x, r va w lar mos ravishda *bajarish, o‘qish* va *yozish* amalini anglatadi.

Keltirilgan jadvalda buxgalteriyaga oid dastur ham subyekt ham obyekt sifatida olingan. Bu foydali tanlov bo‘lib, buxgalteriyaga oid ma’lumotlarni faqat buxgalteriyaga oid dastur tomonidan foydalanish imkonini beradi. Ya’ni, turli buxgalteriya tekshiruvlari va balans haqidagi

ma’lumotlar faqat buxgalteriyaga oid dasturiy ta’minot tomonidan foydalanilishi shart va yuqoridagi matrisada keltirilgan shakl buni ta’minlaydi. Biroq, bu matrisa tizim ma’muri Sem buxgalteriga oid dasturni noto‘g‘ri versiya bilan almashtirish yoki soxta versiya bilan almashtirish orqali ushbu himoyani buzishi mumkinligi sababli bo‘lishi mumkin bo‘lgan barcha hujumlarni oldini olmaydi. Ammo, bu usul Alisa va Bobga buxgalteriya ma’lumotlaridan atayin yoki bexosdan buzilishiga yo‘l qo‘ymasdan foydalanish huquqini beradi.

4.1-jadval

Foydalanishni boshqarish matrisasi

Obyekt / Subyekt	**Operat-sion tizim**	**Buxgalte-riyaga oid dastur**	**Buxgalte-riyaga oid ma’lumot**	**Sug‘urta ma’lu-moti**	**To‘lov qaydno-masi ma’lu-moti**
Bob	rx	rx	r	-	-
Alisa	rx	rx	r	rw	rw
Sem	rwx	rwx	r	rw	rw
Buxgal-teriyaga oid dastur	rx	rx	rw	rw	r

ACL yoki C-list. Foydalanishni boshqarish jadvali avtorizatsiya qarorlariga tegishli barcha ma’lumotlardan tashkil topgan. Biroq, yuzlab (yoki undan ko‘p) subyektlar va minglab (yoki undan ko‘p) obyektlar mavjud bo‘lgan tizimda, millionlab (yoki undan ko‘p) yozuvlarga ega bo‘lgan foydalanishni boshqarish matritsasi yordamida avtorizatsiya amallarini bajarish hisoblash tizimi uchun katta yuklamani keltirib chiqaradi.

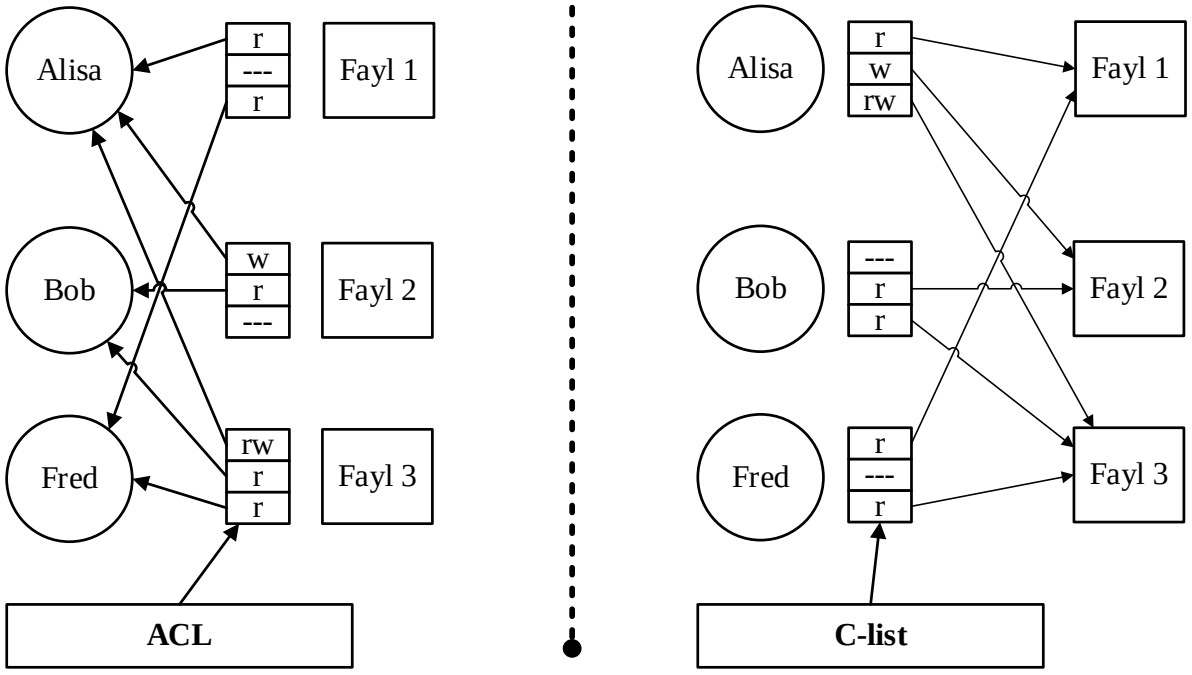
Avtorizatsiya amallarini maqbul amalga oshirish uchun, foydalanishni boshqarish matritsasi boshqariluvchi qismlarga bo‘linishi shart. Foydalanishni boshqarish matritsasini qismlarga ajratishning ikkita usuli mavjud. Birinchi usulga binoan matritsa ustunlar bo‘yicha bo‘linadi va har bir ustun mos obyekt bilan saqlanadi. U holda, obyektdan foydalanishga murojaat bo‘lganida foydalanishni boshqarish matrisasining ushbu ustuni olinadi va amalni bajarishga ruxsat berilganligi tekshiriladi. Ushbu ustunlarni ACL kabi tasavvur qilish mumkin. Masalan, 4.1-jadvaldagi sug‘urta ma’lumotiga tegishli bo‘lgan ACL quyidagicha:

(Bob,-),(Alisa,rw),(Sem,rw),(buxgalteriyaga oid dastur,rw)

Ikkinchi usulga binoan matritsa satrlar bo‘yicha bo‘linadi va har bir satr mos subyekt bilan saqlanadi. U holda, subyekt tomonidan biror amalni bajarishga harakat qilinsa, amalni bajarishga ruxsat borligini bilish uchun foydalanishni boshqarish matritsasining tegishli satriga qaraladi. Mazkur yondashuv imtiyozlar ro‘yxati yoki C-list deb ataladi. Masalan, 4.1-jadvaldagi Alisaning imtiyozlar ro‘yxati yoki C-list quyidagiga teng:

(OT,rx),(buxgalteriyaga oid dastur, rx), (buxgalteriyaga oid ma’lumot, r), (sug‘urta ma’lumoti, rw),(to‘lov qaydnomasi ma’lumoti, rw)

ACL va C-list o‘zaro ekvivalent bo‘lsada, ular bir xil axborotni o‘zida turlicha saqlaydi. Biroq, ular orasida sezilmas farq mavjud. ACL va C-listning o‘zaro qiyosiy tahlili 4.8-rasmda keltirilgan.



4.8-rasm. ACL va C-list

4.8-rasmdagi ko‘rsatkichlar qarama-qarshi yo‘nalishlardaligini, ya’ni, ACL uchun ko‘rsatkichlar resurslardan foydalanuvchilarga qarab yo‘nalgan bo‘lsa, C-list uchun esa ko‘rsatkichlar foydalanuvchilardan resurslarga qarab yo‘nalganligini ko‘rish mumkin. Bu ahamiyatsiz ko‘ringan farq imtiyozlar ro‘yxati (C-list) bilan foydalanuvchilar va fayllar orasidagi aloqadorlik tizim ichida qurilishini anglatadi. ACLga

asoslangan tizimda esa, foydalanuvchilarni fayllarga aloqadorligi uchun alohida usullar talab etilgani bois, C-list ACL ga nisbatan xavfsizlik nuqtai nazaridan, bir qancha afzalliklarga ega va shuning uchun C-list ustida kam sonli ilmiy tadqiqot ishlari olib borilgan.

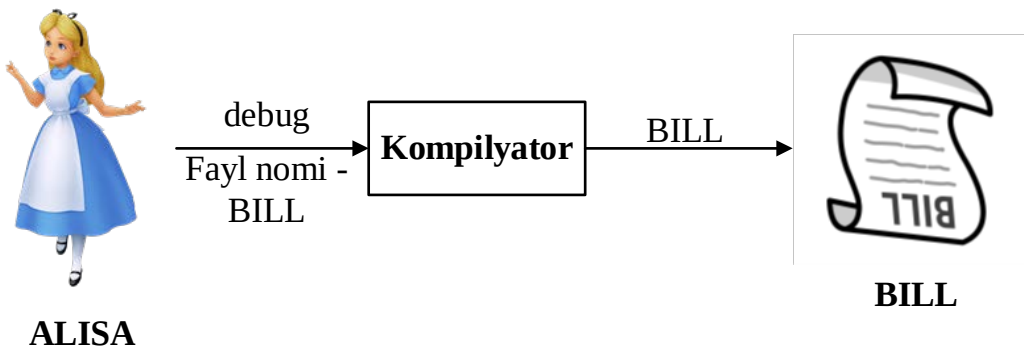
Tartibsiz yordamchi – ko‘p jabhalarda klassik xavfsizlik muammosi. Ushbu muammoni yoritish uchun, ikkita resursga ega tizim olingan: birinchi resurs kompilyator bo‘lsa, ikkinchisi maxfiy to‘lov axborotidan iborat bo‘lgan BILL deb nomlangan fayl va bir foydalanuvchi, Alisadan iborat. Bunda, kompilyator ixtiyoriy faylga yozish imkoniyatiga ega va Alisa kompilyatorni ishga tushira oladi. Buning uchun debaggerlash (dasturdagi xatolikni topish jarayoni) ma’lumoti yoziluvchi fayl nomini kiritish talab etiladi. Biroq, Alisaga BILL nomli faylni zararlashi mumkinligi sababli, unga yozish ruxsati mavjud emas. Ushbu ssenariy uchun foydalanishni boshqarish matritsasi 4.2-jadvalda keltirilgan.

4.2-jadval

Tartibsiz yordamchi holati uchun foydalanishni boshqarish matritsasi

	Kompilyator	**BILL**
Alisa	x	-
Kompilyator	rx	rw

Faraz qilaylik, Alisa kompilyatorni ishga tushirdi va fayl nomi sifatida BILL ni ko‘rsatdi. Alisa ushbu imtiyozga ega bo‘lmagani uchun, mazkur buyruq amalga oshirilmaydi. Biroq, Alisa nomidan ish ko‘ruvchi kompilyator BILL faylini qayta yozish imkoniyatiga ega. Agar kompilyator o‘z imkoniyati bilan ishlasa va u Alisa tomonidan ishga tushirilsa, u holda BILL faylini zararlashi mumkin (4.9-rasm).



4.9-rasm. Tartibsiz yordamchi

Bu nima uchun tartibsiz yordamchi deb ataladi? Kompilyator Alisa tomonida va shuning uchun uning yordamchisi bo‘lgani bois, Alisaning imtiyoziga ko‘ra ish ko‘rish o‘rniga o‘zining imtiyoziga asosan ish ko‘rmoqda.

ACL bilan mazkur holatini oldini olish juda ham murakkab (lekin imkonsiz emas). Boshqa tomondan, C-list yordamida buni osonlikcha bartaraf etish mumkin. Imtiyozga asoslangan tizimlarda, Alisa kompilyatorga murojaatni amalga oshirganida, unga o‘zining C-listini beradi. Bu holda kompilyator Alisaning C-listini tekshiradi va agar imtiyozi bo‘lgan taqdirda debaggerlash faylini yaratadi. Alisani BILL faylini qayta yozishga ruxsati bo‘lmagani sababli, 4.9-rasmdagi holat kuzatilmaydi.

ACL va C-listning foydali tomonlarini o‘zaro taqqoslash juda ham foydali. ACL odatda foydalanuvchi o‘zining ma’lumotlarini boshqarishida va himoya ma’lumotga qaratilgan hollarda afzal ko‘riladi. Bundan tashqari, ACL bilan biror resursga huquqlarni almashtirish oson. Boshqa tomondan, imkoniyatlar ro‘yxati bilan vakolatlar berish oson va foydalanuvchining qo‘shishi yoki o‘chirishi juda ham oson. Vakolat berish qobiliyati tufayli tartibsiz yordamchi muammolaridan osonlik bilan qochish mumkin. Biroq, imkoniyatlarni amalga oshirish biroz murakkab va yuqori harajatni talab etadi. Bu aniq bo‘lmasada, taqsimlangan tizimlarga xos bo‘lgan ko‘plab muammolar undagi imkoniyatlar sababli kelib chiqadi. Shu sababli, ACLdan hozirgi kunda C-listdan ko‘ra ko‘proq foydalaniladi.

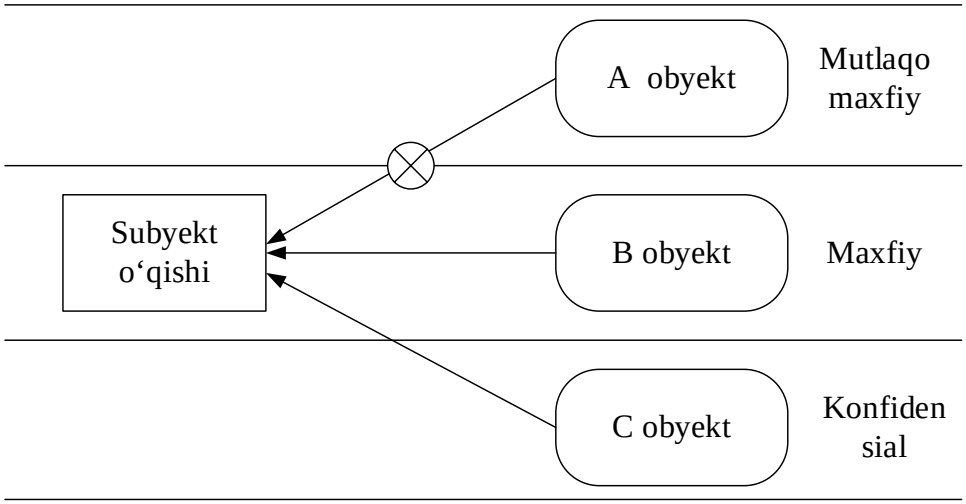
4.3. Ko‘p sathli xavfsizlik modellari

Ko‘p sathli xavfsizlikning (multilevel security, MLC) ko‘pgina modellari mavjud. Kuyida ular orasida eng soddalari bilan tanishib chiqiladi.

Bell-LaPadul modeli. Bell-Lapadul nomi uni yaratuvchilari Bell va LaPadul ismlari bilan bog‘liq. Ushbu model konfidensiallik darajasini hisobga olgan holda, foydalanishning mandatli boshqarish mexanizmlarini formallashtirish uchun ishlatiladi. Ma’lumki, foydalanishni cheklashning mandatli prinsipi obyektlar konfidensialligining iyerarxik sathlarining va ularga mos konfedensiallik belgilarining mavjudligini ko‘zda tutadi.

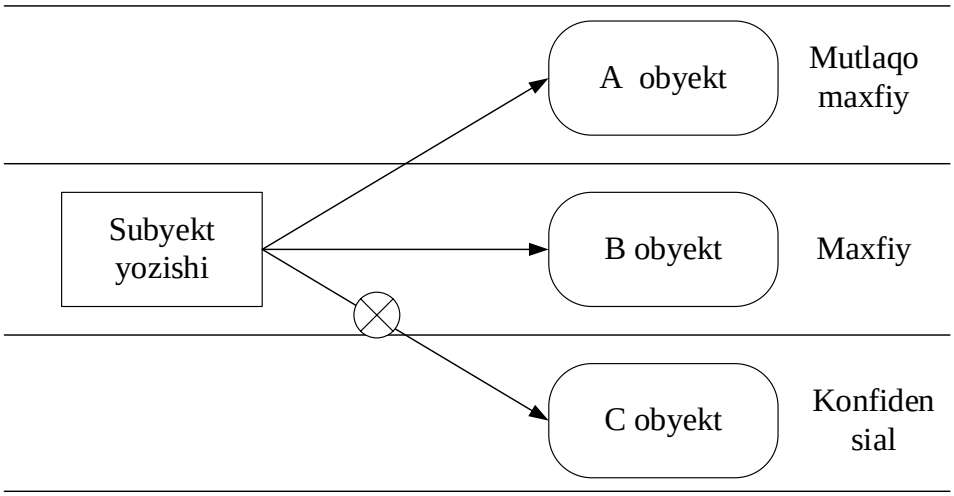
Bell-LaPadul modelida tizimdagi subyektlar va obyektlar maxfiylik grifi bo‘yicha taqsimlanadi va quyidagi mualliflik qoidalari bajariladi:

1. *“Xavfsizlikning oddiy qoidasi” (Simple Security).* Ushbu qoidaga binoan subyekt faqat xavfsizlik sathi o‘zining xavfsizlik sathidan yuqori bo‘lmagan hujjatlardan axborotni o‘qishga haqli. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.10–rasmda keltirilgan.



4.10-rasm. “Simple Security” xususiyati uchun axborot oqimlari sxemasi

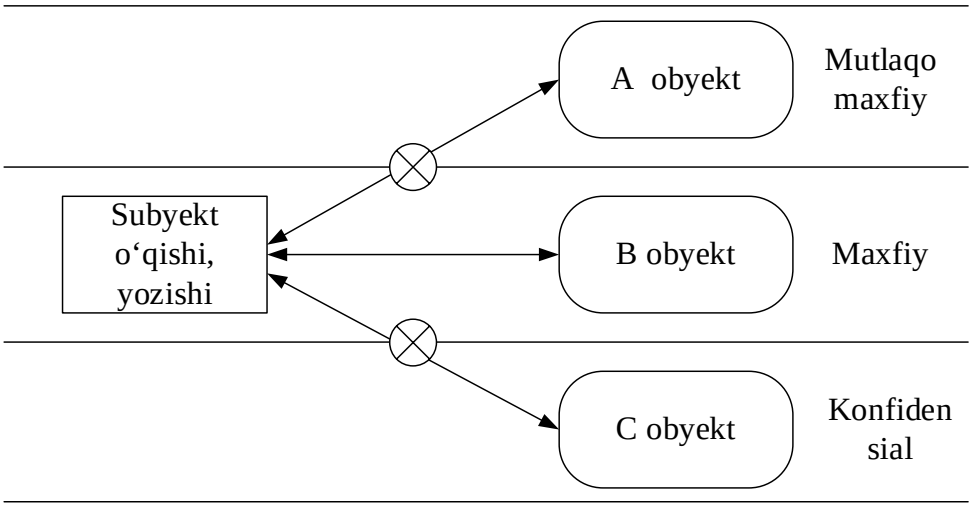
2. *“-Xususiyat” (-Property).* Ushbu qoidaga binoan subyekt xavfsizlik sathi o‘zining xavfsizlik sathidan past bo‘lmagan hujjatlarga axborot kiritishi mumkin. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.11–rasmda keltirilgan.



4.11-rasm. “-Property” xususiyati uchun axborot oqimlari sxemasi

3. *“-Qat’iy xususiyat” (-Strong Property).* Ushbu qoidaga binoan o‘qish va yozish xuquqiga ega subyekt faqat o‘zining sathidagi

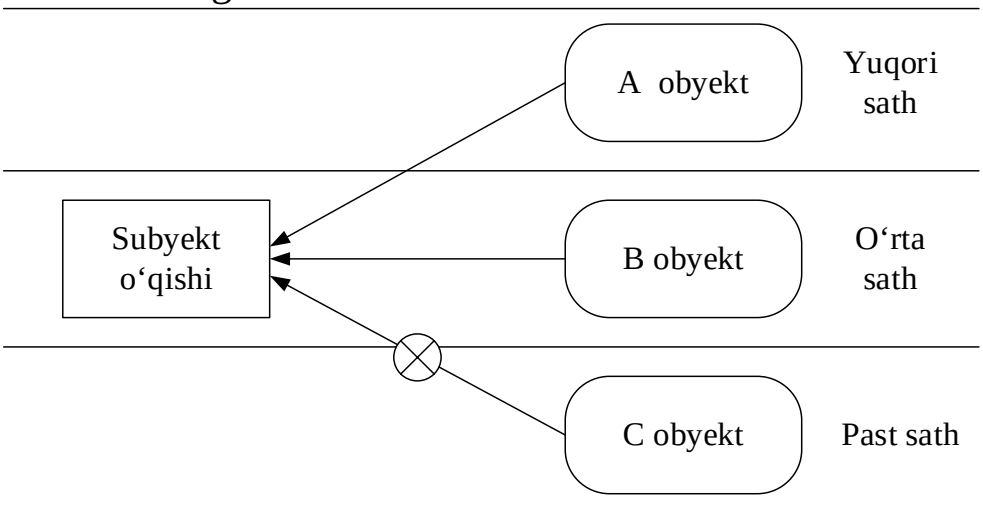
obyektlar bilan amallar bajarishi mumkin. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.12–rasmda keltirilgan.



4.12-rasm. “-Strong-property” xususiyati uchun axborot oqimlari sxemasi

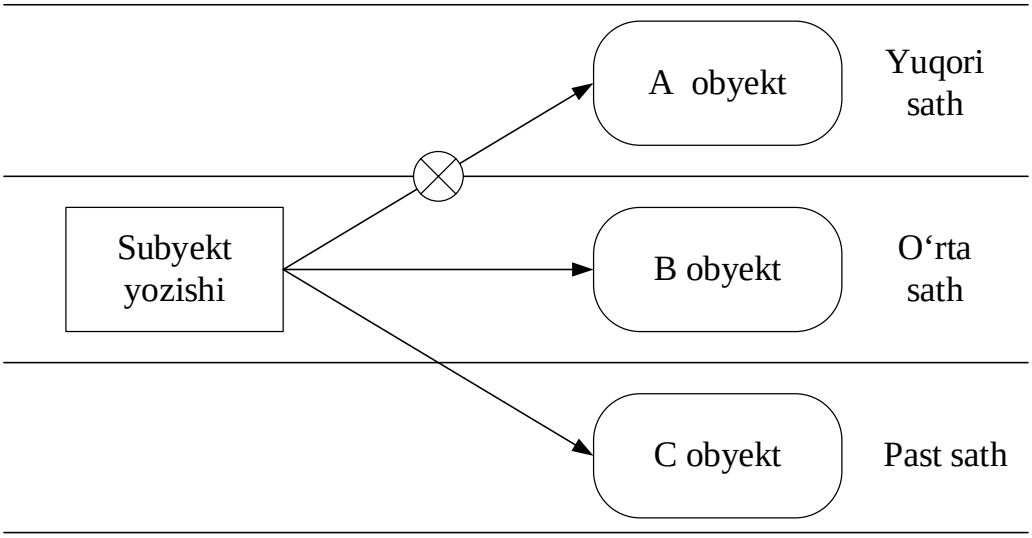
Biba modeli. Ushbu model Bell-LaPadul modelining modifikatsiyasi bo‘lib, ma’lumotlar yaxlitligini ta’minlashga yo‘naltirilgan. Biba modelining bazaviy qoidalari quyidagicha ifodalanadi:

1. *“Yaxlitlikning oddiy qoidasi” (Simple Integrity, SI).* Ushbu qoidaga binoan subyekt o‘zining sathidan past yaxlitlik sathidan axborotni o‘qiy olmaydi. Yaxlitlikning uchta sathiga ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.13–rasmda keltirilgan.



4.13-rasm. “Simple integrity” xususiyati uchun axborot oqimlari sxemasi

2. *“-Yaxlitlik” (-Property).* Ushbu qoidaga binoan subyekt o‘zining sathidan yuqori yaxlitlik sathiga axborotni yoza olmaydi. Yaxlitlikning uchta sathiga ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.14–rasmda keltirilgan.



4.14-rasm. “-Property” xususiyati uchun axborot oqimlari sxemasi

3. *“Chaqiruv xususiyati” (Invocation Property).* Ushbu qoidaga binoan subyekt yaxlitlikning yuqori sathidagi subyektdan servisni so‘ray olmaydi.

Ta’kidlash lozimki, Biba modelidagi yaxlitlik sathlarini ishonchlilik sathi sifatida qabul qilmoq lozim. Mos axborot oqimlarini esa axborotni ma’lumotlarning yuqori ishonchli majmuidan ishonchligi pastrog‘iga va aksincha uzatish kabi qabul qilish lozim.

Mantiqiy va fizik foydalanishlarni boshqarish. Foydalanishni boshqarishning mantiqiy vositalari infrastruktura va uning ichidagi tizimlarda mandat, tasdiqlash, avtorizatsiya va majburiyatlar uchun foydalaniladi. Ushbu komponentlar tizimlar, ilovalar, jarayonlar va axborot uchun foydalanishni boshqarish choralarini qo‘llaydi. Shuningdek, foydalanishni boshqarishning mazkur usuli dastur, operatsion tizim, ma’lumotlar bazasida ham qo‘llanilishi mumkin. Fizik foydalinishni boshqarish mexanik ko‘rinish bo‘lib, qulflanuvchi xonadan fizik foydalanishga o‘xshatish mumkin. Foydalanishni boshqarishni aslida mantiqiy va fizik turga ajratishning o‘zi noaniq hisoblanadi. Masalan, fizik nazoratlash odatda dasturlar, kartadagi chiplar va dasturiy ta’minot orqali ishlovchi elektrik qulflar orqali ishlaydi. Ya’ni, bu o‘rinda fizik foydalanishga mantiqiy deb ham qarash mumkin.

4.4. Ma’lumotlarni fizik himoyalash

Axborot xavfsizligini ta’minlashda amalga oshiriladigan dastlabki choralardan biri – *fizik xavfsizlik*. Ruxsatsiz fizik boshqaruvni, shaxslar amalga oshiradigan va muhitga bog‘liq tahdidlarni oldini olish uchun tashkilotlar mos fizik xavfsizlik boshqaruvi sharoitida bo‘lishi shart. Tizim ma’muri fizik xavfsizlikga qaratilgan tahdidlardan himoyalanish uchun fizik xavfsizlik choralari o‘rnatilganligini va me’yorida ishlayotganligini kafolatlashi zarur.

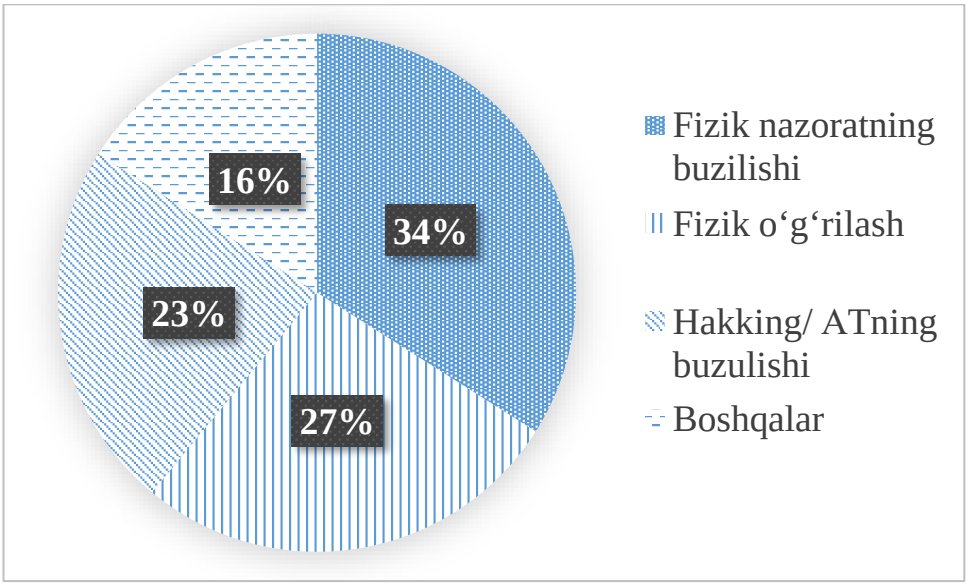
Fizik xavfsizlik qurilmalarni, shaxslarni, tarmoq va ma’lumotlarni hujumlardan himoyalaydi. Ma’lumot, tarmoq va qurilmalar himoyasi o‘zida tabiiy va sun’iy (inson tomonidan qilingan) tahdidlardan himoyalash vositalarini mujassamlashtiradi. Tashkilotlar fizik xavfsizlikni ta’minlash uchun mos himoya vositalaridan foydalanishda o‘z infrastrukturasi va axborot tizimlarining fizik xavfsizligiga ta’sir qiluvchi barcha holatlarni inobatga olishi shart.

Fizik xavfsizlik – tashkilot axborot xavfsizligi dasturining muhim qismlaridan biri bo‘lib, oldingi davrlarda insonlar fizik xavfsizlikni ta’minlashda kalit, qo‘riqchi, to‘siq, eshik va shunga o‘xshash vositalardan foydalanganlar. Hozirgi kunda, fizik xavfsizlikning shakli keskin o‘zgarib bormoqda va tashkilotlardan ishchi kuchlari, aktivlar va ko‘chmas mulklar himoyasining nazorati talab etilmoqda. Mazkur aktivlarning fizik xavfsizligini ta’minlash tashkilot uchun muhim vazifalardan biri bo‘lib, fizik xavfsizlikni loyihalashda binoning arxitekturasiga, jixozlanishiga, ishchi kuchlariga, tabiiy hodisalarga, quvvat manbaiga, haroratni nazoratlashga va boshqalarga e’tibor beriladi.

Fizik xavfsizlikning vazifasi, tashkilot binosini va aktivlarini o‘g‘irlikdan, bosqinchilikdan, tabiy ofatlardan, iqlim o‘zgarishlaridan, muhit o‘zgarishlaridan va inson tahdidlaridan himoyalashdir. Ko‘p sathli himoyalash choralari tashkilotni turli fizik tahdidlardan himoyalaydi. Xavfsizlikning birinchi sathi tashkilot binolariga tashqaridan kirishni va tashqi transport vositalarining harakatini nazoratlaydi. Mazkur himoya sathi tashqaridan keluvchini yoki buzg‘unchini tashkilot binosiga ruxsatsiz kirishini oldini oladi va dastlabki sathda tashkilotga bo‘lishi mumkin bo‘lgan xavflarni kamaytiradi. Himoyaning keyingi sathi transportlarni, insonlarni va boshqa tashkilot aktivlarini ichki va tashqi xavflardan himoyalaydi. Ushbu sathda uzluksiz elektr quvvati bilan ta’minlash, tashkilot asosiy binolarini mashinalar to‘xtash joylaridan ajratish, to‘g‘ri ventilyatsiya tizimiga ega yaxshi jixozlangan suv quvur tizimini mos joyga o‘rnatish, ogohlantirish tizimlari va h. amalga

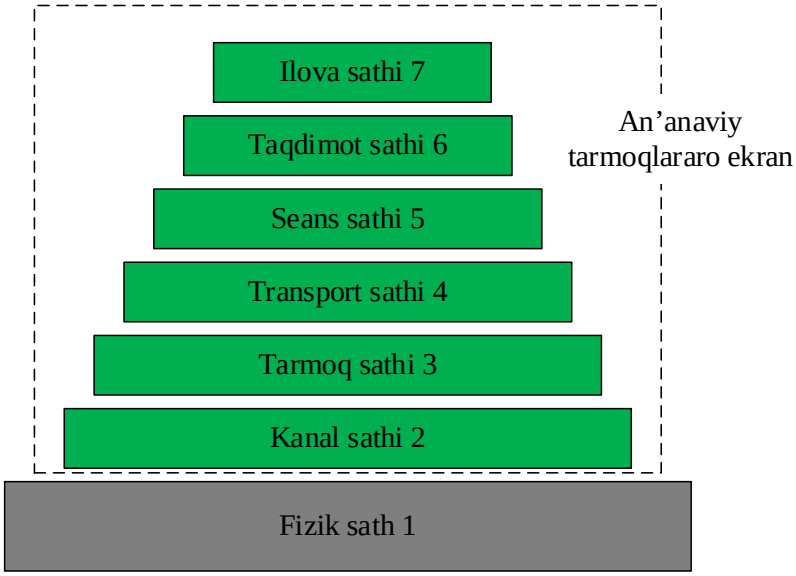
oshiriladi. Keyingi sath fizik himoyaning eng muhim qismi bo‘lib, tashqaridan va ichkaridan kiruvchi (xodimlar) nazoratlanadi. Agar buzg‘unchi fizik aktivga hujumni amalga oshirsa, u tashkilotning maxfiy axborotini qo‘lga kiritishi mumkin.

Fizik xavfsizlikning zaruriyati. Kiberxujumlarning murakkablashuvi hujumchilarning tashkilot fizik xavfsizligini buzishda turli usullardan foydalanishlariga sabab bo‘lmoqda. Hujumchilar tashkilotning fizik xavfsizlik tizimidagi zaifliklardan foydalanib o‘z harakatlarini amalga oshirishadi. AQShning Department of Health and Human Services Breach Portal tashkiloti tadqiqotlari 2015 yilda tashkilotlarda eng ko‘p uchraydigan xavfsizlik insidentlari fizik xavfsizlikni buzishga urinishlar ekanligini ko‘rsatgan (4.15-rasm).



4.15-rasm. HIPAA (Health Insurance Portability and Accountability Act) tadqiqotlariga ko‘ra buzilishlar diagrammasi

Fizik xavfsizlikning buzilishi boshqa xavfsizliklarni buzilishlaridan keskin farq qilib, juda ham kam hollarda texnik ma’lumotisiz amalga oshirilishi mumkin. Ana’naviy xavfsizlik choralari, masalan, tarmoqlararo ekran (FireWall), IDS (Instrusion Detection System) va boshqa himoya vositalarining fizik xavfsizligi ta’minlanmagan bo‘lsa, xavfsizlik muammolari yanada ortadi. Masalan, tarmoqlararo ekran OSI modelining turli sathlarida himoyani tashkil etadi. Biroq, tashkilotning fizik xavfsizligiga ta’sir eta olmaydi (4.16-rasm).



4.16-rasm. Tarmoq sathlarida tarmoqlararo ekranlardan foydalanilishi

Fizik xavfsizlik OSI modelining fizik sathida himoyani ta’minlaydi. Fizik sath quyidagilarni o‘z ichiga oladi:

- barcha kabel va tarmoq tizimlari;
- tizim va kabellarni fizik nazoratlash;
- tizim va kabellarning elektr ta’minoti;
- tizimni madadlash muhiti.

Fizik xavfsizlikka ta’sir qiluvchi omillar. Fizik xavfsizlikning buzilishiga ta’sir qiluvchi omillarni ikki guruhga ajratish mumkin: *tabiiy/ muhit tahdidlari* va *inson tomonidan (sun’iy)* amalga oshiriluvchi tahdidlar.

Tabiiy tahdidlar.

Toshqinlar odatda kuchli yomg‘ir va muzlarning erishi natijasida yuzaga keladi. Toshqinlar natijasida tashkilotning elektr ta’minotiga va server xonalariga zarar yetishi mumkin. Odatda tashkilotlarda server xonalari binolar yerto‘lasida joylashganligi sababli, toshqin yanada ko‘proq zarar yetkazishi mumkin.

Yong‘inlar odatda qisqa tutashuvlar va eski bino materiallari sababli yuzaga keladi. Yong‘in natijasida tashkilotning kompyuter xonalari va ishchi binolari hamda qurilmalar, kabellar va boshqa muhim tashkil etuvchilarga to‘liq yoki qisman zarar yetkazilishi mumkin.

Zilzila yer qobig‘ida seysmik terbanishni yaratuvchi kuchli energiya natijasida to‘satdan yuzaga keladi. U tashkilotning fizik infrastrukturasiga ta’sir etib, tashkilot ichidagi xavfsiz muhitda saqlangan kompyuter va boshqa qurilmalarga va hujjatlarga jiddiy ziyon yetkazishi mumkin.

Chaqmoq va momaqaldiroq muhitning o‘zgarishi natijasida yuzaga kelib, barcha tashqi faoliyatning to‘xtatilishiga olib keladi. Chaqmoq va momaqaldiroq natijasida elektr quvvati o‘zgarib, ish faoliyatiga ta’sir qiladi va tashkilotdagi qurilmalarning xotira qismlariga ta’sir qiladi. Bundan tashqari, chaqmoq va momaqaldiroq natijasida kabellarda va boshqa ulanish tizimlarda qisqa tutashuvlar yuzaga kelishi mumkin.

