O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

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

KIBERXAVFSIZLIK ASOSLARI

O‘quv qo‘llanma

TOSHKENT 2020

UDK: 004

S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – T.: «Aloqachi», 2020, 303 bet.

O‘quv qo‘llanma 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 xavfsizligini nazariy va amaliy asoslarini qo‘llanilishi ifodalagan «Kiberxavfsizlik asoslari» nomi ostidagi fanning bo‘limiga bag‘ishlangan.

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.

KIRISH

Yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat kundan-kun axborot-kommunikatsiya texnologiyalariga tobora ko'proq qaram bo'lib borayotganligini hisobga olib, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega va juda muhim mavzuga aylanmoqda.

Bugungi kunda axborot jamiyatini rivojlantirishning zaruriy sharti bu kiberxavfsizlikdir, uni xavfsizlikning texnik va qonunchilikgacha bo'lgan deyarli cheksiz ro'yxati va ularni hal qilish yo'li bilan ta'minlash mumkin.

Zamonaviy sharoitda, kiberxavfsizlik masalalari alohida kompyuter vositasida axborot xavfsizligi darajasidan har bir davlatning axborot va milliy xavfsizligining ajralmas qismi sifatida yagona kiberhavfsizlik tizimini yaratish darajasigacha boradi.

Shu sababli, har bir tashkilot uchun kiberxavfsizlikni ta’minlash maqsadida mazkur soha bilan shug’ullanuvchi xodimlar jalb qilinmoqda va xodimlarni kiberxavfsizlikka oid bilimlar bilan doimiy tanishtirib boorish uchun qator seminar-treyning mashg’ulotlari tashkil etilmoqda. Oliy ta’lim muassasalarida ham kiberxavfsizlikni fan sifatida o’tilishi buning yaqqol misolidir.

Respublikamizda axborot texnologiyalarining rivojlanishi bilan bir qatorda xo‘jalik va davlat boshqaruvi organlarida axboorot xavfsizligini, xususan, kompyuter bilan bog’liq bo’lgan xavfsizlik muammolarini bartaraf etish yo’nalishida alohida e’tibor qaratilmoqda. 2017-2021 yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida vazifalar belgilab olindi, shular qatorida «...axborot xavfsizligini ta’minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish» va kiber jinoyatchilikni fosh etish masalalariga alohida e’tibor qaratilgan. Bundan tashqari, “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili"da amalga oshirishga oid Davlat dasturi to‘g‘risida”gi O‘zbekiston 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 o’quv qo’llanmalarini ishlab chiqish ham e’tibor berish kerak bo’lgan muhim jihatlardan hisoblanadi.

Mazkur o‘quv qo‘llanma kiberxavfsizlik sohasida dastlabki qadamlarini qo’yayotgan tinglovchilar uchun mo’ljallangan bo’lib, unda kiberxavfsizlikning asosiy tushunchalari, kiberhujumlardan himoyalanishning nazariy asoslari keltirilgan.

Qo‘llanmaning birinchi bobida kiberxavfsizlik asoslari fanining vazifalari va asosiy tushunchalari, uning qo‘llanilish sohasi hamda kiberxavfsizlikda inson omili masalalari ko‘rib chiqilgan. Kiberxavfsizlikning bilim sohalari, kiberxavfsizlikning fan sohasining tuzulishi, kiberxavfsizlik va axborot xavfsizlik tushunchalari o’rtasidagi farqlar misollar asosida keltirilgan.

Ikkinchi bobda axborotning kriptografik himoyasi doirasida uning asosiy tushunchalari, simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, ma’lumotlarni yaxlitligini ta’minlash usullari, disklarni va fayllarni shifrlash hamda ma’lumotlarni xavfsiz o’chirish usullari ko‘rib chiqilgan.

Qo‘llanmaning uchinchi bobi foydalanishlarni nazoratlashga bag’shlangan bo’lib, autentifikatsiya usullari, ma’lumotlarni fizik va mantiqiy boshqarish usullari keltirilgan. Amalda keng qo’llanilgan parolga asoslangan autentifikatsiya usulini matematik tahlili va amalda foydalanish uchun parollarni tanlash bo’yicha tavsiyalar keltirilgan.

To‘rtinchi bob tarmoq xavfsizligiga bag‘ishlangan bo’lib, unda tarmoqda mavjud bo’lgan xavfsizlik muammolari va ularni bartaraf etishda tarmoqlararo ekran va virtual himoyalangan tarmoq vositalarida foydalanish tartibi keltirilgan. Bundan tashqari simsiz tarmoqlarda ham xavfsizlik muammolari va ularni oldini olish tartibi keltirilgan.

Beshinchi bobda tizimning foydalanuvchanlik xususiyati va uning tizim uchun muhimligi, ma’lumotlarning zaxira nusxalash usullari va ma’lumotlarni qayta tiklash usullari haqida ma’lumotlar keltirilgan. Tizim foydalanuvchanligi uchun

auditlash muolajasi muhim hisoblangani bois, Windows OT uchun hodisalarni qayd qilish tartibi bilan yaqindan tanishib chiqiladi.

Oltinchi bob dasturiy vositalar xavfsizligiga bag'ishlangan bo'lib, dasturlardagi xavfsizlik muammolari va ularni oldini olishga qaratilgan fundamental printsiplar keltirilgan. Vazifasi tizimga ziyon etkazish uchun yaratilgan zararli dasturiy vositalar, ularning tahlili va zamonaviy antivirus dasturiy vositalari haqida batafsil ma'lumotlar keltirilgan.

Yettinchi bob axborot xavfsizligi siyosati va risklarni boshqarish masalalarida bag'ishlangan hamda unda tizimlar arxitekturasi, axborot xavfsizligi siyosatini amalga oshirish tartibi va risklarni boshqarish haqida ma'lumotlar keltirilgan.

Sakkizinchi bobda kiberjinoyatchilik, kiberhuquq va kiberetika masalalariga to'xtalib o'tilgan va unda kiberjinoyatchilik uchun tayinlangan jazo turlari haqida ma'lumotlar keltirilgan.

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.

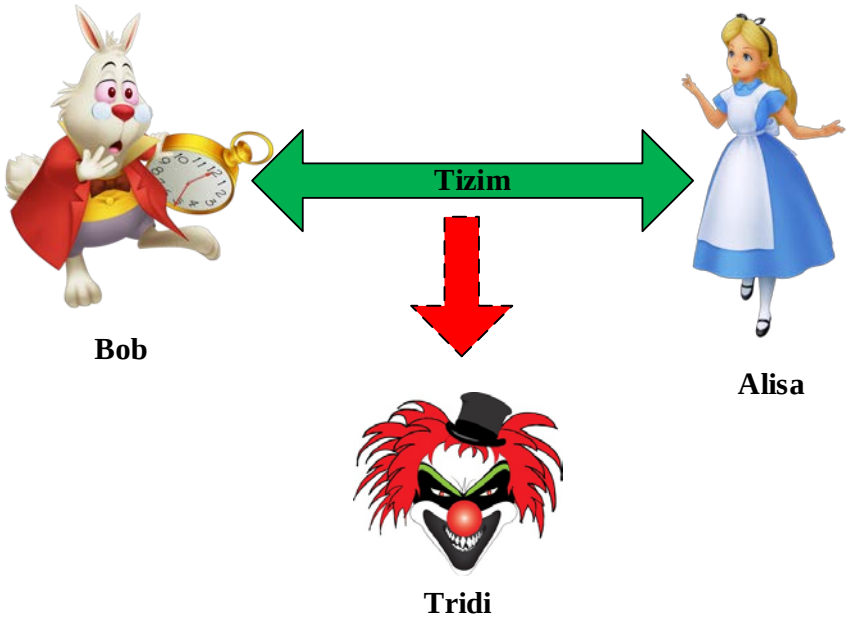
1 BOB. KIBERXAVFSIZLIKNING ASOSIY TUSHUNCHALARI

1.1. Konfidentsiallik, yaxlitlik va foydalanuvchanlik 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.

1.1.1. Axborot xavfsizligining hayotiy timsollari

Axborot xavfsizligi hayotda mavjud timsollarga asoslanadi. Hayotda faqat qonuniy faoliyat olib boruvchi shaxslar mavjud, ular 1-rasmda *Alisa* va *Bob* timsolida akslantirilgan. Biroq, hayotda qonuniy faoliyat yurituvchi insonlarning faoliyatiga qiziquvchi, ularning ishlariga xalaqit beruvchi bo’lgan insonlar ham mavjud va ular 1-rasmda *Tridi* timsolida tasvirlangan. Tridi timsoli barcha g’arazli niyatlarni amalga oshiruvchi shaxslarni ifodalaydi [5].



1-rasm. Axborot xavfsizligining hayotdagi timsollari

O’quv qo’llanmaning keyingi bo’limlarini yoritishda quyidagi hayotiy ssenariyni ko’raylik. Ushbu hayotiy ssenariy *Alisaning onlayn banki (AOB)* deb ataladi. Bunga ko’ra, Alisa onlayn bankning biznes faoliyatini amalga oshiradi.

Mazkur ssenariyda 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.