Hisoblash qurilmalarining mo‘tadil ishlashi uchun ular ma’lum *harorat*li muhitda bo‘lishlari talab etiladi. Kompyuter vositalari yuqori haroratda ishlashga mo‘ljallanmagan. Kompyuter tizimlarida sovutish tizimlari mavjud bo‘lsada, tashqi yuqori harorat ularning ish faoliyatiga salbiy ta’sir ko‘rsatadi. Tashkilotdagi elektr va elektron jixozlar *namlik*ni o‘zgarishiga ta’sir ko‘rsatadi. Yuqori namlik karroziyaga, qisqa tutashuvlarga sababchi bo‘ladi yoki magnetik va optiq saqlagichlarga jiddiy ta’sir qiladi.

Sun’iy tahdidlar.

Fizik komponentlarga va tarmoqqa bo‘ladigan salbiy ta’sirlarning aksariyat qismi insonlar tomonidan bilmay yoki atayin qilingan xato natijasida yuzaga keladi. Fizik xavfsizlik tizimiga insonlar tomonidan bo‘ladigan quyidagi tahdidlar mavjud:

Vandalizim. Xafa bo‘lgan xodimlar yoki sobiq xodimlar tizim komponentlarini buzish yoki zarar yetkazish orqali tizimni obro‘sizlantirishga harakat qilishlari mumkin.

Qurilmaning yo‘qolishi. Ruxsatsiz foydalanish muhim axborot yoki qurilmani yo‘qolishiga sabab bo‘ladi. Agar qurilma himoyasi yetarli darajada bo‘lmasa, uning o‘g‘irlanishiga olib kelishi mumkin.

Fizik qurilmalarning buzilishi. Qurilmalarning noto‘g‘ri ishlashi, masalan, qurilmalarning yoki ma’lumotlarning noto‘g‘ri saqlanganligi, zararlangan qurilmalarni almashtirilmaganligi va zaif kabellar fizik qurilmalarga jiddiy zarar yetkazishi mumkin.

O‘g‘irlash. Xavfsizlik tizimidagi zaifliklar jixozlarning o‘g‘irlanishiga sabab bo‘ladi.

Terrorizm. Tashkilot yaqinidagi yoki uning ichidagi terrorchilik harakatlari, masalan, mashinaga qo‘yilgan, shaxslarda mavjud bo‘lgan yoki masofadan turib boshqariluvchi bomba portlashi natijasida tashkilot fizik xavfsizligiga turlicha zarar yetkazilishi mumkin.

Ijtimoiy injineriya. Ijtimoiy injineriyaga shaxsiy axborotni boshqa shaxslar tomonidan noqonuniy qo‘lga kiritish maqsadida qilgan harakatlari sifatida qaraladi. Buzg‘unchi tashkilot xodimlaridan ijtimoiy injineriya orqali ruxsatsiz fizik nazoratlashdan daromad ko‘radi.

Tizimlarni ruxsatsiz nazoratlash. Har ikkala, ichki va tashki foydalanuvchilar ham tashkilot haqidagi axborotni yoki tizimni ruxsatsiz boshqarishga harakati.

Fizik xavfsizlikni nazoratlash. Biror fizik xavfsizlikni mos xavfsizlik nazoratisiz, amalga oshirish qiyin. Fizik xavfsizlik nazoratini, qaysi darajada amalga oshirilishiga qarab, quyidagicha tasniflash mumkin:

- *ma’muriy nazorat* xavfsizlikni nazoratlashda inson omilini mujassamlashtiradi. Turli lavozimlardagi barcha xodimlar ma’muriy nazoratni qurishda inobatga olinishi kerak. Ma’muriy nazorat har bir foydalanuvchi boshqarishi mumkin bo‘lgan resurslarga asoslanib, boshqaruv cheklanishlarini, amaliy muolajalarni, qayd yozuvini amalga oshirish muolajalari va axborot tizimi uchun mos himoya darajasini o‘z ichiga oladi. U asosan insonni boshqarish uchun shaxsga qaratilgan usullarni amalga oshiradi.
- *fizik nazorat* tashkilotlardagi fizik tizimlarga zarar yetishini oldini olish bilan shug‘ullanib, qurilmalarni, bino yoki biror bir maxfiy muhitni ruxsatsiz boshqarishdan himoyalashni qamrab oladi. Fizik nazorat qurilmaning yo‘qolishi yoki o‘g‘irlanishi, tasodifan zararlanishi yoki yo‘q qilinishi, yong‘in yoki tabiiy ofatlar kabi tahdidlardan himoyalashga xizmat qiladi.
- *texnik nazorat* mantiqiy nazorat kabi tashkilotdagi fizik aktivlardan yoki binolardan foydalanishni nazoratlash texnologiyalaridan foydalanib, odatda taqiqlangan hududda foydalanishlarni nazoratlash uchun kompyuter qurilmalari, dasturlari, amallari va ilovalardan foydalanadi.
- *fizik xavfsizlikni nazoratlash, joylashuv va arxitektura.* Tashkilotlar o‘zlari uchun binolar sotib yoki ijaraga olishdan oldin binoning joylashuvi, qo‘shni binolar, elektr va suv manbalari, kanalizatsiya tizimi, kichik va katta yo‘llarga yaqinligi, transport masalasi, tez yordam ko‘rsatish holati, shifoxona, ayeroportga yaqinligi, mazkur hududdagi jinoyatchilik ko‘rsatkichi yoki turli xavfsizlik insidentlarining mavjudligi va boshqa fizik xavfsizligiga ta’sir qilishi mumkin bo‘lgan barcha omillarni e’tiborga olishlari shart. Tanlangan hudud toshqinlar, tarnadolar, yer silkinishi, dovul, yong‘inlar kabi tabiiy ofatlardan xoli bo‘lishi tavsiya etiladi.

Binolarning joylashuvi haqida yetarlicha axborotga ega bo‘lib, ichki struktura va arxitekturani loyihalash va rejalashtirish vaqtida tashkilot tomondan binodagi barcha aktivlarning ro‘yxati tayyor bo‘lishi lozim.

Tashkilot infrastruktura va arxitekturasini loyihalashda quyidagi jihatlarga e’tibor berishi lozim:

- binoga kirish eshiklarining soni, asosiy kirish, zinalar, lift, mashinalar to‘xtab turish joylari, o‘tish yo‘laklari va qabul qilish hududlarini aniqlashtirilganligiga;
- joylashgan hududga yaqin qo‘shni binolarning ichki va tashqi arxitekturasi va atrofdagilar haqida qo‘shimcha ma’lumot olish uchun binolarning egasi va menedjerlari bilan suhbatlashilganiga;
- halokatli buzilishlar va tashqi tomondan aktivlarni ko‘rinishi orqali zarar yetishi mumkin bo‘lgan tahdidlarga;
- agar bino boshqa tashkilotlar bilan sheriklikda foydalanilsa, ularni sizning shaxsiy ma’lumotlaringizga va muhim aktivlaringizga ta’sirini o‘rganilganligiga;
- fizik xavfsizlikni, maxfiy ma’lumotlarni saqlash va tashkilot faoliyatini samarali tashkil etishini nazoratlash uchun talab etilgan muhim infrastrukturani aniqlashtirishga.

Fizik xavfsizlikni nazoratlash: yong‘inga qarshi tizimlar. Yong‘inga qarshi tizimlar o‘zida *aktiv* va *passiv yong‘inga qarshi himoyani* mujassamlashtirgan bo‘lib, fizik xavfsizlikni ta’minlashda muhim omil hisoblanadi, yong‘in yuzaga kelganini avtomatlashgan yoki avtomatlashmagan holda aniqlaydi (4.17-rasm).

4.17-rasm. Yong‘inga qarshi himoya vositalari

Aktiv yong‘inga qarshi himoya vositalari tashkilotda yong‘in yuzaga kelgani haqida ogohlantirib, odatda tijorat, ishlab chiqarish joylarida va savdo uylarida o‘rnatiladi. Ushbu himoya usulining asosiy maqsadi yong‘inni binoning boshqa qismlariga tarqalmasligini oldini olish

hisoblanib, yong‘inga qarshi chora ko‘rishda ma’lum ishlarning avtomatik yoki noavtomatik tarzda amalga oshirilishi talab etiladi.

Aktiv yong‘inga qarshi himoya tizimi suv sepish, tutun/yong‘indan ogohlantirish tizimlari, o‘t o‘chirish va turli suyuqlik (sprey) sepish tizimlarini o‘zi ichiga oladi.

Aktiv yong‘inga qarshi tizimlar quyidagilarni o‘z ichiga oladi:

- *yong‘inni aniqlash tizimi* yong‘in tarqalishidan oldin uni aniqlashga yordam berib, *tutun aniqlovchilarini, alanga aniqlovchilarini* va *issiqlik aniqlovchilarini* o‘z ichiga oladi.
- *yong‘inni bartaraf etish tizimlari* inson aralashuvisiz yong‘inni dastlabki bosqichlarida uni bartaraf etib, zararni kamaytirishga va qurilmalarni yo‘q qilinishidan himoyalaydi. Yong‘inni bartaraf etish tizimlari avtomatik va avtomatik bo‘lmagan turlarga ajratiladi. Ushbu tizimlarga *o‘to‘chirgichni (ognetushitel), suv purkash tizim*larini misol sifatida keltirsa bo‘ladi.

Yong‘inga qarshi passiv himoya tizimlari bino bo‘ylab yong‘inni tarqalishini oldini olib, yong‘inga qarshi eshiklar, oynalar va devorlar himoya chorasi sifatida qaraladi, boshqa biror tizim tomonidan ishga tushirilishni talab etmaydi.

Amaliyotda ushbu tizimlar quyidagi usullar asosida amalga oshiriladi:

- yonuvchan materiallardan minimal foydalanish;
- binoga yong‘inni tarqalishini oldini olish uchun qo‘shimcha qavat yoki xonalarni qurish;
- binodan foydalanuvchilarni yong‘in sodir bo‘lganda qilinishi zarur bo‘lgan ishlar bilan tanishtirish;
- yong‘inga qarshi tizimlarni to‘g‘ri madadlash;
- yetarli sondagi qo‘shimcha chiqish yo‘llarining yetarlicha sonining mavjudligini ta’minlash.

Fizik xavfsizlikni nazoratlash: fizik to‘siqlar. Fizik xavfsizlikni ta’minlash, odatda turli fizik to‘siqlardan foydalanib, fizik chegarani umumiy hududdan taqiqlangan hududga ajratish yo‘li bilan, tashkilotda ruxsatsiz foydalanishni oldini oladi. To‘siqlarni, joylashuv o‘rniga ko‘ra: *tashqi, o‘rta* va *ichki* to‘siqlarga ajratish mumkin. Tashqi to‘siqlar odatda *g‘ov, devor* va boshqalarni o‘z ichiga oladi. O‘rta to‘siqlardan odatda olamon va insonlarni ruxsatsiz kirishlarini taqiqlashda foydalaniladi. Ichki to‘siqlarni esa eshiklar, derazalar, panjaralar, oynalar, pardalar va boshqalar tashkil etadi (4.18-rasm).

a) Elektr to‘siqlar

b) Metall to‘siqlar

s) Tumbalar

d) Turniket

4.18-rasm. To‘siqlarga misollar

Bino ichida foydalaniluvchi fizik to‘siqlarning quyidagi turlari mavjud:

- *devorlar/ elektr devorlar/ metall to‘siqlar*dan odatda taqiqlangan hududlarni, nazoratlanadigan hududlarni va ruxsatsiz kirishdan himoyani belgilashda foydalaniladi. Fizik to‘siqlarni amalga oshirishdan asosiy maqsad:
  - hujumchini blokirovkalash va ushlab qolish;
  - tashkilot chegarasini belgilash;
  - xavfsiz hududni tashqi hujumlardan himoyalash;
  - transportlarni kirishidan himoyalash;
  - qo‘poruvchilik hujumlaridan himoyalash.
- *tumba* kichik vertikal shaklida bo‘lib, avtomobillarni kirishidan himoyalaydi;
- *turniketlar* shaxs tomonidan mos tanga, bilet, barmoq izi yoki token ko‘rsatilganida bir vaqtda bir shaxsni ichkariga kirishiga yoki chiqishiga ruxsat beradi;

fizik himoyani tashkil qilishda *turli eshiklar, oynalar, panjaralar, deraza pardalaridan* ham foydalaniladi.

Fizik xavfsizlikni nazoratlash: xavfsizlik xodimi (qo‘riqchi) tashkilotning fizik xavfsizligini tashkil etish, monitoringlash va madadlash vazifasini bajarib, maxfiy axborotni yo‘qolishidan, o‘g‘irlanishidan, noto‘g‘ri foydalanishidan himoyalash uchun xavfsizlik tizimini o‘rnatish, baholash va ishlab chiqish uchun javobgardir. Yuqori malakali va tajribaga ega xodim har qanday tashkilotning xavfsizligida muhim rol o‘ynaydi. Tashkilotda xodimlar tomonidan amalga oshirilgan himoya $24x7x365$ tartibida amalga oshirilishi zarur. Fizik xavfsizlikka jalb etilgan shaxslar quyidagilar.

Qo‘riqchilar odatda asosiy kirish eshigi va darvozadan kiruvchilarni va xodimlarni nazorat etishga javobgar bo‘lib, xususan, ulardan begona shaxslarning tashkilot hududiga kirmasligini, turli taqiqlangan

buyumlarni olib kirmasligini ta’minlashi talab etiladi. Tashkilotdagi barcha kirish eshiklaridagi holatlar qo‘riqchilar tomonidan CCTV (Closed-circuit television) kameralar yordamida kuzatib boriladi va yozib olib ma’lum vaqtda saqlanadi.

Tashkilotdagi qo‘riqchilar boshlig‘i. Tashkilotdagi qo‘riqchilar boshlig‘i qo‘riqchilar harakatini kuzatish, talab etilgan vaqtda qo‘riqchilarga ko‘mak berish, olamonni tarqatib yuborish, binodagi qulflarni, yoritish tizimlarini boshqarishga javobgar.

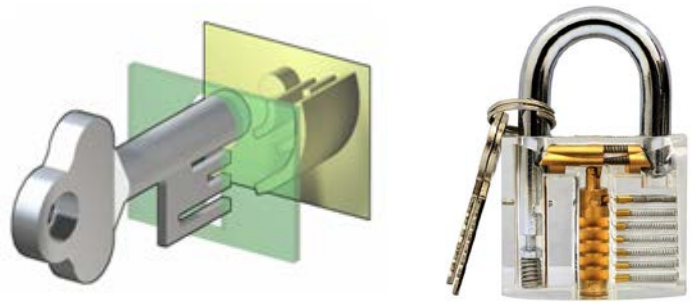
Xavfsizlik xodimi tashkilot atrofida xavfsizlikka aloqador jixozlarni o‘rnatish, boshqarish va ularni to‘g‘ri ishlayotganini kafolatlashi shart.

Axborot xavfsizligining bosh xodimi (Chief Information Security Officer). O‘tgan davrlarda, axborot xavfsizligining bosh xodimi tashkilotdagi barcha xavfsizlikka aloqador jarayonlarni nazoratlashi, hattoki, tarmoq va tizim xavfsizligiga ham javobgar bo‘lgan. Hozirda esa, ushbu shaxslarga, asosan, texnik tomondan bilim va ko‘nikmalar berilishi talab etiladi.

Foydalanishlarni nazoratlash: autentifikatsiya usullari. Tashkilot hududida shaxslarni autentifikatsiyalash vazifasi o‘rta to‘siqlar vazifasini bajaruvchi turniketlar tomonidan yoki qo‘riqchilar tomonidan ham amalga oshirilishi mumkin.

Fizik xavfsizlikni nazoratlash: fizik qulflar ruxsatsiz fizik foydalanishlarni cheklashda foydalaniladi. Har bir tashkilot o‘zining xavfsizlik talablaridan kelib chiqqan holda ularni tanlashi shart. Quyidagi turdagi fizik qulflardan amalda keng foydalanilmoqda:

Mexanik qulflar: tashkilotda fizik foydalanishlarni cheklashning eng oson usuli hisoblanib, kalitli yoki kalitsiz bo‘lishi mumkin. Mexanik qulflarga 4.19-rasmda misollar keltirilgan.



4.19-rasm. Mexanik qulflar

Raqamli qulflar: raqamli qulfli eshiklarni ochish uchun biror narsani (kalitni) olib yurish talab etilmaydi, barmoq izi, smart karta yoki PIN koddan oson foydalaniladi.

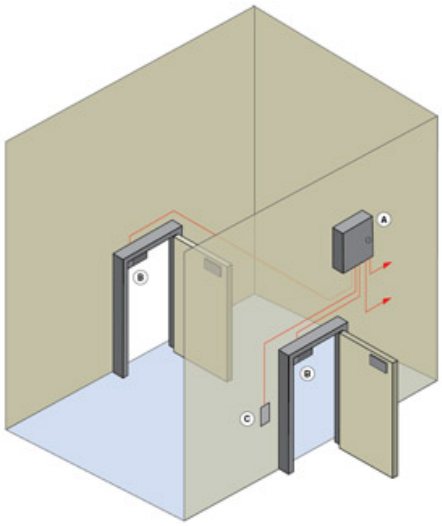
Elektr/ elektromagnetik qulflar: elektr yoki elektron qulflash tizimi elektr quvvatini kamaytirishga asoslangan bo‘lib, natijada eshik ochiladi. Ularni, odatda magnit yoki va elektromotor faollashtiradi va deaktivlashtiradi. Ushbu qulflar ochilishi uchun kalit talab etilmaydi.

Kombinatsion qulflar raqam va simvollar kombinatsiyasidan iborat bo‘lgan maxfiy kodni kiritishni talab etadi.

Fizik xavfsizlikni nazoratlash: Yashirin qurol/ kontrabanda qurilmalarini aniqlash moslamasi. Tashkilotlarda odatda shaxslar tomonidan olib kiriladigan jixozlar yoki vositalar maxsus skanerlar yordamida turli qurollar yoki kontrabanda vositalarini, bombalar, yoki o‘q otar qurilmalari aniqlanadi. Mazkur skanerlarga misol tariqasida, metallni aniqlovchilar, X-ray aniqlash tizimlari va harakat bo‘ylab metallni aniqlash tizimlarini keltirish mumkin (4.20-rasm).

4.20-rasm. X-Ray metall detektorlar

Fizik xavfsizlikni nazoratlash: qopqon chegarani buzib o‘tuvchini tutuvchi fizik xavfsizlikni nazoratlash vositasi hisoblanib, odatda xavfli hududni xavfsiz hududdan ajratadi. Qopqon ikki eshikli mexanik qulflashga asoslangan kichik hudud bo‘lib, ikkinchi eshik ochilishidan oldin birinchi eshik yopiladi. Shaxsni autentifikatsiyalash smart karta, PIN kod yoki biometrik usullar asosida amalga oshirilishi mumkin (4.21-rasm).



4.21-rasm. Qopqon

Fizik xavfsizlikni nazoratlash: xavfsizlik yorliqlari va ogohlantiruvchi signallar. Yorliqlar xavfsizlik darajasi turlicha bo‘lgan axborotdan foydalanishda ruxsatlarni cheklash uchun qulay hisoblanadi. Buning uchun, tashkilotdagi ma’lumotlarga xavfsizlik yorliqlari beriladi. Quyidagi xavfsizlik yorliqlari mavjud:

- ochiq ma’lumotlar (unclassified);
- chegaralangan ma’lumotlar (restricted);
- konfidensial ma’lumotlar (confidential);
- maxfiy ma’lumotlar (secret);
- o‘ta maxfiy ma’lumotlar (top secret).

Axborotdan foydalanishdan oldin uning yorlig‘iga qarab, ruxsatning borligi yoki yo‘qligi aniqlanadi, agar ruxsat bo‘lsa undan foydalanish mumkin.

Ogohlantiruvchi signallardan, odatda, tashkilotdagi ko‘p sonli xodimlarning ruxsatsiz harakatlarini cheklash uchun foydalaniladi. Ogohlantiruvchi signallarga “TAQIQLANGAN HUDUD” (RESTRICTED AREA), “OGOHLANTIRISh” (WARNING), “XAVFLI” (DANGER) iboralarini misol tariqasida keltirish mumkin (4.22-rasm).

4.22-rasm. Ogohlantiruvchi belgilar

Fizik xavfsizlikni nazoratlash: video kuzatuv vositalari tashkilot aktivlarining fizik xavfsizligini ta’minlashda muhim komponent hisoblanadi. Video kuzatuv moslamalari odatda tashkilotning kirish eshiklarida, zallarida va ishchi hududlarida o‘rnatilib, kirish va chiqish harakatlarini kuzatishga yordam beradi. Zamonaviy video kuzatuv vositalari nafaqat harakatlarni qaydlashga, balki nomaqbul harakatlarni aniqlash imkonini ham beradi. Masalan, taqiqlangan jixoz olib kirilayotgan yoki olib chiqilayotgan holatni aniqlaydi yoki janjal bo‘layotgan holatni aniqlab, ogohlantirish signalini yuboradi. Video kuzatuv vositalari sifatida hozirgi kunda quyidagi kameralardan foydalanib kelinmoqda (4.23-rasm).

a) Dome CCTV *b) Bullet CCTV* *c) C-mount CCTV* *d) Day/ night CCTV*

4.23-rasm. Kuzatuv kameralari

Fizik xavfsizlikni nazoratlash: fizik xavfsizlik siyosati va muolajalari. Har bir tashkilot samarali fizik xavfsizlikni amalga oshirish uchun talab qilingan fizik xavfsizlik siyosatini va muolajalarini amalga oshirishi zarur. Turli tashkilotlar uchun fizik xavfsizlik siyosati turlicha bo‘lishi mumkin. Xususan, tashkilot fizik xavfsizligining siyosati o‘zida quyidagilarni mujassamlashtiradi:

- xodimlarning huquq va vazifalari;
- foydalanishlarni boshqarishning nazorati;
- qaydlash va audit.

Fizik xavfsizlik muolajalari o‘z ichiga quyidagilarni oladi:

- qulflash tizimini boshqarish;
- suqilib kirish insidentlarini qaydlash;
- tashrif buyuruvchilarni boshqarish;
- konfidensial materiallarni yo‘q qilish;
- qog‘ozdagi axborot uchun *toza stol* siyosatini va axborotni ishlashda *toza ekran* siyosatini amalga oshirish.

Toza stol siyosatiga ko‘ra tashkilot uchun muhim bo‘lgan axborotni xodimlar tomonidan nazoratsiz qoldirilmasligi va ish joyidan tashqariga olib chiqmasligi zarur. *Toza ekran* siyosati esa xodim o‘z kompyuteridan foydalanishi davomida uni nazoratsiz qoldirmaslikka e’tibor qaratadi.

Boshqa fizik xavfsizlik choralari: yoritish tizimlari. Yoritish tizimlari tashkilot binosi xavfsizligini ta’minlashda muhim ahamiyat kasb etadi. Tashkilot binolarining atrofini yetarlicha yoritmaslik boshqa xavfsizlik vositalarining samaradorligiga salbiy ta’sir etadi. Masalan, agar tashkilotning kirishida, mashina turar joylarida yoki kuzatuv kamerasi o‘rnatilgan boshqa hududlarda yoritish tizimi talabga javob bermasa, ushbu hududlardagi noqonuniy harakatlarni aniqlash imkoniyati kamayadi. Muhitning yoritish tizimi holat va sezuvchanligiga ko‘ra quyidagilarga bo‘linadi:

- *doimiy yoritish tizimlari* – tashkilot binosi atrofida o‘rnatilgan yoritish vositalari;
- *kutish rejimidagi yoritish tizimlari* – biror bir ogohlantiruvchi signal ta’sirida avtomatik yoki noavtomatik tarzda ishlaydigan yoritish vositalari;
- *harakatlanuvchi yoritish tizimlari* – qo‘lda boshqariluvchi yoritish vositalari bo‘lib, qorong‘uda zaruriyat bo‘lganida yoritish uchun foydalaniladi;
- *favqulotda yoritish tizimlari* – elektr energiyasi manbalari ishdan chiqqanida tashkilot binolarini vaqtinchalik yoritish uchun foydalaniladi.

Boshqa fizik xavfsizlik choralari: energiya manbalari. Energiya manbalari nafaqat tashkilotning axborot texnologiyalari tizimiga, balki fizik xavfsizlikni ta’minlash tizimlariga ham katta ta’sir qiladi. Energiyaning yetarli darajada bo‘lmasligi yoki tez-tez uzilib qolishi natijasida jixozlarga zarar yetishi mumkin. Tashkilotlarda energiya manbaining uzilishi natijasida yuzaga keladigan zararni kamaytirish uchun quyidagi xavfsizlik choralarini ko‘rish lozim:

- energiya tebranishlariga tayyor turish;
- energiya uzilishi kuzatilganida uzluksiz energiya manbalaridan (UPS – Unintrruptible power supply) foydalanish;
- vositalarni tahdidlardan himoyalash tizimlarini o‘rnatish;
- ish joylarida statik elektr ta’siridan himoyalash tizimlarini o‘rnatish;
- elektr energiyasida ishlaydigan vositalardan to‘g‘ri foydalanish.

Ish joyining xavfsizligi: qabulxona. Tashkilotning qabulxonasi har doim mehmon va tashkilotlar orasida o‘zaro aloqa o‘rnatishda muhim joy hisoblanadi. Tashkilot qabulxonasida deyarli har kuni turli mehmonlar, hamkorlar, xodimlar va h. bo‘lishadi. Shu sababli, qabulxonadagilar ularning har birini tanib olishga harakat qilishlari va qaydlashlari lozim.

Ish joyining xavfsizligi: Server/ zaxira nusxalash qurilmalarining xavfsizligi. Har bir tashkilot o‘z serverining va zaxira nusxalash vositalarining fizik xavfsizligini ta’minlashga e’tibor berishi lozim. Ushbu vositalarga nisbatan fizik ruxsatlarning cheklanganligi bois, ulardan faqat ruxsat etilgan shaxslar foydalana olishlari mumkin. Server va zaxira nusxalash qurilmalarining fizik xavfsizligini ta’minlash uchun quyidagilar amalga oshiriladi:

- server va zaxira nusxalash qurilmalarini alohida xonada saqlash. Bu chora ushbu qurilmalarning noma’lum shaxslar yoki xodimlar tomonidan ruxsatsiz boshqarilishini cheklaydi;
- server va zaxira nusxalash vositalari joylashgan xonaga yoki muhitga kuzatuv kameralarini va smart karta yoki biometrik parametrlarga asoslangan autentifikatsiyani joriy etish;
- serverlarni, o‘g‘irlinishidan va zararlanishidan himoyalash uchun, maxsus tagliklarga o‘rnatish;
- turli energiya o‘zgarishidan himoyalash uchun serverlarni zaxira UPS vositasiga ulash;
- qurilmalarni qulflanuvchi xonalarda saqlash;
- xodimlar tomonidan ruxsatsiz zaxira nusxalamasligini va server vositalarini olib chiqib ketilmasligini ta’minlash.

Ish joyining xavfsizligi: Muhim aktivlar va olib yuriluvchi qurilmalar. Tashkilot har doim o‘zining server va zaxira nusxalash vositalari bilan bir qatorda, boshqa muhim aktivlar, ishchi stansiyalar, routerlar va svitchlar, printerlar, olib yuriluvchi vositalar va boshqalarning xavfsizligiga e’tibor berishi lozim. Tashkilotga kiruvchi va chiquvchi barcha ma’lumotlar axborot tarmog‘i orqali harakatlanganligi sababli, tashkilot tarmoq kabellarining joylashuvi va ularning xavfsizligiga ham jiddiy e’tibor berish lozim.

Ish joyining xavfsizligi: olib yuriluvchi vositalar. Hozirgi kunda har bir tashkilotda turli olib yuriluvchi vositalardan foydalanilmoqda. Ularga leptoplar, planshetlar, proyektorlar va boshqalar misol bo‘lib, ular osonlik bilan o‘g‘irlanishi, yo‘qolishi va ularga zarar yetkazilishi mumkin. Ushbu vositalarni fizik xavfsizligini ta’minlashda turli mexanik qulflardan

foydalanish yoki ularni xavfsiz xonalarda saqlash choralarini ko‘rish talab etiladi (4.24-rasm).

4.24-rasm. Noutbuklarni stolga qulflash vositasi

Muhitni nazoratlash: isitish, ventilyatsiya va havoni sovitish tizimlari (Heating, ventilating and air-conditioning system, HVAC). Mazkur tizimlar xona yoki bino ichidagi muhitni nazoratlash uchun ishlatiladi va tashkilotdagi qurilmalar ishlashi uchun zurur bo‘lgan muhitni yaratishga xizmat qiladi. Ba’zi HVAC tizimlarida muzlatish tizimi ham mavjud bo‘lib, ular HVAC&R (Refrigeration) tizimlari deb ataladi. Ular nafaqat qurilmalar ishlovchi mos sharoitni yaratish uchun, balki xodimlar ishlashi va tashkilot faoliyati uchun zarur bo‘lgan muhitni yaratish uchun ham qo‘llaniladi.

Muhitni nazoratlash: elektromagnit shovqinlarni ekranlash. Tashkilotda elektron qurilmalardan hosil bo‘ladigan elektromagnit shovqinlar atrofdagi boshqa qurilmalar ishiga ta’sir etishi mumkin. Elektromagnit shovqinlarni ekranlashda elektron vositalar metall bilan qoplanadi, natijada tarqaluvchi elektr to‘lqinining boshqa vositalarga ta’siri keskin kamayadi. Bundan tashqari, qurilmalarni maxsus materiallar bilan to‘sish orqali boshqa qurilmalardan ajratish mumkin. Tashkilotlarda elektron qurilmalar soni ko‘p bo‘lgan hollarda (masalan, telekommunikatsiya yoki shifoxonalarda) ularni ekranlash zaruriyati yanada ortadi.

Fizik xavfsizlik: ogohlik / o‘qitish. Yaxshi o‘qitilgan va malakaga ega bo‘lgan xodim tashkilotning fizik xavfsizligiga bo‘lgan risklarni minimallashtirishi mumkin. Yuqori fizik xavfsizlikni ta’minlashda tashkilot o‘z xodimlari uchun ogohlik mashg‘ulotlarini tashkil etishi lozim. Ogohlantirish yoki o‘qitish dasturlari quyidagilarni nazarda tutishi shart:

- hujumlarni kamaytiruvchi usullarni ta’minlashni;
- maxfiy axborotni olib yurishdagi risklarni;
- xavfsizlik xodimlarining muhimligini;

- barcha qurilma va ma’lumotlarga bo‘lishi mumkin bo‘lgan hujumlar ehtimolini baholashni.

Tashkilotlar fizik xavfsizlik bo‘yicha ogohlik/ o‘qitish kurslarini tashkil etishda turli usullardan foydalanishlari mumkin:

- *sinf mashg‘ulotlari* – ma’ruzaga asoslangan interaktiv sinf mashg‘ulotlarining afzalligi:
  - barcha noravshan va noaniq masalalar shu joyning o‘zida aniqlanadi;
  - webga asoslangan yoki uchrashuvga asoslangan o‘qitish sessiyalarini amalga oshiradi;
  - rol o‘ynash yoki simulyatsiya o‘yinlari orqali yanada interaktiv bo‘lishi mumkin.
- *Aylana stol mashg‘ulotlari* - mazkur kurslar odatda oylik yoki xaftalik bo‘lib, fizik xavfsizlik zarur bo‘lganda tashkilot xodimlarini o‘qitish uchun amalga oshiriladi.
- *Xavfsizlik haqida xabardor qiluvchi web sayt* – xavfsizlik haqida xabardor qiluvchi web saytni yaratish orqali xodimlar o‘zlariga biriktirilgan vazifalarni chuqurroq o‘rganadilar. Bunda turli rasm, video va misollar asosida mavjud holat tushuntiriladi.
- *Master klass darslari* – parolni almashtirish yoki parolni bilmasdan uni olib tashlash master klass darslarida amalga oshiriladi.

Fizik xavfsizlikni amalga oshirilganligi quyidagilar orqali baholanadi:

1. Ruxsatsiz foydalanishlarni oldini olish uchun mos foydalanishlarni nazoratlash usullarining o‘rnatilganligi.
2. Muhim hududlar to‘g‘ri yoritish tizimi asosida kuzatilayotganligi.
3. Turli tahdidlar, yong‘in, tutun, elektr, suv va boshqalarni aniqlovchi va ogohlantiruvchi tizimlar o‘rnatilganligi va ularni to‘g‘ri ishlayotganligi.
4. Eshiklarni qulflash tizimini to‘g‘ri o‘rnatilganligi va ularni to‘g‘ri ishlayotganligi.
5. Tashkilot binosi va hududi yetarli sondagi qo‘riqchilar tomonidan qo‘riqlanayotganligi.
6. Xavfsizlik xodimlarini o‘quv mashg‘ulotlariga yuborilganligi.
7. Xavfsizlik xodimlarini ishonchli agentliklardan olinganligi.
8. Tashkilotdagi kuzatuv kameralari to‘g‘ri o‘rnatilganligi va uzluksiz ishlayotganligi.
9. Fizik xavfsizlik insidentlarini aniqlashda va qaydlashda muolajalarning to‘g‘ri amalga oshirilganligi.

10. Favqulotda vaziyatlarda xodimlar bilan aloqa o‘rnatishga oid axborotning mavjudligi.

Nazorat savollari

1. Ruxsatlarni nazoratlashning asosiy tushunchalari.
2. Foydalanuvchilarni autentifikatsiyalash usullari va ularning o‘ziga xos xususiyatlari nimadan iborat?
3. Parolga asoslangan autentifikatsiya usuli, uning afzallik va kamchiliklari.
4. Parollar ma’lumotlar bazasida qanday saqlanadi va ularni taqqoslash usullari.
5. Axborotning fizik himoyasi va uning muhimligini tushuntiring.
6. Axborotni fizik xavfsizligiga ta’sir qiluvchi tabiiy va sun’iy omillar.
7. Yong‘inga qarshi himoyalash usullari.
8. Tashkilotda qo‘riqlash xodimlari va kuzutuv kameralarining o‘rni.
9. Foydalanishni mantiqiy boshqarish deganda nimani tushunasiz?
10. Foydalanishni boshqarishning DAC usuli va uning xususiyatlari.
11. Foydalanishni boshqarishning MAC usuli va uning asosiy xususiyatlari.
12. Foydalanishni boshqarishning RBAC usuli va uning asosiy xususiyatlari.
13. Foydalanishni boshqarishning ABAC usuli va uning asosiy xususiyatlari.
14. Foydalanishni boshqarish matritsasi, ACL va C-list tushunchalarini tushuntiring.
15. Bell-LaPadul modeli va uning asosiy maqsadi.
16. Biba modeli va uning asosiy maqsadi.

5 BOB. TARMOQ XAVFSIZLIGI

5.1. Kompyuter tarmoqlarining asosiy tushunchalari

Kompyuter tarmoqlari resurslarni almashish maqsadida bir necha kompyuterlarning birlashuvidan iborat. Fayllar, dasturlar, printerlar, modemlar va har qanday tarmoq uskunasi birgalikda foydalaniluvchi yoki taqsimlanuvchi resurslar bo‘lishi mumkin. Kompyuterlarni birlashtirish uchun ma’lumotlarni uzatuvchi turli xil vositalardan foydalaniladi: aloqa kanallari, telekommunikatsiya vositalari, retranslyatorlar va h.

Mos tarmoq servislaridan foydalanish orqali turli xil tarmoq resurslarini taqdim etish vazifasi yuklatilgan tarmoq kompyuteri *server* deb ataladi. Tarmoq resurslaridan va turli tarmoq servislaridan foydalanish maqsadida serverga so‘rov yuboruvchi tarmoq qurilmalari *mijozlar* deb ataladi. Avtonom ishlovchi yoki mijoz sifatida tarmoqqa ulangan kompyuterni, odatda, *ishchi stansiyasi* deb atashadi.

Kompyuter tarmoqlarini quyidagicha tasniflash mumkin:

– xududiy alomat bo‘yicha;
– ma’murlash usuli bo‘yicha;
– topologiya bo‘yicha.

Hududiy alomat bo‘yicha lokal (LAN, Local Area Network) va global (WAN, Wide Area Network) hisoblash tarmoqlari farqlanadi.

Lokal hisoblash tarmog‘i katta bo‘lmagan hududda, xonada yoki binoda joylashgan kompyuter tarmog‘idan iborat. Lokal tarmoq o‘lchami tarmoq texnik arxitekturasi va ulash xiliga (kabel turiga) bog‘liq. Odatda lokal hisoblash tarmog‘ining diametri 2,5 km. dan oshmaydi.

Global hisoblash tarmog‘i katta geografik muhitni qamrab olgan va tarkibida aloqaning magistral liniyalari yordamida birlashtirilgan ko‘plab hisoblash tarmoqlari va masofadagi kompyuterlar bo‘lgan hududiy taqsimlangan tizimdan iborat. Megapolis va region doirasida tashkil etilgan tarmoqlar mos holda shahar tarmog‘i (MAN, Metropolitan Area Network) va regional tarmoq (PAN, Personal Area Network) deb yuritiladi. Eng mashhur global tarmoq Internet TCP/IP protokollari steki bazasiga asoslangan megatarmoq hisoblanadi. Ba’zi adabiyotlarda “korporativ tarmoq” iborasi ishlatiladi. Bu ibora orqali turli texnik, dasturiy va informatsion prinsiplarda qurilgan bir necha tarmoqlarning birlashmasi tushuniladi.

Megatarmoq Internet foydalanuvchilarini birlashtirish uchun ishlatiluvchi global tarmoq Ekstranet (extranet) deb yuritiladi. TCP/IP

protokoli bazasida amalga oshirilgan, ammo megatarmoq Internetdan ajratilgan tarmoq Intranet (Intranet) deb ataladi.

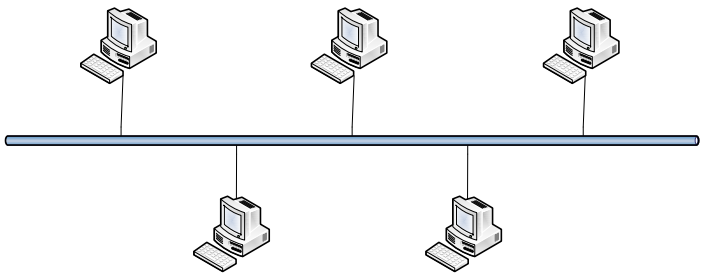
Ma’murlash usuli bo‘yicha tarmoqlar “bir rutbali (одноранговый)” va “mijoz serverli” turlariga bo‘linadi. Bir rutbali tarmoqlarda barcha kompyuterlar ham mijoz, ham server bo‘lishi mumkin. UNIX tarmoqlari bunga misol bo‘ladi.

Mijoz-server texnologiyasi bo‘yicha qurilgan tarmoqlarda maxsus ajratilgan server mavjud. Ajratilgan serverlarga quyidagilar misol bo‘la oladi: fayl server, bosma server, ilovalar serverlari.

Ro‘yxatga olish serverlari (domenlar kontrollerlari), web serverlar, elektron pochta serverlari, masofadan foydalanish serverlari, terminal serverlar, telefon serverlar, proksi serverlar va h.

“Mijoz-server” tarmoqlarida markazlashgan arxitektura hisobiga ma’murlash va masshtablash funksiyalarini, xavfsizlikni va tiklanishni ta’minlash osongina amalga oshiriladi. Ammo, bunday tarmoqlarning zaif joyi (barcha markazlashgan tizimlardagi kabi) server hisoblanadi. Serverning buzilishi butun tizimning ishdan chiqishiga olib keladi. Undan tashqari, “mijoz-server” tarmoqni qurish uchun serunum kompyuter va mos operatsion server muhiti talab etiladi. Mos holda, bunday tarmoqlar professional tarmoq ma’muriga ega bo‘lishi shart.

Tarmoq topologiyasi bo‘yicha umumiy shinali (bus), xalqasimon (ring), yulduzsimon (star), uyali (mesh) va aralash topologiyali tarmoqlar farqlarnadi. *“Umumiy shina”* topologiyasi bitta chiziq bo‘yicha yotqizilgan tarmoqdan iborat. Kabel bitta kompyuterdan keyingi kompyuterga, so‘ngra undan keyingisiga o‘tadi (5.1-rasm).

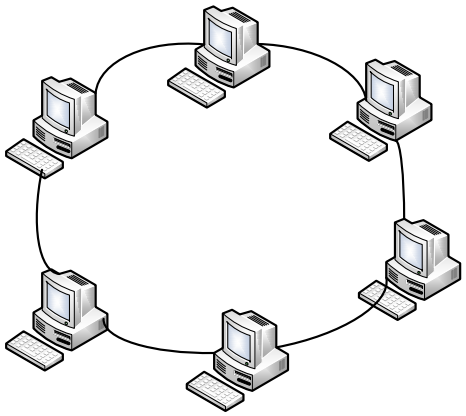


5.1-rasm. “Umumiy shina” topologiyasi

Shinaning har bir uchida terminator (signalning akslanishini istisno qiluvchi) bo‘lishi lozim. Shinaning bir uchi yerga ulanishi kerak. Shinali topologiya “passiv” hisoblanadi, chunki kompyuterlar signallarni regenerasiyalamaydi. Signal so‘nishi muammosini hal etishda tarkorlagichlardan foydalaniladi. Shinaning uzilishi butun tarmoq

ishlashining buzilishiga sabab bo‘ladi (signalning akslanishi hisobiga). Tizimning fizik sathida axborotning sust himoyalanganligini aytish lozim. Chunki, bir kompyuterning ikkinchi kompyuterga yuborgan xabari boshqa ixtiyoriy kompyuterda qabul qilinishi mumkin.

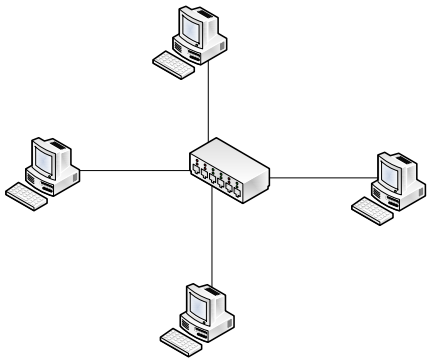
“Xalqasimon” topologiyada har bir kompyuter boshqa ikkita kompyuter bilan ulangan va signal aylana bo‘yicha o‘tadi (5.2-rasm).



5.2-rasm. “Xalqasimon” topologiya

Xalqasimon topologiya “aktiv” hisoblanadi, chunki har bir kompyuter keyingi kompyuterga signal regeneratsiyalaydi. Topologiyaing kamchiligi sifatida masshtablashning murakkabligini hamda umumiy shina topologiyasidagidek uzilish sodir bo‘lganida tarmoqning ishdan chiqishini va axborotning sust himoyalanganligini ko‘rsatish mumkin.

“Yulduzsimon” topologiya har bir kompyuterni markaziy konsentrator bilan ulash orqali tashkil etiladi (5.3-rasm).



5.3-rasm. “Yulduzsimon” topologiya

Ushbu topologiyaning afzalligi uzilishlarga barqarorligi (faqat bitta kompyuter uziladi), kompyuterlarni qo‘shish imkoniyatining kamchiligi sifatida konsentratorga xarajatni ko‘rsatish mumkin.

“Uyali” topologiyada har bir kompyuter boshqalari bilan ulangan. Shu tufayli ulanishlarning uzilishiga eng yuqori barqarorlikka erishiladi. Topologiyaning kamchiligi sifatida kabelli ulanishlarga xarajatni ko‘rsatish mumkin.

Ta’kidlash lozimki, topologiya fizik va mantiqiy bo‘lishi mumkin. Fizik topologiya kabel yotqiziladigan yo‘lni, mantiqiy topologiya esa signal o‘tadigan yo‘lni ko‘zda tutadi. Masalan, Token Ring arxitektura fizik nuqtai nazardan yulduzsimon topologiyani ifodalasa, mantiq nuqtai nazariyadan xalqasimon topologiyani ifodalaydi.

Tarmoqqa qo‘yiladigan talablar:

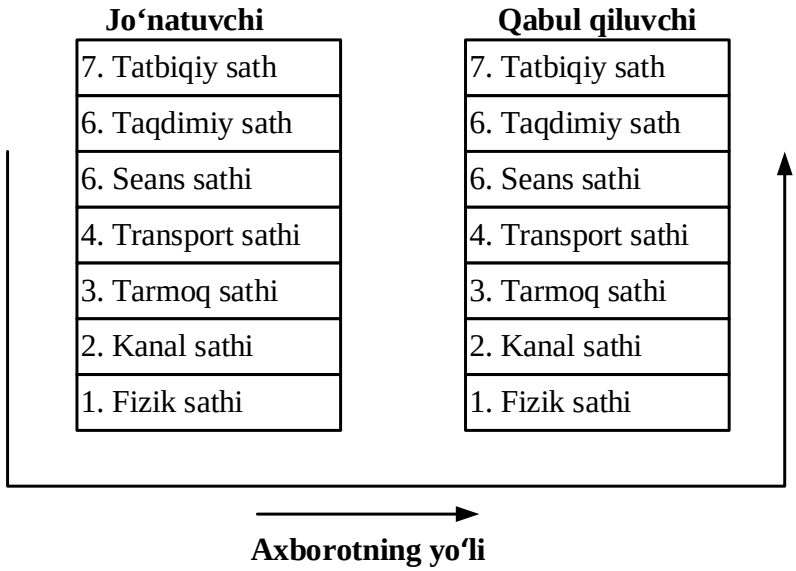
– *ochiqlilik* – tarmoqning mavjud komponentlarining texnik va dasturiy vositalarini o‘zgartirmay qo‘shimcha abonent kompyuterlarini hamda aloqa liniyalarini (kanallarini) kiritish imkoniyati;

– *moslashuvchanlik* – kompyuterni yoki aloqa liniyalarini ishdan chiqishi natijasida struktura o‘zgarishining ishga layoqatlikka ta’sir etmasligi;

– *samaradorlik* – kam sarf-xarajat evaziga foydalanuvchilarga xizmat qilishning talab etiladigan sifatini ta’minlash.

Tarmoq – turli uskunalarning birlashmasi, demak ularni birgalikda ishlatish muammosi jiddiy muammolardan hisoblanadi. Ishlab chiqaruvchilarning uskuna qurilishidagi umumiy qoidalarga rioya qilmaslaridan turli tarmoqlarni qurishda taraqqiyotga erishish mumkin emas. Shu sababli kompyuter sohasidagi yuksalishlar standartlarda akslanadi. Boshqacha aytganda, har qanday texnologiya, uning mazmuni standartlarda o‘z aksini topganidagina “qonuniy” himoyaga ega bo‘ladi.

1980 – yilning boshlarida standartlash bo‘yicha qator tashkilotlar tomonidan yaratilgan model tarmoqlar rivojida muhim rol o‘ynadi. Bu model ochiq tizimlarning o‘zaro aloqa modeli (Open System Interconnection) yoki OSI modeli deb yuritiladi. OSI modeli tizimlarning o‘zaro aloqasining turli sathini belgilaydi, ularga standart nomlar beradi va har bir sathning qanday vazifalarni bajarishini ko‘rsatadi. Ushbu modelning talablariga muvofiq tarmoqning har bir tizimi ma’lumotlar kadrini uzatish orqali o‘zaro aloqada bo‘lishlari lozim. OSI modeliga binoan kadrlarni hosil qilish va uzatish 7 ta ketma-ket harakatlar yordamida amalga oshiriladi (5.4-rasm). Bu harakatlar “ishlash sathlari” nomini olgan.



5.4-rasm. Axborotning OSI modeli bo‘yicha abonetdan abonentga o‘tish yo‘li

Ushbu modelning asosiy g‘oyasiga muvofiq har bir sathga aniq vazifa yuklanadi. Natijada ma’lumotlarni uzatish masalasi osongina ko‘zga tashlanadigan alohida masalalarga ajratiladi. OSI modelida o‘zaro aloqa vositalari yettita sathga bo‘linadi: tatbiqiy, taqdimiy, seans, transport, tarmoq, kanal va fizik. Har bir sath tarmoq qurilmalari orasidagi aloqaning ma’lum sathi bilan ish ko‘radi.

Faraz qilaylik, ilova so‘rov bilan tatbiqiy sathga, masalan, fayl xizmatiga murojaat etsin. Ushbu so‘rovga binoan tatbiqiy sathning dasturiy ta’minoti axborotning standart formatini shakllantiradi. Oddiy axborot sarlavxa va ma’lumotlar hoshiyasidan iborat bo‘ladi. Axborot shakllanganidan so‘ng tatbiqiy sath uni pastga-taqdimiy sathga uzatadi. Taqdimiy sathning protokoli tatbiqiy sathning sarlavhasidan olingan axborotga asosan talab qilingan harakatlarni bajaradi va ma’lumotga o‘zining xususiy xizmat axborotini-taqdimiy sathning sarlavhasini qo‘shadi. Natijada olingan axborot pastga-seans sathiga uzatiladi. Seans sathning protokoli taqdimiy sathning sarlavhasidan olingan axborotga asosan talab qilingan xarakatlarni bajaradi va ma’lumotga o‘zining xizmat axborotini – seans sathning sarlavhasini qo‘shadi. Bu sarlavhada mashina adresatining seans sathi protokoli uchun ko‘rsatmalar bo‘ladi. Natijada olingan axborot pastga, transport sathiga uzatiladi. Transport sathi o‘z navbatida o‘zining sarlavhasini qo‘shadi. Nihoyat, axborot pastki – fizik sathga yetib boradi. Fiziq sath o‘zining sarlavhasini qo‘shib, axborotni mashina adresatiga aloqa liniyalari orqali uzatadi. Bu paytga kelib, axborot barcha sath ilovalariga “o‘sadi”. Axborot mashina-adresatiga

yetib kelganidan so‘ng yuqoriga qarab sathlar bo‘yicha ko‘chiriladi. Har bir sath, ushbu sathga mos vazifalarni bajargani holda, o‘z sathi sarlavhasini tahlillaydi va ishlatadi. So‘ngra bu sarlavhani chiqarib tashlab, axborotni yuqori sathga uzatadi.

OSI modelida protokollarning ikki xili farqlanadi. *Ulanishni o‘rnatishli* (connection oriented) protokollarida ma’lumotlarni almashishdan avval uzatuvchi va qabul qiluvchi ulanishni o‘rnatishi va ehtimol, ma’lumotlar almashishida ishlatiladigan protokolning ba’zi parametrlarini tanlashi lozim. Muloqot tugaganidan so‘ng ular ulanishni uzib tashlashlari lozim. Ulanishni o‘rnatishga asoslangan o‘zaro aloqaga misol sifatida telefonni ko‘rsatish mumkin.

Protokollarning ikkinchi guruhi – oldindan ulanishni o‘rnatishsiz (connection less) protokolidir. Bunday protokollarni *datagrammali* protokollar ham deb yuritiladi. Uzatuvchi axborotni u tayyor bo‘lganida uzatadi. Oldindan ulanishni o‘rnatishsiz aloqaga misol sifatida xatni pochta qutisiga tashlashni ko‘rsatish mumkin. Kompyuterlarning uzaro aloqasida protokollarning ikkala xili ishlatiladi.

5.2. Tarmoq xavfsizligi muammolari

Axborot, Internet va kompyuter xavfsizligida aksariyat foydalanuvchilar tahdid, zaiflik va hujum tushunchalaridan tez-tez foydalanadilar. Biroq, aksariyat foydalanuvchilar tomonidan ularni almashtirish holatlari kuzatiladi.

Zaiflik – “portlaganida” tizim xavfsizligini buzuvchi kutilmagan va oshkor bo‘lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik.

Taxdid (axborot xavfsizligiga taxdid) - axborot xavfsizligini buzuvchi bo‘lishi mumkin bo‘lgan yoki real mavjud xavfni tug‘diruvchi sharoitlar va omillar majmui.

Hujum – bosqinchining operatsion muhitini boshqarishiga imkon beruvchi axborot tizimi xavfsizligining buzilishi.

Hozirda tarmoq orqali amalga oshiriluvchi masalalarning ortishiga quyidagi omillar sabab bo‘lmoqda:

Qurilma yoki dasturiy vositaning noto‘g‘ri sozlanishi. Xavfsizlik bo‘shliqlari, odatda, tarmoqdagi qurilma yoki dasturiy vositalarning noto‘g‘ri sozlangani bois vujudga keladi. Masalan, noto‘g‘ri sozlangan yoki shifrlash mavjud bo‘lmagan protokoldan foydalanish tarmoq orqali yuboriluvchi maxfiy ma’lumotlarning oshkor bo‘lishiga sababchi bo‘lishi mumkin.

Tarmoqni xavfsiz bo‘lmagan tarzda va zaif loyihalash. Noto‘g‘ri va xavfsiz bo‘lmagan holda loyihalangan tarmoq turli tahdidlarga va ma’lumotlarning yo‘qotilishi ehtimoliga duch kelishi mumkin. Masalan, agar tarmoqlararo ekran, IDS va virtual shaxsiy tarmoq (VPN) texnologiyalari xavfsiz tarzda amalga oshirilmagan bo‘lsa, ular tarmoqni turli tahdidlar uchun zaif qilib qo‘yishi mumkin.

Tug‘ma texnologik zaiflik. Agar qurilma yoki dasturiy vosita ma’lum turdagi tarmoq hujumlarini bartaraf eta olmasa, u ushbu hujumlarga zaif bo‘ladi. Masalan, agar tizimlarda foydalanilgan web brauzer yangilanmagan bo‘lsa, u taqsimlangan hujumlarga ko‘proq bardoshsiz bo‘ladi.

Foydalanuvchilarning e’tiborsizligi. Eng oxirgi tarmoq foydalanuvchilarining e’tiborsizligi tarmoq xavfsizligiga jiddiy ta’sir qilishi mumkin. Inson harakatlari natijasida ma’lumotlarning yo‘qolishi, sirqib chiqishi kabi jiddiy xavfsizlik muammolari paydo bo‘lishi mumkin.

Foydalanuvchilarni qasddan qilgan harakatlari. Xodim ishdan bo‘shab ketgan bo‘lsada, taqsimlangan diskdan foydalanish imkoniyatiga ega bo‘lishi mumkin. U mazkur holda tashkilot maxfiy axborotini chiqib ketishiga sababchi bo‘lishi mumkin. Bu holatga foydalanuvchilarning qasddan qilgan harakatlari sifatida qaraladi.

Tarmoq xavfsizligiga tahdid turlari. Tarmoqqa qaratilgan tahdidlar odatda ikki turga ajratiladi (5.5-rasm):

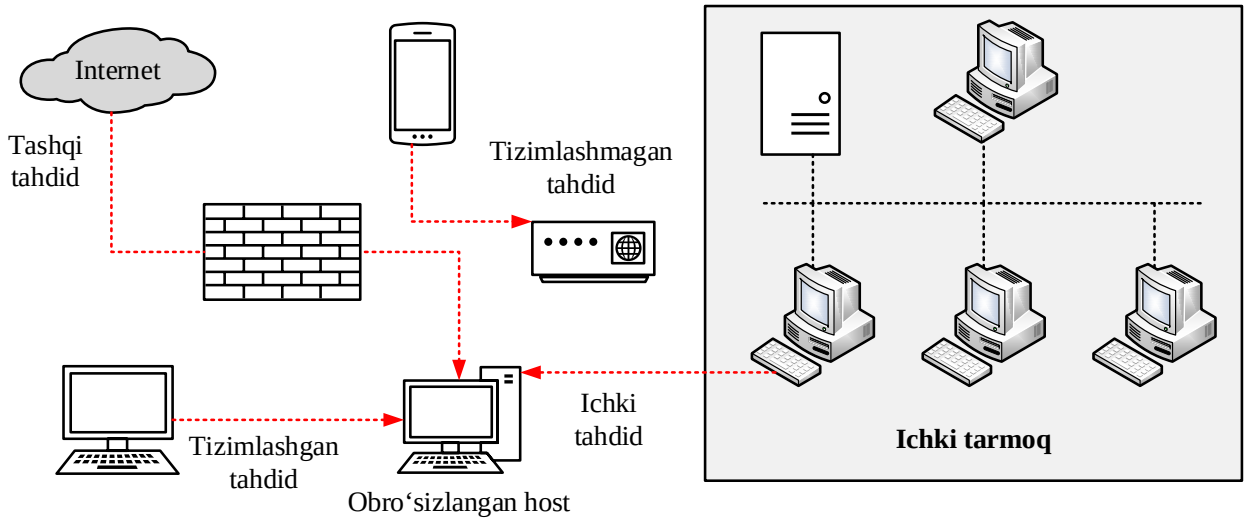
- ichki tahdidlar;
- tashqi tahdidlar.

Ichki tahdidlar. Kompyuter yoki Internetga aloqador jinoyatchiliklarning 80% ini ichki hujumlar tashkil etadi. Bu hujumlar tashkilot ichidan turib, xafa bo‘lgan xodimlar yoki g‘araz niyatli xodimlar tomonidan amalga oshirilishi mumkin. Ushbu hujumlarning aksariyati imtiyozga ega tarmoq foydalanuvchilari tomonidan amalga oshiriladi.

Tashqi tahdidlar. Tashqi hujumlar tarmoqda allaqachon mavjud bo‘lgan zaiflik natijasida amalga oshiriladi. Hujumchi shunchaki qiziqishga, moddiy foyda yoki tashkilotni obro‘sini tushirish uchun ushbu hujumlarni amalga oshirishi mumkin. Mazkur holda hujumchi yuqori malakali va guruh bo‘lib hujumni amalga oshirishi mumkin.

Tashqi tahdidlar odatda ikki turga ajratiladi: *tizimlashgan* va *tizimlashmagan* tashqi tahdidlar (5.5-rasm). Tizimlashgan tashqi tahdidlar yuqori malakali shaxslar tomonidan amalga oshiriladi. Ushbu shaxslar tarmoqdagi mavjud zaifliklarni tezkorlik bilan aniqlash va undan o‘z maqsadlari yo‘lida foydalanishlari uchun imkoniyatga ega bo‘ladilar.

Tizimlashmagan tashqi tahdidlar odatda malakali bo‘lmagan shaxslar tomonidan turli tayyor buzish vositalari va skriptlar (senariylar) yordamida amalga oshiriladi. Ushbu hujum turlari odatda shaxs tomonidan o‘z imkoniyatini testlash yoki tashkilotda zaiflik mavjudligini tekshirish uchun amalga oshiriladi.



5.5-rasm. Tarmoqqa qaratilgan turli tahdidlar

Tarmoqqa qaratilgan hujumlar sonini ortib borishi natijasida tashkilotlar o‘z tarmoqlarida xavfsizlikni ta’minlashda qiyinchiliklarga duch kelishmoqda. Bundan tashqari, hujumchilarning yoki xakerlarning tarmoqqa kirishning yangidan - yangi usullaridan foydalanishlari, ular motivlarining turlichaligi bu murakkablikni yanada oshiradi. Tarmoq hujumlari odatda quyidagicha tasniflanadi.

Razvedka hujumlari. Razvedka hujumlari asosiy hujumni oson amalga oshirish maqsadida tashkilot va tarmoq haqidagi axborotni to‘playdi va bu hujumchilarga mavjud bo‘lishi mumkin bo‘lgan zaifliklarni aniqlash imkonini beradi.

Razvedka hujumining asosiy maqsadi quyidagi toifaga tegishli ma’lumotlarni yig‘ish hisoblanadi:

- tarmoq haqidagi;
- tizim haqidagi;
- tashkilot haqidagi.

Razvedka hujumlarining quyidagi turlari mavjud:

- *Aktiv razvedka hujumlari.* Aktiv razvedka hujumlari asosan portlarni va operaesion tizimni skanerlashni maqsad qiladi. Buning uchun, hujumchi maxsus dasturiy vositalardan foydalangan holda, turli paketlarni yuboradi. Masalan, maxsus dasturiy vosita router va

tarmoqlararo ekranga boruvchi barcha IP manzillarni to‘plashga yordam beradi.

Passiv razvedka hujumlari. Passiv razvedka hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Buning uchun hujumchi sniffer deb nomlanuvchi dasturiy vositadan foydalanadi. Bundan tashqari, hujumchi ko‘plab vositalardan foydalanishi mumkin.

Kirish hujumlari. Mo‘ljaldagi tarmoq haqida yetarlicha axborot to‘planganidan so‘ng, hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. Ya’ni, tizim yoki tarmoqni boshqarishga harakat qiladi. Bu turdagi hujumlar kirish hujumlari deb ataladi. Bularga ruxsatsiz foydalanish, qo‘pol kuch hujumi, imtiyozni orttirish, o‘rtada turgan odam hujumi va boshqalarni misol sifatida keltirish mumkin.

Parolga qaratilgan hujumlar. Parolga qaratilgan hujumlar nishondagi kompyuter tizimi uchun nazoratni qo‘lga kiritish yoki ruxsatsiz foydalanish maqsadida amalga oshiriladi. Parolga qaratilgan hujumlar maxfiy kattaliklarni o‘g‘irlashni maqsad qiladi. Buning uchun turli usul va vositalardan foydalaniladi. Keng tarqalgan hujumlarga quyidagilar misol bo‘la oladi:

- lug‘atga asoslangan hujum;
- qo‘pol kuch hujumi yoki barcha variantlarni to‘liq tanlash hujumi;
- gibrid hujum (lug‘atga va qo‘pol kuch hujumlariga asoslangan);
- Rainbow jadvali hujumlari (oldindan hisoblangan keng tarqalgan parollarning xesh qiymatlari saqlanuvchi jadvallar).

O‘rtada turgan odam hujumi. O‘rtada turgan odam (Man in the middle attack, MITM) hujumida hujumchi o‘rnatilgan aloqaga suqilib kiradi va aloqani uzadi. Bunda nafaqat tomonlar o‘rtasida almashinadigan ma’lumotlarga, balki, soxta xabarlarni ham yuborish imkoniyatiga ega bo‘ladi. MITM hujumi yordamida hujumchi real vaqt rejimidagi aloqani, so‘zlashuvlarni yoki ma’lumotlar almashinuv jarayonini boshqarishi mumkin.

Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari. Xizmatdan voz kechishga qaratilgan hujumlarda hujumchi mijozlarga, foydalanuvchilarga tashkilotlarda mavjud bo‘lgan biror xizmatni cheklashga urinadi. DOS hujumlari biror axborotning o‘g‘irlanishiga yoki yo‘qolishiga olib kelmasada, tashkilot funksiyasini bajarilmasligiga sababchi bo‘ladi. DOS hujumlari tizimda saqlangan

fayllar va boshqa maxfiy ma’lumotlarga, hattoki web-saytning ishlashiga ham ta’sir qiladi. Ushbu hujum bilan web-sayt faoliyatini to‘xtatib qo‘yish mumkin.

Taqsimlangan DOS hujumlar: (Distributed DOS, DDOS). DDOS keng qamrovli nishondagi tizim va tarmoq resurlarida xizmatdan foydalanishni buzishga qaratilgan hujum bo‘lib, Internetdagi ko‘plab zombi kompyuterlar orqali bilvosita amalga oshiriladi. Bunda, hujum ostidagi xizmatlar asosiy nishon deb qaralib, tizimlarni obro‘sizlantirish (zombi holatiga olib kelish) ikkilamchi nishon deb qaraladi.

Zararli hujumlar. Zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi. Zararli dastur – fayl bo‘lib, kompyuter tizimiga tahdid qilish imkoniyatiga ega va troyanlar, viruslar, “qurt”lar ko‘rinishida bo‘lishi mumkin.

Zararli dasturiy vositalari foydalanuvchining ruxsatisiz hujumchi kabi g‘arazli amallarni bajarishni maqsad qilgan vosita hisoblanib, ular yuklanuvchi kod (.exe), aktiv kontent, skript yoki boshqa ko‘rinishda bo‘lishi mumkin. Hujumchi zararli dasturiy vositalardan foydalangan holda tizim xafsizligini obro‘sizlantirishi, kompyuter amallarini buzishi, maxfiy axborotni to‘plashi, web saytdagi kontentlarni modifikatsiyalashi, o‘chirishi yoki qo‘shishi, foydalanuvchi kompyuteri boshqaruvini qo‘lga kiritishi mumkin. Bundan tashqari, zararli dasturlardan hukumat tashkilotlaridan va korporativ tashkilotlardan katta hajmdagi maxfiy axborotni olish uchun ham foydalanish mumkin. Zararli dasturlarning hozirda quyidagi ko‘rinishlari keng tarqalgan:

- *viruslar:* o‘zini o‘zi ko‘paytiradigan dastur bo‘lib, o‘zini boshqa dastur ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi;
- *troyan otlari:* bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida o‘zini ko‘rsatsada, yashiringan zararli koddan iborat;
- *adware:* marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchi faoliyatini kuzatib boruvchi dasturiy ta’minot;
- *spyware:* foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod;
- *rootkits:* ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun o‘z harakatlarini yashiradi;
- *backdoors:* zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan, aylanib o‘tib tizimga kirish imkonini beradi, masalan, ma’mur parolisiz imtiyozga ega bo‘lish;

- *mantiqiy bombalar:* zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi;
- *botnet:* Internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi;
- *ransomware:* mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki blokirovkalab, to‘lov amalga oshirilishini talab qiladi.

5.3. Tarmoq xavfsizligini ta’minlovchi vositalar

Hozirda tarmoq xavfsizligini ta’minlovchi vositalarga tarmoqdan foydalanishni cheklashning bazaviy vositalari (tarmoqlararo ekran) va ma’lumotlarni himoyalangan holda uzatish vositalari (kriptoshlyuzlar va VPN yechimlar), hamda himoyalanganlikni ta’minlovchi qo‘shimcha tarmoq vositalari, trafikni monitoringlash vositalari, yolg‘on tarmoq nishonlari va h. taalluqli.

Tarmoqlararo ekranlash. Tarmoqlararo ekran (firewall, brandmaver) – trafikni filtrlash mexanizmiga asoslangan tarmoqdan foydalanishni cheklashning bazaviy vositasi. Filtratsiya mexanizmi o‘tuvchi trafikni ma’lum qoidalar (filtrlar) bilan taqqoslashni va tarmoq paketlarini o‘tkazish yoki o‘tkazmaslik xususida qaror qabul qilishni ko‘zda tutadi.

Tarmoqlararo ekranlarni, odatda, ishlatiladigan filtrlash texnologiyasiga va OSI modelining bazaviy sathiga nisbatan tasniflashadi (5.1-jadval).

5.1-jadval

Tarmoqlararo ekran turlari

OSI modeli sathlari	**Filtratsiya texnologiyalari**	**Tarmoqlararo ekran turlari**
Tatbiqiy sath	Proksi	Tatbiqiy vositachi
Seans sathi	Proksi	Seans vositachisi
	Paketlar inspektori	Holat inspektori
	Paketlar filtrasiyasi	Dinamik filtr
Tarmoq sathi	Paketlar filtrasiyasi	Ekranlovchi marshrutizator, paket filtri

Kanal sathi	Trafikni segmentlash	Boshqariluvchi (ekranlovchi) kommutator

Kanal sathida ishlatiluvchi boshqariluvchi kommutatorlar, masalan, MAC-adreslar, portlar va kadrlar sarlavhalaridan olingan boshqa parametrlar asosida, trafikni filtrlash vazifasining bajarilishiga imkon beradi. Boshqariluvchi kommutatorlarning afzalligi sifatida tarmoq qurilmalari guruhini ma’murlashning qulayligini, lokal tarmoq unumdorligining oshishini ko‘rsatish mumkin. Funksionallikning cheklanganligi, fizik rekonfiguratsiyalashning noqulayligi va MAC-adresni almashtirish hujumiga zaifligi boshqariluvchi kommutatorlarning kamchiligi hisoblanadi.

Tarmoq sathining paket filtrlari va marshrutizatorlar IP-adres, portlar, protokol turi va h. bo‘yicha filtrlash vazifasining bajarilishiga imkon beradi. Tarmoq va transport sathlari funksionalliklarining cheklanganligi va IP-adresni almashtirish hujumiga zaifligi paket filtrlarining kamchiligi hisoblanadi.

Seans sathining paket filtrlari, seansga mos filtrlash parametrlarining katta sonini hisobga olgan holda, filtrlashni bajarishga imkon beradi.

Vositachilar - oraliq tarmoq vositalari o‘ziga tegishli ulanishni amalga oshirib, trafikni qo‘shimcha qurilmada ishlaydi. Bu o‘z navbatida quyidagi vazifalarni bajarishga imkon beradi:

- autentifikatsiyani;
- mijozlar va serverlarning asinxron muloqotini;
- adreslarning translyatsiyasini va yashirishni;
- tarmoq yukini qayta taqsimlash maqsadida adresni o‘zgartirishni;
- almashish unumdorligini oshirish maqsadida xeshlashni;
- trafikni qaydlashni.

Ayni paytda, vositachilardan foydalanilganda, trafik qo‘shimcha qurilmada takroriy ishlangani sababli, tarmoq perimetri bo‘yicha istalgan unumdorlikni ta’minlash masalasini yechish talab etiladi.

Vositachi tomonidan amalga oshiriluvchi marshrutlash texnologiyasiga alohida e’tibor berish lozim. Unga binoan tarmoq adreslarining translyatsiyasi (Network Address Translation, NAT) amalga oshiriladi, ya’ni hostning ichki adresi vositachining shaxsiy

adresiga almashtiriladi. Boshqacha aytganda, NAT ichki tarmoq adreslarini tashqi tomondan yashirish siyosatini amalga oshiradi va ichki tarmoq uchun vositachiga bitta IP-adresni belgilash imkoniyatini yaratadi. Adreslarni translyatsiyalash statik va dinamik tarzda belgilanishi mumkin.

Seans sathidagi vositachilarga, yuqori unumdorlikka, adreslarni yashiruvchi samaradorli apparatga va TCP/UDP – trafikni ajratish imkoniyatiga ega SOCKet Secure (SOCKS5) vositachisi taalluqli. Tatbiqiy vositachi sifatida HTTP/HTTPS vositachilari va FTP vositachi keng tarqalgan. Ushbu vositachilar tatbiqiy protokol kontenti bo‘yicha filtrlashga imkon tug‘diradi.

Holat inspektorlari (seans sathining imkoniyati kengaytirilgan filtrlari), seans sathidagi protokollar sarlavhalaridan olinuvchi ma’lumotlar asosida, intelektual filtrlashni bajaradi. Bu yuqori sathlarda filtrlash effektini olishga imkon beradi. Bunday tarmoqlararo ekranlar vositachini o‘rnatishni talab qilmaydi. Shu sababli, tarmoq unumdorligi pasaymaydi, ammo xavfsizlikning kerakli darajasi ta’minlanadi. Holat inspektorining afzalligiga masshtablashning qulayligini ham qo‘shish mumkin.

Amaliyotda axborot resurslarining tarmoqlararo himoyasini ta’minlashda UTM (Unifield Threat Management) qurilma tushunchasini va keyingi avlod tarmoqlararo ekranlarini (Next Generation, NG firewall) uchratish mumkin.

UTM – qurilma perimetrli himoyalash masalasining kompleks yechimi hisoblanadi. Uning tarkibida tarmoqlararo ekranlash modullaridan tashqari, suqilib kirishlarni aniqlash tizimlari, oqimli antivirus, spamga qarshi yechim, kriptoshlyuz va h. mavjud bo‘lishi mumkin.

NG firewall UTMga o‘xshash va portlar bo‘yicha filtrlash texnikasini, suqilib kirishlardan ogohlantirish tizimlarini va ilovalar sathida trafikni filtrlashni birlashtirish maqsadida yaratilgan.

Virtual xususiy tarmoqlar. Virtual xususiy tarmoq (Virtual Private Network, VPN) deganda ma’lumotlarni inkapsulyatsiyalash mexanizmlari, hamda qo‘shimcha autentifikatsiya, shifrlash, yaxlitlikni nazoratlash bazasida vaqtinchalik himoyalangan aloqa kanalini yaratish yo‘li bilan uzatiluvchi ma’lumotlarni himoyalash vositasi tushuniladi. Nomidan ko‘rinib turibdiki, VPNning asosiy g‘oyasi vaqtinchalik (seans davrida) ma’lumotlarni uzatish uchun inkapsulyatsiyalash, ya’ni bir sathning tarmoq paketini yuqori sathning yagona paketiga birlashtirish

yo‘li bilan himoyalangan tunnelni yaratishdan iborat. Aynan, doimiy himoyalangan kanalni yoki ajratilgan liniyani ijaraga olishni tashkil etish oldida, vaqtinchalik tunnelni tashkil etish imkoniyatining afzalligi namoyon.