1.1.2. Kiberxavfsizlikning asosiy tushunchalari

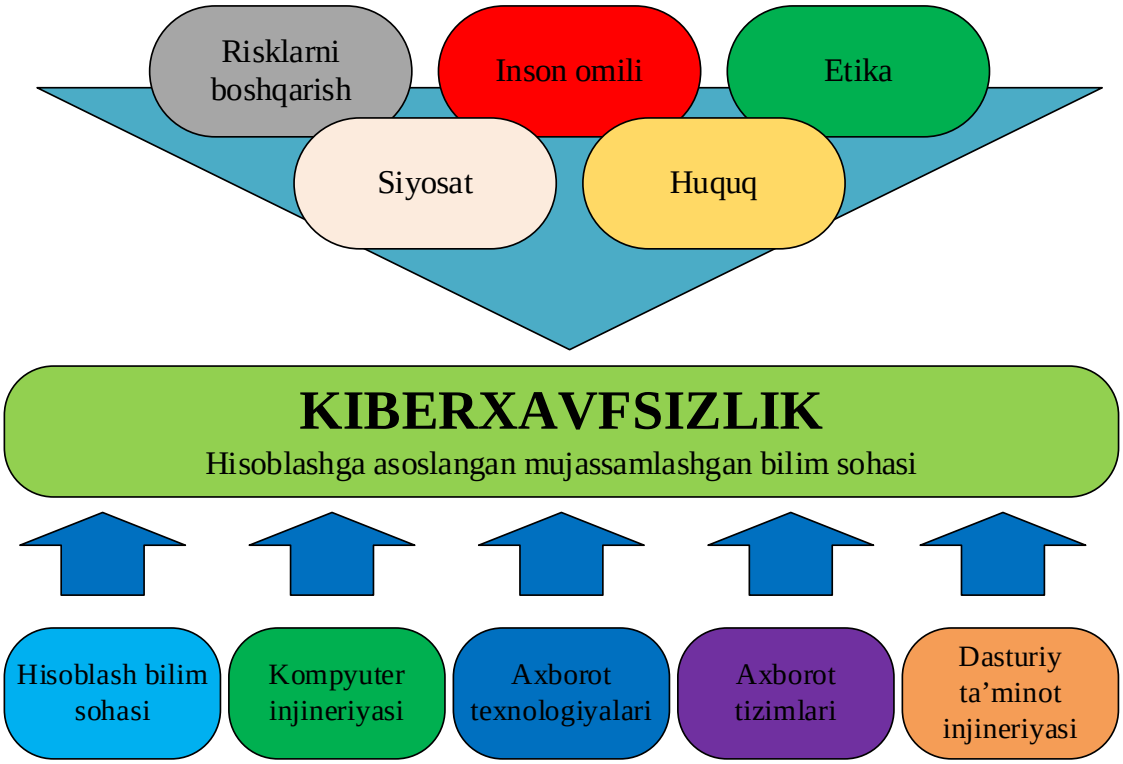
Kompyuter tizimlari va tarmoqlarida axborotni himoyalash va axborot xavfsizligiga tegishli bo’lgan ayrim tushunchalar bilan tanishib chiqaylik.

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 [1]: *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.*

Tarmoqlar sohasida faoliyat yuritayotgan *Cisco* tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan [2]: *Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo’q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar soni va turlarining kattaligi va buzg’unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.*

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilgandan boshlab paydo bo’la boshlagan. Bunda mazkur qurilmalarni va ularning vazifalari himoyasi uchun ko’p qatlamli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo’lishiga olib keldi.

Hozirgi kunda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassisdan kiberxavfsizlikning fundamental bilimlariga ega bo’lishi talab etiladi. Demak, kiberxavfsizlik fani sohasining tuzilishini quyidagicha tasvirlash mumkin (2-rasm).



2 – rasm. Kiberxavfsizlik fani sohasining tuzilishi

Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida mualliflar kiberxavfsizlikni quyidagi 6 atamasi keltirishgan [1]:

Konfidensiallik – axborot yoki uni eltuvchining shunday holati bo’lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo’ladi. Konfidensiallik axborotni ruxsatsiz “o’qish”dan himoyalash bilan shug’ullanadi. AOB ssenariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o’z balansida qancha pul borligini Tridi 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 ssenariysida Alisaning banki qayd yozuvi butunligini Tididan himoyalashi shart. Masalan, Bob akkauntida balansning o’zgarishi yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

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

Foydaluvchanlik - avtorizasiyalangan mantiqiy obyekt so’rovi bo’yicha uning tayyorlik va foydalanuvchanlik holatida bo’lishi xususiyati. Foydalanuvchanlik axborotni (yoki tizimni) ruxsatsiz “bajarmaslik”dan himoyalash bilan shug’ullanadi. AOB ssenariysida AOB veb 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) [11].

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 [14].

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

Kiberxavfsizlik yoki axborot xavfsizligida risklar salbiy ko’rinishda qaraladi.

Hujumchi kabi fikrlash - bo’lishi mumkin bo’lgan xavfni oldini olish uchun qonuniy foydalanuvchini 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 chuqur 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 sathi 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 hisoblanadi. Masalan, xonada saqlanayotgan tashkilot hujjati qo'g'oz ko'rinishda bo'lganligi sababli, yonib ketishi mumkin.

Boshqarish vositasi – riskni o'zgartiradigan harakatlar bo'lib, boshqarish 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. Bundan tashqari, yong'in bo'lganda 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 qarash mumkin.

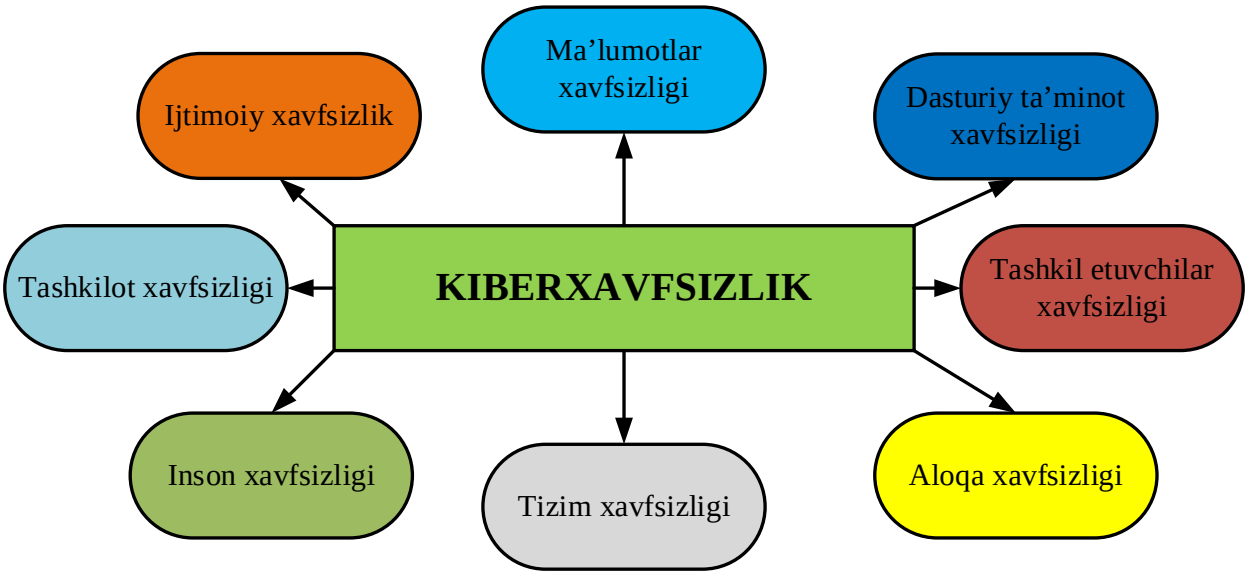
1.1.3. Axborot xavfsizligi va kiberxavfsizlik o’rtasidagi farq

“Kiberxavfsizlik” va “axborot xavfsizligi” atamalaridan, tez-tez o’rnilari almashingan holatda, foydalaniladi. Ba’zilar kiberxavfsizlikni axborot xavfsizligi, axborot texnologiyalari xavfsizligi va (axborot) risklarni boshqarish tushunchalariga sinonim sifatida foydalanadilar. Ayrimlar esa, xususan, hukumat sohasidagilar kiberxavfsizlikka kompyuter jinoyatchiligi va muhim infratuzilmalar himoyasini o’z ichiga olgan milliy xavfsizlik bilan bog’liq bo’lgan 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’rinishdagi, elektron va insonlar fikrlashida, og’zaki va vizual aloqada intelektual huquqlarini himoyalash bilan shug’ullanadi. *Kiberxavfsizlik* esa elektron shakldagi axborotni (barcha holatlardagi, 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 tegishlidir. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo’nalishi deb tushunish uni to’g’ri anglashga yordam beradi [15].

1.1.4. Kiberxavfsizlikning bilim sohalari

CSEC2017 JTF manbasiga ko’ra kiberxavfsizlik 8 ta bilim sohasiga bo’lingan bo’lib, o’z o’rnida ularning har biri qismsohalarga bo’linadi (3-rasm) [16].



3-rasm. Kiberxavfsizlikning bilim sohalari

“*Ma’lumotlar xavfsizligi*” bilim sohasi ma’lumotlarni saqlash, ishlash va uzatishda himoyani ta’minlashni maqsad qiladi. 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 ta’minotlarni 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 ularning 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 etibor qaratib, o’zida fizik va mantiqiy ulanishni mujassamlashtiradi.

“*Tizim xavfsizligi*” bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo’lgan tizim xavfsizligining jixatlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun nafaqat, uning tarkibiy qismlari va ularning bog’lanishini tushunish, balki yaxlitlikni 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’lanishining xavfsizligi va undan yuqori tizimlarda foydalanish masalasini hal qiladi.

“*Inson 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.