Ma’lumotlar paketining yuqori sath paketiga inkapsulyatsiyasi esa ma’lumotlarni shifrlash va ularning yaxlitligini nazoratlash talablarini osongina qondirishga imkon beradi.

Virtual xususiy tarmoqlarni, asosan OSI-modeli sathlari va ulanish usullari bo‘yicha tasniflash qabul qilingan. Ulanish bo‘yicha “nuqta-nuqta” (“uzel-uzel”), “nuqta-tarmoq” va “tarmoq-nuqta” usullari farqlanadi. 5.2-jadvalda virtual xususiy tarmoqning eng ommaviy protokollari keltirilgan.

5.2-jadval

Virtual xususiy tarmoq protokollari

OSI modeli sathlari	**Tunnellashning bazaviy protokoli**	**Shifrlash vositalari**
Seans sathi	SOCKS	Quyidagi protokollardan foydalanadi.
Transport sathi	SSH	AES, 3DES, Blowfish
	SSL/TLS	AES, 3DES, IDEA, RC4 va h.
Tarmoq sathi	IPSec (ESP)	AES, 3DES va h.
Kanal sathi	L2TP	Yuqoridagi protokollardan foydalanadi.
	PPTP	MPPE (RC4)

PPTP (Point-to-Point Tunneling Protocol) – “nuqta-nuqta” xilidagi kanal sathining tunnel protokoli. Ushbu protokol, tunnelga xizmat qilish uchun, qo‘shimcha TCP-ulanish yordamida PPP-kadrlarni IP-paketlarga inkapsulyatsiyalaydi. Mijozlarni autentifikatsiyalash uchun masofaviy foydalanishning turli protokollarini, jumladan MSCHAPv2 protokolini, madadlaydi. Shifrlashda RC4 algoritmni amalga oshiruvchi MPPE protokol madadlanadi.

L2TP (Layer 2 Tunneling Protocol) – PPP-kadrlarni tarmoq sathi paketlariga inkapsulyatsiyalovchi kanal sathining tunnel protokoli. Protokolning afzalligi sifatida foydalanish ustuvorliklarini va multiprotokollikni (nazariy jixatdan IPga bog‘liq emaslikni) madadlashini

ko‘rsatish mumkin. Shifrlash mexanizmi o‘zidan yuqori sathga ishonib topshiriladi, masalan IPSec apparat yordamida amalga oshirilishi mumkin. PPTPdan farqli holda, TCP/IP tarmoqlarida ushbu protokol transport protokoli UDPga moslangan.

IPSec (IP Security) protokoli ikkita rejimda – transport va tunnel rejimida ishlaydi. Transport rejimida (ushbu rejim hostlar orasidagi ulanishlarni o‘rnatishda ishlatiladi) IPSecdan, qandaydir boshqa usul, xususan, shifrlash funksiyasi bo‘lmagan L2TP tomonidan tashkil etilgan “nuqta-nuqta” xilidagi tunnellarni himoyalashda foydalanish mumkin. Tunnel rejimi shunday tunnelarni yaratishga imkon beradiki, shifrlangan butun paket (transport rejimidan farqli holda, butun paket sarlavhasi bilan shifrlangan) adresatga yetkazish uchun yuqori sathga inkapsulyatsiyalanadi.

Tarmoq xavfsizligini ta’minlovchi qo‘shimcha vositalar.

Suqilib kirishlarni aniqlash tizimlari (Intrusion Detection System, IDS). IDSning asosini tarkibida mos shablonlar, signaturalar yoki profillar bo‘lgan hujumlarning ma’lumotlar bazasi tashkil etadi va aynan ushbu baza bilan sensorlardan olingan ma’lumotlar taqqoslanadi. Shu sababli, IDSning samaradorligi hujumlarning ma’lumotlar bazasining nufuziga bog‘liq. Suqilib kirishlarni aniqlashda quyidagi usullardan foydalanish mumkin:

– signatura usuli – qandaydir hujumga xarakterli ma’lumotlar nabori bo‘yicha suqilib kirishlarni aniqlash;

– anomallarni aniqlash usuli –normal holatiga harakterli bo‘lmagan alomatlarni aniqlash;

– xavfsizlik siyosatiga asoslangan usul – xavfsizlik siyosatida belgilangan parametrlarning buzilganligini aniqlash.

Monitoring darajasi bo‘yicha IDS – tizimlar quyidagilarga bo‘linadi:

– tarmoq sathi IDSi (Network based IDS, NIDS);

– uzel sathi IDSi (Host based IDS, HIDS).

NIDS tarmoq segmentiga ulangan bir necha xostlardan keluvchi tarmoq trafigini monitoringlash orqali ushbu xostlarni himoyalashi mumkin. HIDS yagona kompyuterda yig‘ilgan, asosan operatsion tizimning va axborotni himoyalash tizimining jurnallaridan, foydalanuvchi profilidan va h. yig‘ilgan, axborot bilan ish ko‘radi. Shu sababli NIDSdan kompyuter hujumlarini oldinroq aniqlashda foydalanish

qulay hisoblansa, HIDSdan ruxsatsiz foydalanishning ishonchli faktini qaydlashda foydalaniladi.

IDSning aktiv (in-line) xili suqilib kirishlarni ogohlantirish tizimi (Intrusion Prevention System, IPS) deb ataladi.

Himoyalanganlikni tahlillash vositalari. Texnik audit bo‘yicha mutaxassislar bo‘lishi mumkin bo‘lgan va real zaifliklarni aniqlashda turli himoyalanganlikni tahlillash vositalaridan foydalanishadi. Himoyalanganlikni tahlillash vositalarining quyidagi sinflari mavjud:

- zaifliklarning tarmoq skanerlari;
- web-ilovalar xavfsizligining skanerlari;
- tizim konfiguratsiyasini tahlillash vositalari;
- testlashning maxsus vositalari.

Zaifliklarning tarmoq skanerlari maxsus dasturiy vositalar bo‘lib, undagi kirish axboroti sifatida skanerlanuvchi IP-adreslarning ro‘yxati, chiqish axboroti sifatida esa aniqlangan zaifliklar xususidagi hisobot ishtirok etadi. Asosiy ishlash prinsipi – masofadagi uzelda o‘rnatilgan dasturiy ta’minotning aniq versiyasini aniqlash va zaifliklarning yangilanuvchi lokal bazasiga dasturiy ta’minotning ushbu versiyasi uchun xarakterli zaifliklar xususidagi axborotni qidirish.

Web-ilovalar xavfsizligining skanerlari maxsus dasturiy vositalar bo‘lib, web-tizimlar strukturasini tahlillaydi. Natijada axborotni kiritishning bo‘lishi mumkin bo‘lgan variantlari aniqlanadi va zaiflikdan foydalanish maqsadida so‘rov shakllantiriladi.

Tizim konfiguratsiyasini tahlillash vositalari – tizim himoyalanganligini uning sozlanishi bo‘yicha baholovchi dastur. Bu xil yechim kompleks mahsulot yoki lokal skript (senariy) sifatida ifodalanishi mumkin.

Testlashning maxsus vositalari:

- parollarni online va offline saralash dasturlari;
- zaifliklardan foydalanish freymworklari;
- ma’lum tarmoq hujumlarini amalga oshiruvchi dasturlar (masalan, ARP-spoofing);
- web-serverga uzatiluvchi HTTP so‘rovlarni o‘zgartirish uchun loakl HTTP proksilar va h.

Zaifliklarning turli onlayn – bazalari mavjud. CVE (Common Vulnerabilities and Exposures, cve.mitre.org) zaifliklar bazasi mashhur.

Ma’lumotlarning sirqib chiqishini oldini olish tizimlari (Data Leakage Prevention, DLP). Ushbu tizimlardan, tarkibida tijoriy, kasbiy

yoki boshqa turdagi sir bo‘lgan ma’lumotlarning noqonuniy tarzda tashqi tarmoqqa jo‘natilishini aniqlashda va blokirovkalashda foydalaniladi. DLP tizimlar ulanish sxemasi bo‘yicha IDS – yechimlarga o‘xshash – tahlillanuvchi axborot tarmoq sathida yoki host sathida yig‘ilishi mumkin.

Axborot oqimlarini, ularda konfidensial axborotning mavjudligini aniqlash maqsadida, nazoratlashning ikkita usuli qo‘llaniladi:

– hujjatda berilgan belgilar bo‘yicha aniqlash;
– ma’lumotlar nabori kontenti bo‘yicha aniqlash.

Birinchi usul bo‘yicha axborotni dastlabki kategoriyalash va markirovkalash amalga oshiriladi. Bunda konfidensial hujjatga (masalan, faylga, ma’lumotlar bazasi yozuviga va h.) qandaydir ajralmaydigan formal alomat (masalan, nazorat yig‘indisi, inventar nomeri, konfidensiallik grifi) moslashtiriladi. So‘ngra, uzatiluvchi axborot oqimida ushbu alomat aniqlansa, mos hujjat blokirovkalanadi. Bunday yondashish hujjatni faqat butunligicha himoyalashga qodir. Yondashishning afzalligi sifatida huquqiy risklarning pasayishini va turli xil yolg‘on nishonlar ishlashi darajasining yuqori emasligini ko‘rsatish mumkin.

Yolg‘on nishonlar yoki tuzoqlar (honeypot). Tarmoq xavfsizligini ta’minlovchi ushbu vositadan niyati buzuq tomonidan yolg‘on nishonlarni aniqlash, hamda buzib ochish usullarini tadqiqlash maqsadida hujumni yuzaga keltirishga urinishda foydalaniladi.

Yolg‘on nishonlarni tasniflashda alomat sifatida ularning interaktivligi ishlatiladi, ya’ni quyidagi tuzoqlar farqlanadi:

– interaktiv tuzoqlar;
– interaktivlik darajasi past tuzoqlar;
– interaktivlik darajasi yuqori tuzoqlar.

Interaktivlik darajasi past tuzoqlar bitta tarmoq servisining, masalan, FTP-servisning emulyatsiyasi bo‘lishi mumkin. Joylashtirilishining va nazoratlanishining osonligi bunday tuzoqlarning afzalligi hisoblansa, kamchiligi sifatida ular yordamida ko‘pincha faqat hujum faktining aniqlanishini ko‘rsatish mumkin.

Interaktivlik darajasi yuqori tuzoqlarni to‘laqonli operatsion tizimga va servislar naboriga ega virtual mashina sifatida tasavvur etish mumkin. Bunday tuzoqlar niyati buzuq xususida ancha ko‘p axborotni yig‘ishga imkon beradi (ayniqsa, u bilan intellektual teskari bog‘lanish tashkil etilgan bo‘lsa).

“Bo‘sh” tarmoqlar (DarkNet) tuzoqlarning alohida sinfi hisoblanadi. Ularga muvofiq korporativ tarmoqda, biznes-masalalarni yechishda real ishlatilmaydigan, tashqi adreslar diapazoni ajratiladi. “Bo‘sh” tarmoqqa har qanday murojaat konfiguratsiyadagi xatolikni yoki noqonuniy faoliyatni anglatadi.

Ta’kidlash lozimki, IDS va DLP – yechimlar hujumlarning ma’lum sinfiga mo‘ljallangan. Amaliyotda axborot tizimi ishlashidagi har qanday xavfsizlik va ishonchlik hodisalarni yig‘ish masalasi paydo bo‘ladi. Bunday tizimlarga quyidagilar taaluqli:

– jurnallarni boshqarish tizimlari (log management). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishni tashkil etish uchun mo‘ljallangan;

– xavfsizlik xususidagi axborotni boshqarish tizimlari (Security Information Management, SIM). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishga, hamda turli hisobotlarni shakllantirishga va tahlillashga mo‘ljallangan;

– xavfsizlik hodisalari hususidagi axborotni boshqarish tizimlari (Security Event Manager, SEM). Ushbu tizimlar vaqtning real rejimida monitoringlashga, axborot xavfsizligi hodisalarini korrelyatsiyalashga mo‘ljallangan;

– xavfsizlik va xavfsizlik hodisalari xususidagi axborotni boshqarish tizimlari (Security Information and Event Management, SIEM). Ushbu tizimlar monitoring tizimlari rivojining keyingi qadami hisoblanadi, chunki SEM va SIM funksionalliklarini kombinasiyalaydi.

Qo‘shimcha sifatida aytish mumkinki, tarmoqlararo ekranlar uchun belgilangan mexanizm – filtratsiya, VPN uchun – inkapsulyatsiya, SIEM uchun esa korrelyatsiya.

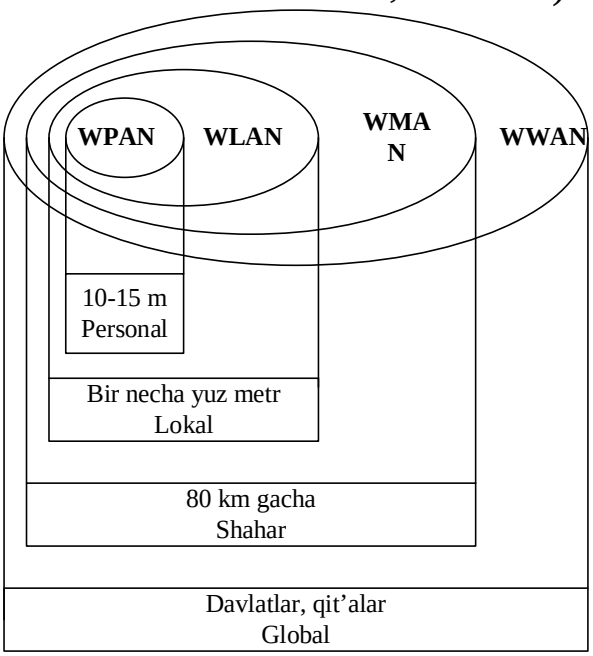
5.4. Simsiz tarmoq xavfsizligi

Simsiz tarmoq turlari. Ma’lumki, radio ixtiro etilganidan so‘ng, ko‘p o‘tmay telegraf aloqani simsiz amalga oshirish imkoniyati paydo bo‘ldi. Aslida, hozirgi raqamli kodni radiokanal bo‘yicha uzatishda o‘sha prinsipdan foydalanishadi, ammo ma’lumotlarni uzatish imkoniyati bir necha bor oshdi.

Zamonaviy simsiz tarmoqlarni ta’sir doirasi va vazifasi bo‘yicha quyidagilarga ajratish mumkin (5.6-rasm):

- shaxsiy (Wireless Personal Area Network, WPAN);
- lokal (Wireless Local Area Network, WLAN);
- shaxar (Wireless Metropolitan Area Network, WMAN);

- global (Wireless Wide Area Network, WWAN).



5.6-rasm. Simsiz tarmoqlar tasnifi

5.3-jadvalda yuqorida keltirilgan simsiz tarmoqlarning xarakteristikalari keltirilgan.

5.3-jadval

Simsiz tarmoqlarning asosiy xarakteristikalari

Simsiz tarmoqlar / Xarakte-ristikalar	**WPAN (shaxsiy simsiz tarmoqlar)**	**WLAN (lokal simsiz tarmoqlar)**	**WMAN (shaxar simsiz tarmoqlar)**	**WWAN (global simsiz tarmoqlar)**
Ko‘llanish sohasi	Tashqi qurilma simlarini almashtirish	Simli tarmoqlarning mobil kengaytirishlari	Keng polosali simsiz foydalanish	Bino tashqarisida Internetdan mobil foydalanish
Taxnologi-yalar	Bluetooth, UMB, ZigBee	Wi-Fi (802.11)	WiMax (802.16), MBWA-m (802.20)	GSM, GPRS, WCDMA, EDGE, HSPA+, WiMax, LTE

Simsiz tarmoqlarda axborot xavfsizligiga asosiy tahdidlar. Xavfsiz simsiz ilovani yaratish uchun simsiz “hujumlar” amalga oshirilishi mumkin bo‘lgan barcha yo‘nalishlarni aniqlash talab etilsada, ilovalar

xech qachon to‘liq xavfsiz bo‘lmaydi. Ammo, simsiz texnologiyalardagi xavf-xatarni sinchiklab o‘rganish har holda himoyalanish darajasini oshishiga yordam beradi. Demak, mumkin bo‘lgan tahdidlarni tahlillab, tarmoqni shunday qurish lozimki, hujumlarga xalaqit berish va nostandart “hujumlar”dan himoyalanishga tayyor turish imkoni mavjud bo‘lsin.

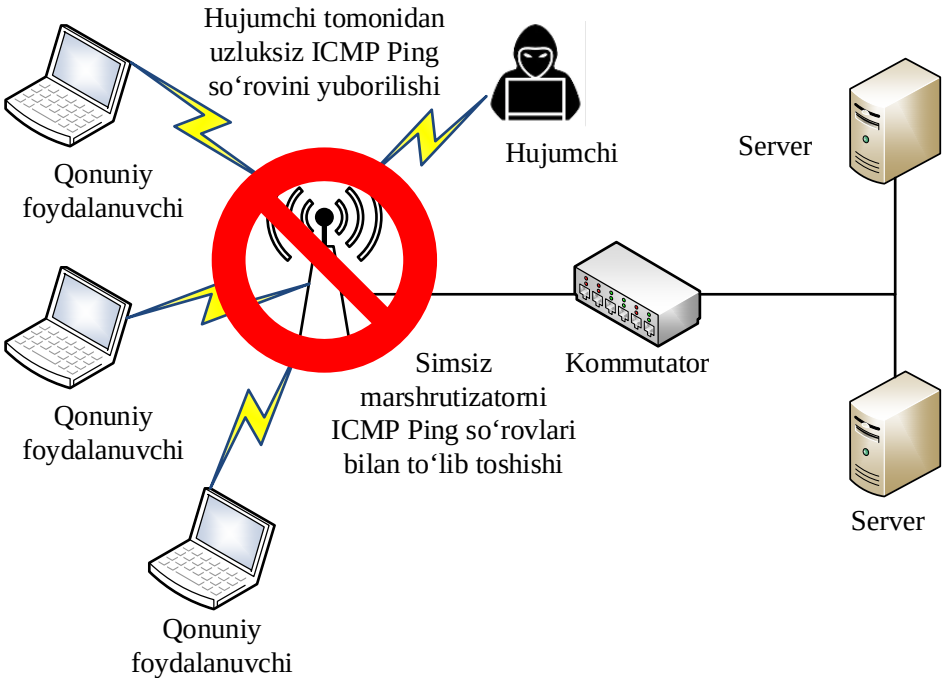
Nazoratlanmaydigan hudud. Simli va simsiz tarmoqlar orasidagi asosiy farq – simsiz tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan hududning mavjudligi. Uyali tarmoqlarning yetarlicha keng makonida simsiz muhit aslo nazoratlanmaydi. Zamonaviy simsiz texnologiyalar tarmoq makonini boshqarish vositalarining chegaralangan to‘plamini taqdim etadi. Bu simsiz strukturalarning yaqinidagi hujum qiluvchilarga simli dunyoda mumkin bo‘lmagan hujumlarni amalga oshirishga imkon beradi.

Ruxsatsiz suqilib kirish. Agar simsiz tarmoq himoyasi amalga oshirilmasa, ixtiyoriy simsiz ulanish imkoniyatiga ega qurilma undan foydalanishi mumkin. Mazkur holda, odatda, kirish joyining yopiq eshittirish diapazoni 50-100 metrni tashkil qilsa, tashqi maydonda 300 metrgacha bo‘lishi mumkin.

Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda eng tarqalgan muammo - anonim hujumlarning mavjudligi bo‘lib, uzatishni ushlab qolish uchun niyati buzuq uzatgich (передатчик) oldida bo‘lishi lozim. Ushlab qolishning bunday turlarini umuman qaydlash mumkin emas va ularga halaqit berish undan ham qiyin. Antennalar va kuchaytirgichlardan foydalanish, ushlab qolish jarayonida niyati buzuqlarga nishondan aytarlicha uzoq masofada bo‘lishlariga imkon beradi.

Simsiz tarmoqlarda foydalaniluvchi barcha protokollar ham xavfsiz emasligi sababli, yashirincha eshitish usuli katta samara berishi mumkin. Masalan, simsiz lokal tarmoqlarda WEP protokolidan foydalanilgan bo‘lsa, katta ehtimollik bilan tarmoqni eshitish imkoniyati tug‘iladi.

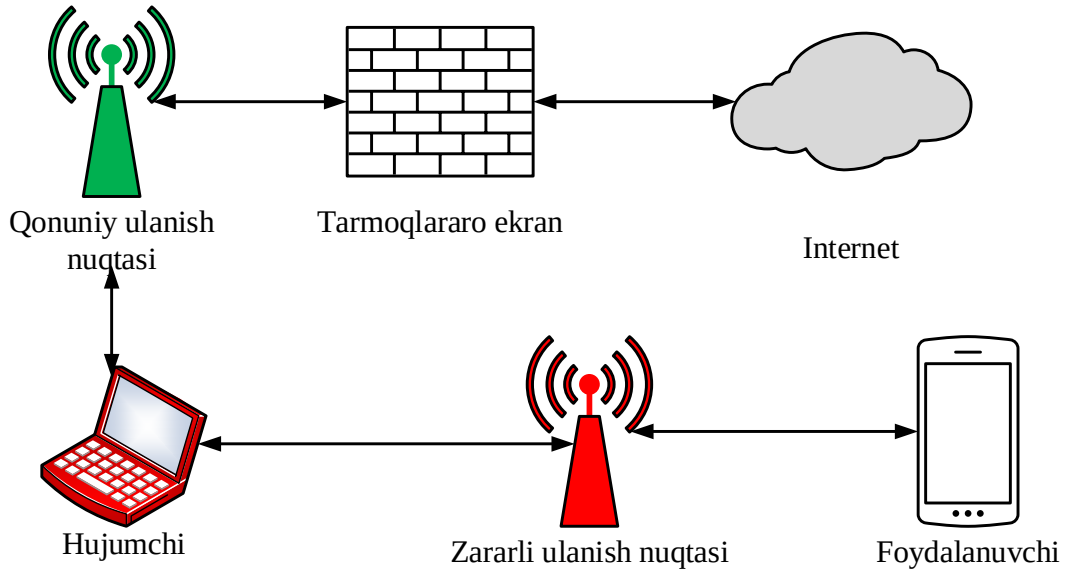
Xizmat ko‘rsatishdan voz kechishga undash. Butun tarmoqda, jumladan, bazaviy stansiyalarda va mijoz terminallarida, shunday kuchli interferensiya paydo bo‘ladiki, stansiyalar bir-birlari bilan bog‘lana olmasligi sababli, DoS xilidagi xujum tarmoqni butunlay ishdan chiqarishi mumkin. Bu xujum ma’lum doiradagi barcha kommunikatsiyani o‘chiradi (5.7-rasm).



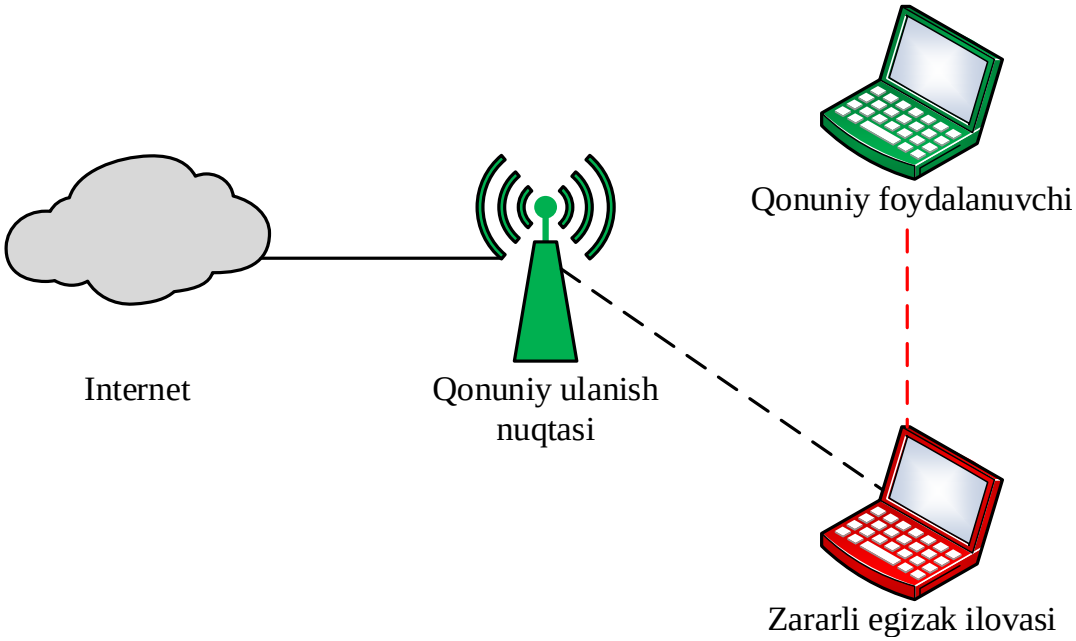
5.7-rasm. Simsiz tarmoqda DoS hujumining amalga oshirilishi

O‘rtada turgan odam hujumi. MITM xujumi yuqorida tavsiflangan suqilib kirish hujumlariga o‘xshash, ular turli shakllarda bo‘lishi mumkin va aloqa seansining konfidensialligini va yaxlitligini buzish uchun ishlatiladi. MITM xujumlar anchagina murakkab, chunki ularni amalga oshirish uchun tarmoq xususidagi batafsil axborot talab etiladi. Niyati buzuq, odatda, tarmoq resurslaridan birining identifikatsiyasini amalga oshiradi. Hujum qurboni ulanishni boshlaganida, firibgar uni ushlab qoladi va istalgan resurs bilan ulanishni tugallaydi va so‘ngra ushbu resurs bilan barcha ulanishlarni o‘zining stansiyasi orqali o‘tkazadi (5.8-rasm). Bunda hujum qiluvchi axborotni jo‘natishi, jo‘natilganini o‘zgartirishi yoki barcha muzokaralarni yashirincha eshitishi va so‘ngra rasshifrovkalashi mumkin.

Tarmoqdan foydalanishning yolg‘on nuqtalari (zararli egizak hujumi). Tajribali hujumchi tarmoq resurslarini imitatsiya qilish bilan foydalanishning yolg‘on nuqtalarini tashkil etishi mumkin. Abonentlar, hech shubhalanmasdan foydalanishning ushbu yolg‘on nuqtasiga murojaat etadilar va uni o‘zining muhim rekvizitlaridan, masalan, autentifikatsiya axborotidan xabardor qiladilar. Hujumning bu xili tarmoqdan foydalanishning xaqiqiy nuqtasini “bo‘g‘ish” maqsadida ba’zida to‘g‘ridan-to‘g‘ri bo‘g‘ish bilan birgalikda amalga oshiriladi (5.9-rasm). Buning uchun odatda hujumchi joriy simsiz ulanish nuqtasiga qaraganda kuchli bo‘lgan signal tarqatish qurilmasidan foydalanadi.



5.8-rasm. MITM hujumining amalga oshirilishi



5.9-rasm. Zararli egizak hujumi

Rouming muammosi. Simsiz tarmoqning simli tarmoqdan yana bir muxim farqi foydalanuvchining tarmoq bilan aloqani uzmasdan joyini o‘zgartirish qobiliyatidir. Rouming konsepsiyasi turli simsiz aloqa standartlari CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) va simsiz Ethernet uchun bir xil bo‘lib, TCP/IPning ko‘pgina tarmoq ilovalari server va mijoz IP-adreslarining o‘zgarmasligini talab etadi. Ammo, tarmoqdagi rouming jarayonida abonent albatta uning bir joyini tark etib, boshqa joyiga qo‘shiladi. Simsiz tarmoqlarda mobil IP-adreslarning va boshqa rouming mexanizmlarining ishlatilishi ushbu talabga asoslangan.

Yelka orqali qarash. Jamoat joylarida simsiz tarmoqqa ulanish davomida buzg‘unchi tomonidan bog‘lanish sozlanmalari osonlik bilan (yelkasi bo‘ylab qarash orqali) qo‘lga kiritilishi mumkin. Bu esa simsiz tarmoqdan to‘laqonli foydalanish imkonini taqdim etadi.

Simsiz tarmoqlardan foydalanishda bo‘lishi mumkin bo‘lgan xavfsizlik muammolarini oldini olish choralari:

Joriy sozlanish parolini almashtirish. Aksariyat tarmoq qurilmalari, jumladan, simsiz tarmoq qurilmalari, joriy sozlanish paroliga ega va ular barchaga ma’lum. Ba’zida tarmoq ma’muri tomonidan ushbu parollarni almashtirish esdan chiqadi va buning natijasida jiddiy muammo yuzaga keladi. Shuning uchun, tarmoq qurilmalaridan foydalanishdan oldin joriy o‘rnatilgan parollarni almashtirish zarur.

Foydalanishni cheklash. Tarmoqdan foydalanishni faqat ruxsatga egalar uchun joiz bo‘lishini ta’minlash muhim ahamiyatga ega. Har bir qurilma ajralmas MAC (Media access control) manziliga ega, ushbu manzillarni tekshirish orqali ularga foydalanishni taqdim etish mumkin. Boshqacha aytganda, simsiz tarmoq qurilmasi xotirasida ulanishi mumkin bo‘lgan qurilmalarning MAC manzillari mavjud bo‘ladi. Yangi manzilga ega bo‘lganlar esa ushbu tarmoq nuqtasiga ulanish imkoniyatiga ega bo‘lmaydi.

Tarmoq orqali uzatiluvchi ma’lumotlarni shifrlash. Agar simsiz tarmoq orqali uzatilayotgan har bir ma’lumot shifrlangan taqdirda, ularni ruxsatsiz o‘qishdan himoyalash mumkin bo‘ladi. Simsiz lokal tarmoqlarda tarmoq nuqtasi va foydalanuvchi qurilmalari orasidagi ma’lumotlar odatda Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 va WPA3 protokollari asosida shifrlangan holda uzatiladi. Ular orasida WPA3 protokoli bardoshli hisoblansada, amalda zaif hisoblangan qolgan protokollar ham keng qo‘llanilmoqda.

Simsiz tarmoq qurilmasini (SSID, Service Set Identifier) himoyalash. Tarmoq tashqarisidan simsiz tarmoqni osonlik bilan boshqarilishini oldini olish uchun, SSIDni oshkor etmaslik talab etiladi. Barcha Wi-Fi qurilmalar SSID ni himoyalash imkoniyatiga ega, bu hujumchining simsiz tarmoqni topishini qiyinlashtiradi. Ushbu kattalikni joriy holda qoldirish tavsiya etilmaydi va kamida SSID ni yangilash talab etiladi.

Tarmoqlararo ekran vositasini o‘rnatish. Simsiz qurilmalarda bevosita hostga asoslangan tarmoqlararo ekranni o‘rnatish yoki uy tarmog‘i uchun modemga asoslangan tarmoqlararo ekranni o‘rnatish

tavsiya etiladi. Ushbu himoya chorasi hujumchini to‘g‘ridan-to‘g‘ri tarmoqqa ulanishini oldini oladi.

Fayl almashishini ehtiyotkorlik bilan amalga oshirish. Tomonlar orasida faylni almashtirishga zaruriyat bo‘lmagan taqdirda, ushbu imkoniyat o‘chirilgan holatda bo‘lishi kerak. Fayl almashishini har doim shaxsiy yoki uy tarmog‘ida amalga oshirish zarur. Ochiq bo‘lgan tarmoqda fayllarni almashtirish tavsiya etilmaydi. Bundan tashqari, uzatilayotgan har bir fayllarni parol asosida himoyasini ta’minlash zarur (faylni blokirovkalash).

Simsiz tarmoq nuqtasida foydalaniluvchi dasturiy vositalarni muntazam yangilab borish. Ishlab chiqaruvchilar tomonidan qurilmalar uchun doimiy ravishda yangi versiyalar ishlab chiqiladi va ular mavjud versiyadagi xavfsizlik muammolarini oldini olishga qaratilgan bo‘ladi. Shu sababli, simsiz tarmoq qurilmalarini dasturiy jixatdan yangilab borish tavsiya etiladi.

Internet provayderi yoki simsiz tarmoq qurilmasini ishlab chiquvchilar tavsiyalariga quloq solish. Odatda simsiz tarmoq qurilmalarini ishlab chiqaruvchilar tomonidan o‘ziga tegishli web sahifalarda, qurilmalardan xavfsiz foydalanish tavsiyalari beriladi. Ushbu tavsiyalarga amal qilish, aksariyat hollarda bo‘lishi mumkin bo‘lgan xavfsizlik muammosini oldini olishga katta yordam beradi.

5.5. Risklar va risklarni boshqarish

Risk kiberxavfsizlikka oid bo‘lgan tushunchalardan biri hisoblanadi. Quyida risk tushunchasi va uni boshqarish bo‘yicha batafsil ma’lumotlar keltirilgan.

Risk – belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish. Bundan tashqari, riskni quyidagicha tushunish mumkin:

- *Risk* – ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo‘qotilishi yoki boshqa salbiy ta’sir ko‘rsatishi mumkin bo‘lgan hodisa.
- *Risk* – manbaga zarar keltiradigan ichki yoki tashqi zaiflik tahdidi bo‘lishi ehtimoli.
- *Risk* – hodisa sodir bo‘lishi ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta’siri.

Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish mavjud bo‘lib, ularni quyidagicha ifodalash mumkin:

$$RISK = Tahdid \times Zaiflik \times Ta'sir.$$

Boshqa tomondan, hodisaning axborot texnologiyalari aktiviga ta’siri – aktivdagi yoki manfaatdor tomonlar uchun aktivning qiymatidagi zaiflikning natijasi, ya’ni:

$$RISK = Tahdid \times Zaiflik \times Aktiv\ qiymati.$$

Risk o‘zida quyidagi ikkita omilni mujassamlashtiradi:

- zararli hodisaning yuzaga kelishi ehtimoli;
- va zararli hodisa oqibatlarining ehtimoli.

Risk ta’siri. Risk normal amalga oshirish jarayoniga va loyiha narxiga yoki kutilgan qiymatga ta’sir etadi. Risk ta’siri tashkilot, jarayon yoki tizimga zararli muhit sababli yuzaga keladi. Ta’sir riskning kuzatilishi ehtimoli jiddiyligini ko‘rsatadi.

Risk chastotasi. Riskni aniqlash va baholash nuqtai nazaridan risklarni tasniflashda ularning takrorlanish chastotasiga va ko‘p sonliligiga asoslanadi. Chastota va ko‘p sonlilik risklarni monitoringlashda muhim hususiyat hisoblanib, risklar ikki guruhga: *minor risklar* – e’tibor talab qilmaydigan va *major risklar* – alohida e’tibor va kuzatuv talab qiluvchilarga ajratiladi.

Risk darajasi. Risk darajasi tarmoqga (yoki tizimga) natijaviy ta’sirning bahosi bo‘lib, quyidagi tenglik bilan ifodalanadi:

$$Risk\ darajasi = natija \times ehtimollik.$$

Risk darajalari 4 ta: ekstremal yuqori, yuqori, o‘rta va past.

Ekstremal yuqori yoki *yuqori* risk paydo bo‘lishini va salbiy ta’sirini kamaytirish maxsus yo‘naltirilgan qarshi choralarni talab etadi. Bu darajadagi risklar yuqori yoki o‘rtacha ta’sirning yuqori ehtimolligiga ega bo‘ladi. Mazkur darajadagi risklar jiddiy xavfga sabab bo‘ladi va shuning uchun, zudlik bilan aniqlash hamda qarshi chora ko‘rish talab etiladi.

O‘rta darajali risklar yuqori ehtimollikka ega past natijali hodisa yoki past ehtimollikka ega yuqori natijali hodisa bo‘lishi mumkin. Alohida qaralganida, yuqori ehtimollikka ega past natijali hodisalar loyiha narxiga yoki kutilgan natijaga kam ta’sir qiladi. Past ehtimollikka ega yuqori natijali hodisalar doimiy monitoringni talab etadi. O‘rta darajali risklarga zudlik bilan chora ko‘rish talab etilmasada, himoyani dastlabki vaqtda o‘rnatish talab etiladi.

Past darajali risklar odatda e’tibor bermasa bo‘ladigan yoki keyingi baholashlarda e’tibor bersa bo‘ladigan risklar toifasi bo‘lib, ularni bartaraf etish qisqa muddatda amalga oshirilishni talab qilmaydi yoki ortiqcha sarf xarajatga sabab bo‘lmaydi.