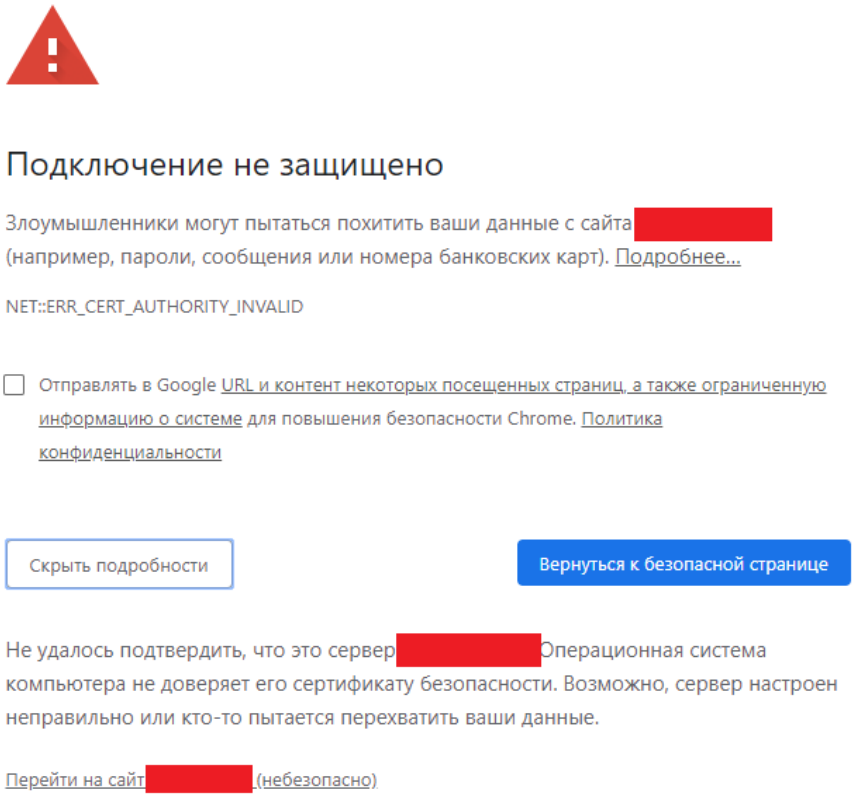
Demak, aytish mumkinki, kiberxavfsizlik sohasi axborot texnologiyalari mutaxassislari uchun zarur soha hisoblanadi.

1.2. Kiberxavfsizlikda inson omili

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 veb-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, ularni amalga oshishi uchun foydalanuvchi “ishtirok”i talab etiladi (4-rasm). 4-rasmda 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 [13]. Endi parolga asoslangan autentifikasiya usulini ko’rib chiqaylik. 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 esa, murakkab parollardan foydalanish va ularni turli eltuvchilarda saqlash (masalan, qog’ozda qayd etish) esa, ushbu muammoni yanada oshirib yuboradi.

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



4-rasm. SSL protokolidagi xavfsizlik ogohlantirishi

Nazorat savollari

1. Axborot xavfsizligining xayotiy timsollari va ularning vazifalari nimalardan iborat?
2. Kiberxavfsizlik tushunchasiga izoh bering?
3. Kiberxavfsizlik fan sifatida qanday tuzilishga ega?
4. Kiberxavfsizlikning asosiy tushunchalarini aytib bering?
5. Axborotni konfidensialligini ta’minlash deganda nimani tushunasiz?
6. Axborotni yaxlitligini ta’minlash deganda nimani tushunasiz?
7. Axborot uchun foydalanuvchanlikning muhimligi?
8. Risk nima 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 tushunchalarini bir-biridan farqi?
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.

2 BOB. AXBOROTNING KRIPTOGRAFIK HIMOYASI

2.1. Kriptografiyaning asosiy tushunchalari

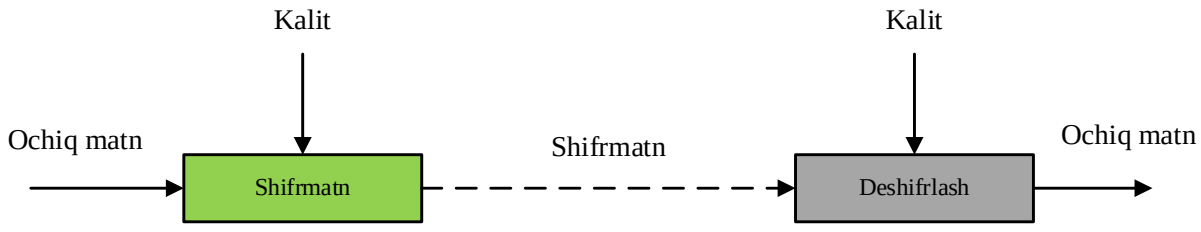
Kriptografiya – axborotni aslidan o’zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug’ullanadi. Dastlabki kriptografik uslublar eramiz boshida, Yuliy Sezarning ish yuritish yozishmalarida uchraydi.

Axborotni himoyalash masalalari bilan *kriptologiya* (*kryptos* - mahfiy, *logos*-ilm) fani shug’ullanadi. Kriptologiya maqsadlari o’zaro qarama-qarshi bo’lgan ikki yo’nalishga ega [17]: – *kriptografiya* va *kriptoanaliz*.

“Kripto”ning asosiy tushunchalari quyidagilarni o’z ichiga oladi [13]:

- *Kriptologiya* - “maxfiy kodlar”ni yaratish va buzish fani va san’ati;
- *Kriptografiya* – “maxfiy kodlar”ni yaratish bilan shug’ullanadi.
- *Kriptotahlil* – “maxfiy kodlar”ni buzish bilan shug’ullanadi;
- *Kripto* – yuqoridagi tushunchalarga (hattoki bundanda ortig’iga) sinonim bo’lib, kontekst ma’nosiga ko’ra farqlanadi.

Shifr yoki *kriptotizim* ma’lumotni *shifrlash* uchun ishlatiladi. Haqiqiy, shifrlanmagan ma’lumot *ochiq matn* deb, shifrlash natijasi esa *shifrmatn* deb ataladi. Haqiqiy ma’lumotni qayta tiklash uchun shifrmatnni *deshifrlash* zarur bo’ladi. *Kalitdan* kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi. Kriptotizimning “qora quti” sifatidagi ko’rinishi 5 – rasmda keltirilgan [13].



5-rasm. Kriptotizimning “qora quti” sifatidagi ko’rinishi

Shifrlash va deshifrlash masalalariga tegishli bo’lgan, ma’lum bir *alfavitda* tuzilgan ma’lumotlar *matnlarni* tashkil etadi. *Alfavit* - axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to’plami. Misollar sifatida:

- o’ttiz oltita belgidan (harfdan) iborat o’zbek tili alfaviti;
- o’ttiz ikkita belgidan (harfdan) iborat rus tili alfaviti;

– yigirma sakkizta belgidan (harfdan) iborat lotin alfaviti;

– ikki yuzi ellik oltita belgidan iborat ASSII kompyuter belgilarining alfaviti;

– binar alfavit, ya’ni 0 va 1 belgilardan iborat alfavit;

– sakkizlik va o’n oltilik sanoq sistemalari belgilaridan iborat alfavitlarni keltirish mumkin.

Simmetrik shifrlarda ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi. Bundan tashqari *ochiq kalitli* (*assimetrik*) kriptotizimlar mavjud bo’lib, unda shifrlash va deshifrlash uchun turli kalitlardan foydalaniladi. Turli kalitlardan foydalanilganligi bois, shifrlash kalitini oshkor qilsa bo’ladi va shuni uchun ochiq kalitli kriptotizim deb ataladi. Ochiq kalitli kriptotizimlarda shifrlash kaliti *ochiq kalit* deb atalsa, deshifrlash kaliti *shaxsiy kalit* deb ataladi. Simmetrik kalitli kriptotizimlarda esa kalit - *simmetrik kalit* deb ataladi.

2.1.1. Kerkxofs prinsipi

Ideal shifrlar uchun shifrmatndan kalitsiz ochiq matnni tiklashning imkoni bo’lmasligi zarur. Bu shart, hattoki hujumchilar uchun ham o’rinli. Hujumchi algoritm (shifrlash algoritmi) haqidagi barcha ma’lumotlarni bilgan taqdirda ham kalitsiz ochiq matnni tiklashning imkoniga ega bo’lmasligi zarur. Ushbu qo’yilgan maqsad amalda bundan farqli bo’lishi mumkin.

Kriptografiyaning fundamental nazariyasiga ko’ra kriptotizimning ichki ishlash prinsipi hujumchiga to’liq oshkor bo’lishi mumkin. Hujumchiga faqat kriptotizimda foydalanilgan kalit noma’lum bo’lishi zarur. Bu ta’limot *Kerkxofs prinsipi* deb ataladi.

Xo’sh, Kerkxofs prinsipining asosiy mohiyati nimada? Agar hujumchi kriptotizimni qanday ishlashini bilmasa, uning kriptotizimga hujum qilishi yanada qiyinlashadi. U holda, nima uchun xujumchining ishi osonlashtirilmoqda? Kriptotizim xavfsizligi uchun sir tutilgan loyihalashga ishonishning bir nechta muammolari mavjud. Birinchidan, “sir tutilgan” kriptotizimlarning tafsilotlari kamdan-kam hollarda uzoq vaqt sirligicha qoladi. Dasturiy ta’minotdan algoritmni tiklash uchun *teskari muhandislik* usullaridan foydalanish mumkin va ular orqali

hattoki qurilmalarda yozilgan algoritmlarni qayta tiklash (aniqlash) mumkin. Bundan tashqari yana bir muhim jihat shundaki, uzoq vaqt sir tutilgan kriptotizim ommaga oshkor bo'lishi xavfsiz emasligi isbotlangan. Sir tutilgan kriptotizimlar kichik doiradagi foydalanuvchilar (mutaxassislar) tomonidan ishlab chiqilgani va testlanganligi bois, ko'p sonli foydalanuvchilar (ommaga oshkor etilganida) tomonidan testlanishi natijasida uning xavfsiz emasligi ko'p hollarda aniqlangan. Bunga misol sifatida, Microsoft tomonidan kriptotizimlarni ishlab chiqishda Kerkxofs prinsipiga amal qilinmaganligi va buning natijasida teskari muhandislik asosida olingan ma'lumotlarni http://web.elastic.org/~fche/mirrors/cryptome.org/beale-sci-crypt.htm havolasida ko'rish mumkin [13].

2.1.2. Kodlash va shifrlash orasidagi farq

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 foydalaniladi. Masalan, *ASCII, UNICODE, URL Encoding, base64*. Quyidagi 6-rasmda *ASCII* standarti asosida kodlash sxemasi keltirilgan.

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

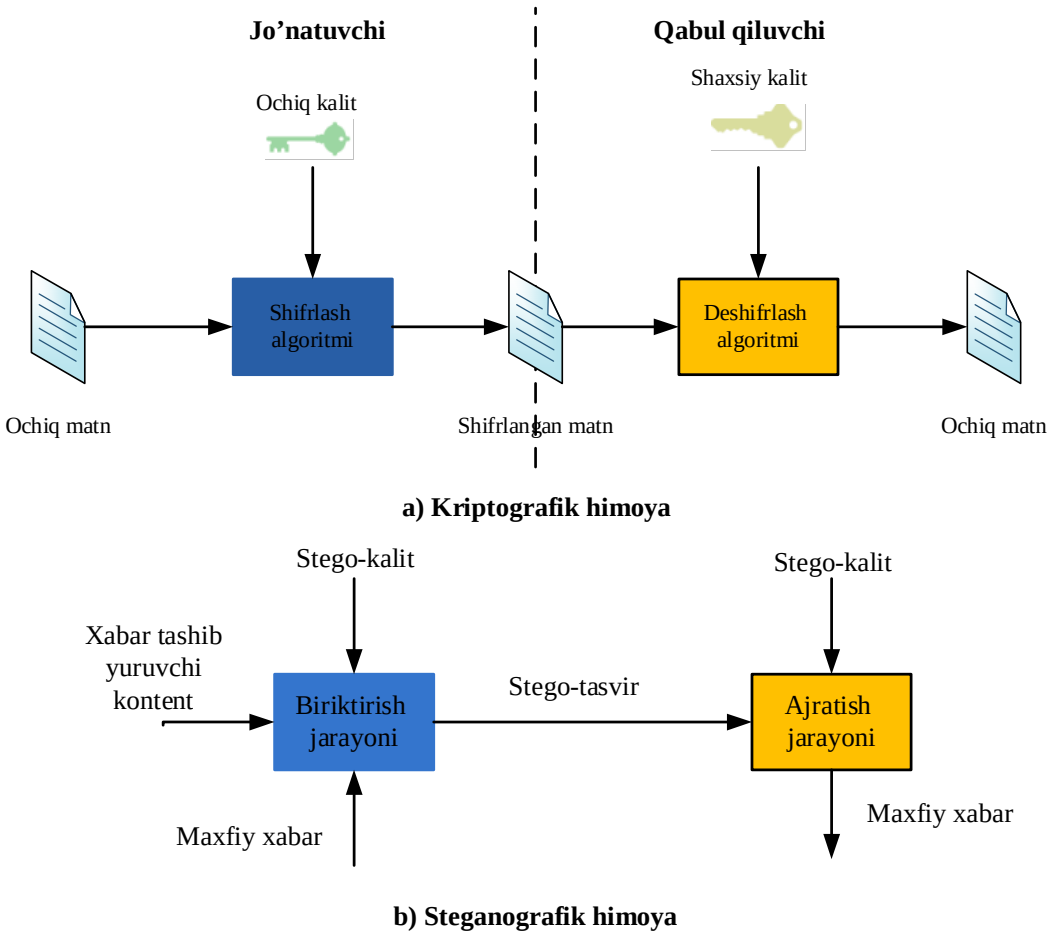
Dekodlash jarayoni ham deshifrlash jarayoni kabi kodlash uchun teskari jarayon hisoblanib, biror ochiq sxema yordamida o'zgartirilgan ma'lumotlar xuddi shu sxema asosida teskarisiga o'zgartiriladi [18]. Masalan, ASCII asosida "Z" ni 16 sanoq tizimiga o'zgartirilganda (kodlaganda) u "5A" ga teng bo'lgan bo'lsa, "5A" ni dekodlash jarayonida u "Z" ga qayta o'zgartiriladi.

Dec	Hex	Oct	Binary	Char		Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char
0	00	000	0000000	NUL	(null character)	32	20	040	0100000	Space	64	40	100	1000000	@	96	60	140	1100000	`
1	01	001	0000001	SOH	(start of header)	33	21	041	0100001	!	65	41	101	1000001	A	97	61	141	1100001	a
2	02	002	0000010	STX	(start of text)	34	22	042	0100010	"	66	42	102	1000010	B	98	62	142	1100010	b
3	03	003	0000011	ETX	(end of text)	35	23	043	0100011	#	67	43	103	1000011	C	99	63	143	1100011	c
4	04	004	0000100	EOT	(end of transmission)	36	24	044	0100100	$	68	44	104	1000100	D	100	64	144	1100100	d
5	05	005	0000101	ENQ	(enquiry)	37	25	045	0100101	%	69	45	105	1000101	E	101	65	145	1100101	e
6	06	006	0000110	ACK	(acknowledge)	38	26	046	0100110	&	70	46	106	1000110	F	102	66	146	1100110	f
7	07	007	0000111	BEL	(bell (ring))	39	27	047	0100111	'	71	47	107	1000111	G	103	67	147	1100111	g
8	08	010	0001000	BS	(backspace)	40	28	050	0101000	(	72	48	110	1001000	H	104	68	150	1101000	h
9	09	011	0001001	HT	(horizontal tab)	41	29	051	0101001	)	73	49	111	1001001	I	105	69	151	1101001	i
10	0A	012	0001010	LF	(line feed)	42	2A	052	0101010	*	74	4A	112	1001010	J	106	6A	152	1101010	j
11	0B	013	0001011	VT	(vertical tab)	43	2B	053	0101011	+	75	4B	113	1001011	K	107	6B	153	1101011	k
12	0C	014	0001100	FF	(form feed)	44	2C	054	0101100	,	76	4C	114	1001100	L	108	6C	154	1101100	l
13	0D	015	0001101	CR	(carriage return)	45	2D	055	0101101	-	77	4D	115	1001101	M	109	6D	155	1101101	m
14	0E	016	0001110	SO	(shift out)	46	2E	056	0101110	.	78	4E	116	1001110	N	110	6E	156	1101110	n
15	0F	017	0001111	SI	(shift in)	47	2F	057	0101111	/	79	4F	117	1001111	O	111	6F	157	1101111	o
16	10	020	0010000	DLE	(data link space)	48	30	060	0110000	0	80	50	120	1010000	P	112	70	160	1110000	p
17	11	021	0010001	DC1	(device control 1)	49	31	061	0110001	1	81	51	121	1010001	Q	113	71	161	1110001	q
18	12	022	0010010	DC2	(device control 2)	50	32	062	0110010	2	82	52	122	1010010	R	114	72	162	1110010	r
19	13	023	0010011	DC3	(device control 3)	51	33	063	0110011	3	83	53	123	1010011	S	115	73	163	1110011	s
20	14	024	0010100	DC4	(device control 4)	52	34	064	0110100	4	84	54	124	1010100	T	116	74	164	1110100	t
21	15	025	0010101	NAK	(negative acknowledge)	53	35	065	0110101	5	85	55	125	1010101	U	117	75	165	1110101	u
22	16	026	0010110	SYN	(synchronize)	54	36	066	0110110	6	86	56	126	1010110	V	118	76	166	1110110	v
23	17	027	0010111	ETB	(end transmission block)	55	37	067	0110111	7	87	57	127	1010111	W	119	77	167	1110111	w
24	18	030	0011000	CAN	(cancel)	56	38	070	0111000	8	88	58	130	1011000	X	120	78	170	1111000	x
25	19	031	0011001	EM	(end of medium)	57	39	071	0111001	9	89	59	131	1011001	Y	121	79	171	1111001	y
26	1A	032	0011010	SUB	(substitute)	58	3A	072	0111010	:	90	5A	132	1011010	Z	122	7A	172	1111010	z
27	1B	033	0011011	ESC	(escape)	59	3B	073	0111011	;	91	5B	133	1011011	[	123	7B	173	1111011	{
28	1C	034	0011100	FS	(file separator)	60	3C	074	0111100	<	92	5C	134	1011100	\	124	7C	174	1111100	|
29	1D	035	0011101	GS	(group separator)	61	3D	075	0111101	=	93	5D	135	1011101	]	125	7D	175	1111101	}
30	1E	036	0011110	RS	(record separator)	62	3E	076	0111110	>	94	5E	136	1011110	^	126	7E	176	1111110	~
31	1F	037	0011111	US	(unit separator)	63	3F	077	0111111	?	95	5F	137	1011111	_	127	7F	177	1111111	DEL

6-rasm. ASCII kodlash standarti

2.1.3. Kriptografiya va steganografiya

Bundan tashqari 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 [18]. Boshqacha aytganda steganografiyaning asosiy g'oyasi – maxfiy ma'lumotlarning mavjudligi haqidagi shubhani oldini olish. Steganografik va kriptografik jarayonlarning umumiy ko'rinishi 7-rasmda keltirilgan.