Risk matritsasi risklarni paydo bo‘lish ehtimolini ularning natijasi va ta’siri orqali aniqlaydi hamda risk jiddiyligini va unga qarshi himoya chorasi sathini grafik taqdim etadi. Risk matritsasi riskning ortib boruvchi ko‘rinishi uchun foydalaniluvchi sodda jarayon bo‘lib, qarshi choralarni ko‘rishda yordam beradi. Risk matritsasi risklarni turli darajalarda aniqlash va jiddiylik nuqtai nazaridan guruhlash imkonini beradi (5.4-jadval).

5.4-jadval

Risk matrisasi

Ehtimollik (ravshan)		**Oqibat/ ta’sir**					
			Muhim emas	Kam	O‘rta	Ko‘p	Jiddiy
81-100%	**Ehtimollik (noravshan)**	Juda yuqori	Past	O‘rta	Yuqori	O‘ta yuqori	O‘ta yuqori
61-80%		Yuqori	Past	O‘rta	Yuqori	Yuqori	O‘ta yuqori
41-60%		Teng	Past	O‘rta	O‘rta	Yuqori	Yuqori
21-40%		Past	Past	Past	O‘rta	O‘rta	Yuqori
1-20%		Juda past	Past	Past	O‘rta	O‘rta	Yuqori

Yuqorida taqdim etilgan risk matritsasi risklarni vizual taqdim etish va o‘zaro taqqoslash imkonini beradi va undagi har bir yacheyka ehtimollik va oqibat kattaliklarining kombinasiyasidan iborat. Riskning jiddiyligi uning ehtimoli va ta’sir darajasiga bog‘liq. Keltirilgan risk matritsasida paydo bo‘lish ehtimoli bo‘yicha ular 5 ta guruhga ajratilgan. Shunga mos ravishda, risk oqibati ham 5 ta darajaga ajratilgan.

Risklarni boshqarish. Risklarni boshqarish – risklarni aniqlash, baholash, javob berish va bo‘lishi mumkin bo‘lgan ta’sirga tashkilot tomonidan javob berilishini amalga oshirish jarayoni. Risklarni boshqarish xavfsizlikning hayotiy siklida o‘zining muhim o‘rniga ega, u davomiy va hattoki murakkablashib boruvchi jarayon hisoblanadi. Risklar turli tashkilotlar uchun turlicha bo‘lsada, risklarni boshqarishga

tayyorgarlik ko‘rish barcha tashkilotlar uchun umumiy. Risklarni boshqarishdan asosiy maqsad quyidagilar:

- bo‘lishi mumkin bo‘lgan risklarni aniqlash;
- risk ta’sirini aniqlash va tashkilotlarga risklarni yaxshiroq boshqarish strategiyasi va rejasini ishlab chiqishga yordam berish;
- jiddiylik darajasiga asoslangan holda risklarni tasniflash va yordam berish uchun risklarni boshqarish usullari, vositalari va texnologiyalaridan foydalanish;
- risklarni tushunish, tahlillash va aniqlangan risk hodisalarini qaydlash;
- risklarni nazorat qilish va risk ta’siriga qarshi kurashish;
- xavfsizlik xodimlarini ogohlantirish va risklarni boshqarish strategiyasini ishlab chiqish.

Risklarni boshqarish ularni aniqlashda tizimlashgan yondashuvni ta’minlaydi va quyidagi afzalliklarga ega:

- bo‘lishi mumkin bo‘lgan risk ta’siri sohasiga e’tibor qaratadi;
- risklarni darajalari bo‘yicha manzillaydi;
- risklarni tutish jarayonini yaxshilaydi;
- kutilmagan holatlarda xavfsizlik xodimini samarali harakat qilishiga ko‘mak beradi;
- resurslardan samarali foydalanish imkonini beradi.

Risklarni boshqarishda muhim rollar va javobgarliklar. Risklarni boshqarishda rollar va javobgarliklar xodimlar o‘rtasida quyidagicha taqsimlangan:

Bosh boshqaruvchi. Bosh boshqaruvchi tashkilotda risklarni boshqarish jarayonini olib borishga rahbar hisoblanib, risklar paydo bo‘lganiga qadar ularni aniqlash uchun talab qilinadigan siyosat va usullarni ishlab chiqadi. Bundan tashqari, kelajakda bo‘lishi mumkin bo‘lgan risklarni tutib olish uchun zarur ishlarni amalga oshirish ham uning vazifasi hisoblanadi.

Axborot texnologiyalari bo‘yicha direktor. Mazkur lavozim egasi tashkilot axborot va kompyuter texnologiyalarini madadlash uchun zarur bo‘lgan siyosat va rejalarni amalga oshirishga javobgar. Ushbu lavozim egasi uchun asosiy javobgarlik – xodimlarni xavfsizlik bo‘yicha o‘qitish hamda axborot texnologiyalarida bo‘lishi mumkin bo‘lgan risklarning biznes jarayonlariga ta’sirini boshqarish.

Tizim va axborot egalari. Tizim va axborot egalarining vazifasi, asosan, axborot tizimlari uchun ishlab chiqilgan rejalar va siyosatlarni monitoringlab borish bo‘lib, quyidagi javobgarliklarni o‘z ichiga oladi:

– sozlanishlarni boshqarish jarayoniga bog‘liq barcha muzokaralarda ishtirok etish;

– axborot texnologiyalari komponentlari qaydlarini saqlash;

– axborot tizimlarida barcha o‘zgarishlarni va ularning ta’sirlarini tadqiqlash;

– barcha tizimlar uchun xavfsizlik holati bo‘yicha hisobotlarni tayyorlash;

– axborot tizimlarini himoyalash uchun zarur bo‘lgan xavfsizlik nazoratini yangilab borish;

– doimiy ravishda xavfsizlikka oid hujjatlarni yangilab borish;

– mavjud xavfsizlik nazoratining samaradorligini ta’minlash bo‘yicha tekshirish va baholash.

Biznes va funksional menejerlar. Mazkur lavozim egalari tashkilotdagi barcha boshqaruv jarayonlarini madadlash uchun javobgar va bu vazifani bajarishlarida tashkilot rahbariyati tomonidan qo‘llab quvvatlanadi. Funksional menejeri turlari:

– rivojlantirish jamoasi menejeri;

– savdo menejeri;

– mijozlarga xizmat ko‘rsatuvchi menejer.

AT xavfsizlik dasturi menedjerlari va kompyuter xavfsizligi bo‘limi direktori. Ushbu lavozim egalari tizimni himoyalashda xavfsizlik nazoratini tanlash orqali axborot tizimi egalarini qo‘llab quvvatlaydi.

AT xavfsizlik amaliyotchilari. AT xavfsizlik amaliyotchilari tashkilotda shaxsiy, fizik va axborot xavfsizligini amalga oshirib quyidagilarga javobgardirlar:

– tashkilotda xavfsizlikning yaxshiroq usullarini yaratish;

– tashkilot standartlariga to‘liq mos keluvchi usullarni ishlab chiqish;

– risklarni boshqarish va biznesni rejalashtirish uchun tashkilot xavfsizlik yondashuvlarini tekshirish;

– xavfsizlik insidentlarini tutish va qaydlash;

– tashkilotda xavfsizlik uchun rol va javobgarliklarni belgilash;

– tashkilotdagi barcha xavfsizlik o‘lchovlarini nazoratlash.

Xavfsizlik bo‘yicha murabbiy. Xavfsizlik bo‘yicha murabbiy tashkilotda tayyorgarlik va o‘quv kurslarini amalga oshiradi. Bu vazifaning, odatda, soha mutaxassislari tomonidan bajarilishi tavsiya etiladi.

Muhim risk ko‘rsatkichlari. Muhim risk ko‘rsatkichlari risklarni samarali boshqarish jarayonida asosiy tashkil etuvchi bo‘lib, dastlabki

bosqichlarda harakatlarning xavflilik darajasini ko‘rsatadi. Muhim risk ko‘rsatkichlarini to‘g‘ri aniqlash tashkilot maqsadini tushunishni talab etadi. U tashkilotdagi risk ehtimolini ko‘rsatuvchi o‘lchov sifatida quyidagilarni amalga oshirishda yordam beradi:

- hodisa ta’sirini aniqlash;
- chegara qiymatda ogohlantirish;
- risk hodisalarini qayta ko‘rish.

Muhim risk ko‘rsatkichi aniqlik bilan hisoblanishi va tashkilotning amalga oshirish ko‘rsatkichlariga salbiy ta’sirlarni aks ettirishi kerak. Bu yerda, tashkilotning amalga oshirish ko‘rsatkichi tashkilotni o‘zining maqsadalariga erishish jarayonini baholash ko‘rsatkichi hisoblanadi.

Risklarni boshqarish bosqichlari. Risklarni boshqarish uzluksiz jarayon va har bir bosqichning muvaffaqqiyatli amalga oshirilishi talab etiladi. U aniqlangan va faol ishlaydigan xavfsizlik dasturidan foydalangan holda xavfni maqbul darajada oldini oladi. Risklarni boshqarish jarayoni quyidagi asosiy to‘rtta bosqichga ajratiladi:

1. Risklarni aniqlash.
2. Risklarni baholash.
3. Risklarni bartaraf etish.
4. Risk monitoringi va qayta ko‘rib chiqish.

Har bir tashkilot risklarni boshqarish jarayonida yuqorida keltirilgan bosqichlarni bosib o‘tadi.

Risklarni aniqlash. Risklarni boshqarishdagi dastlabki qadam bo‘lib, uning asosiy maqsadi riskni tashkilotga zarar yetkazmasidan oldin aniqlash hisoblanadi. Risklarni aniqlash jarayoni mas’ul mutaxassislar qobiliyatiga bog‘liq bo‘lganligi tufayli, turli tashkilotlarda turlicha bo‘ladi. Risklarni aniqlash o‘zida tashkilot xavfsizligiga ta’sir qiluvchi ichki va tashqi risklarning manbasini, sabablarini, natijasini va h. aniqlashni mujassamlashtirgan. Risklar odatda quyidagi 4 ta muhim sohalarda vujudga keladi:

- Muhit. Muhitga aloqador bo‘lgan risklar o‘zida ish joyidagi kamchiliklar, turli halaqitlar, issiq/ sovuq muhit, tutun, past yoritilganlik va elektr xavflari kabilarni birlashtiradi.
- Jihoz. Jihozga aloqador risklar sifatida jihozlarning past ta’mirlanishi muhitini, ishlamasligini, mavjud bo‘lmasligini va vazifaga nomutanosibligini keltirish mumkin.
- Mijoz. Mijozlar bilan bog‘liq risklar odatda muhim o‘zgarishlar, kutilmagan ko‘chishlar va zaif aloqa natijasida yuzaga keladi.

- Vazifalar. Vazifalarga aloqador bo‘lgan risklarga yetarli bo‘lmagan bajarish vaqti, takroriy vazifalar, ishni loyihalash va xodimlar sonini yetarli bo‘lmasiligi orqali paydo bo‘luvchi risklar misol bo‘la oladi.

Riskni aniqlash risklarni boshqarish jarayonidagi turli og‘ishlarni kamaytiradi va bu, o‘z navbatida, kelajakda ta’sir qiluvchi omillar ehtimolini kamaytiradi. Risklarni aniqlashning ko‘plab usullari mavjud, ular asosida turli dasturiy vositalar ishlab chiqilgan. Aksariyat risklarni aniqlash jarayoni maxsus shakllantirilgan jamoa tomonidan amalga oshiriladi. Risklarni aniqlash jarayoni bir qancha omillarga, masalan, tarmoqning holati va jamoa a’zolarining risklarni boshqarishdagi qobiliyatlariga asoslanadi.

Risklarni baholash. Risklarni baholash bosqichida tashkilotdagi risklarga baho beriladi va bu risklarning ta’siri yoki yuzaga kelish ehtimoli hisoblanadi. Risklarni baholash - uzluksiz davom etuvchi jarayon riskka qarshi kurashish rejalarini amalga oshirish uchun imtiyozlarni belgilaydi. Risklarni baholash ularning miqdoriy va sifatiy qiymatini aniqlaydi. Har bir tashkilot risklarni aniqlash, darajalarga ajratish va yo‘q qilish uchun o‘zining riskni baholash jarayonini qabul qilishi kerak.

Risklarni baholash taqdim etilgan risk turini, riskning ehtimoli va miqdorini, uning darajasini hamda uni nazoratlash uchun rejani aniqlaydi. Tashkilotlar risklarni baholash jarayonini odatda xavf aniqlanganida va uni zudlik bilan nazoratlay olmaganlarida amalga oshiradilar. Riskni baholashdan so‘ng ma’lum vaqt mobaynida barcha axborot vositalarini yangilash talab etiladi.

Risklar baholanganidan so‘ng, ular tashkilotga keltiradigan miqdoriy zararga ko‘ra darajalanadi. Darajalarga ajratish risklarga qarshi kurashishga va resurslarni joylashtirishga yordam beradi. Taqdim etilgan risklarning darajalari ularning miqdoriga bog‘liq bo‘ladi:

– darajasi 1-2 ga teng bo‘lgan risklarni zudlik bilan bartaraf etish yoki bartaraf etish imkoni bo‘lmasa, nazorat harakatlari orqali uning xavflilik darajasini tushirish talab etiladi.

– darajasi 3-4 ga teng bo‘lgan risklarni qandaydir biror vaqt mobaynida bartaraf etish yoki xavfni nazoratga olish zarur hisoblanadi.

– darajasi 5-6 ga teng risklarni imkoni bor bo‘lgan vaqtda bartaraf etish yoki imkoni bo‘lmasa xavfni nazoratga olish zarur.

Risklarni baholash quyidagi ikki bosqichda amalga oshiriladi:

Riskni tahlillash: risk tabiatini aniqlash va uning paydo bo‘lishi darajasini hisoblash bosqichi, risklarni nazoratlashga yordam beradi.

Riskni darajalarga ajratish: risklarni tahlillash jarayonida ularning miqdoriy jihatdan reytingini aniqlash va qarshi choralarni loyihalash bosqichi.

Risklarni bartaraf etish. Risklarni bartaraf etish jarayoni aniqlangan risklarni modifikatsiyalash maqsadida mos nazoratni tanlash va amalga oshirishni ta’minlab, miqdoriy darajasi yuqori bo‘lganlariga birinchi murojaat qilinadi. Ushbu bosqichda qaror qabul qilish riskni baholash natijasiga asoslanadi. Ushbu bosqichning asosiy vazifasi jiddiy hisoblangan risklarni nazoratlash uchun qarshi choralarni aniqlash bo‘lib, risklarni individual ravishda yo‘q qilish, monitoringlash va qayta ko‘rib chiqish uchun ularni darajalarga ajratish amalga oshiriladi. Risklarni yo‘q qilishdan oldin quyidagi axborotni to‘plash talab etiladi:

- mos himoya usulini tanlash;
- himoya usuli uchun javobgar shaxsni tayinlash;
- himoya narxini inobatga olish;
- himoya usulining afzalligini asoslash;
- muvaffaqqiyatga erishish ehtimolini aniqlash;
- himoya usulini o‘lchash va baholash usulini aniqlash.

Agar aniqlangan risklarni bartaraf etish talab etilsa, risklarni boshqarish rejasini doimiy qayta ko‘rib chiqish va ishlab chiqish zarur bo‘ladi. Turli himoya usullari riskdan qochish, ularni kamaytirish va ular uchun javobgarliklarni boshqaga o‘tkazish kabi imkoniyatlarni taqdim etadi.

Xodimlardan risklarni kamaytirish yoki minimallashtirish uchun quyidagilarni amalga oshirishlari talab etiladi:

- risklarni nazoratlash rejasini ishlab chiqish;
- ko‘rsatilayotgan xizmatga risklarni ta’sirini aniqlash;
- risklarni nazoratlash rejasini tugallash uchun qat’iy cheklovlarni qo‘yish;
- risklarni nazoratlash strategiyasini amalga oshirish;
- risklarni nazoratlashda mijoz harakatini aniqlash;
- risklarni nazoratlash mobaynida madadlovchi xodimlar bilan aloqani o‘rnatish;
- risklarni nazoratlash jarayonining bir qismi risklarni nazoratlash rejasini to‘liq hujjatlashtirish.

Risk monitoringi va qayta ko‘rib chiqish. Samarali risklarni boshqarishning rejasi risklarni aniqlashni va baholashni kafolatli amalga oshirishda risk monitoringi va qayta ko‘rib chiqishni talab etadi. Risk monitoringi quyidagi imkoniyatlarni beradi:

- yangi risklarni paydo bo‘lish imkoniyatini aniqlaydi;
- riskni bartaraf etuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi;
- shuningdek, risk monitoringi riskning ehtimoli, ta’siri, holati va oshkor bo‘lishini o‘z ichiga oladi.

Riskni qayta ko‘rib chiqish:

- orqali amalga oshirilgan risklarni boshqarish strategiyasining samaradorligi baholanadi;
- yuqori ehtimollik risklardan ogoh bo‘lishni boshqarishni kafolatlaydi.

Tashkilotda risklarni boshqarishning freymworki (strukturasi) (Enterprise Risk Management Framework, ERM Framework). Risklarni boshqarish freymworki tashkilotning risklarni boshqarish usuliga amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo‘yicha faoliyatni birlashtiruvchi tarkibiy jarayonni ta’minlaydi. Tashkilotda risklarni boshqarish freymworki quyidagi harakatlarni aniqlaydi, tahlillaydi va amalga oshiradi:

- riskka olib keluvchi harakatlarni bekor qilish orqali riskdan qochish;
- risk ta’siri yoki ehtimolini minimallashtirish orqali riskni kamaytirish;
- risklarni boshqarish jarayoni standartlarini taqdim qilish.

Tashkilotda risklarni boshqarish freymworkining asosiy maqsadlari quyidagilardan iborat:

- tashkilotda risklarni boshqarishni tashkilot faoliyatini boshqarish bilan birlashtirish;
- risklarni boshqarishning afzalliklarini o‘zaro bog‘lash;
- risklarni boshqarish uchun tashkilotda rollarni va vazifalarni belgilash;
- risklar to‘g‘risida hisobot berish va rivojlanish jarayonini standartlashtirish;
- tashkilotda risklarni boshqarish uchun standart yondashuvlarni o‘rnatish;
- risklarni boshqarishda resurslarga ko‘maklashish;
- tashkilotda risklarni boshqarish doirasini va ilovalarini o‘rnatish;
- tashkilotda risklarni boshqarishni takomillashtirish uchun vaqti-vaqti bilan tekshirish amalga oshiriladi.

Amalda tashkilotda risklarni boshqarish freymworklari sifatida NIST ERM, COSO ERM va COBIT ERM kabilardan keng foydalaniladi.

Risklarni boshqarishning axborot tizimlari (Risk Management Information Systems, RMIS). RMIS bu – boshqaruv axborot tizimi bo‘lib, axborotni saqlashni boshqarish, tahlillash va tashkilot tarmog‘i uchun risk to‘g‘risida ma’lumot olish imkoniyatini taqdim qiladi. Tashkilotlar risklarni boshqarish jarayonini optimallashtirish uchun RMIS bilan risklarni boshqarish freymworkini birlashtiradi. RMIS tizimlari quyidagi afzalliklarga ega:

- ma’lumot ortiqchaligi va xatoligini kamaytirish orqali ma’lumot ishonchligini yaxshilaydi;
- RMIS orqali xabarlar boshqaruvining yaxshilanishi natijasida tashkilotdagi xarajatlar kamayadi;
- RMIS, tashkilotning standartlariga muvofiq, risklarni boshqarish siyosatidan samarali foydalanishda yordam beradi.

RMIS turli omillar bo‘yicha hisobotlarni shakllantiradi va ushbu hisobotlar tashkilotda tarmoq risklari to‘g‘risida yaxlit tasavvurga ega bo‘lishga hamda ularni boshqarishga imkon beradi. Hosil qilingan RMIS hisoboti turlari unga yuborilgan so‘rov turiga bog‘liq bo‘ladi. RMIS quyidagi turdagi hisobotlarni shakllantiradi:

- *Standart hisobotlar:* yuborilgan umumiy so‘rovlarga javob sifatida standart hisobotlarni shakllantiradi. Ushbu hisobot guruhga ajratilgan ma’lumotlardan tashkil topmaydi.
- *Maxsus hisobotlar:* maxsus so‘rovlarga nisbatan turli guruhga tegishli ma’lumotlardan tashkil topgan maxsus javoblarni generatsiyalaydi.

Amalda RMIS tizimining turli ko‘rinishidagi vositalaridan keng foydalaniladi. Ularga misol sifatida, Aon Enterprise Risk Management, Stars RMIS, RiskEnvision, RiskonnectRMIS, INFORM, Traveler’s e-CARMA vositalarini keltirish mumkin.

Nazorat savollari

1. Kompyuter tarmog‘i va uning turlari.
2. Tarmoq topologiyasi va uning turlari.
3. Tarmoq qurilmalari va ularning asosiy vazifalari.
4. Asosiy tarmoq protokollari va ularning vazifalari.
5. Tahdid, zaiflik va hujum tushunchalariga izoh bering.
6. Tarmoq muammolarini yuzaga kelishining asosiy sabablari.

7. Tahdidlarning turlari va ularga misollar keltiring.
8. Tarmoq xavfsizligining buzilishi biznes faoliyatiga qanday ta’sir qiladi?
9. Tarmoq xavfsizligi zaifliklari va ularning turlari.
10. Tarmoq xavfsizligiga qaratilgan hujum turlari.
11. Razvedka hujumlarining asosiy maqsadi.
12. Kirish hujumlariga misollar keltiring.
13. Zararli dasturiy vositalarga asoslangan hujumlarning asosiy maqsadi nima?
14. Tarmoqlararo ekran vositasining asosiy vazifasi.
15. Tarmoqlararo ekran vositalarining tasniflanishi.
16. VPN tarmoq va uning asosiy vazifasi.
17. VPN tarmoqni qurish usullari.
18. Risk tushunchasiga izoh bering.
19. Risk darajasi tushunchasiga izoh bering.
20. Risk matritsasi va uning asosiy vazifasini tushuntiring.
21. Risklarni boshqarish va uning asosiy bosqichlari.
22. Tashkilotda risklarni boshqarish freymworki va uning asosiy vazifasi.
23. Risklarni boshqarishning axborot tizimlariga misollar keltiring.

6 BOB. FOYDALANUVCHANLIKNI TA’MINLASH USULLARI

6.1. Foydalanuvchanlik tushunchasi va zaxira nusxalash

Foydalanuvchanlik. Kompyuter xavfsizligi axborot va axborot tizimlarini ruxsatsiz foydalanish, ochish, buzish, o‘zgartirish yoki yo‘q qilishdan himoya qilishni anglatib, uning eng muhim maqsadi axborot konfidensialligini, yaxlitligini va foydalanuvchanligini ta’minlashdir. Kompyuter tizimlaridan ma’lumotlarni saqlash va ishlash uchun foydalanilsa, xavfsizlikni nazoratlash vositalari ma’lumotlarning suiste’mol qilinishidan himoyalashda ishlatiladi. O‘z navbatida, axborot tizimlarining o‘z maqsadiga erishishiga imkon beruvchi foydalanuvchanlikni ta’minlash muhim hisoblanadi.

Foydalanuvchanlik tushunchasiga turli soha korxonalari va olimlar tomonidan turlicha ta’riflar keltirilgan, xususan:

- konfidensial ma’lumotlarga yoki manbalarga ehtiyoji bo‘lganlar uchun foydalanish imkonini berish;
- vakolatli foydalanuvchilarning ma’lumotlardan va axborot tizimlaridan o‘z vaqtida va ishonchli foydalanish imkoniyati;
- obyektlardan qonuniy foydalanish imkoniga ega vakolatli shaxslarning tizimga kirishiga to‘sqinlik qilmaslik;
- tizimlarning tezkor ishlashini va qonuniy foydalanuvchilarga rad etilmaslikni kafolatlash.

Hozirda barcha sohalarda axborot texnologiyalarining keng joriy qilinishi tashkilot yoki korxonalar faoliyatini yuritishda muhim ahamiyat kasb etayotgan bo‘lsada, tashkilotda axborot tizimlari bilan bog‘liq muammo kuzatilsa, uning faoliyati katta yo‘qotishlarga duch kelishi mumkin. Faraz qilaylik, xosting provayderlarida xizmat ko‘rsatishda 99% foydalanuvchanlik ta’minlangan bo‘lsin. Bu qiymat ko‘rinishdan katta bo‘lsada, bir yilda 87 soat (3.62 kun) xizmat ko‘rsatilmaganligini anglatadi. Bu vaqt ichida tashkilot, xizmat ko‘rsatish hajmiga bog‘liq, turlicha zarar ko‘rgan bo‘lishi mumkin. Yuqoridagi holda, hattoki 99.9% xizmat ko‘rsatishda foydalanuvchanlikka erishilgan bo‘lsada, yiliga 9 soat yo‘qotish kuzatiladi.

Xizmat ko‘rsatishdagi mazkur zararlarni kamaytirish nafaqat Facebook yoki Amazon kabi yirik korporasiyalar uchun, balki barcha tashkilotlar uchun ham muhim hisoblanadi. Xususan, 2013 yilda 30 daqiqa davomida www.amazon.com saytining ishlamay qolishi kompaniyaga 2 million dollarga (daqiqasiga 66 240 $) tushgan.

Yuqoridagi misollar har bir tashkilot uchun foydalanuvchanlikni ta’minlash qanchalik muhimligini anglatadi. Yuqori foydalanuvchanlik o‘zida quyidagi 3 ta omilni birlashtiradi:

- *xatolarga bardoshlilik:* bu omil tizimda xatolik kuzatilgan taqdirda ham ishlamay qolmaslik shartini ko‘rsatadi;
- *taqdim etilayotgan xizmatlarning kafolati:* xizmatlar, shuningdek, tizimlar ham har doim mavjud bo‘lishi kerak;
- *ma’lumotlar xavfsizligi:* infrastruktura tarkibidagi ma’lumotlar yaxlitligi, undagi jarayonlar va xodimlar ishlamay qolgan taqdirda ham ta’minlanishi shart.

Yuqori darajadagi foydalanuvchanlik o‘zida birorta ham xatolikni qamrab olmaydi. Boshqacha aytganda, hosting provayderlarining yuqori foydalanuvchanlikni ta’minlashi uchun o‘zidagi biror tarmoq qurilmasi (masalan, marshrutizator yoki tarmoqlararo ekran) ishlamay qolishini oldini olish talab etiladi.

Tizim yoki xizmat foydalanuvchanligini buzilishiga olib keluvchi hujum – *xizmat ko‘rsatishdan voz kechishga undash (DoS)* hujumi hisoblanib, mazkur hujumning asosiy maqsadi tizim yoki tarmoqni qonuniy foydalanuvchilar uchun xizmat ko‘rsatishini to‘xtatishidan iborat. Ushbu hujum turli usul va vositalardan foydalanilib, turli tizim va muhit xususiyati asosida amalga oshiriladi.

Xizmat ko‘rsatishdan voz kechishga undash hujumini oldini olish va foydalanuvchanlikni ta’minlash uchun kompleks himoya choralarini ko‘rish tavsiya etiladi.

Zaxira nusxalash. Hozirgi kunda ma’lumotlarning yo‘qolishi tashkilotlar uchun asosiy xavfsizlik muammolaridan biri bo‘lib, buning natijasida tashkilot katta zarar ko‘rishi mumkin. Shuning uchun, tashkilotdan muhim ma’lumotlarni muntazam zaxira nusxalab borish talab etiladi.

Ma’lumotlarni zaxira nusxalash – muhim ma’lumotlarni nusxalash yoki saqlash jarayoni bo‘lib, ma’lumot yo‘qolgan vaqtda qayta tiklash imkoniyatini beradi. Ma’lumotlarni zaxira nusxalashdan asosiy maqsad quyidagilar:

– zarar yetkazilganidan so‘ng tizimni normal ish holatiga qaytarish;

– tizimda saqlanuvchi muhim ma’lumotlarni yo‘qolganidan so‘ng uni qayta tiklash.

Tashkilotlarda ma’lumotlar yo‘qolishi moliyaviy tomondan va mijozlarga aloqador holda ta’sir qilishi bilan xarakterlansa, shaxsiy

kompyuterda esa shaxsiy fayllarni, rasmlarni va boshqa qimmatli ma’lumotlarni yo‘qolishiga sababchi bo‘ladi.

Ma’lumotlarni yo‘qolishiga quyidagilar sababchi bo‘lishi mumkin:

- *Inson xatosi:* qasddan yoki tasodifan ma’lumotlarning o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmaganligi yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
- *G‘arazli hatti-harakatlar:* tashkilotdagi muhim ma’lumotlarning modifikatsiyalanishi yoki o‘g‘irlanishi.
- *Tabiiy sabablar:* energiyaning o‘chishi, dasturiy ta’minotning tasodifiy o‘zgarishi yoki qurilmaning zararlanishi.
- *Tabiy ofatlar:* zilzila, yong‘in va h.

Tashkilotda yoki shaxsiy kompyuterda ma’lumotlarni zaxira nusxalash quyidagi imkoniyatlarni taqdim etadi:

- muhim ma’lumotlardan yo‘qolgan va zararlangan taqdirda ham foydalanish;
- tashkilotlarni o‘z faoliyatining to‘xtatilishidan himoyalash va ma’lumotlarni ixtiyoriy vaqtda tiklash;
- tashkilotdagi yo‘qolgan ma’lumotlarni tiklash.

Ma’lumotlarni zaxira nusxalashning ideal strategiyasi ma’lumotni to‘g‘ri tanlashdan boshlab, to ma’lumotni kafolatli tiklash jarayonigacha bo‘lgan bosqichlarni o‘z ichiga oladi. Turli tashkilotlarda zaxira nusxalash farq qilsada, ma’lumotlarni zaxira nusxalashdan oldin quyidagi hususiyatlarga e’tibor qaratish muhim hisoblanadi:

- ma’lumotlarni zaxira nusxalash strategiyasi ixtiyoriy tashqi qurilmalardan ma’lumotlarni tiklash imkoniyatiga ega bo‘lishi shart. Ushbu qurilmalarga misol sifatida serverlar, host mashinalar, noutbuklar va boshqalarni ko‘rsatish mumkin.
- agar tabiiy ofat natijasida ma’lumot yo‘qolsa, zaxira nusxalash strategiyasi faqat chekli sondagi insidentlarga qarshi himoya bilan cheklanmasligi zarur. Tabiiy ofat yuz bergan taqdirda ham strategiya o‘zida ma’lumotlarni tiklash usullarini mujassamlashtirishi shart;
- strategiya dastlabki bosqichlarda ma’lumotlarni qayta tiklash uchun muhim qadamlardan iborat bo‘lishi kerak;
- zaxira nusxalash narxining qimmat bo‘lmasligi tashkilot uchun moliyaviy madad hisoblanadi;
- inson tomonidan bo‘lishi mumkin bo‘lgan xatoliklarni tezlik bilan oldini olish uchun ma’lumotlarni zaxira nusxalash avtomatik tarzda amalga oshirilishi kerak.

Tashkilotlarda zaxira nusxalarni saqlovchilarni tanlash umumiy muammolardan biri hisoblanib, mos bo‘lmagan zaxira saqlovchi vositaning tanlanishi ma’lumotlarning sirqib chiqishiga olib kelishi mumkin. Zaxira nusxalar saqlanuvchi vositalarni tanlash saqlanuvchi ma’lumotlarning turiga bog‘liq va quyidagi omillarga asoslanadi:

- *Narx:* har bir tashkilot o‘zining byudjetiga mos zaxira nusxalash vositasiga ega bo‘lishi shart. Saqlanuvchi ma’lumotlar hajmidan katta hajmga ega vositalarga ega bo‘lish ortiqcha sarf xarajatni keltirib chiqaradi.
- *Ishonchlilik:* tashkilotlar o‘z ma’lumotlarini buzilishsiz ishlaydigan zaxira saqlash vositalarida saqlanishiga erishishlari kerak.
- *Tezlik:* tashkilotlar zaxira nusxalash jarayonida inson aralashuvini imkoni boricha kam talab etadigan saqlash vositalarini tanlashlari kerak.
- *Foydalanuvchanlik:* ma’lumot yo‘qolganidan yoki zararlanganidan so‘ng zaxira nusxalash vositasidan foydalanishda muammolar bo‘lishi mumkin. Shuning uchun, tashkilotlar zaxira nusxalash vositalarining doimo foydalanishga yaroqli bo‘lishiga e’tibor qaratishlari kerak.
- *Qulaylik:* tashkilot foydalanish uchun qulay zaxira nusxalash vositasini tanlashi shart. Bu, o‘z navbatida, zaxira nusxalash jarayonida moslashuvchanlikni ta’minlashda muhim hisoblanadi.

Hozirda ma’lumotlarni zaxira nusxalarini saqlashda quyidagi vositalardan foydalanilmoqda:

Optik disklar (DVD, Blu-ray). DVD disklar 8.55 GBaytgacha ma’lumotlarni saqlash imkoniyatiga ega bo‘lib, ularda faqat o‘qish imkoniyati mavjud. Ushbu ma’lumot saqlagichlarining afzalligi narxining pastligi va foydalanishdagi qulayligi bilan asoslansa, katta hajmdagi ma’lumotlarni saqlay olmasligi uning kamchiligi hisoblanadi.

Ko‘chma qattiq disklar/ USB xotiralar. Ko‘chma qattiq disklar DVD, Blu-ray disklarga qaraganda kichikroq hajmli zaxira ma’lumotlarini saqlash uchun yaxshi vosita hisoblanadi. Flesh disklar esa turli o‘lchamli bo‘lib, katta hajmdagi ma’lumotlarni ham saqlash imkoniyatiga ega. Qattiq disklardan foydalanishning yana bir varianti – RAID (Redundant Array of Independent Disks) hisoblanadi.

Lentali disklar. Lentali disklar ma’lumotlarni zaxira saqlash uchun eng mos saqlagichlar bo‘lib, tashkilot sathida ma’lumotni zaxira nusxalashni amalga oshiradi. Ushbu saqlagichlardan ma’lumotlarni va dasturlarni saqlash uchun foydalaniladi. Ushbu zaxira saqlagichi olib

yurish uchun qulay, foydalanuvchi ishtirokini talab etmaydi va to‘liq avtomatlashgan tarzda amalga oshiriladi. Uning asosiy kamchiligi oddiy foydalanuvchilar uchun qimmatligi va oddiy kompyuterlardan foydalanishi uchun qo‘shimcha apparat va dasturiy vositani talab qilishi.

6.2. Ma’lumotlarni zaxiralash texnologiyalari va usullari

Aksariyat tashkilotlar muhim ma’lumotlarini RAID texnologiyasi asosida zaxira nusxalashni amalga oshiradilar. RAID texnologiyasida ma’lumotlar bir qancha disklarning turli sohalarida saqlangani bois, IO (kirish/ chiqish) amallarining bajarilishi osonlashadi. RAID texnologiyasi ko‘plab qattiq disklarni bitta mantiqiy disk sifatida o‘rnatish orqali ishlaydi. Ushbu texnologiya disklar massivi bo‘ylab bir xil ma’lumotlarni muvozanatlashgan shaklda saqlash imkoniyatini beradi. Ushbu texnologiya odatda serverlarda ma’lumotlarni saqlashga mo‘ljallangan, shaxsiy kompyuterlardan foydalanish zaruriyati mavjud emas.

RAID texnologiyasida amallarni samarali bajarish uchun 6 ta sath mavjud: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10 va RAID 50. RAIDning har bir sathi quyidagi xususiyatlarga ega:

- *xatoga bardoshlilik:* agar biror disk ishlashdan to‘xtasa, boshqa disklar normal ishlashini davom ettiradi;
- *unumdorlik:* RAID ko‘plab disklar bo‘ylab o‘qish va yozishda yuqori unumdorlik darajasiga ega.

Disklarning ma’lumotlarni saqlash imkoniyati mos RAID sathini tanlashga asoslanadi. Saqlash hajmi individual RAID disklar o‘lchamining bir xil bo‘lishini talab etmaydi. Barcha RAID sathlari quyidagi saqlash usullariga asoslanadi:

- *bloklash:* ma’lumotlar ko‘plab bloklarga ajratiladi. Mazkur bloklar keyinchalik RAID tizimi orqali yoziladi. Bloklash ma’lumotlarni saqlanishini yaxshilaydi.
- *akslantirish:* akslantirish ma’lumotlarning nusxalanishini va RAID bo‘ylab uzluksiz saqlanishini amalga oshiradi. Bu usul xatoga bardoshli va amalga oshirilishining yuqori darajasiga ega.
- *nazorat qiymati:* nazorat qiymati ma’lumotlar bloki yaxlitligini tekshirish funksiyasini amalga oshirishda bloklash funksiyasidan foydalanadi. Disk buzilganida nazorat qiymati xatolikni tuzatish funksiyasi yordamida ma’lumotlarni tiklashga harakat qiladi.