7-rasm. Kriptografik va steganografik jarayonlar

*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 tutishdir.

2.1.4. Kriptografiyaning asosiy bo'limlari

Kriptografiyani quyidagi bo'limlarga ajratish mumkin:

1. *Simmetrik kalitli kriptografiya.* Simmetrik kalitli kriptografiyaning umumiy ko'rinishi 2.1-rasmdagi kabi bo'lib, ma'lumotni shifrlash va deshifrlashda yagona kalitdan (simmetrik kalitdan) foydalaniladi. Shuning uchun ham simmetrik kalitli kriptotizimlarni – *bir kalitli* kriptotizimlar ham deb yuritiladi. 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 assimetrik kriptografiya deb ham ataladi) ma’lumotni shifrlash qabul qiluvchining *ochiq kaliti* bilan amalga oshirilsa, uni deshifrlash 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 2.3-rasm “a”da keltirilgan. 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 deshifrlashning imkoni mavjud emas. Xuddi shuningdek, shaxsiy kalit bilan ma’lumotni shifrlash imkoni ham mavjud emas. Shifrmatnni deshifrlash esa faqat shaxsiy kalit egasiga joiz. Demak, shaxsiy kalit egasi tomonidan xavfsiz saqlanishi va o’zidan boshqa hyech 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 keltirish mumkin. Quyida “$hello$” xabarini turli xesh funksiyalardagi qiymatlari keltirilgan:

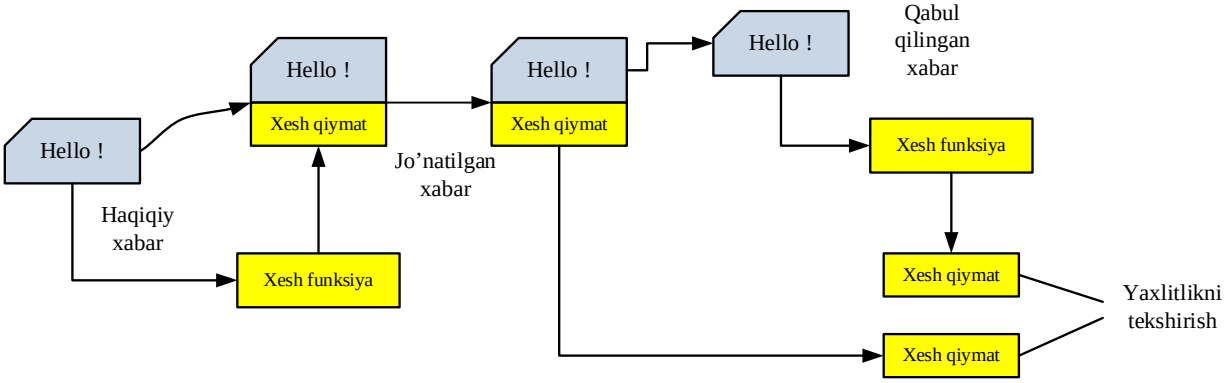
- $MD5(hello) = 5d41402abc4b2a76b9719d911017c592$
- $SHA1(hello) = aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d$
- $SHA256(hello) =$ $2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e7304336$
- $2938b9824$

Xesh funksiyalar quyidagi xususiyatlarga ega [13]:

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'lumot yaxlitligini tekshirishning sodda ko'rinishi 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 solishtiradi. Agar har ikkala xesh qiymat teng bo'lsa, u holda ma'lumotning yaxlitligi o'zgarmagan, aks holda o'zgargan deb topiladi. Odatda xesh funksiyalar kirishda ma'lumotdan tashqari xech qanday qiymatni talab etmagani bois, *kalitsiz kriptografik funksiyalar* deb ham ataladi (kalit talab qiluvchi ma'lumotni yaxlitligini ta'minlash usullari ham mavjud, ular bilan keyingi qismlarda tanishib chiqiladi).



8-rasm. Xesh funksiya asosida ma'lumot yaxlitligini tekshirish

Simmetrik va ochiq kalitli kriptotizimlardan ma'lumotlarning maxfiyligini ta'minlashda, xesh funksiyalardan esa ma'lumotlarni yaxlitligini tekshirishda foydalaniladi.

2.1.5. Kriptografik akslantirishlar

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

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

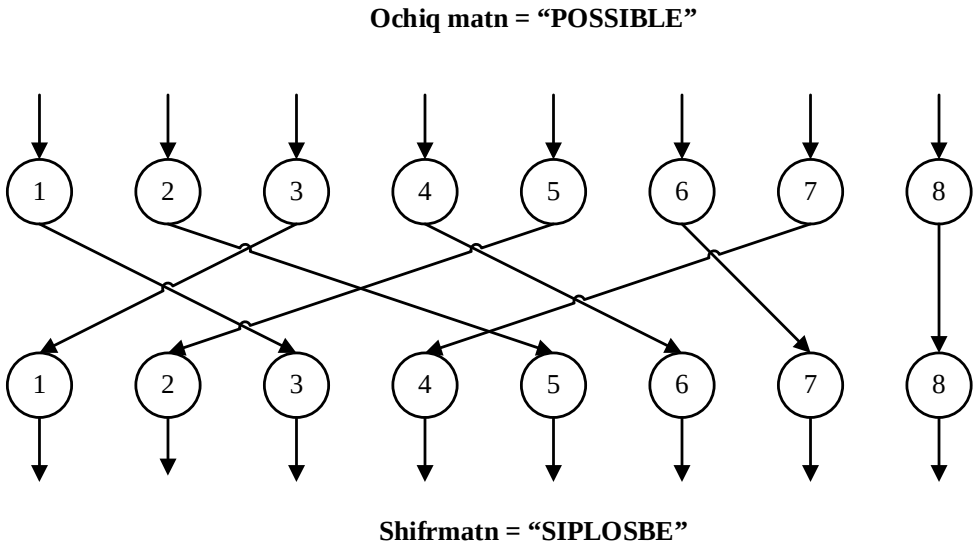
Sodda ko’rinishda olingan o’rniga qo’yish akslantirishi asosida shifrlash uchun olingan matn quyida keltirilgan. Ushbu sodda shifrlash usuli Sezar nomi bilan mashhur. Masalan, agar ochiq matn “HELLO” ga teng bo’lsa, unga mos holda shifrmatn “KHOOR” ga teng bo’ladi. Mazkur holda shifrmatn alifbosi ochiq matn alifbosidan 3 taga surish natijasida hosil qilingan va shuning uchun shifrlash kalitini 3 ga teng deb qarash mumkin. Deshifrlash jarayonida esa shifrmatn simvollari shifrmatn alifbosidan olinib, unga mos ochiq matn alifbosidagi simvolga almashtiriladi. Masalan, shifrmatn “ILUVW” ga teng bo’lsa, unga mos ochiq matn “FIRST” ga teng bo’ladi.

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’rniga qo’yish akslantirishida ochiq matndagi simvollar shifrmatnda bo’lmasligi mumkin. Biroq, ochiq matndagi simvollarning takrorlanish chastotasi shifrmatndagi simvollarda ham bir xil bo’ladi (ko’p alifboli o’rniga qo’yish usullari bundan mustasno). Masalan, yuqoridagi misolda ochiq matndagi “L” simvolining takrorlanish chastotasi 2 ga teng. Uning o’rniga qo’yilgan shifrmatndagi “O”

simvolining ham takrorlanish chastotasi ham 2 ga teng. Bu holat ochiq matndagi qolgan simvollar uchun ham o’rinli. Bu esa ushbu akslantirishni *chastotalar tahlili* usuliga bardoshsizligini anglatadi.

O’rin almashtirish akslantirishi. Ushbu akslantirishga ko’ra, ochiq matn simvollarining o’rni biror qoidaga ko’ra o’zaro almashtiriladi. Bunda ochiq matdga ishtirok etgan simvollar shifrmatnda ham ishtirok etib, faqat ularning o’rni almashgan holda bo’ladi (9-rasm).



9-rasm. Sodda o’rin almashtirish usuliga misol

2.1.6. Kriptografiyaning tarixi

Ma’lumotlarni shifrlashning dastlabki ko’rinishlaridan ming yillar avval foydanib 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 [21]:

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 alifboli o'rniga qo'yishga asoslangan bo'lib, ularga Vijiner, Atbash usullarini misol keltirish mumkin. Ushbu davrdagi shifrlar birinchi davr shifrlariga qaraganda bardoshligi yuqori bo'lgan.
3. *1 va 2 – jaxon urishlari davri (1 va 2- jaxon urishlari davridagi klassik shifrlar).* Ushbu davr kriptotizimlari asosan elektromexanikaga asoslangan bo'lib, radioto'lqin orqali shifrmatnni uzatishni (Morze alifbosi) amalga oshirgan. Mazkur davrga oid shifrlash usullariga Zimmermann telegrammi, Enigma shifri, SIGABA mashinalarini misol keltirish mumkin.
4. *Kompyuter davri (zamonaviy shifrlar).* Ushbu davr shifrlari hisoblash qurilmalariga mo'ljallangan bo'lib, yuqori xavfsizlik darajasiga ega hisoblanadi. Zamonaviy shifrlarga misol sifatida DES, AES, GOST 28147-89, IDEA, A5/1, RC4 (barchasi simmetrik) va RSA, El-Gamal (ochiq kalitli) larni keltirish mumkin.