RAID tizimlari sathga bog‘liq holda o‘ziga xos afzalliklar va kamchiliklarga ega.

RAID tizimlarining afzalliklari:

Unumdorlik va ishonchlilik: RAID texnologiyasi disklarda ma’lumotlarni o‘qish va yozish unumdorligini oshiradi. Ushbu texnologiya IO jarayonini taqsimlash orqali unumdorlikni yaxshilaydi va jarayon tezligi, yagona diskda ma’lumotlarni saqlashga qaraganda, yuqori bo‘ladi.

Xatolikni nazoratlash: buzilgan diskda saqlangan ma’lumotlarni qolgan diskdagi ma’lumotlar bilan taqqoslash orqali ularni tiklashni yoki tuzatishni amalga oshiradi.

Ma’lumotlar ortiqchaligi (ma’lumotlarni nusxalash): diskning buzilishi istalgan vaqtda yuzaga kelishi mumkin. RAID texnologiyasi qurilma buzilganida ma’lumotlarni nusxalash orqali uning qayta tiklanishini ta’minlaydi.

Disklarni navbatlanishi: ma’lumotlarni o‘qish/ yozish unumdorligini oshiradi. Ma’lumotlar kichik bo‘laklarga bo‘linib, bir qancha disklar bo‘ylab tarqatiladi. RAID tizimida ma’lumotlarni o‘qish va yozish bir vaqtda bajariladi.

Tizimning ishlash davomiyligi: ushbu o‘lchov kompyuterning ishonchligini va barqarorligini belgilaydi. Tizimning ishlash davomiyligi tizimning avtomatik ishlash vaqtini belgilaydi.

RAID tizimlarining kamchiliklari:

Tarmoq drayverlarini yozish: RAID texnologiyasi asosan serverlarda foydalanish uchun loyihalangani bois, uning asosiy kamchiligi - barcha tarmoq drayverlarini yozish.

Mos kelmaslik: tizimlar turli RAID drayverlarini madadlaydi. Muayyan apparat yoki dasturiy komponent serverda sozlangan RAID tizimi bilan mos kelmasligi mumkin. Mos kelmaslik RAID tizimining o‘z vazifasini to‘g‘ri amalga oshirilmasligiga olib kelishi mumkin.

Ma’lumotlarning yo‘qolishi: RAID drayverlari mexanik muammolar tufayli o‘z funksiyalarini bajara olmasliklari mumkin. Disklar ketma-ket buzilishga uchraganida ma’lumotlarning yo‘qolishi xavfi ortadi.

Qayta tiklashning uzoq vaqti: katta hajmli disklardan foydalanish ma’lumotlarni uzatish tezligini ortishiga olib keladi. Biroq, katta hajmli disklarda ma’lumotlarni tiklash va buzilgan disklarni qayta sozlash uzoq vaqt talab etadi.

Narxining yuqoriligi: RAID texnologiyasini amalga oshirish iqtisodiy jihatdan katta mablag‘ni talab etadi. Bundan tashqari, tizim

ishini yaxshilash uchun qo‘shimcha RAID kontrollerlarini va qurilma drayverlarini sotib olish talab etiladi.

Mos RAID sathini tanlash tashkilot zaruriyatidan kelib chiqqan holda va har bir sathning taqdim qilayotgan imkoniyatlariga asoslanishi zarur. RAID sathini tanlashda ularni xususiyatlariga ham e’tibor berish talab etiladi (6.1-jadval).

6.1-jadval

RAID texnologiyalarining tahlili

RAID	**Diskdan foydalanish**	**Buzilishga bardoshligi**	**Katta ma’lumotlar transferi**	**IO darajasi**	**Ma’lumot foydalanuvchanligi**	**Asosiy kamchiligi**
Yagona disk	Bir xil 100%	Yo‘q	Yaxshi	Yaxshi	Yagona diskning MTBF davri	Disk buzilsa, ma’lumot yo‘qoladi
RAID 0	A’lo 100%	Ha	Juda yaxshi	Juda yaxshi	Diskning past MTBF davri	
RAID 1	O‘rtacha 50%	Ha	Yaxshi	Yaxshi	Yaxshi	Disk hajmidan 2 marta kam foydalanish
RAID 3	Yaxshi-juda yaxshi	Ha	Juda yaxshi	Yaxshi	Yaxshi	Disk buzilsa, ma’lumot yo‘qoladi
RAID 5	Yaxshi-juda yaxshi	Ha	Yaxshi-juda yaxshi	Yaxshi	Yaxshi	Disk buzilsa, kam o‘tkazuvchanlik
RAID 0+1	O‘rtacha 50%	Ha	Yaxshi	Juda yaxshi	Yaxshi	Disk hajmidan 2 marta kam foydalanish
RAID 1+0	O‘rtacha 50%	Ha	Juda yaxshi	Juda yaxshi	Juda yaxshi	Juda qimmat, keng ko‘lamli emas
RAID 30	Yaxshi-juda yaxshi	Ha	Juda yaxshi	A’lo	A’lo	Juda qimmat
RAID 50	Yaxshi-juda yaxshi	Ha	Yaxshi-juda yaxshi	A’lo	A’lo	Juda qimmat

Izoh: MTBF – Mean Time Between Failures (buzilishlar o‘rtasidagi o‘rtacha vaqt).

Zaxira nusxalash usullari. Tashkilot o‘zining moliyaviy imkoniyati va AT infrastrukturasi asosida zaxira nusxalash usulini tanlaydi. Ma’lumotlarni zaxira nusxalashning quyidagi usullari mavjud.

Issiq zaxiralash. Ma’lumotlarni zaxira nusxalashning mazkur usuli amalda keng qo‘llaniladi va dinamik yoki aktiv zaxira nusxalash usuli deb ham ataladi. Ushbu usulga binoan foydalanuvchi tizimni boshqarayotgan vaqtida zaxira nusxalash jarayonini ham amalga oshirishi mumkin. Mazkur zaxiralash usulini amalga oshirish tizimning harakatsiz vaqtini kamaytiradi. Zaxiralash davomida ma’lumotlardagi o‘zgarish yakuniy zaxira nusxasiga ta’sir qilmaydi. Ravshanki, zaxiralashni amalga oshirish vaqtida tizimning ishlash jarayoni sekinlashadi.

Sovuq zaxiralash. Ushbu zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz usuli bo‘lib, ma’lumotlarni nusxalashda turli tahdidlardan himoyalaydi.

Iliq zaxiralash. Ushbu zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi. Bu ma’lumotlarni akslantirish yoki nusxalash hollarida muhim hisoblanadi. Ushbu usulda ma’lumotlarni zaxiralash uzoq vaqt oladi va jarayon biror vaqt intervalida amalga oshiriladi (kundan xaftagacha).

Zaxira nusxalashda ma’lumotlarni saqlash manzilini tanlash muhim hisoblanadi. Zaxira nusxalarni quyidagi manzillarda saqlash mumkin.

Ichki (onsite) zaxiralash. Ushbu zaxiralash usuli tashkilot ichida amalga oshirilib, tashqi qurilmalar, lentali saqlagichlar, DVD, qattiq disk va boshqa saqlagichlardan foydalaniladi. Ichki zaxiralash qurilmalari zaxira saqlanuvchi ma’lumotlar hajmiga muvofiq tanlanadi.

Tashqi (offsite) zaxiralash. Tashqi zaxiralash mosofadagi manzilda amalga oshirilib, fizik disklarda ma’lumotlarni saqlash onlayn yoki uchinchi tomon xizmati orqali amalga oshirilishi mumkin.

Bulutli tizimda zaxiralash. Ushbu zaxiralash usuli onlayn usuli deb ham ataladi. U zaxiralangan ma’lumotlarni ochiq tarmoqda yoki ma’lum serverda saqlaydi. Odatda ma’lum server vazifasini uchinchi tomon xizmati amalga oshirishi mumkin.

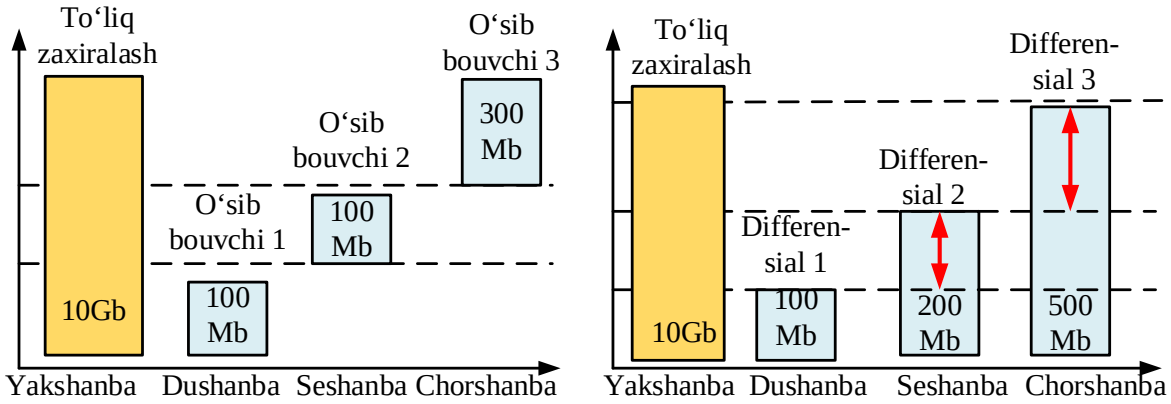
Zaxiralash turlari. Mos zaxiralash turi tarmoqqa ortiqcha yuklama qo‘shmaydi hamda narx, vaqt va resursni kam talab qiladi. Amalda uchta turdagi zaxiralash turlari mavjud: *to‘liq, differensial* va *o‘sib boruvchi*.

To‘liq zaxiralash: ushbu usul normal zaxiralash deb ham atalib, jadvalga ko‘ra avtomatik tarzda amalga oshiriladi. Bunda, barcha fayllar

nusxalanadi va zichlangan tarzda saqlanadi. Ushbu usul nusxalangan ma’lumotlar uchun samarali himoyani ta’minlaydi.

O‘sib boruvchi zaxiralash: ushbu usulga ko‘ra zaxiralanuvchi ma’lumotlarga nisbatan o‘zgarish yuz berganida zaxiralash amalga oshiriladi. Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usulidan foydalanish mumkin. Shuning uchun, o‘sib boruvchi zaxiralashni amalga oshirishdan oldin, tizim to‘liq zaxiralashni amalga oshirishi shart.

Faraz qilaylik, zaxira nusxalash jadvaliga ko‘ra to‘liq zaxiralash yakshanba kuniga, ortib boruvchi zaxiralash esa seshanbadan shanbagacha amalga oshirilishi belgilangan bo‘lsin. Yakshanba kuni to‘liq zaxiralash amalga oshirilganidan so‘ng, dushanba kunidagi o‘zgarishlar seshanba kuni o‘sib boruvchi usul asosida amalga oshiriladi. Ushbu jarayoni shanbagacha davom ettiriladi (6.1 – rasm “a”).



a) O‘sib boruvchi zaxiralash b) Differensial zaxiralash

6.1-rasm. Zaxiralash turlari

Differensial zaxiralash: ushbu zaxiralash usuli to‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalash amalga oshiriladi.

Masalan, yuqoridagi misolni qaraylik. To‘liq zaxiralash yakshanba kuni, differensial nusxalash esa shanbagacha amalga oshirilishi jadvalda keltirilgan bo‘lsin. Yakshanba kuni to‘liq zaxira nusxalash amalga oshirilganidan so‘ng, dushanba kuni differensial zaxiralash kun o‘tishi bilan amalga oshiriladi. Bu holat o‘sib boruvchi zaxiralashga o‘xshab ketadi. Biroq, seshanbada, zaxira nusxalash yakshanba va dushanbadagi o‘zgarishlar uchun amalga oshiriladi. Shundan so‘ng, chorshanbada zaxiralash yakshanba, dushanba va seshanba kunlari uchun amalga oshiriladi (6.1 – rasm “b”).

6.3. Ma’lumotlarni qayta tiklash va hodisalarni qaydlash

Ma’lumotlarni qayta tiklash. Ma’lumotlarning yo‘qolishi har qanday tashkilot uchun jiddiy muammo hisoblanadi. Shu sababli, ma’lumotlarni qayta tiklash usullaridan foydalanish talab etiladi. Ushbu jarayon ma’lumotlarning qanday yo‘qolganiga, ma’lumotlarni qayta tiklash dasturiy vositasiga va ma’lumotlarni tiklash manziliga bog‘liq.

Ma’lumotlarni eltish vositalarida, USB xotirada, qattiq diskda, DVD va boshqa saqlagichlarda ma’lumotlarni qayta tiklash mumkin. Qayta tiklash jarayonining muvaffaqqiyatli amalga oshirilishi foydalanuvchining malakasiga bog‘liq. Ma’lumotlarni qayta tiklash jarayonida bilim va to‘g‘ri tanlangan vosita muhim hisoblanadi.

Ma’lumotlarni qayta tiklash har doim ham muvaffaqiyatli bo‘lmasligi mumkin. Agar saqlagichda xatolik mavjud bo‘lsa yoki unga ko‘p zarar yetgan bo‘lsa, ma’lumotlarni tiklashning imkoni bo‘lmasligi mumkin. Ma’lumotlarning qayta tiklanishi ehtimoli ularning yo‘qolishi sababiga bog‘liq. Ma’lumotlarni yo‘qolishiga sabab bo‘luvchi hollar quyidagilar:

Faylni o‘chirish: agar fayl o‘chirilsa, ushbu soha qaytadan yozilgunga qadar saqlagichda mavjud bo‘ladi. Ma’lumotlar saqlangan sohadagi kichik xotiraga ma’lumotlar yozilishi butun ma’lumotlarni tiklanmasligiga sababchi bo‘lishi mumkin. Windows OTda NTFS fayl tizimida ma’lumotlarni o‘chirish algoritmi mavjud va ma’lumotlarni tiklash ham ushbu algoritm asosida amalga oshiriladi.

Faylning zararlanishi: agar OT zararlansa, ma’lumotlarni diskning qismlar jadvali yordamida tiklash mumkin. Agar diskning qismlar jadvali ham zararlangan bo‘lsa, qayta tiklashning maxsus vositalaridan foydalanishga to‘g‘ri keladi.

Qattiq diskning fizik zararlanishi: qattiq diskka fizik ta’sir bo‘lishi, faylni zararlanishiga qaraganda, katta yo‘qotishlarga sabab bo‘lishi mumkin. Bu esa ma’lumotlarni qayta tiklashning maxsus sathidan foydalanishni talab etadi. Zararlangan fizik diskdan ma’lumotlarni tiklash vaqtida, tiklash jarayonining muhiti turli ifloslanishlardan holi bo‘lishi zarur. Ya’ni, bu jarayon toza xonada amalga oshirilishi shart. Chang bo‘lgan sohalarda ma’lumotlarning qayta tiklanishi qiyin bo‘ladi.

Ma’lumotlarni qayta tiklashda quyidagilarni esda saqlash zarur:

- ma’lumotlar yo‘qolgan qattiq diskga qayta tiklangan ma’lumotlarni yozmaslik;
- turli zaxira nusxalarni amalga oshirish va ularni turli manzillarda saqlash;

- ma’lumotlarni qayta tiklash har doim ham 100% samara bermasligi.

Amalda saqlagichlardagi yo‘qolgan ma’lumotlarni tiklashda maxsus dasturiy vositalardan foydalaniladi. Ularga *Recovery My Files*, *EASEUS Data Recovery Wizard*, Advanced Disk Recovery, Handy Recovery, R-Studio, Data Recovery Pro, Recuva, Total Recall, Pandora Recovery kabilarni misol sifatida keltirish mumkin.

Hodisalarni qaydlash. Xatolik yuz berganida, tizim ma’muri yoki madadlash xodimi xatoning sababini aniqlashi, yo‘qolgan ma’lumotlarni qayta tiklashga urinishi va xatoning takrorlanishiga yo‘l qo‘ymasligi lozim. Ilovalar, operatsion tizim va boshqa tizim xizmatlari muhim voqealarni, masalan, xotira hajmining kamligi yoki diskdan foydalanishga haddan tashqari ko‘p urinishlarni qayd etishi muhim hisoblanadi. Keyinchalik tizim ma’muri xato sababini aniqlashi va u sodir bo‘lgan kontekstni aniqlash uchun hodisalar jurnalidan (log fayl deb ataladi) foydalanishi mumkin.

Hodisalarni qaydlash quyidagilarni o‘z ichiga olishi shart:

operatsion tizim hodisalari:

– tizimni ishga tushirish va o‘chirish;

– xizmatni boshlash va tugatish;

– tarmoq ulanishidagi o‘zgarishlar yoki muvaffaqiyatsizliklar;

– tizim xavfsizligini sozlash va boshqarish vositalarini o‘zgartirishga urinishlar.

OT audit yozuvlari:

– tizimga kirishdagi urinishlar (muvaffaqiyatli yoki muvaffaqiyatsiz);

– tizimga kirgandan so‘ng bajariladigan funksiyalar (masalan, muhim faylni o‘qish yoki yangilash, dasturni o‘rnatish);

– qayd yozuvini o‘zgartirish (masalan, yozuvni yaratish va yo‘q qilish, imtiyozlarni tayinlash);

– imtiyozli qayd yozuvidan muvaffaqiyatli / muvaffaqiyatsiz foydalanish.

ilova qayd yozuvi to‘g‘risidagi ma’lumot:

– ilovani muvaffaqiyatli va muvaffaqiyatsiz autentifikatsiya qilishga urinishlar;

– hisob qaydnomasidagi o‘zgartirishlar (masalan, qayd yozuvini yaratish va yo‘q qilish, qayd yozuvi imtiyozlarini tayinlash);

– dastur imtiyozlaridan foydalanish.

ilova amallari:

– dasturni ishga tushirish va o‘chirish;
– dastur xatolari;
– dastur konfigurasiyasidagi asosiy o‘zgarishlar.

Har bir hodisa uchun qaydlangan tafsilotlar farqlanadi, ularni quyidagi parametrlar bo‘yicha qaydlash tavsiya qilinadi:

– vaqt belgisi;
– hodisa, holat va / yoki xatolik kodlari;
– servic / buyruq / ilova nomi;
– foydalanuvchi yoki tizim bilan bog‘liq voqea;
– amaldagi qurilma (masalan, IP va manba manzili, terminal sessiyasi identifikatori, web brauzer va h.).

Audit jurnallarida barcha harakatlar qaydlangani bois, niyatibuzuqlar ularni tahrirlash orqali o‘z faoliyatini yashirishi mumkin. Shuning uchun, audit jurnalidan foydalanishlarni nazoratlash muhim vazifa hisoblanadi.

Windows OTda hodisa turlari. Windows OTda besh turdagi hodisa ro‘yxatga olinadi. Bularning barchasi uchun aniq belgilangan ma’lumotlar mavjud bo‘lib, biror bir hodisa haqidagi xabar faqat bitta turga tegishli bo‘ladi (6.2-jadval).

6.2-jadval

Windows OT hodisalari turlari

Hodisa	**Tavsifi**
1	**2**
Xatolik	Ma’lumotlarni yoki funksionallikni yo‘qotish kabi muhim muammoni ko‘rsatadigan hodisa. Masalan, biror xizmat ishga tushirishi paytida yuklanmasa, mazkur xatolik hodisasi qayd etiladi.
Ogohlantirish	Hodisa juda ahamiyatli bo‘lmasada, kelajakda yuzaga kelishi mumkin bo‘lgan muammolarni ko‘rsatishi mumkin. Masalan, diskda bo‘sh joy kam bo‘lsa, ogohlantirish hodisasi qayd etiladi.
Axborot	Ilova, drayver yoki xizmatning muvaffaqiyatli ishlashini tavsiflaydigan hodisa. Masalan, tarmoq drayveri muvaffaqiyatli yuklanganida, hodisalarni axborot qaydlaydi.

1	2
Muvaffaqiyatli audit	Muvaffaqiyatli tekshirilgan xavfsizlikka oid kirish urinishlarini yozib boradigan hodisa. Masalan, foydalanuvchining tizimga kirishga muvaffaqiyatli urinishi muvaffaqiyatli audit hodisasi sifatida qaydlanadi.
Muvaffaqiyatsiz audit	Tekshirilgan xavfsizlikdan foydalanishga urinish muvaffaqiyatsiz tugaganida, bu hodisa qaydlanadi. Masalan, agar foydalanuvchi tarmoq drayveriga kirishida muvaffaqiyatsizlikka uchrasa, bu hodisa qaydlanadi.

Quyidagi hodisalar qaydlanishi shart:

Resurs muammolari. Xotirani ajratishda xatolik yuz bergan taqdirda ogohlantirish hodisasini qaydlash kam xotirali vaziyatning sababini ko‘rsatishga yordam beradi.

Uskuna bilan bog‘liq muammolar. Tarmoq kartasi, qattiq disk, tezkor xotira va boshqa qurilma drayveri bilan bog‘liq hodisalar qaydlanishi shart.

Axborot hodisalari. Server dasturi (masalan, ma’lumotlar bazasi serveri) foydalanuvchining ro‘yxatdan o‘tkazilishi, ma’lumotlar bazasidagi amallar va boshqa hodisalar qaydlanishi shart.

Hodisalarni qaydlash jurnali ustida quyidagi amallar bajarilishi mumkin:

- zaxira nusxalash (BackupEventLog funksiyasi yordamida);
- tozalash (ClearEventLog funksiyasi yordamida);
- monitoringlash (NotifyChangeEventLog funksiyasi yordamida);
- so‘rov yuborish (boshqa dasturlar tomonidan, GetOldestEventLogRecord, GetNumberOfEventLogRecords funksiyalari yordamida);
- o‘qish (ReadEventLog funksiyasi yordamida);
- yozish (ReportEvent funksiyasi yordamida).

Windows XP/2000 operatsion tizimlarda hodisalarni qaydlash jurnalida turli qayd yozuvlari uchun berilgan imtiyozlar mavjud (6.3-jadval).

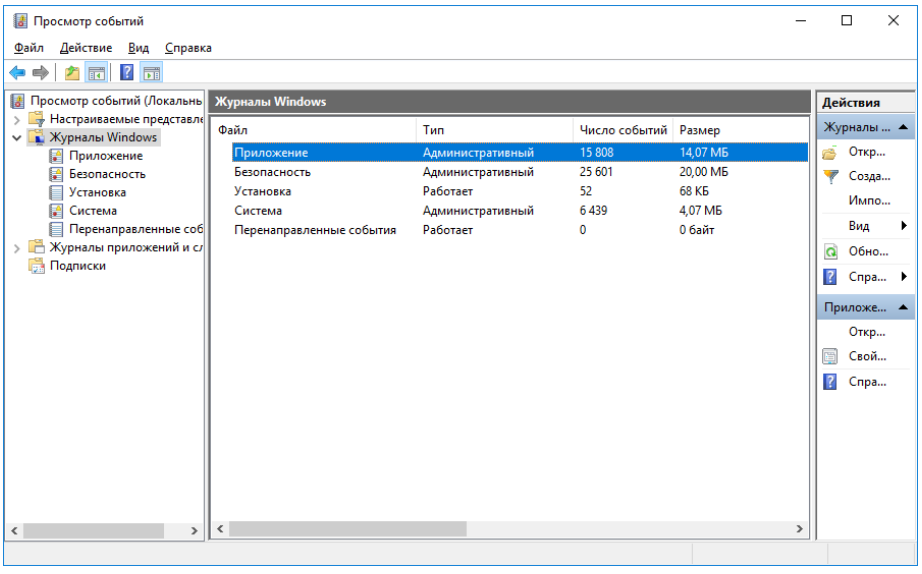
6.3-jadval

Windows XP/2000 operatsion tizimda hodisa jurnalida mavjud imtiyozlar

Log	Qayd yozuvi	O‘qish	Yozish	Tozalash
Ilovaga tegishli	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-
Tizimga tegishli	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	-	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	-	-
Tanlovga ko‘ra yaratilgan log fayl	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-

Windows OT da hodisalarni qaydlash fayllarini (log faylni) ko‘rish uchun quyidagi ketma-ketlik amalga oshiriladi:

1. Kompyuterda Win+R tugmalar kombinatsiyasi bosiladi.
2. Hosil bo‘lgan oynadagi maydonda *eventvwr* kiritiladi va Enter tugmasi bosiladi.
3. Hosil bo‘lgan hodisalarni ko‘rish oynasidan *Windows Logs* bandi tanlanadi (6.2-rasm).



6.2-rasm. Windows OTning hodisalar jurnali oynasi

Nazorat savollari

1. Foydalanuvchanlik tushunchasi va uning tizim uchun muhimligi.
2. Zaxira nusxalash va uning turlari.
3. Ma’lumotlarni yo‘qolishiga olib keluvchi asosiy sabablar.
4. Zaxira nusxalashda bajariluvchi vazifalar ketma-ketligi.
5. Zaxira nusxalarni saqlovchi vositalar va ularning xususiyatlari.
6. RAID texnologiyasi va uning asosiy xususiyatlari.
7. Zaxiralash turlari va ularning afzalliklari va kamchiliklari.

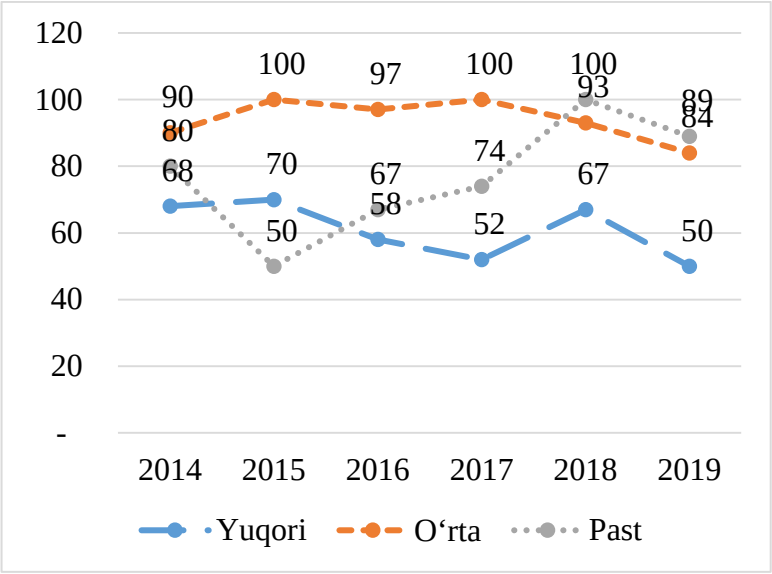
7 BOB. DASTURIY VOSITALAR XAVFSIZLIGI

7.1. Dasturiy vositalardagi xavfsizlik muammolari

Hozirda dasturiy vositalar xavfsizligi axborot xavfsizligining kriptografiya, foydalanishni nazoratlash va xavfsizlik protokollari kabi muhim sohalardan hisoblanadi. Bunga sabab - axborotning virtual xavfsizligi dasturiy vositalar orqali amalga oshirilishi. Dasturiy vosita tahdidga uchragan taqdirda xavfsizlik mexanizmi ham ishdan chiqadi.

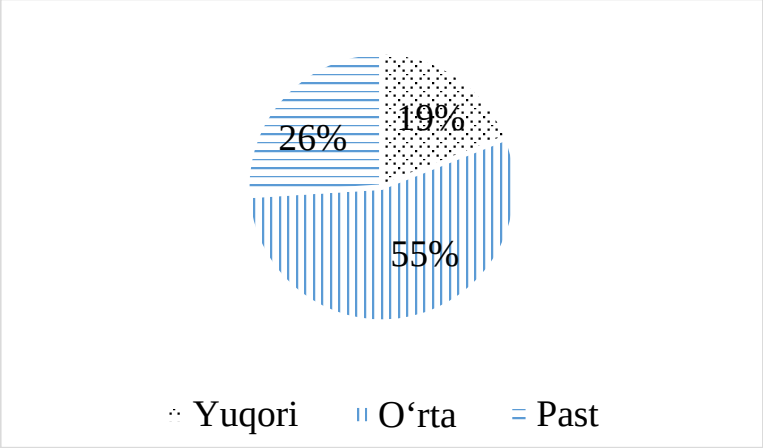
Barcha dasturiy vositalarda zaifliklar mavjud, ularning muhimlik darajalari turlicha. Masalan, narxi 165 mln. $ ni tashkil etgan NASA Mars Lander Mars sayyorasi yuzasiga qo‘nish vaqtida halokatga uchragan. Bunga sabab, oddiy ingliz va xalqaro metr uzunlik o‘lchovlari orasidagi farq bo‘lgan. Bundan tashqari, Denver xalqaro aeroportidagi yuklarni boshqarish tizimida foydalanilgan dasturiy vositadagi kamchilik natijasida 11 oy davomida kuniga 1 mln. $ dan zarar ko‘rilgan.

So‘nggi yillarda ushbu zaiflik muammolarining soni va jiddiylik darajasi ortib bormoqda. Xususan, 7.1-rasmda Positive Technologies tashkiloti tomonidan veb-saytlardagi turli darajadagi zaifliklarni yillar bo‘yicha ortib borishi keltirilgan.



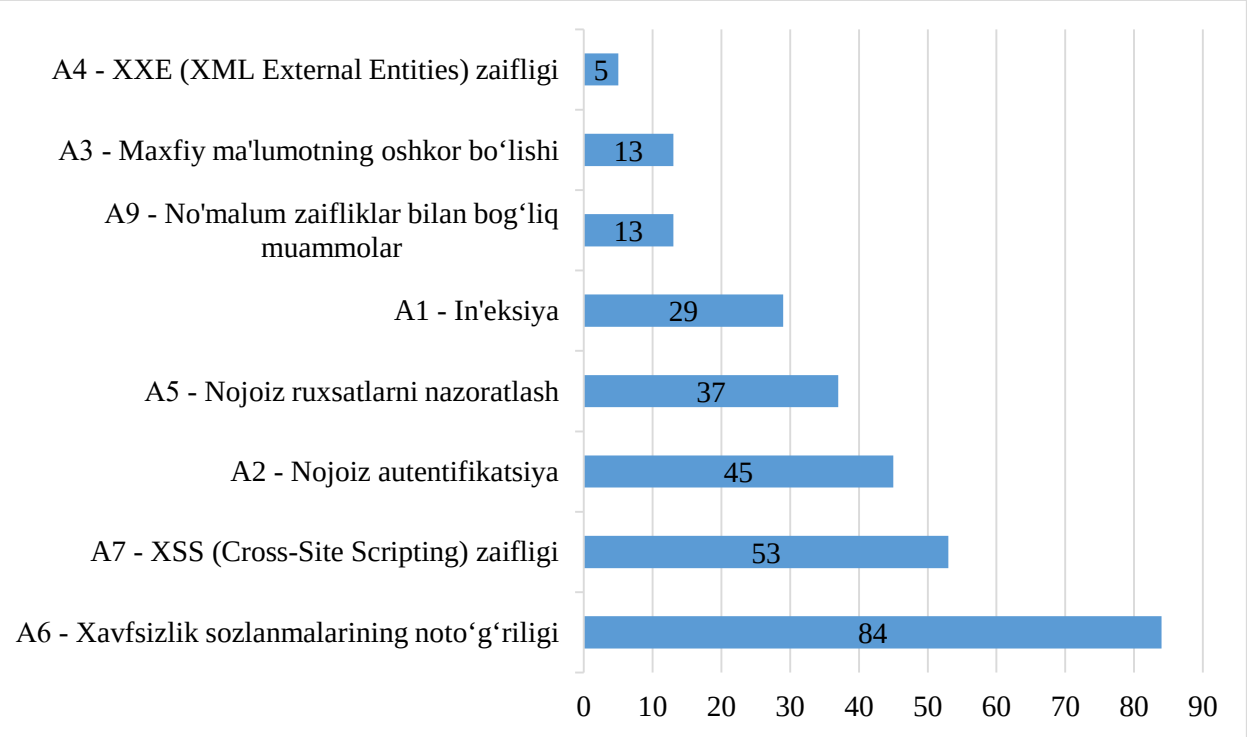
7.1 – rasm. Turli darajadagi zaifliklarga ega Web-saytlar soni

2019 yilda aniqlangan web-saytlardagi muammolarning jiddiyligi bo‘yicha taqsimoti 7.2-rasmda keltirilgan.



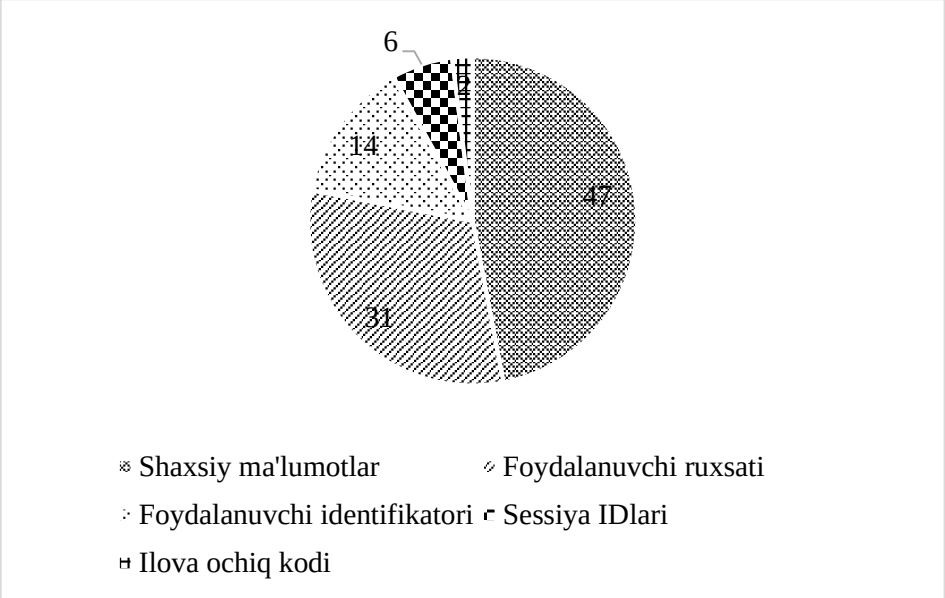
7.2-rasm. Web-sayt muammolarining jiddiyligi bo‘yicha taqsimoti

2019 yilda veb-saytlarda keng tarqalgan zaifliklar va ularning ulushi, OWASP (Open Web Application Security Project) tomonidan berilgan ma’lumotga ko‘ra, quyidagicha bo‘lgan (7.3-rasm).



7.3-rasm. OWASP tashkiloti 2019 yilda uchragan zaifliklar va ularning ulushi

Yuqorida keltirilgan zaifliklar natijasida turli ma’lumotlarni hujumchilar tomonidan qo‘lga kiritish maqsad qilingan (7.4-rasm).



7.4-rasm. Zaifliklar natijasida qo‘lga kiritishga mo‘ljallangan ma’lumotlar

Dasturiy vositalardagi mavjud tahdidlar, odatda, dasturlash tillari imkoniyatlari bilan belgilanadi. Masalan, nisbatan quyi dasturlash tillari dasturchidan yuqori malakani talab etgani bois, ularda ko‘plab xavfsizlik muammolari paydo bo‘ladi. C# va Java dasturlash tillarida ko‘plab muammolar avtomatik tarzda kompilyasiya jarayonida aniqlanganligi sababli, C yoki C++ dasturlash tillariga nisbatan, xavfsiz hisoblanadi.

Odatda zararli dasturiy vositalar ikki turga bo‘linadi:

– dasturlardagi zaifliklar (atayin yaratilmagan);
– zararkunanda dasturlar (atayin yaratilgan).

Birinchi turga, dasturchi tomonidan yo‘l qo‘yilgan xatolik natijasidagi dasturlardagi muammolar misol bo‘lsa, ikkinchi turga buzg‘unchilik maqsadida yozilgan maxsus dasturiy mahsulotlar (masalan, viruslar) misol bo‘la oladi.

Dasturiy vositalarda xavfsizlik muammolarining mavjudligi quyidagi omillar orqali belgilanadi:

– dasturiy vositalarning ko‘plab dasturchilar tomonidan yozilishi (komplekslilik);
– dasturiy mahsulotlar yaratilishida inson ishtiroki;
– dasturchining malakasi yuqori emasligi;
– dasturlash tillarining xavfsiz emasligi.

Dasturiy vositalarning bir necha million qator kodlardan iborat bo‘lishi xavfsizlik muammosini ortishiga sababchi bo‘ladi (7.1-jadval). Boshqacha aytganda, katta hajmli dasturiy vositalar ko‘plab dasturchilar tomonidan yoziladi va yakunida biriktiriladi. Dasturchilar orasidan

bittasining bilim darajasi yetarli bo‘lmasligi, butun dasturiy vositaning xavfsizligini yo‘qqa chiqarishi mumkin.

7.1 – jadval

Turli OTlar kodlarining uzunligi

Tizim	**Dasturdagi kod uzunligi**
Netscape	17 mln.
Space Shuttle	10 mln.
Linuxkernel 2.6.0	5 mln.
Windows XP	40 mln.
Mac OS X 10.4	86 mln.
Boeing 777	7 mln.

Tahlillar natijasi har 10 000 ta qator kodda 5 ta bag mavjudligini ko‘rsatadi. Boshqacha aytganda, o‘rtacha 3kbayt .exe faylda 50 tacha bag bo‘ladi.

Dasturiy vositalar injineriyasida dasturning o‘z vazifasini kafolatli bajarishiga harakat qilinsa, *xavfsiz* dasturiy vositalar injineriyasida esa o‘z vazifasini xavfsiz bajarishi talab etiladi. Biroq, amalda butunlay xavfsiz dasturiy vositaning bo‘lishi mumkin emas.

Dasturiy mahsulotlarda zaiflikka tegishli quyidagi tushunchalar mavjud.

Nuqson. Dasturni amalga oshirishdagi va loyihalashdagi zaifliklarning barchasi nuqson hisoblanadi va uning dasturiy vositalarda mavjudligi yillar davomida bilinmasligi mumkin.

Bag. Baglar dasturiy ta’minotni amalga oshirish bosqichiga tegishli muammo bo‘lib, ularni osongina aniqlash mumkin. Misol sifatida dasturlashdagi *buferning to‘lib-toshishi* (Buffer overflow) holatini keltirish mumkin.

Xotiraning to‘lib-toshishi. Amalda ko‘p uchraydigan dasturlash tillaridagi kamchiliklar, odatda, taqiqlangan formatdagi yoki hajmdagi ma’lumotlarning kiritilishi natijasida kelib chiqadi. Bu turdagi tahdidlar ichida keng tarqalgani – xotiraning to‘lib-toshishi tahdidi.

Masalan, foydalanuvchidan web-saytga ma’lumotlar kiritilishi talab etilsa (ismi, familiyasi, yili va h.), foydalanuvchi tomonidan kiritilgan “ism” maydonidagi ma’lumot serverdagi N ta belgi hajmiga ega sohaga yoziladi. Agar kiritilgan ma’lumot uzunligi N dan katta bo‘lsa, xotiraning to‘lib-toshishi hodisasi sodir bo‘ladi.

Agar buzg‘unchi tomonidan o‘ziga “kerakli” ma’lumot kiritilsa, bu o‘z navbatida kompyuterning buzilishiga olib keladi.

Quyida C dasturlash tilida yozilgan kod keltirilgan, agar bu kod kompilyasiya qilinsa, xotiraning to‘lib-toshishi hodisasi sodir bo‘ladi.

```
int main()
  {
  int buffer [10];
  buffer [20] =37;
  }
```

Bu yerda mavjud muammo - 10 bayt o‘lchamli xotiraga 20 baytli ma’lumot yozilishi. Bu esa xotiraning ruxsat etilmagan manziliga ham murojaatga sabab bo‘ladi.

7.2. Dasturiy vosita xavfsizligining fundamental prinsiplari

Dasturiy ta’minot yaratilganida va foydalanilganida qator prinsiplarga amal qilish talab qilinadi. Quyida OWASP tashkiloti tomonidan taqdim etilgan prinsiplar keltirilgan:

Hujumga uchrashi mumkin bo‘lgan soha maydonini minimallashtirish. Dasturiy ta’minotga qo‘shilgan har bir xususiyat dasturga ma’lum miqdordagi xavf darajasini ham qo‘shadi. Dasturni xavfsiz amalga oshirishning maqsadi – hujumga uchrashi mumkin bo‘lgan sohani toraytirish orqali umumiy dasturdagi xavfni kamaytirish. Masalan, web saytlarda onlayn yordamini amalga oshirish uchun qidirish funksiyasi mavjud. Biroq, ushbu imkoniyat web saytga SQL – inyeksiya hujumi bo‘lishi ehtimolini keltirib chiqarishi mumkin. Qidiruv imkoniyati autentifikatsiyadan o‘tgan foydalanuvchilar uchun bo‘lsa, hujum bo‘lishi ehtimoli kamayadi. Agar qidiruv ma’lumotlari markazlashgan tarzda tekshirilsa, ushbu hujum ehtimoli yanada kamayadi.

Xavfsiz standart sozlanmalarini o‘rnatish. Amalda, aksariyat dasturiy ta’minotlarda va operatsion tizimlarda ko‘plab xavfsizlik sozlanmalari standart tartibda o‘rnatilgan bo‘ladi. Biroq, bu foydalanuvchilar tomonidan yaxshi qabul qilinmaydi va shuning uchun, aksariyat hollarda, ushbu sozlanmalarni o‘chirib qo‘yish amalga oshiriladi. Masalan, operatsion tizimlarda parollarni eskirish vaqti standart holda o‘rnatilgan bo‘lsada, aksariyat foydalanuvchilar tomonidan ushbu sozlanma o‘chirib qo‘yiladi.

Minimal imtiyozlar prinsipi. Axborot xavfsizligi, informatika, dasturlash va boshqa sohalarda keng qo‘llaniluvchi minimal imtiyozlar prinsipi (Principle of least privilege) – hisoblash muhitidagi u yoki bu abstraksiya darajasida resurslarga murojaatni tashkil qilish. Bunga ko‘ra har bir modul o‘z vazifasini to‘laqonli bajarishi uchun zarur bo‘lgan resurs yoki axborotdan minimal darajada foydalanish talab etiladi.

Bu prinsip foydalanuvchi yoki dasturchiga faqat o‘z vazifasi uchun zarur bo‘lgan imtiyozlarga ega bo‘lishi kerakligini anglatadi. Masalan, vaqt o‘tkazish uchun ishlab chiqilgan turli mobil o‘yin dasturlari SMS xabarni o‘qish yoki qo‘ng‘iroq qiluvchilar ro‘yxatini bilish imkoniyatiga ega bo‘lishi shart emas. Masalan, dasturlash tillarida (Java dasturlash tilida keltirilgan) obyektlardan foydanishni cheklash uchun turli kalit so‘zlardan foydalaniladi (7.2-jadval).

7.2-jadval

Java dasturlash tilidagi foydalanuvchi imtiyozlari

Imtiyoz / Xususiyat	**Default**	**Private**	**Protected**	**Public**
Bir xil klass	+	+	+	+
Bir paket qismklassi	+	-	+	+
Bir paket qismklassi bo‘lmagan	+	-	+	+
Turli paket qismklasslari	-	-	+	+
Turli paket qismklassi bo‘lmagan	-	-	-	+

Teran himoya prinsipi. Ushbu prinsipga binoan, bitta nazoratning bo‘lishi yaxshi, ko‘plab nazoratlardan foydalanish esa yaxshiroq deb qaraladi. Teran himoyada foydalanilgan nazoratlar turli zaiflik orqali bo‘lishi mumkin bo‘lgan tahdidlarni oldini oladi. Xavfsiz dastur yozish orqali esa, foydalanish qiymatini tekshirish, markazlashgan auditni boshqarish va foydaluvchilarning barcha sahifalardan foydalanishlari ta’minlanishi mumkin.

Agar to‘g‘ri ishlab chiqilgan ma’mur interfeysi, tarmoqdan foydalanish qoidalarini to‘g‘ri bajarsa, foydalanuvchilarning avtorizatsiyasini tekshirsa va barcha holatlarni qaydlasa, u anonim hujumga bardoshsiz bo‘lishi mumkin emas.

Xavfsizlikning buzilishi. Ilovalar, amalga oshirilishi jarayonida turli sabablarga ko‘ra, buzilishlarga uchraydi. Masalan, quyida e’tiborsizlik oqibatida qoldirilgan xavfsizlik holati keltirilgan.

```
isAdmin = true;
try {
  codeWhichMayFail();
  isAdmin = isUserInRole( “Administrator” );
}
catch (Exception ex) {
  log.write(ex.toString());
}
```

Mazkur holda `codeWhichMayFail()` yoki `isUserInRole()` funksiyalarida xatolik bo‘lsa yoki biror `Exception` kuzatilgan taqdirda ham foydalanuvchi ma’mur rolida qolaveradi. Bu ko‘rinib turgan xavfsizlik riski hisoblanadi.

Xizmatlarga ishonmaslik. Hozirgi kunda ko‘plab tashkilotlar uchinchi tomon, sheriklarining hisoblash imkoniyatidan foydalanadi. Masalan, bir tashkilot o‘z ma’lumotlarini o‘z sherigiga tegishli dasturiy ta’minot bilan ishlashi mumkin. Bu holda ularga ishonish kafolatlanmaydi. Masalan, Payme yoki shunga o‘xshash ilovalar bir necha bank kartalaridagi ma’lumotlarni taqdim qiladi. Mazkur holda, har bir bank foydalanuvchi tomonida o‘z ma’lumotlarining to‘g‘ri akslantirilganini tekshirishi lozim.

Vazifalarni ajratish. Firibgarlikni oldini olishga qaratilgan asosiy chora – vazifalarni ajratish. Masalan, tashkilotda kompyuter olish bo‘yicha talab yuborgan odam tomonidan uni qabul qilinmasligi shart. Sababi, bu holda u ko‘plab kompyuterlarni so‘rashi va qabul qilib olganini rad qilishi mumkin. Ba’zi holda, bir rol uchun oddiy foydalanuvchilarga nisbatan ishonch darajasi turlicha bo‘ladi. Masalan, ma’murlar tizimni o‘chirishi yoki yoqishi, parollar siyosatini o‘rnata olishi kerak. Biroq, ular onlayn savdo do‘koniga imtiyozga ega foydalanuvchi sifatida kira olmasligi, xususan, tovarlarni boshqalar nomidan sotib olish imkoniyatiga ega bo‘lmasligi kerak.

Xavfsizlikni noaniqlikdan saqlash. Noaniqlikka asoslangan xavfsiz – zaif xavfsizlik bo‘lib, birinchi nazoratning o‘zida xatolikka uchraydi. Bu biror sirni saqlash yomon g‘oya ekanligini anglatmasada, xavfsizlikning muhim jihatlari tafsilotlarining yashirin bo‘lishiga asoslanmasligini bildiradi.

Masalan, dastur xavfsizligi uning ochiq kodidan xabardor bo‘linganida barbod bo‘lmasligi kerak. Xavfsizlik ko‘plab boshqa omillarga, masalan, parolning oqilona siyosatiga, tarmoq arxitekturasiga, auditni boshqarish vositalariga tayanishi lozim.

Bunga amaliy misol sifatida, Linux operatsion tizimini keltirish mumkin. Ushbu operatsion tizimning kodi ochiq hisoblansada, to‘g‘ri himoyalangan va shuning uchun, hozirgi kundagi mustahkam operatsion tizimlardan biri hisoblanadi.

Xavfsizlikni soddaligi. Hujumga uchrash soha maydoni va soddalik bir-biriga bog‘liq. Ba’zi dasturiy ta’minot muhandislari kodning sodda ko‘rinishidan ko‘ra murakkabligini afzal ko‘radilar. Biroq, sodda va tushunishga oson ko‘rinish tezkor bo‘lishi mumkin. Shuning uchun, dasturiy ta’minotni yaratish jarayonida murakkablikdan qochishga harakat qilish zarur.

Dasturiy mahsulotlarga qo‘yilgan xavfsizlik talablari. Dasturiy ta’minotni ishlab chiqishda unga ko‘plab talablar qo‘yiladi.

Dasturiy mahsulotlarga qo‘yiladigan talablar uch turga bo‘linadi:

- vazifaviy talablar:
    - tizim amalga oshirilishida kerak bo‘lgan vazifalar.
- novazifaviy talablar:
    - tizimning xususiyatlariga qo‘yilgan talablar.

Vazifaviy talablar. Bu talablar quyidagilarni o‘z ichiga oladi:

- tizim kutgan kirishga qo‘yilgan talablar;
- tizimdan chiqqan natijaga qo‘yilgan talablar;
- kirish va chiqishga aloqador bo‘lgan talablar.

Novazifaviy talablar. Novazifaviy talablarga quyidagilar taalluqli:

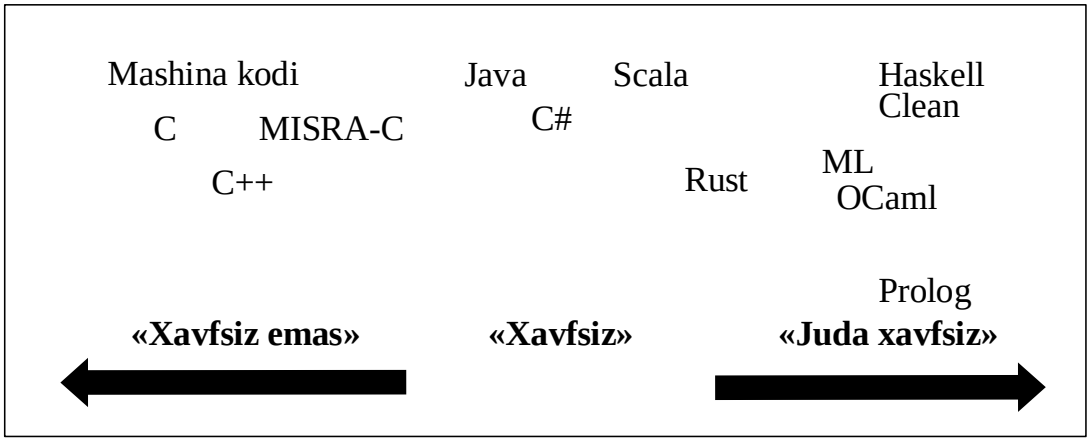
- audit qilish imkoniyati;
- kengaytirish mumkinligi;
- foydalanishga qulayligi;
- bajarilishi;
- ixchamligi;
- ishonchliligi;
- xavfsizligi;
- testlash imkoniyati;

- foydalanuvchanligi va h.

Xususiy xavfsizlik talablariga quyidagilar taalluqli:

– maxfiylik talabiga misol:
  - tizim ruxsat berilgan foydalanuvchigagina .doc fayllarni ko‘rsatishi kerak;
  - xavfsiz aloqa kanalidan foydalanish.
– ruxsatlarni nazoratlash talabiga misol:
  - tizim paroldan foydalanishni talab etishi kerak;
  - rollarga asoslangan foydalanishga ruxsatlarni nazoratlash amalga oshirilishi kerak.
– butunlik talabiga misol:
  - ochiq (public) turdagi foydalanuvchilar uchun faqat o‘qish, maxfiy (private) turidagi foydalanuvchilar uchun ham o‘qish ham yozish huquqi berilishi.
– foydalanuvchanlik talabiga misol:
  - barcha qayd yozuvlarda parol bo‘lishi shart;
  - 3 ta muvaffaqqiyatsiz urinishdan so‘ng qayd yozuvi blokirovkalanishi shart;
  - qayd yozuviga 5 min davomida tahdid amalga oshirilmasa u blokirovkadan yechilishi shart.

Dasturlash tiliga asoslangan xavfsizlik. Turli dasturlash tillari o‘ziga xos imkoniyatlarga ega, dasturlash sathida xavfsizlikni ta’minlash muhim ahamiyat kasb etadi. Mavjud dasturlash tillarini xavfsiz yoki xavfsiz emas turlariga ajratish nisbiy tushuncha bo‘lib, ularni quyidagicha tasvirlash mumkin (7.5-rasm).



7.5 – rasm. Dasturlash tillarining xavfsizlik darajasining sodda ko‘rinishi

7.3. Kompyuter viruslari va virusdan himoyalanish muammolari

Kompyuter virusining ko‘p ta’riflari mavjud. Birinchi ta’rifni 1984 yili Fred Koen bergan: “Kompyuter virusi – boshqa dasturlarni, ularga o‘zini yoki o‘zgartirilgan nusxasini kiritish orqali, ularni modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko‘payish qobiliyatini saqlaydi”. Virusning o‘z-o‘zidan ko‘payishi va hisoblash jarayonini modifikatsiyalash qobiliyati bu ta’rifdagi tayanch tushunchalar hisoblanadi. Kompyuter virusining ushbu xususiyatlari tirik tabiat organizmlarida biologik viruslarning parazitlanishiga o‘hshash.

Hozirda kompyuter virusi deganda quyidagi xususiyatlarga ega bo‘lgan dasturiy kod tushuniladi:

– asliga mos kelishi shart bo‘lmagan, ammo aslining xususiyatlariga (o‘z-o‘zini tiklash) ega bo‘lgan nusxalarni yaratish qobiliyati;

– hisoblash tizimining bajariluvchi obyektlariga yaratiluvchi nusxalarning kiritilishini ta’minlovchi mexanizmlarning mavjudligi.

Ta’kidlash lozimki, bu xususiyatlar zaruriy, ammo yetarli emas. Ko‘rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta’sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to‘ldirish lozim.

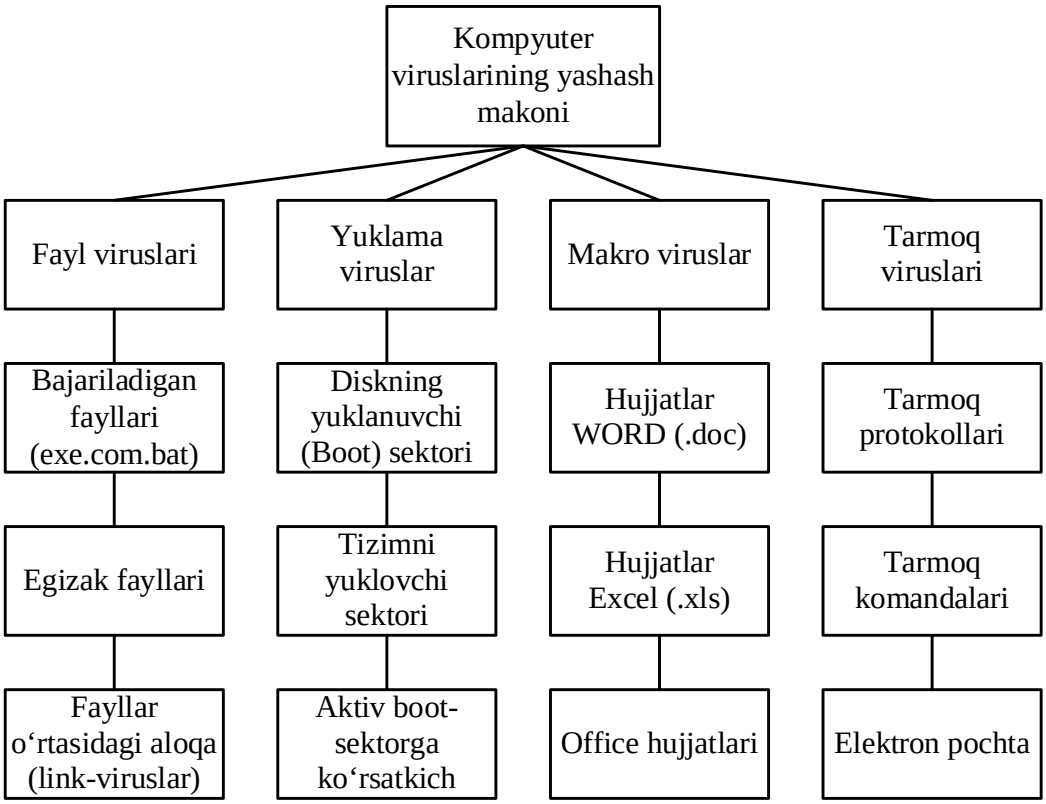
Viruslarni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

– yashash makoni;
– operatsion tizim;
– ishlash algoritmi xususiyati;
– destruktiv imkoniyatlari.

Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo‘yicha turkumlash keng tarqalgan (7.6-rasm).

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko‘p tarqalgan viruslar xili), yoki fayl-egizaklarni (kompanon viruslar) yaratadi yoki faylli tizimlarni (link-viruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o‘zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (MasterBootRecord) bo‘lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.



7.6-rasm. Yashash makoni bo‘yicha kompyuter viruslarining turkumlanishi

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan Microsoft Word, Microsoft Excel va h. kabi ommaviy muharrirlarning fayl-hujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba’zida tarmoq viruslarini “qurt” xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo‘yicha tarqaladi), IRC-qurtlarga (chatlar, InternetRelayChat) bo‘linadi.

Kompyuter viruslarining ko‘pgina kombinasiyalangan xillari ham mavjud, masalan – tarmoqli makrovirus tahrirlanuvchi hujjatlarni zaxarlaydi, hamda o‘zining nusxalarini elektron pochta orqali tarqatadi. Boshqa bir misol sifatida fayl-yuklama viruslarini ko‘rsatish mumkinki, ular fayllarni hamda disklarning yuklanadigan sektorini zaharlaydi.

*Viruslarning hayot davri.*Har qanday dasturdagidek kompyuter viruslari hayot davrining ikkita asosiy bosqichini - saqlanish va bajarilish bosqichlarini ajratish mumkin.

Saqlanish bosqichi virusning diskda u kiritilgan obyekt bilan birgalikda shundaygina saqlanish davriga to‘g‘ri keladi. Bu bosqichda

virus virusga qarshi dastur ta’minotiga zaif bo‘ladi, chunki u faol emas va himoyalanish uchun operatsion tizimni nazorat qila olmaydi.

Kompyuter viruslarining *bajarilish davri,* odatda, beshta bosqichni o‘z ichiga oladi:

1. Virusni xotiraga yuklash.
2. Qurbonni qidirish.
3. Topilgan qurbonni zaharlash.
4. Destruktiv funksiyalarni bajarish.
5. Boshqarishni virus dastur-eltuvchisiga o‘tkazish.

Virusni xotiraga yuklash. Virusni xotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi obyekt bilan bir vaqtda amalga oshiriladi. Masalan, agar foydalanuvchi virus bo‘lgan dasturiy faylni ishga tushirsa, ravshanki, virus kodi ushbu fayl qismi sifatida xotiraga yuklanadi. Oddiy holda, virusni yuklash jarayoni-diskdan operativ xotiraga nusxalash bo‘lib, so‘ngra boshqarish virus badani kodiga uzatiladi. Bu harakatlar operatsion tizim tomonidan bajariladi, virusning o‘zi passiv holatda bo‘ladi. Murakkabroq vazifalarda virus boshqarishni olganidan so‘ng o‘zining ishlashi uchun qo‘shimcha harakatlarni bajarishi mumkin. Bu bilan bog‘liq ikkita jihat ko‘riladi.

Birinchisi viruslarni aniqlash muolajasining maksimal murakkablashishi bilan bog‘liq. Saqlanish bosqichida ba’zi viruslar himoyalanishni ta’minlash maqsadida yetarlicha murakkab algoritmdan foydalanadi. Bunday murakkablashishga virus asosiy qismini shifrlashni kiritish mumkin. Ammo faqat shifrlashni ishlatish chala chora hisoblanadi, chunki yuklanish bosqichida rasshifrovkani ta’minlovchi virus qismi ochiq ko‘rinishda saqlanishi lozim. Bunday holatdan qutilish uchun viruslarni ishlab chiquvchilar rasshifrovka qiluvchi kodni “mutatsiyalash” mexanizmidan foydalanadi. Bu usulning mohiyati shundan iboratki, obyektga virus nusxasi kiritilishida uning rasshifrovka qilinishiga taalluqli qismi shunday modifikatsiyalanadiki, original bilan matnli farqlanish paydo bo‘ladi, ammo ish natijasi o‘zgarmaydi.

Kodni mutatsiyalash mexanizmidan foydalanuvchi viruslar *polimorf viruslar* nomini olgan. Polimorf viruslar (polymorphic)-qiyin aniqlanadigan viruslar bo‘lib, signaturalarga ega emas, ya’ni tarkibida birorta ham kodining doimiy qismi yo‘q. Polimorfizm faylli, yuklamali va makroviruslarda uchraydi.

Stels-algoritmlardan foydalanilganda viruslar o‘zlarini tizimda to‘la yoki qisman bekitishlari mumkin. stels-algoritmlaridan foydalanadigan viruslar – *stels-viruslar* (Stealth) deb yuritiladi. Stels viruslar operatsion

tizimning shikastlangan fayllarga murojaatini ushlab qolish yo‘li bilan o‘zini yashash makonidaligini yashiradi va operatsion tizimni axborotni shikastlanmagan qismiga yo‘naltiradi.

Ikkinchi jihat *rezident viruslar* deb ataluvchi viruslar bilan bog‘liq. Virus va u kiritilgan obyekt operatsion tizim uchun bir butun bo‘lganligi sababli, yuklanishdan so‘ng ular, tabiiy, yagona adres makonida joylashadi. Obyekt ishi tugaganidan so‘ng u operativ xotiradan bo‘shaladi. Bunda bir vaqtning o‘zida virus ham bo‘shalib saqlanishning passiv bosqichiga o‘tadi. Ammo ba’zi viruslar xili xotirada saqlanish va virus eltuvchi ishi tugashidan so‘ng faol qolish qobiliyatiga ega. Bunday viruslar rezident nomini olgan. Rezident viruslar, odatda, faqat operatsion tizimga ruxsat etilgan imtiyozli rejimlardan foydalanib yashash makonini zaharlaydi va ma’lum sharoitlarda zararkunandalik vazifasini bajaradi. Rezident viruslar xotirada joylashadi va kompyuter o‘chirilishigacha yoki operatsion tizim qayta yuklanishigacha faol holda bo‘ladi.

Rezident bo‘lmagan viruslar faqat faollashgan vaqtlarida xotiraga tushib zaharlash va zarakunandalik vazifalarini bajaradi. Keyin bu viruslar xotirani butunlay tark etib yashash makonida qoladi.

Ta’kidlash lozimki, viruslarni rezident va rezident bo‘lmaganlarga ajratish faqat fayl viruslariga taalluqli. Yuklanuchi va makroviruslar rezident viruslarga tegishli.

Qurbonni qidirish. Qurbonni qidirish usuli bo‘yicha viruslar ikkita sinfga bo‘linadi. Birinchi sinfga operatsion tizim funksiyalaridan foydalanib faol qidirishni amalga oshiruvchi viruslar kiradi. Ikkinchi sinfga qidirishning passiv mexanizmlarini amalga oshiruvchi, ya’ni dasturiy fayllarga tuzoq qo‘yuvchi viruslar taalluqli.

Topilgan qurbonni zaharlash. Oddiy holda zaharlash deganda qurbon sifatida tanlangan obyektda virus kodining o‘z-o‘zini nusxalashi tushuniladi.

Avval fayl viruslarining zaharlash xususiyatlarini ko‘raylik. Bunda ikkita sinf viruslari farqlanadi. Birinchi sinf viruslari o‘zining kodini dasturiy faylga bevosita kiritmaydi, balki fayl nomini o‘zgartirib, virus badani bo‘lgan yangi faylni yaratadi. Ikkinchi sinfga qurbon fayllariga bevosita kiruvchi viruslar taalluqli. Bu viruslar kiritilish joylari bilan xarakterlanadi. Quyidagi variantlar bo‘lishi mumkin:

1. Fayl boshiga kiritish. Ushbu usul MS-DOSning *com*-fayllari uchun eng qulay hisoblanadi, chunki ushbu formatda xizmatchi sarlavhalar ko‘zda tutilgan.

2. Fayl oxiriga kiritish. Bu usul eng ko‘p tarqalgan bo‘lib, viruslar

kodiga boshqarishni uzatish dasturning birinchi komandasi (*com*) yoki fayl sarlavhasini (*exe*) modifikatsiyalash orqali ta’minlanadi.

3. Fayl o‘rtasiga kiritish. Odatda bu usuldan viruslar strukturasi oldindan ma’lum fayllarga (masalan, *Command.com* fayli) yoki tarkibida bir xil qiymatli baytlar ketma-ketligi bo‘lgan, uzunligi virus joylashishiga yetarli fayllarga tatbiqan foydalaniladi.

Yuklama viruslar uchun zaharlash bosqichining xususiyatlari ular kiritiluvchi obyektlar – qayishqoq va qattiq disklarning yuklanish sektorlarining sifati va qattiq diskning bosh yuklama yozuvi (MBR) orqali aniqlanadi. Asosiy muammo-ushbu obyekt o‘lchamlarining chegaralanganligi. Shu sababli, viruslar o‘zlarining qurbon joyida sig‘magan qismini diskda saqlashi, hamda zaharlangan yuklovchi original kodini tashishi lozim.

Makroviruslar uchun zaharlash jarayoni tanlangan hujjat-qurbonda virus kodini saqlashdan iborat. Ba’zi axborotni ishlash dasturlari uchun buni amalga oshirish oson emas, chunki hujjat fayllari formatining makroprogrammalarni saqlashi ko‘zda tutilmagan bo‘lishi mumkin.

Destruktiv funksiyalarni bajarish. Destruktiv imkoniyatlari bo‘yicha beziyon, xavfsiz, xavfli va juda xavfli viruslar farqlanadi.

Beziyon viruslar - o‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi viruslar. Ular tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydi xolos.

Xavfsiz viruslar – tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq viruslar, bo‘sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydi.

Xavfli viruslar – kompyuter ishlashida jiddiy nuqsonlarga sabab bo‘luvchi viruslar. Natijada dastur va ma’lumotlar buzilishi mumkin.

Juda xavfli viruslar – dastur va ma’lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o‘chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar.

Boshqarishni virus dastur – eltuvchisiga o‘tkazish. Ta’kidlash lozimki, viruslar buzuvchilar va buzmaydiganlarga bo‘linadi.

Buzuvchi viruslar dasturlar zaharlanganida ularning ishga layoqatligini saqlash xususida qayg‘urmaydilar, shu sababli ularga ushbu bosqichning ma’nosi yo‘q.

Buzmaydigan viruslar uchun ushbu bosqich xotirada dasturni korrekt ishlanishi shart bo‘lgan ko‘rinishda tiklash va boshqarishni virus dastur-eltuvchisiga o‘tqazish bilan bog‘liq.

Zarar keltiruvchi dasturlarning boshqa xillari. Viruslardan tashqari zarar keltiruvchi dasturlarning quyidagi xillari mavjud:

– troyan dasturlari;

– mantiqiy bombalar;

– masofadagi kompyuterlarni yashirincha ma’murlovchi xaker utilitalari;

– Internetdan va boshqa konfidensial axborotdan foydalanish parollarini o‘g‘rilovchi dasturlar.

Ular orasida aniq chegara yo‘q: troyan dasturlari tarkibida viruslar bo‘lishi, viruslarga mantiqiy bombalar joylashtirilishi mumkin va h.

Troyan dasturlar o‘zlari ko‘paymaydi va tarqatilmaydi. Tashqaridan troyan dasturlar mutlaqo beozor ko‘rinadi, hatto foydali funksiyalarni tavsiya etadi. ammo foydalanuvchi bunday dasturni kompyuteriga yuklab, ishga tushirsa, dastur bildirmay zarar keltiruvchi funksiyalarni bajarishi mumkin. Ko‘pincha troyan dasturlar viruslarni dastlabki tarqatishda, Internet orqali masofadagi kompyuterdan foydalanishda, ma’lumotlarni o‘g‘rilashda yoki ularni yo‘q qilishda ishlatiladi.

Mantiqiy bomba – ma’lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari. Mantiqiy bomba, masalan, ma’lum sana kelganida yoki ma’lumotlar bazasida yozuv paydo bo‘lganida yoki yo‘q bo‘lganida va h. ishga tushishi mumkin. Bunday bomba viruslarga, troyan dasturlarga va oddiy dasturlarga joylashtirilishi mumkin.

Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari. Kompyuterlar va korporativ tarmoqlarni himoyalovchi samarador tizimni yaratish uchun qayerdan xavf tug‘ilishini aniq tasavvur etish lozim. Viruslar tarqalishning juda xilma-xil kanallarini topadi. Buning ustiga eski usullarga yangisi qo‘shiladi.

Tarqatishning klassik (mumtoz) usullari. Fayl viruslari dastur fayllari bilan birgalikda disketlar va dasturlar almashishda, tarmoq kataloglaridan, Web- yoki FTP – serverlardan dasturlar yuklanishida tarqatiladi. Yuklama viruslar kompyuterga foydalanuvchi zaharlangan disketani diskovodda qoldirib, so‘ngra operatsion tizimni qayta yuklashida tushib qoladi. Yuklama virus kompyuterga viruslarning boshqa xili orqali kiritilishi mumkin. Makrokomanda viruslari Microsoft Word, Excel, Access fayllari kabi ofis hujjatlarining zaxarlangan fayllari almashinishida tarqaladi.

Agar zaharlangan kompyuter lokal tarmoqqa ulangan bo‘lsa virus

osongina fayl-server disklariga tushib qolishi, u yerdan kataloglar orqali tarmoqning barcha kompyuterlariga o‘tishi mumkin. Shu tariqa virus epidemiyasi boshlanadi. Virus tarmoqda shu virus tushib qolgan kompyuter foydalanuvchisi xuquqlari kabi xuquqqa ega ekanligini tizim ma’muri unutmasligi lozim. Shuning uchun u foydalanuvchi foydalanadigan barcha kataloglarga tushib qolishi mumkin. Agar virus tarmoq ma’muri ishchi stansiyasiga tushib qolsa oqibati juda og‘ir bo‘lishi mumkin.

Elektron pochta. Hozirda Internet global tarmog‘i viruslarning asosiy manbai hisoblanadi. Viruslar bilan zaharlanishlarning aksariyati MicroSoftWord formatida xatlar almashishda sodir bo‘ladi. Elektron pochta makroviruslarni tarqatish kanali vazifasini o‘taydi, chunki axborot bilan bir qatorda ko‘pincha ofis hujjatlari jo‘natiladi.

Viruslar bilan zaharlash bilmasdan va yomon niyatda amalga oshirilishi mumkin. Masalan, makrovirus bilan zaharlangan muharrirdan foydalanuvchi o‘zi shubha qilmagan holda, adresatlarga zaharlangan xatlarni jo‘natishi mumkin. Ikkinchi tarafdan niyatibuzuq atayin elektron pochta orqali harqanday xavfli dasturiy kodni jo‘natishi mumkin.

Troyan Web-saytlar. Foydalanuvchilar virusni yoki troyan dasturni Internet saytlarining oddiy kuzatishda, troyan Web-saytni ko‘rganida olishi mumkin. Foydalanuvchi brauzerlaridagi xatoliklar ko‘pincha troyan Web-saytlari faol komponentlarining foydalanuvchi kompyuterlariga zarar keltiruvchi dasturlarni kiritishiga sabab bo‘ladi. Troyan saytni ko‘rishga taklifni foydalanuvchi oddiy elektron xat orqali olishi mumkin.

Lokal tarmoqlar. Lokal tarmoqlar ham tezlikda zaharlanish vositasi hisoblanadi. Agar himoyaning zaruriy choralari ko‘rilmasa, zaharlangan ishchi stansiya lokal tarmoqqa kirishda serverdagi bir yoki bir necha xizmatchi fayllarni zaharlaydi. Bunday fayllar sifatida Login.com xizmatchi faylni, firmada qo‘llaniluvchi Excel-jadvallar va standart hujjat-shablonlarni ko‘rsatish mumkin. Foydalanuvchilar bu tarmoqqa kirishida serverdan zaharlangan fayllarni ishga tushiradi, natijada virus foydalanuvchi kompyuteridan foydalana oladi.

Zarar keltiruvchi dasturlarni tarqatishning boshqa kanallari. Viruslarni tarqatish kanallaridan biri dasturiy ta’minotning qaroqchi nusxalari hisoblanadi. Disketlar va CD-disklardagi noqununiy nusxalarda ko‘pincha turli-tuman viruslar bilan zaharlangan fayllar bo‘ladi. Viruslarni tarqatish manbalariga elektron anjumanlar va FTP va BBS fayl-serverlar ham taalluqli.