2.1.7. 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 1 - jadvalda keltirilgan [13]. Alifbo simvollari va ularga mos bit qiymatlari barcha uchun ochiq va sir saqlanmaydi (ASCII jadvali kabi).

1-jadval

Belgilar	E	H	I	K	L	R	S	T
Binar qiymat	000	001	010	011	100	101	110	111

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

H	E	I	L	H	I	T	L	E	R
001	000	010	100	001	010	111	100	000	101

Bir martali bloknot usulida shifrlashda ochiq matn uzunligiga teng bo’lgan tasodifiy tanlangan kalitdan foydalaniladi. Ochiq matnga kalitni XOR amali orqali shifrmatn hosil qilinadi (*R – ochiq matn, K – kalit* va *S – shifrmatn* deb belgilansa): $C = P \oplus K$. XOR amali ($\oplus$) binar amal hisoblanib, 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’ramiz. Shuning uchun bir martali parol bilan deshifrlash uchun shifrmatnga kalitni XOR amalida bajarilishining o’zi yetarli hisoblanadi: $P = C \oplus K$.

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

111 101 110 101 111 100 000 101 110 000

A tomon ushbu kalit asosida shifrmatnni quyidagicha hisoblaydi:

	H	E	I	L	H	I	T	L	E	R
Ochiq matn:	001	000	010	100	001	010	111	100	000	101
Kalit:	111	101	110	101	111	100	000	101	110	000
Shifrmatn:	110	101	100	001	110	110	111	001	110	101

	S	R	L	H	H	H	T	H	S	R

A tomonidan jo’natilgan shifrmatn B tomonda bir xil kalitdan foydalanib osongina deshifrlanadi:

	S	R	L	H	H	H	T	H	S	R
Shifrmatn:	110	101	100	001	110	110	111	001	110	101
Kalit:	111	101	110	101	111	100	000	101	110	000
Ochiq matn:	001	000	010	100	001	010	111	100	000	101
	H	E	I	L	H	I	T	L	E	R

Ushbu shifrlash algoritmi uchun quyidagi ikki holatni qarab chiqish muhim: faraz qilaylik, *A* tomonning dushmani *M* A tomon quyidagi kalitdan foydalangan deb biladi:

101 111 000 101 111 100 000 101 110 000

Agar *M* dushman ushbu kalitni *B* tomonga uzata olsa, u holda *B* tomon shifrmatnni quyidagicha deshifrlaydi:

	S	R	L	H	H	H	T	H	S	R
Shifrmatn:	110	101	100	001	110	110	111	001	110	101
“Kalit”:	101	111	000	101	111	100	000	101	110	000
“Ochiq matn”:	011	010	100	100	001	010	111	100	000	101
	K	I	L	L	H	I	T	L	E	R

Agar *B* tomon kriptografiyadan xabari bo’lmasa, u holda *A* tomonning qarori muhokamaga sabab bo’ladi.

Ikkinchi holat: faraz qilamiz *A* foydalanuvchi dushmani *M* tomonidan qo’lga olindi va shifrmatnga ega bo’ldi. Dushman shifrmatnni o’qiy olmaydi va shuning uchun *A* tomondan uning kalitini talab etadi. *A* tomon o’zini har ikkala tomonga “o’ynashini” aytib, shifrmatni deshifrlash kaliti deb quyidagini aytadi:

111 101 000 011 101 110 001 011 101 101

Ushbu kalit orqali dushman *M* shifrmatnni deshifrlaganda quyidagi ochiq matn hosil bo’ladi:

	S	R	L	H	H	H	T	H	S	R
Shifrmatn:	110	101	100	001	110	110	111	001	110	101
“Kalit”:	111	101	000	011	101	110	001	011	101	101
“Ochiq matn”:	001	000	100	010	011	000	110	010	011	000
	H	E	L	I	K	E	S	I	K	E

Agar dushman kriptografiya haqida ma’lumotga ega bo’lmasa, ushbu ochiq matnga ishonadi va *A* tomonni qo’yib yuboradi.

Yuqoridi keltirilgan misollar bir martali bloknot shifrini *bardoshli* ekanini ko’rsatadi. Bir martali bloknotda agar kalit tasodifiy tanlansa va bir marta foydalanilgan taqdirda hujumchi shifrmatndan ochiq matn haqida biror axborotga ega bo’la olmaydi (albatta ma’lumotning uzunligidan tashqari). Ya’ni, berilgan shifrmatn uchun mos “kalit” yordamida shifrmatn uzunligidagi ixtiyoriy “ochiq matnlar”ni generasiyalash mumkin va bunda barcha ochiq matnlar bir xil o’xshashlikka ega. Shuning uchun shifrmatndan ochiq matn haqida biror foydali axborotni olishning imkoni yo’q. Kriptografiya nuqtai nazardan shifrmatnlar o’zidan ortiq ma’lumotni bera olmaydi.

Buning uchun albatta, bir martali bloknotdan to’g’ri foydalanish, kalitni tasodifiy tanlash va undan bir marta foydalanilish hamda faqat A va B tomonlarga ma’lum bo’lishi talab etiladi.

Bir martali bloknot yuqori bardoshlikni ta’minlashiga qaramasdan, har doim undan foydalanilmaydi. Sababi, har bir ochiq matn uchun uning uzunligiga teng bo’lgan tasodifiy kalitni (bloknotni) generasiyalash va uni qabul qiluvchiga xavfsiz uzatishning kafolati yo’qligi. Agar ochiq matn uzunligidagi kalitni (bloknotni) xavfsiz uzatishning imkoniyati mavjud bo’lsa, u holda kalitning o’rniga ochiq matnni uzatish foydali emasmi? Uni shifrlashdan nima ma’no?

Bir martali bloknot usulidan tarixda cheklangan uzunlikdagi ma’lumotlarni shifrlashda qisman foydalanilgan bo’lsada, hozirgi kundagi katta hajmli ma’lumotlarni uzatish uchun bir martali bloknotni to’liq amaliy tomondan qo’llab bo’lmaydi.

Bir martali bloknotda kalitlardan faqat bir marta foydalanishdan maqsad nima? Faraz qilaylik, quyidagi ikki ochiq matn P_1 va P_2 bitta kalit K dan foydalanib shifrlangan: $C_1 = P_1 \oplus K$ va $C_2 = P_2 \oplus K$. Kriptografiyada ushbu holatni “xavflilik” deb ataladi va bir martali bloknot xavfli holatda deb tushuniladi. Ya’ni, foydalanilgan kalit ortiq muammo tug’dirmaydi:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Mazkur holda shifrmatn haqiqiy ochiq matn xususida ba’zi axborotni oshkor qiladi. Agar bir kalitdan foydalanib ko’p marta shifrlash amalga oshirilsa bu katta xavfga olib kelishi mumkin. Mazkur holat quyidagi misolda ko’rib chiqilgan. Faraz qilaylik, quyidagi ikkita ochiq matn berilgan bo’lsin (belgilarning binar kodi yuqoridagi jadvaldagi kabi):

$P_1 = LIKE = 100\ 010\ 011\ 000$ va $P_2 = KITE = 011\ 010\ 111\ 000$.

Har ikkala ochiq matn yagona kalit $K = 110\ 011\ 101\ 111$ yordamida shifrlangan va shifrmatnlar quyidagiga teng bo’lgan:

	L	I	K	E
P_1:	100	010	011	000
K:	110	011	101	111
C_1:	010	001	110	111
	I	H	S	T

va

	K	I	T	E
P_2:	011	010	111	000
K:	110	011	101	111
C_2:	101	001	010	111
	R	H	I	T

Agar hujumchi kriptotahlil bilan yaqindan tanish bo’lsa va har ikkala ochiq matn bir xil kalit yordamida shifrlanganini bilsa, ochiq matnlardagi 2- va 4-simvollarning bir xilligini osongina aniqlaydi. Sababi, mos o’rindagi shifrmatn simvollari bir xil. Bundan tashqari, hujumchi taxminiy P_1 ochiq matn oladi va uni to’g’riligini P_2 ochiq matn bilan tekshirib ko’radi. Faraz qilaylik, hujumchi birinchi

ochiq matn sifatida $P_1 = KILL = 011\ 010\ 100\ 100$ ni olgan bo'lsin. Bu holda u ochiq matnga mos taxminiy kalitni quyidagicha hisoblaydi:

	K	I	L	L
Taxminiy P_1:	011	010	100	100
C_1:	010	001	110	111
Taxminiy K:	001	011	010	011

Olingan kalit K yordamida esa ikkinchi shifrmatndan ochiq matnni hisoblaydi:

C_2:	101	001	010	111
Taxminiy K:	001	011	010	111
Taxminiy P_2:	100	010	000	100
	L	I	E	L

Hisoblangan kalit K ikkinchi ochiq matn P_2 uchun mos bo'lmagani sababli, hujumchi taxmin qilgan birinchi ochiq matni P_1 ni noto'g'riligini biladi. Shu tarzda hujumchi qachonki birinchi ochiq matnni $P_1 = LIKE$ tarzida taxmin qilsa, ikkinchi ochiq matnni to'g'ri $P_2 = KITE$ topa oladi.

2.1.8. Kodlar kitobi

Kodlar kitobi ko'rinishidagi klassik shifrlash birinchi jahon urushi davrida ommalashgan. Kodlar kitobi lug'atga o'xshash bo'lib, so'zlar (ochiq matn so'zlari)dan va unga mos bo'lgan kod so'zlar (shifrmatn)dan tashkil topgan. Shifrlash uchun ushbu kodlar kitobidan zarur bo'lgan so'z aniqlanadi va unga mos bo'lgan kod so'z shifrmatn sifatida olinadi. Deshifrlashda esa ushbu jarayonning teskarisi amalga oshiriladi. Ya'ni, kodlar kitobidan shifrmatndagi kod so'z topiladi va ochiq matn sifatida unga mos bo'lgan so'z tanlanadi. Birinchi jahon urushi davrida Nemislar tomonidan foydalanilgan kodlar kitobi na'munasi quyidagi jadvalda keltirilgan [13].

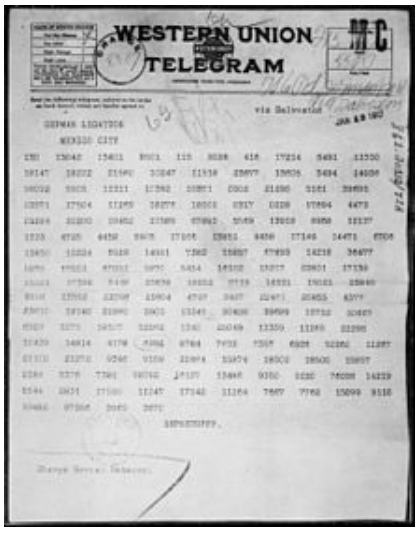
2-jadval

Kodlar kitobidan olingan na’muna

Ochiq matn	**Shifrmatn**
Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
⋮	⋮

Masalan, “Februar” so’zini shifrlash uchun butun so’z 5-simvolli kod so’z 13605 bilan almashtirilgan. Kodlar kitobi shifrlash uchun, deshifrlash uchun esa kod so’zlar ustuni bo’yicha tartiblangan kod so’zlar kitobidan foydalanilgan. Kod so’zlar kitobi o’rniga qo’yish akslantirishiga asoslangan bo’lib, bunda bir simvol emas balki butun so’z, ba’zida esa butun ibora o’rniga kod so’z qo’yilgan.

2-jadvalda keltirilgan kod so’zlar mashhur Zimmermann telegrammini shifrlash uchun foydalanilgan. 1917 yil birinchi jaxon urushi davrida, Germaniya tashqi ishlar vaziri Artur Zimmerman Germaniyaning Meksikadagi elchisiga shifrlangan ko’rinishdagi telegramma yuboradi. 10-rasmda keltirilgan shifrlangan xabar Britaniyaliklar tomonidan tutib olinadi. Bu vaqtda Britaniya va Fransiya Germaniya bilan urush va AQSh bilan betaraf holatida edi.



10-rasm. Zimmerman telegrammi

Ruslar Nemislarning kodlar kitobini zararlangan versiyasini tiklab, uni Britaniyaga yuboradi. Murakkab tahlillardan so’ng, Britaniyaliklar Zimmerman telegrammi yozilgan vaqtidagi kodlar kitobining bo’shliqlarini to’ldirishadi va uni deshifrlashadi. Telegrammda aytilishicha, Germaniya hukumati cheklanmagan suvosti urushi boshlashni rejalashtirayotgani va bu AQSh bilan urushga olib kelishi mumkinligi haqida mulohazalar borligi bayon etilgan. Shu sababli, Zimmerman o’z elchisiga Meksikani AQShga nisbatan urushda Germaniya ittifoqchisi bo’lishga undashi kerakligini aytadi. Xususan, Meksikani Texas, Yagni Meksika va Arizona shtatlaridagi hududlarini qaytarib olishga undagan. AQShda ushbu telegramma oshkor bo’lgandan so’ng, jamoatchilik Germaniyaga qarshi turadi. Shundan so’ng, AQSh urushga kiradi. Zimmerman telegrammini to’liq deshifrlangan ko’rinishi 11-rasmda keltirilgan [22].

We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.
Signed, ZIMMERMANN

11-rasm. Zimmerman telegrammining deshifrlangan ko’rinishi

2.2. Simmetrik kriptografik algoritmlar

Quyida simmetrik kriptotizimlar, shuningdek ularning ikki tarmog’i: *oqimli* va *blokli* simmetrik shifrlash algoritmlariga to’xtalib o’tiladi. Simmetrik shifrlash algoritmlarida ma’lumotlarni shifrlash va deshifrlashda yagona kalitdan foydalaniladi. Ular ma’lumotlarni shifrlash va deshifrlash jarayonlarini amalga oshirish tartibi bilan farq qilib, foydalanilayotgan tizim xususiyatidan kelib chiqqan holda tanlanadi.

Simmetrik kriptotizimlarning ishlashi bilan tanishishda quyidagi belgilanishlarni aniqlab olamiz:

- ochiq matn P ni simmetrik kalit K bilan shifrlash: $C = E(P, K)$;
- shifrmatn C ni simmetrik kalit K bilan deshifrlash: $M = D(C, K)$.

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

2.2.1. Oqimli simmetrik shifrlash algoritmlari

Oqimli simmetrik shifrlash algoritmi bir martali bloknotga asoslangan bo'lib, undan farqli jihati – bardoshligi yetarlicha past va boshqariladigan kalitga asoslanishi. Ya'ni, kichik uzunlikdagi kalitdan ochiq matn uzunligiga teng bo'lgan ketma-ketlik hosil qilinadi va bir martali bloknot sifatida foydalaniladi.

Oqimli shifr n bitli kalit K ni qabul qiladi va ochiq matnni uzunligiga teng bo'lgan ketma – ketlik S ga uzaytiradi. Ketma – ketlik S esa ochiq matn P bilan XOR amalida bajariladi va shifrmatn C hosil qilinadi. Bu o'rinda ketma-ketlikni qo'shish bir martali bloknotni qo'shish kabi bir xil bo'ladi.

Oqimli shifrni quyidagicha sodda ko'rinishda yozish mumkin:

$$StreamCipher(K) = S$$

Bu yerda K kalit, S esa natijaviy ketma-ketlik. Shuni esda saqlash zarurki, bu yerda 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, mos bitlarni XOR amali orqali shifrmatn 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 deshifrlash uchun, yana ketma-ketlik S dan foydalaniladi:

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

Yuboruvchi 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 bunda asosiy e’tibor amaliy tomondan qo’llashga qaratiladi.

2.2.2. A5/1 oqimli shifrlash algoritmi

Ushbu oqimli shifrlash algoritmi GSM mobil aloqa tizimlarida ma’lumotni konfidensialligini ta’minlash uchun foydalaniladi. Mazkur algoritm algebraik tuzilishga ega bo’lsada, uni sodda diagramma bilan ham tasvirlash imkoniyati mavjud.

A5/1 shifrlash algoritmi uchta *chiziqli siljitish registr*laridan iborat bo’lib, ular mos holda X, Y va Z kabi belgilanadi. X registr o’zida 19 bit $(x_0, x_1, \dots, x_{18})$, Y registr esa 22 bit $(y_0, y_1, \dots, y_{21})$ va Z registr esa 23 bit $(z_0, z_1, \dots, z_{22})$ ma’lumotni saqlaydi. Uchta registrlarning mazkur o’lchamdagi bitlarni saqlashi bejiz emas. Sababi, chiziqli siljitish registrlari o’zida jami bo’lib 64 bitni saqlaydi. Shu sababli, A5/1 shifrlash algoritmida foydalaniluvchi kalit K ning uzunligi 64 bitga teng bo’ladi va ushbu kalit uchta registrni dastlabki to’ldirish uchun foydalaniladi. Shundan so’ng, oqimli shifrlash algoritmi talab etilgan uzunlikdagi (ochiq matn uzunligiga teng bo’lgan) ketma-ketliklarni generasiyalaydi. Ketma-ketliklarni generasiyalash tartibini o’rganishdan oldin, uchta registrlar haqida ba’zi ma’lumotlarni bilish talab etiladi.

X registr siljigan vaqtida, quyidagi amallar ketma-ketligi bajariladi:

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$$

$$i = 18,17,16, \dots ,1 \text{ uchun } x_i = x_{i-1}$$

$$x_0 = t$$

Shunga o’xshash, Y va Z registrlar uchun ham quyidagilar bajariladi:

$$t = y_{20} \oplus y_{21}$$

$$i = 21,20,19, \dots ,1 \text{ uchun } y_i = y_{i-1}$$

$$y_0 = t$$

va

$$t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$$

$$i = 22,21,20, \ldots, 1 \text{ uchun } z_i = z_{i-1}$$

$$z_0 = t$$

Berilgan uchta bit x, y va z uchun $maj(x, y, z)$ funksiyasi eng ko'p bitni qaytaradi. Agar x, y va z bitlar 0 ga teng bo'lsa, u holda funksiya 0 ni qaytaradi, aks holda birni qaytaradi. 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 generasiyalash uchun quyidagilar bajariladi. Dastlab, $m = maj(x_8, y_{10}, z_{10})$ funksiya qiymati hisoblanadi.

Shundan so'ng 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.