O‘quv yurtlarida va Internet-markazlarida o‘rnatilgan va umumfoydalanish rejimida ishlovchi kompyuterlar ham osongina viruslarni tarqatish manbaiga aylanishi mumkin. Agar bunday kompyuterlardan biri navbatdagi foydalanuvchi disketidan zaharlangan bo‘lsa, shu kompyuterda ishlovchi boshqa foydalanuvchilar disketlari ham zaharlanadi.

Kompyuter texnologiyasining rivojlanishi bilan kompyuter viruslari ham, o‘zining yangi yashash makoniga moslashgan holda, takomillashadi. Har qanday onda yangi, oldin ma’lum bo‘lmagan yoki ma’lum bo‘lgan, ammo yangi kompyuter asbob-uskunasiga mo‘ljallangan kompyuter viruslari, troyan dasturlari va qurtlar paydo bo‘lishi mumkin. Yangi viruslar ma’lum bo‘lmagan yoki oldin mavjud bo‘lmagan tarqatish kanallaridan hamda kompyuter tizimlarga tatbiq etishning yangi texnologiyalaridan foydalanishi mumkin. Virusdan zaharlanish xavfini yo‘qotish uchun korporativ tarmoqning tizim ma’muri, nafaqat virusga qarshi usullardan foydalanishi, balki kompyuter viruslari dunyosini doimo kuzatib borishi shart.

Zararli dasturiy vositalarni aniqlash. Zararli dasturiy vositalarni aniqlashda asosan uchta yondashuvdan foydalaniladi. Birinchisi va eng keng tarqalgani *signaturaga asoslangan aniqlash* bo‘lib, zararli dasturdagi shablon yoki signaturani topishga asoslanadi. Ikkinchi yondashuv *o‘zgarishlarni aniqlashga* asoslangan bo‘lib, o‘zgarishga uchragan fayllarni aniqlaydi. O‘zgarishi kutilmagan fayl o‘zgarganida zararlangan deb topiladi. Uchinchi yondashuv *anomaliyaga asoslangan*, noodatiy yoki virusga o‘xshash fayllarni va holatlarni aniqlashga asoslanadi.

Signaturaga asoslangan aniqlash. Signatura bu – faylda topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. Biroq, bu usul kam moslashuvchanlik darajasiga ega bo‘lib, virus yozuvchilari tomonidan osongina chetlanib o‘tilishi mumkin.

Masalan, W32/Beast virusi (1999 yilda aniqlangan Microsoft Word hujjatini zararlashga qaratilgan virus) uchun 83EB 0274 EBOE 740A 81EB 0301 0000 signaturasi foydalanilgan. Bu holda tizimdagi barcha fayllar ichida ushbu signatura qidiriladi. Biroq, biror fayl ichida ushbu signatura aniqlangan vaqtda ham to‘liq virusni topdik deb aytish mumkin emas. Sababi, biror virus bo‘lmagan fayl tarkibida ham ushbu signatura bo‘lishi mumkin. Agar qidiriladigan fayllarda bitlar tasodifiy bo‘lsa, ushbu holatning bo‘lishi ehtimoli $1/2^{112}$ ga teng bo‘ladi. Biroq, kompyuter

dasturlari va ma’lumotlar ichidagi bitlar tasodifiylikdan yiroq va bu ehtimolni yanada ortishini anglatadi. Boshqacha aytganda, biror fayldan signatura aniqlangan taqdirda ham, uni qo‘shimcha tekshirish amalga oshirilishi zarur.

Signaturaga asoslangan aniqlash usuli virus aniq bo‘lganida va umumiy bo‘lgan signaturalar ajratilgan holatda juda yuqori samaradorlikka ega. Bundan tashqari, ushbu usulga binoan foydalanuvchi va ma’murga minimal yuklama yuklanadi va ularga faqat signaturalarni saqlash va uzluksiz yangilash vazifasi qo‘yiladi.

Biroq, signaturalar saqlangan faylning hajmi katta bo‘lib, 10 yoki 100 minglab signaturaga ega fayl yordamida skanerlash juda ko‘p vaqt oladi. Bundan tashqari, biror aniqlangan virusni kichik o‘zgartirish orqali ushbu usulni osonlik bilan aldab o‘tish mumkin.

Hozirgi kunda signaturaga asoslangan tanib olish usuli zamonaviy antivirus yoki zararli dasturlarga qarshi himoya vositalarida keng qo‘llaniladi.

O‘zgarishlarni aniqlovchi usul. Zararli dasturlar ma’lum manzilda joylashganligi sababli, tizimdagi biror joyda o‘zgarish aniqlansa, zararlangan joyini ko‘rsatish mumkin. Ya’ni, agar o‘zgarishga uchragan fayl aniqlansa, u virus orqali zararlangan bo‘lishi mumkin.

O‘zgarishlarni qanday aniqlash mumkin? Ushbu muammoni yechishda xesh-funksiyalar mos keladi. Faraz qilaylik, tizimdagi barcha fayllar xeshlanib, xesh qiymatlari xavfsiz manzilda saqlangan bo‘lsin. U holda vaqti-vaqti bilan ushbu faylning xesh qiymatlari qaytadan hisoblanadi va dastlabkilari bilan taqqoslanadi. Agar faylning bir yoki bir nechta bitlari o‘zgarishga uchragan bo‘lsa, xesh qiymatlar bir biriga mos kelmaydi va fayl virus tomonidan zararlangan hisoblanadi.

Ushbu usulning afzalliklaridan biri shuki, agar fayl zararlangan bo‘lsa, uni to‘liq aniqlash mumkin. Bundan tashqari, oldin noma’lum bo‘lgan zararli dasturni ham aniqlash mumkin.

Biroq, ushbu usul kamchiliklarga ham ega. Tizimdagi fayllar odatda tez-tez o‘zgarib turadi va natijada yolg‘ondan zararlangan deb topilgan holatlar soni ortadi. Agar virus tizimdagi tez-tez o‘zgaruvchi fayl ichiga joylashtirilgan bo‘lsa, ushbu usulni osonlik bilan aylanib o‘tish mumkin. Bu holda ushbu fayldagi o‘zgarishni log fayl orqali aniqlash ko‘p vaqt talab qiladi va bu signaturaga asoslangan usuldagi kabi muammolarga olib keladi.

Anomaliyaga asoslangan aniqlash. Anomaliyaga asoslangan usul noodatiy yoki virusga o‘xshash yoki bo‘lishi mumkin bo‘lgan zararli

harakatlarni yoki xususiyatlarni topishni maqsad qiladi. Ushbu g‘oya IDS tizimlarida ham foydalaniladi.

Ushbu usulning fundamental muammosi - qaysi holatni normal va qaysi holatni normal bo‘lmagan deb topish hamda ushbu ikki holat orasidagi farqni aniqlash hisoblanadi. Bundan tashqari, normal holatning o‘zgarishi va tizimning bu holatga moslashish muammosi ham mavjud. Bu esa ko‘plab noto‘g‘ri signallarni paydo bo‘lishiga sabab bo‘ladi. Ushbu usulning afzalligi sifatida oldin noma’lum bo‘lgan zararli dasturlarni aniqlash imkonini ko‘rsatish mumkin.

Antivirus dasturiy vositalarining kamchiligi. Antivirus dasturiy vositasiga kompyuterni himoyalashda amalga oshirilish lozim bo‘lgan zaruriy shart sifatida qaraladi. Umuman olganda, antivirus kompyuter uchun zararli dasturlarni skanerlashni, himoyalashni, karantin holatiga tushirishni va boshqa amallarni bajaradi. Antivirus dasturiy vositalarini CD-disklardan va Internet tarmog‘idan foydalangan holda o‘rnatish mumkin. Antivirus dasturiy vositalari bir biridan ko‘plab o‘ziga xos xususiyatlari bilan ajralib turadi. Masalan, Internet tarmog‘idan foydalanilganda reklamalarni blokirovkalash, Internet tarmog‘idan kirib keluvchi zararli dasturlarni blokirovkalash va h. Biroq, foydalanuvchilar to‘liq antivirus dasturiy vositalarining imkoniyatilariga ishonib qolmasliklari lozim.

Viruslarni doimiy aniqlash uchun antivirus dasturiy vositalari eng yangi va yangilangan ma’lumotlarni o‘z ichiga olgan namunaviy fayllarga muxtoj. Biroq, antivirus ishlab chiqaruvchilari yangi virus uchun namunaviy fayllar yaratgunlaricha virus ishlab chiqaruvchilari tomonidan katta hajmdagi yangi viruslar yaratiladi. Bu esa, yangi virus uchun vaksinani tayyorlash yetarlicha ko‘p vaqtni talab qiladi.

Bundan tashqari, antivirus dasturi Rootkit tipidagi zararli dasturlarni aniqlashda foydasi tegmasligi mumkin. Rootkit tipidagi zararli dasturlar kompyuter operatsion tizimining markaziga hujum qilishni maqsad qiladi.

Antivirus dasturiy vositalari sifatini baholash omillari. Antivirus dasturiy vositalari quyidagi omillarga ko‘ra baholanishi mumkin:

- *ishonchlik va foydalanishdagi qulaylik* – antivirus dasturiy vositasini “qotib qolishi” va foydalanish uchun turli tayyorganlikni talab etmasligi;
- barcha keng tarqalgan viruslarni sifatli aniqlash, hujjat fayllari/ jadvallari (MS Word, Excel), paketlangan, arxivlangan fayllarni skanerlash va zararlangan obyektlarni davolash qobiliyati;

- barcha mashhur platformalar uchun mavjudligi (DOS, Windows NT, Novell NetWare, OS/2, Alpha, Linux va boshq), talab bo‘yicha va tezkor skanerlash rejimlarining mavjudligi;
- ishlash tezligi va boshqa xususiyatlari.

Antivirus dasturiy komplekslari. Har bir antivirus dasturiy vositalar o‘ziga xos afzallik va kamchiliklarga ega. Faqat bir necha antivirus dasturiy vositalaridan kompleks foydalanish to‘liq himoyani ta’minlashi mumkin. Amalda ko‘plab antivirus dasturiy vositalar mavjud, ularga quyidagilarni misol sifatida keltirish mumkin (7.3-jadval).

7.3-jadval

Turli antivirus dasturlarining xususiyatlari

Mahsulot / Xususiyati	**McAfee AntiVirus Plus**	**Semantec Norton AntiVirus Plus**	**Kaspersky Anti-Virus**	**Bitdefender Antivirus Plus**	**Webroot SecureAnywhere Antivirus**	**Eset Nod32 Antivirus**	**Trend Micro Antivirus+ Security**	**F-secure Anti-Virus**	**VoodooSoft VoodooShield**	**The Kure**
Narxi	19.99$	19.99$	29.99$	29.99$	18.99$	27.99$	29.95$	39.99$	19.99$	19.99$
Talabga ko‘ra skanerlash	+	+	+	+	+	+	+	+	-	-
Doimiy skanerlash	+	+	+	+	+	+	+	+	+	-
Web saytni baholash	+	+	+	-	+	-	+	-	-	-
Zararli URL ni bloklash	+	+	+	+	+	+	+	+	-	-
Fishingdan himoyalash	+	+	+	+	+	+	+	-	-	-
Xususi-yatga ko‘ra aniqlash	+	+	+	+	+	+	+	+	+	-
Zaifliklarni skanerlash	+	-	+	+	-	-	-	-	-	-

Profilaktik choralar. Viruslar va virus yuqtirilgan fayllarni o‘z vaqtida aniqlash, aniqlangan viruslarni har bir kompyuterda to‘liq yo‘q qilish orqali virus epidemiyasining boshqa kompyuterlarga tarqalishini

oldini olish mumkin. Har qanday virusni aniqlaydigan va yo‘q qilinishini kafolatlaydigan mutlaqo ishonchli dasturlar mavjud emas. Kompyuter viruslariga qarshi kurashishning muhim usuli - o‘z vaqtida profilaktika qilishdir. Virusdan zararlanish ehtimolini sezilarli darajada kamaytirish va disklarda ma’lumotlarning ishonchli saqlanishini ta’minlash uchun quyidagi profilaktik choralar ko‘rilishi kerak:

- faqat litsenziyali dasturiy ta’minotdan foydalanish;
- kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta’minlash va uni muntazam yangilab borish;
- boshqa komyuterdan yozib olingan ma’lumotlarni o‘qishdan oldin har bir saqlagichni antivirus tekshiruvidan o‘tkazish;
- arxivlangan fayllarni ajratgandan so‘ng skanerlashni amalga oshirish;
- kompyuter disklarini takroriy antivirus dasturlari tekshiruvidan o‘tkazish;
- kompyuter tarmoqlaridan olingan barcha bajariladigan fayllarni nazoratlashda antivirus dasturidan foydalanish.

Nazorat savollari

1. Dasturiy mahsulotlarda xavfsizlik ta’minlanishining muhimligi.
2. Dasturiy mahsulotlarda xavfsizlik muammolarining kelib chiqish sabablari.
3. Nuqson, bag, xotirani to‘lib toshishi tushunchalari.
4. Dasturiy vosita xavfsizligini fundamental prinsiplari.
5. Dasturiy vositalarga qo‘yilgan talablar.
6. Dasturiy vositalarga qo‘yilgan xavfsizlik talablari.
7. Dasturiy vositalar xavfsizligini ta’minlashda dasturlash tillarining o‘rni.
8. Xavfsiz va xavfsiz bo‘lmagan dasturlash tillari.
9. Zararli dasturlar va ularning asosiy turlari.
10. Kompyuter viruslari nima?
11. Zararli dasturiy vositalardan himoyalanish usullari va vositalari.
12. Antivirus dasturiy vositalarini tanlashdagi talablar.

FOYDALANILGAN ADABIYOTLAR

1. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 140 b.
2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.
3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.
4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –T.: «Aloqachi», 2008, 382 bet.
5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
6. Марков А. С., Барабанов А. В., Дорофеев А. В., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С.Маркова. –М.: ДМК Пресс, -2017. – 224с.
7. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoyeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 192 bet.
8. Akbarov D.Y. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, 394 bet.
9. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
10. Raef Meeuwisse. Cybersecurity for Beginners (2nd. ed.). Cyber Simplicity Ltd, London, England, 2017, - 224 p.
11. Manjikian M. Cybersecurity ethics: an introduction. – Routledge, 2017, -328 p.
12. Kostopoulos G. Cyberspace and cybersecurity. – CRC Press, 2017, -316 r.
13. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity. – Springer Nature, 2020. – S. 384.
14. Pande J. Introduction to Cyber Security. Uttarakhand Open University, 2017, -152 p.
15. Cybersecurity Fundamentals Study Guide, ISACA 2015, -196 p.
16. Easttom C. Computer security fundamentals. – Pearson IT Certification, 2019, -447 p.

17. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.
18. Shinder D. L., Cross M. Scene of the Cybercrime. – Elsevier, 2008.
19. Scarfone K. et al. Guide to storage encryption technologies for end user devices //NIST Special Publication. – 2007. – T. 800. – S. 111.
20. Curricula Cybersecurity. Curriculum guidelines for post-secondary degree programs in cybersecurity. – 2017.
21. Purdy G. ISO 31000: 2009—setting a new standard for risk management //Risk Analysis: An International Journal. – 2010. – T. 30. – №. 6. – S. 881-886.
22. Zlatanov N. Hard Disk Drive and Disk Encryption, 2015, DOI: 10.13140/RG.2.1.1228.9681.
23. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z., Selection suitable biometrics for cryptographic key generators // TUIT BULLETIN, Tashkent, 2016, №4 (40), – P. 80-92
24. Rathgeb C., Uhl A. A survey on biometric cryptosystems and cancelable biometrics //EURASIP Journal on Information Security, 2011, №1, – P. 1-25.
25. Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2015, 2016, and 2017. U.S. Department of Health and Human Services Office for Civil Rights. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2015-2016-2017.pdf

Internet manbalari

1. ACR39U smart card rader [sayt]: http://smartkardtechnologies.com/productdetails/acr39u-smart-card-rader (murojaat vaqti: 29.10.2020).
2. Certified Network Defender [sayt]: https://iclass.eccouncil.org/our-courses/certified-network-defender-cnd/ (murojaat vaqti: 29.10.2020).
3. 3D Airport Security X-ray Machine [sayt]: https://www.turbosquid.com/3d-models/3d-airport-x-ray-machine-security-1405223 (murojaat vaqti: 29.10.2020).
4. Web Applications vulnerabilities and threats: statistics for 2019 [sayt]: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/ (murojaat vaqti: 29.10.2020).

5. How to Spot Phishing Emails [sayt]: https://www.nuigalway.ie/itsecurity/howtospotphishingemails/ (murojaat vaqti: 29.10.2020).
6. Beware of fake microsoft security essentials [sayt]: https://techjaws.com/beware-of-fake-microsoft-security-essentials/ (murojaat vaqti: 29.10.2020).
7. The Best Antivirus Protection for 2020 [sayt]: https://www.pcmag.com/roundup/256703/the-best-antivirus-protection (murojaat vaqti: 29.10.2020).
8. Securing Wireless Networks [sayt]: https://www.us-cert.gov/ncas/tips/ST05-003 (murojaat vaqti: 29.10.2020).
9. Why High Availability Is Important for Your Business [sayt]: https://blog.layershift.com/why-high-availability-for-your-business/ (murojaat vaqti: 29.10.2020).
10. Rutoken [sayt]: https://www.rutoken.ru/ (murojaat vaqti: 29.10.2020).
11. Comparison of disk encryption software [sayt]: https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software (murojaat vaqti: 29.10.2020).
12. G20 summit: NSA targeted Russian president Medvedev in London [sayt]: https://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit (murojaat vaqti: 29.10.2020).
13. CRADC Data Destruction and Return of Restricted Data Policy [sayt]: https://ciser.cornell.edu/wp-content/uploads/2017/01/CRADC_Destruction_and_Return_of_Restricted_Data.pdf (murojaat vaqti: 29.10.2020).
14. Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements [sayt]: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis (murojaat vaqti: 29.10.2020).
15. Best Keylogger for Windows 10 in 2020 [sayt]: https://www.pctattletale.com/blog/1505/best-keylogger-software-windows-10 (murojaat vaqti: 29.10.2020).
16. Windows Event Logging and Forwarding [sayt]: https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding (murojaat vaqti: 29.10.2020).

QISQARTMA SO‘ZLAR RO‘YXATI

ABAC - Attribute-based access control
AES - Advanced Encryption Standard
APT - Advanced persistent threats
ASSII – American Standard Code for Information Interchange
AT – Axborot texnologiyalari
CBC - Cipher Block Chaining
CCTV - Closed-circuit television
CDMA - Code Division Multiple Access
CSEC2017 JTF – Cybersecurity Curricula 2017 Joint Task Force
CVE - Common Vulnerabilities and Exposures
DAC - Discretionary access control
DES - Data Encryption Standard
DLP - Data Leakage Prevention,
DoD – Department of Defense
DOS - Denial of service
ECB - Electronic codebook mode
FAR - False Acceptance Rate
FRR - False Rejection Rate
FTP – File Transfer Protocol
GNFS - General Number Field Sieve
GSM – Global System for Mobile Communications
HMAC – hash-based message authentication code
HTTP - Hypertext Transfer Protocol
HTTPS - Hypertext Transfer Protocol Secure
IDS - Instrusion Detection System
IPS - Intrusion Prevention System
IPSec - IP Security
ISO – International Organization for Standardization
IV - Initialization Vector
KDC - Key Destribution Center
L2TP - Layer 2 Tunneling Protocol
LAN - Local Area Network
MAC - Mandatory access control
MAC - Message Authentication Code
MAN - Metropolitan Area Network
MITM - Man in the middle attack
NAT - Network Address Translation
OWASP - Open Web Application Security Project

PAN - Personal Area Network
PIN - Personal Identification Number
PKI - Public key infrastructure
PPP – Point-to-Point Protocol
PPTP - Point-to-Point Tunneling Protocol
RAID - Redundant Array of Independent Disks
RBAC - Role-based access control
RFID – Radio Frequency IDentification
SIM - Security Information Management
SSID - Service Set Identifier
SSL - Secure Sockets Layer
TCP/IP – Transmission Control Protocol/Internet Protocol
USB – Universal Serial Bus
UTM - Unifield Threat Management
VPN – Virtual Private Network
WAN - Wide Area Network
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WMAN - Wireless Metropolitan Area Network
WPA - Wi-Fi Protected Access
WPAN - Wireless Personal Area Network
WWAN - Wireless Wide Area Network
AOB - Alisaning onlayn banki
ATM – Automated teller machine
MAC - Media access control
OT – Operatsion tizim
ERI - Elektron raqamli imzo

ATAMALARNING RUS, O‘ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG‘ATI

Авторизация - представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.
Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.
Authorization – granting the user certain access rights based on the positive result of authentication in the system.

Администратор защиты - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.
Himoya ma’muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.
Security administrator - the subject of the access responsible for the protection of the automated system against unauthorized access to the information.

Администратор системы - лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.
Tizim ma’muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta’minlashga javobgar shaxs.
System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.

Актив - 1. Информация или ресурсы, подлежащие защите. 2. Все, что имеет ценность для организации. 3. Главное приложение, общая система поддержки, высоко авторитетная программа, материальная часть, миссия критической систем, персонал, оборудование или логически связанная группа систем.
Aktiv - 1. Himoyalanuvchi axborot yoki resurslar. 2. Tashkilot uchun qiymatli barcha narsalar. 3. Bosh ilova, umumiy madadlovchi tizim, yuqori nufuzli dastur, moddiy qism, kritik tizim missiyasi, xodimlar, jihozlar yoki mantiqiy bog’langan tizimlari guruhi.
Asset - 1. Information or resources that should be protected. 2. Anything that has value to the organization. 3. A major application, general support

system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Активная угроза - угроза преднамеренного несанкционированного изменения состояния системы.
Faol tahdid – tizim holatini atayin ruxsatsiz o'zgartirish tahdidi.
Active threat – a threat that can make a deliberate unauthorized change to the system.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.
Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.
Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.
Kriptografik algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.
Cryptographic algorithm - the algorithm that implements the calculation of one cryptographic functions.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.
Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.
Decryption algorithm – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function.

Алгоритм хеширования - в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и

программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritm. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

Hashing algorithm – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.

Алгоритм цифровой подписи - асимметричный алгоритм, используемый для цифровой подписи данных.

Raqamli imzo algoritmi - ma'lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

Digital signature algorithm – asymmetric algorithm used for digitally signing data.

Алгоритм шифрования RSA - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Анализ - изучение значимости полученных данных и доказательственной ценности к случаю.
Tahlil – olingan ma’lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o’rganish.
Analysis – the examination of acquired data for its significance and probative value to the case.

Анализаторы сетевые (сниффер) - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.
Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini “tinglash”ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.
Network analyzers (sniffer) - programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. Еще - программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.
Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo’q qiluvchi dastur. Agar virus yo’q qilinmasa, zaharlangan dastur yo’q qilinadi. Yana – viruslardan himoyalashga, zaxarlangan dasturiy modullar va tizimli makonlarni aniqlashga, hamda zaxarlangan obyektlarning dastlabki holatini tiklashga mo’ljallangan dastur.
Antivirus - the program that detect or detect and remove viruses. If virus remove not possible, then the infected program is destroyed. Another program, designed to protect against viruses, detecting infected software modules and system areas as well as restore the original state of infected object.

Аппаратное средство защиты информации - специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.
Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.
Hardware data protection - a special protective device or fixture included in the kit technical tools of information processing.

Апплеты вредоносные - небольшие приложения, которые автоматически загружаются и выполняются, и которые реализуют несанкционированные функции информационной системы.
Zararli appletlar - axborot tizimida ruxsat etilmagan funksiyalarni amalga oshiruvchi, avtomatik yuklanuvchi va bajariluvchi kichik ilovalar.
Malicious applets – small application that are automatically downloaded and executed and that perform an unauthorized function on an information system.

Архитектура IT безопасности - описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.
AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.
IT security architecture – a description of security principles and an overall approach for complying with the principles that drive the system design.

Архитектура информационной безопасности - встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информационной безопасности, персональных и организационных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.
Axborot xavfsizligining arxitekturasi - tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo’linmalarini, ularni tashkilot missiyasi va strategik rejalariga tenglashtirishni ko’rsatish bilan tavsiflovchi tashkilot arxitekturasining o’rnatilgan, ajratib bo’lmas qismi.

Information security architecture – an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Атака «противник в середине» — атака на протокол криптографический, в которой противник C выполняет этот протокол как с участником A, так и с участником B. Противник C выполняет сеанс с участником A от имени B, а с участником B от имени A. В процессе выполнения противник пересылает сообщения от A к B и обратно, возможно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для B под именем A.

«Dushman o'rtada» xujumi – kriptografik protokolga hujum bo'lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o'zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o'rtada» hujumining muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o'zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi.

Attack "the opponent in the middle" - attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack "the opponent in the middle" allows authenticate itself to the enemy in the name of A.

Атака на отказ в обслуживании — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo'luvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy

foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.
Denial-of-service attack - attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult.

Атака пассивная — атака на криптосистему или протокол криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.
Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta'sir etmaydi.
Passive attack - attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate.

Атака со словарем паролей — атака на криптосистему, основанная на переборе значений пароля.
Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizimga hujum.
Attack with a dictionary of passwords - the attack on the cryptosystem based on iterating the value of a password.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.
Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.
Authenticator - means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user.

Аутентификация - проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.
Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikasiyasini tekshirish; saqlanuvchi va uzatuvchi ma’lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.
Authentication - checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

Аутентификация биометрическая — способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.
Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko’z pardasining to’ri va h.) asosidagi autentifikatsiyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo’lmasligi. Ularni esdan chiqarishning, yo’qotishning yoki boshqa foydalanuvchiga berishning iloji yo’q.
Biometric authentication - the method of authentication of a subscriber (user), based on a verification of biometric characteristics (fingerprints, hand geometry, face, voice, eye retina image, etc.). The advantages of this method is the inseparability of biometric characteristics from user: they cannot be forgotten, lost or transferred to another user.

Аутентификация двухфакторная — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.
Two-factor authentication - user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

Аутентификация на основе паролей одноразовых — технология аутентификации с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства – токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.
Bir martali parollar aosidagi autentifikatsiya - bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funksiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.
One time password based authentication - technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device – taken, or technology OOB (out of band) based on the transmission password disposable using additional channels, other than where the user accesses the application system.

Аутентификация сообщений - добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.
Xabarlar autentifikatsiyasi – ma’lumotlarda har qanday o’zgarishlarni aniqlash maqsadida ma’lumotlar blokiga nazorat hoshiyasini qo’shish. Ushbu hoshiya qiymatini hisoblashda faqat ma’lumotlar priyemnigiga ma’lum kalitlar ishlatiladi.

Message authentication - adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информационной моделью предметной области. База данных, как правило, представляются тремя уровнями абстракции: внешним, концептуальным и внутренним.

Ma'lumotlar bazasi - tatbiqiy dasturlarga bog'liq bo'lmagan holda ma'lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy prinsiplarini ko'zda tutuvchi, ma'lum qoidalar bo'yicha tashkil etilgan ma'lumotlar majmui. Predmet sohasining informatsion modeli hisoblanadi. Ma'lumotlar bazasi odatda abstraksiyaning tashqi, konseptual va ichki satxlari orqali ifodalanadi.

Database - a collection of data organized according to certain rules, providing general principles for describing, storing and manipulating data independent of the application programs. An information domain model. The database, usually presented in three levels of abstraction: external, conceptual and internal.

Безопасность - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще - состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Xavfsizlik - ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma'lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko'rib chiqilishi va modifikatsiyalanishi mumkin bo'lmagan holat.

Security - the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be

used, viewed and modified by unauthorized persons (including the system staff), computers or software.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение; еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.
Axborot xavfsizligi - axborot holati bo'lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz uning olinishiga yo'l qo'yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalanish darajasi holati.
Information security - status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

Безопасность информационная общества - то же, что и «безопасность, информационная личности» применительно к организованному коллективу людей и к обществу в целом.
Jamiyat axborot xavfsizligi – "shaxs axborot xavfsizligi" kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo'llaniladi.
Society information security - what "safety information personality" when applied to organized team of people and to society as a whole.

Безопасность информационной сети - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.
Axborot tarmog'i xavfsizligi – axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.

Network security - measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами; еще - является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).
Tarmoqlararo ekran – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to'sig'i hisoblanadi.
Firewall - a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software).

Кибер инфраструктура - включает электронную информацию и коммуникационные системы, и службы и информацию, содержавшуюся в этих системах и службах.
Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o'z ichiga oladi.
Cyber infrastructure – includes electronic information and communications systems and services and the information contained in these systems and services.

Кибер инцидент - действия, использующие компьютерные сети, приводящие к фактическому или потенциальному ущербу в информационной системе и/или содержащейся в ней информации.
Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo'luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.
Cyber incident – actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Кибер-атака - атака, через киберпространство, предназначенная для использования предприятием киберпространства в целях, отключения, уничтожения или злонамеренного контроля вычислительной среды/инфраструктуры**.**
Kiber-hujum – hisoblash muhiti/ infrastrukturasini, o'chirish, buzish yoki g'arazli nazoratlash yoki ma'lumot yaxlitligini buzish yoki nazoratlanuvchi axborotni o'g'irlash maqsadida kiberfazodan foydalanuvchi tashkilotga atalgan kiberfazo orqali amalga oshiriluvchi hujum.
Cyber-attack – an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disabling, destroying, or maliciously controlling a computing environment/infrastructure.

Кибербезопасность - возможность охранять или защитить использование киберпространства кибератаками.
Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo'riqlash yoki himoyalash imkoniyati.
Cybersecurity – the ability to protect or defend the use of cyberspace from cyber-attacks.

Киберпреступность — действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях.
Kiberjinoyatchilik - g'arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o'g'irlashga yoki buzishga yo'naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.
Cyber cryme — the actions of individuals or groups aimed at cracking computer security systems, theft or destruction of information for selfish or destructive purposes.

Киберпространство - глобальный домен в информационной среде, состоящий из взаимозависимой сети инфраструктур информационных систем включая Интернет, сети телекоммуникации, компьютерные системы, и встроенные процессоры и контроллеры.
Kiberfazo – Internet, telekommunikatsiya tarmoqlari, kompyuter tizimlari va o'rnatilgan prosessorlar va kontrollerlarni o'z ichiga olgan,

o’zaro bog’langan axborot tizimlari infrastrukturalar tarmog’idan tashkil topgan axborot muhitidagi global domen.
Cyberspace – a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Кибертерроризм — действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных общественно опасных последствий.
Kiberterrorizm - insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug’diruvchi kompyuter tizimlarini izdan chiqarish bo’yicha harakatlar.
Cyber terrorism — action disruption of computer systems, creating a danger of loss of life, significant property damage or other socially dangerous consequences.

Привилегии - права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.
Imtiyozlar - hisoblash tizimida ma’lum obyektlardan foydalanish va ularda ishlashdan iborat foydalanuvchilarning yoki dasturning huquqlari.
Privilege - rights of the user or a program, consisting in the availability of certain objects and actions in a computing system.

Приложение – программное обеспечение (программа) информационной системы, выполняющая определенную функцию непосредственно для пользователя без доступа к системе управления, мониторинга или административным привилегиям.
Ilova – bevosita foydalanuvchi uchun boshqarish, monitoringlash tizimlaridan yoki ma’muriy imtiyozlardan foydalanmay aniq funksiyani bajaruvchi axborot tizimining dasturiy ta’minoti (dasturi).
Application – a software (program) hosted by an information system. In addition, software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Программа антивирусная — программа компьютерная, предназначенная для защиты от вирусов компьютерных. Осуществляет обнаружение, восстановление, блокирование и/или удаление зараженных программных модулей и системных областей.
Virusga qarshi dastur - kompyuter viruslaridan himoyalashga mo'ljallangan kompyuter dasturi. Zaharlangan dasturiy modullarni va tizim sohalarini aniqlashni, tiklashni, blokirovka qilishni va/yoki yo'q qilishni amalga oshiradi.
Antivirus program - a computer program designed to protect the viruses from the computer. Detection, recovery, blocking and/or deleting infected software modules and system areas.

Виртуальная частная сеть - виртуальная сеть, построенная на основе существующих физических сетей, обеспечивающая безопасный туннель коммуникации для передачи данных или другой информации, передаваемой между сетями.
Virtual shaxsiy tarmoq - tarmoqlar orasida almashiniluvchi ma'lumotlar yoki boshqa axborotni uzatish uchun xavfsiz kommunikatsiya tunnelini ta'minlovchi, mavjud fizik tarmoqlar asosida qurilgan virtual tarmoq.
Virtual private network – a virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

Контроль доступа на основе ролей - модель для управления доступом к ресурсам, когда разрешенные действия на ресурсы идентифицированы с ролями, а не с личными идентификаторами субъекта.
Rollarga asoslangan ruxsatni nazoratlash - resurslardan foydalanishni boshqarish modeli bo'lib, resurslarda ruxsat berilgan harakatlar shaxsiy subyekt identifikatorining o'rniga rollar bilan identifikatsiyalanadi.
Role-based access control – a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Конфиденциальность – 1. Некоторый класс данных, получение либо использование которых неавторизованными для этого лица не может стать причиной серьезного ущерба для организации. 2. Свойство информации, состоящее в том, что она не может быть

обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.
Konfidensiallik – 1. Avtorizatsiyalanmagan shaxs tomonidan olinishi yoki foydalanishi tashkilot uchun jiddiy zarar sababi bo'la olmaydigan ma'lumotlarning qandaydir sinfi. 2. Alohida shaxslar, modullar, jarayonlar ruxsatisiz aniqlanishi, va foydalanishi mumkin bo'lmagan axborot xususiyati.
Confidentiality – 1. Some class data, obtaining or the use of which by unauthorized persons could not cause serious damage to the organization. 2. The quality of information, consisting in that it cannot be detected and made available without the permission of individuals, modules or processes.

Менеджмент риска — полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.
Risk menejmenti — axborot-telekommunikatsiya texnologiya resurslariga ta'sir etishi mumkin bo'lgan xavfli xodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to'liq jarayoni.
Risk management — the complete process of identification, control, eliminate or mitigate the consequences of hazardous events that may affect resources of information and telecommunication technologies.

Целостность - свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому физическому её состоянию).
Yaxlitlik - axborotning buzilmagan ko'rinishda (axborotning qandaydir fizik holatiga nisbatan o'zgarmagan shaklda) mavjud bo'lishida ifodalangan xususiyati.
Integrity - the property of information, namely, its existence in an undistorted view (unchanged with respect to some physical condition).

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, 2020

“Kiberxavfsizlik asoslari”

5330300 – Axborot xavfsizligi, 5330500 – Kompyuter injiniringi (Kompyuter injiniringi, AT-servisi, Multimedia texnologiyalari), 5330600 – Dasturiy injiniring, 5350100 - Telekommunikatsiya texnologiyalari (Telemommunikatsiya, teleradiouzatish, mobil tizimlar), 5350200 – Televizion texnologiyalar (Audiovizual texnologiyalar, telestudiya tizimlari va ilovalari), 5350300 – Axborot-kommunikatsiya texnologiyalari sohasida iqtisodiyot va menejment, 5350400 – Axborot-kommunikatsiya texnologiyalari sohasida kasb ta’limi, 5350500 – Pochta aloqasi texnologiyasi va 5350600 – Axborotlashtirish va kutubxonashunoslik yo‘nalishlari talabalari uchun o‘quv qo‘llanma.

Kriptologiya kafedrasi majlisida
ko‘rib chiqildi va nashr etishga ruxsat etildi.
2020 yil 9 may 36 - sonli bayonnoma

“AX” fakulteti UK majlisida
ko‘rib chiqildi va nashr etishga ruxsat etildi.
2020 yil 27 may 9 - sonli bayonnoma

Muhammad al-Xorazmiy nomidagi
TATU Kengashi majlisida ko‘rib chiqildi, nashr etishga va nashr guvohnomasini olishga ruxsat etildi
2020 yil 4 iyul 9(702) - sonli bayonnoma

Tuzuvchilar:

S.K.Ganiev
A.A.Ganiev
Z.T.Xudoyqulov

Taqrizchilar:

K.A.Tashev
O.P.Axmedova

Mas’ul muharrir: S.K.Ganiev

Musahhih: S.X.Abdullayeva