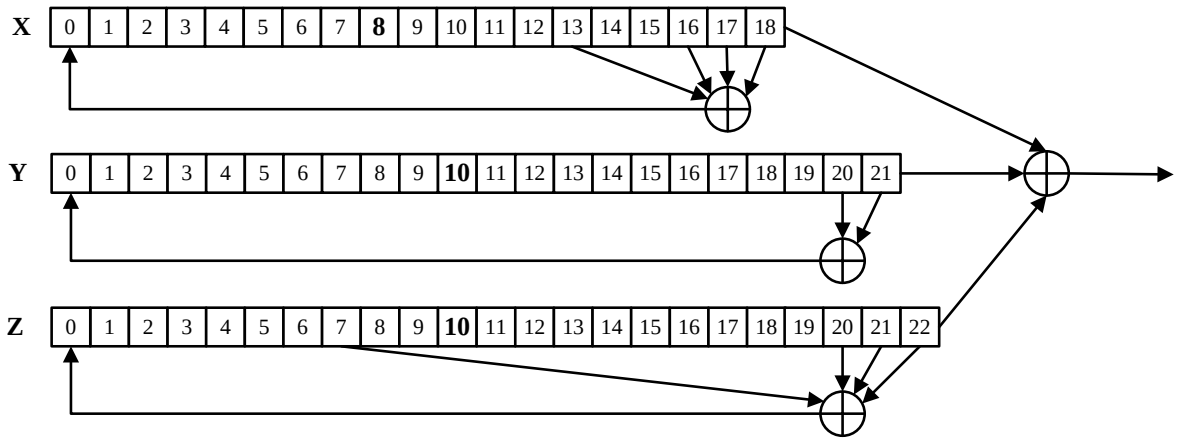
Shundan so'ng, ketma-ketlikning bir biti s quyidagicha generasiyalanadi va ochiq matn biti bilan XOR amali bajariladi (agar shifrlansa) yoki shifrmatn biti bilan XOR amali bajariladi (agar deshifrlansa).

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

Yuqorida keltirilgan ketma-ketlikdagi amallar talab etilgunga qadar takrorlanadi (ochiq matn yoki shifrmatn uzunligiga teng).

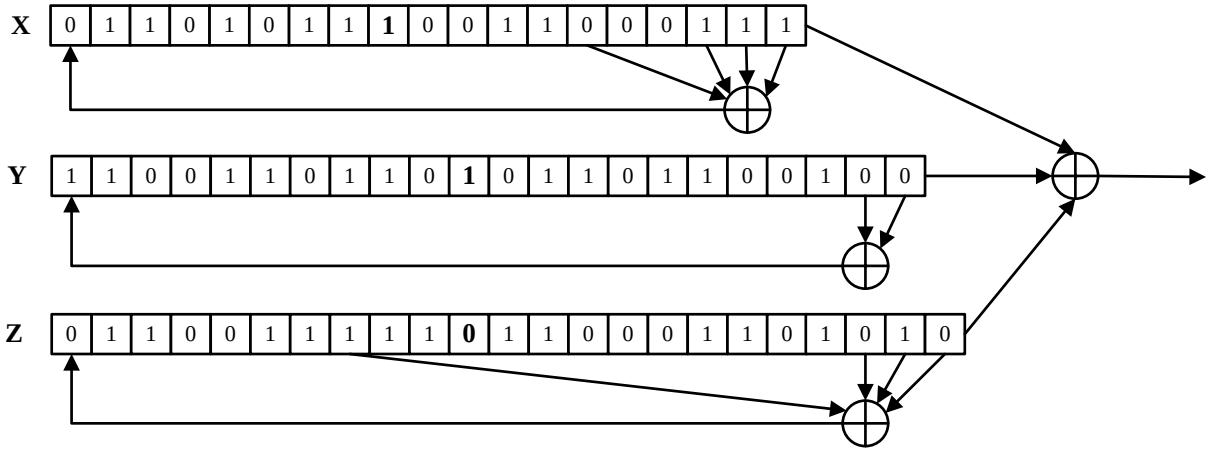
Agar biror registr siljitilsa, uning to'liq holati siljish natijasida o'zgaradi. Ketma-ketlikning bir bitini hosil qilishda uchta registrdan kamida ikkitasi siljiydi va shuning uchun yuqoridagi ketma-ketlikni davom ettirgan holda yangi bitlar ketma-ketligini hosil qilish mumkin bo'ladi.

A5/1 oqimli shifrlash algoritmi murakkab ko'rinsada, qurilmada amalga oshirilganida yuqori tezlik qayd etadi. Umumiy holda A5/1 oqimli shifrni 12 - rasmdagi kabi ifodalash mumkin.



12 -rasm. A5/1 ketma-ketlik generatori

Misol. Faraz qilamiz, 64 bitli kalit K ni X, Y va Z registorlariga bo'lib, yozish natijasi quyidagicha bo'lsin (13 - rasm).



13 - rasm. A5/1 ketma-ketlik generatori

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

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18} = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$

$$i = 18,17,16, \dots ,1 \text{ uchun } x_i = x_{i-1}$$

$$x_0 = 1$$

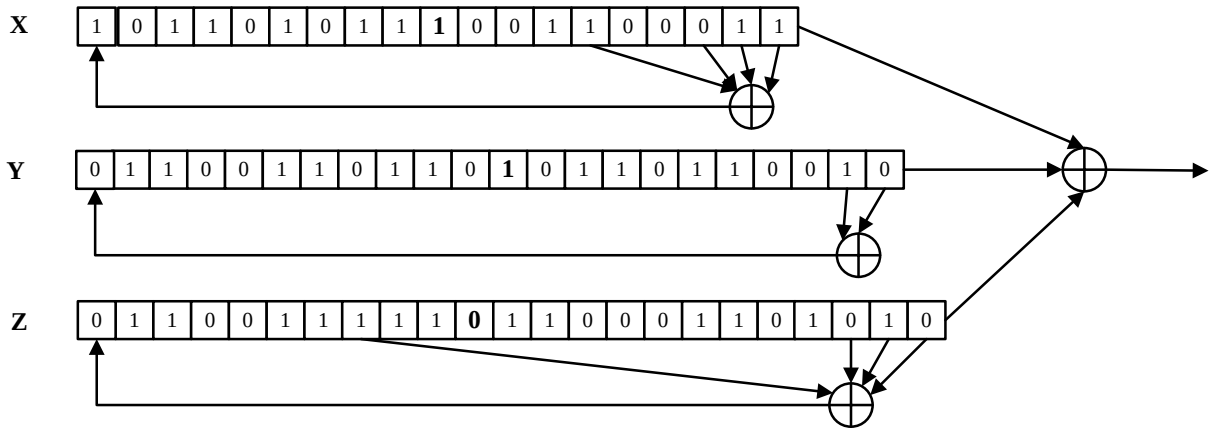
Shunga o'xshash, Y registr uchun ham quyidagilar bajariladi:

$$t = y_{20} \oplus y_{21} = 0 \oplus 0 = 0$$

$$i = 21,20,19, \dots ,1 \text{ uchun } y_i = y_{i-1}$$

$$y_0 = 0$$

X va *Y* registrlari siljiganidan keyingi holat esa quyidagicha bo’ladi (14 - rasm):



14 - rasm. A5/1 ketma-ketlik generatori

Siljigan holatdan so’ngi registrlar holatidan generasiyalangan bir bit $s = x_{18} \oplus y_{21} \oplus z_{22} = 1 \oplus 0 \oplus 0 = 1$ bo’ladi. Shu tartibda, talab etilgan bitlar ketma-ketligi generasiyalanadi.

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’plashi talab etiladi. Bu esa so’zlashuvda to’xtalishga olib keladi. Bundan tashqari, ma’lumotni shifrlab uzatish jarayonida shifrmatnga 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 oshirilish imkoniyatiga ega.

2.2.3. Blokli simmetrik shifrlash algoritmlari

Takroriy amalga oshiriluvchi blokli shifrlash ochiq matnni cheklangan uzunlikdagi bloklarga ajratadi va shifrmatnning cheklangan uzunlikdagi bloklarini hosil qiladi. Aksariyat blokli simmetrik shifrlar loyihasida, shifrmatn - ochiq matnni funksiya F orqali biror miqdordagi *raund*lar soni davomida takroran bajarish 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 yaratishdagi asosiy maqsad – bu 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. Ular orasida quyidagi tarmoqlar amalda keng qo'llaniladi [19]:

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

Feystel tarmog'i - bu aynan bir blokli shifr hisoblanmay, simmetrik blokli shifrni loyihalashning umumiy prinsipi sanaladi. Feystel tarmog'iga ko'ra ochiq matn bloki P teng ikki 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 *kalit generatori* algoritmi orqali

hisoblanadi. Yakuniy, shifrmatn bloki C esa oxirgi raund natijalariga teng bo'ladi, ya'ni:

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

Feystel tarmog'ida deshifrlash 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, deshifrlangan matnni beradi: $P = (L_0, R_0)$.

Har bir raundda foydalaniluvchi Feystel tarmog'ining F funksiyasi qaytuvchi (teskari funksiyasiga ega) bo'lishi talab etilmaydi. Biroq, olingan har qanday F funksiya to'liq xavfsiz bo'la olmaydi.

2.2.4. TEA blokli shifrlash algoritmi

TEA (Tiny Encryption Algorithm) algoritmi Feystel tarmog'iga asoslanmagan bo'lsada, sodda va unga o'xshash algoritm. Boshqacha aytganda, shifrlash va deshifrlash funksiyalari bir-biridan farq qiladi.

TEA algoritmida 64-bit uzunlikdagi ochiq matn bloklari va 128 bitli kalitdan foydalaniladi. Algoritm 32 bitli so'zlar bilan amallar bajarishga mo'ljallangan va shuning uchun $mod 2^{32}$ amalidan foydalaniladi. Ushbu algoritmda raundlar soni o'zgaruvchan bo'lib, xavfizlik nuqtai nazaridan raundlar soni kamida 32 ga teng qilib olinishi shart. TEA algoritmining har bir raundi Feystel tarmog'ining ikki raundiga o'xshash.

Blokli shifrlarni loyihalashda raund funksiyasining murakkabligi va raundlar soni orasida balans bo'lishi lozim. Masalan, raund funksiyasi sodda bo'lsa, raundlar soni kamroq yoki aksincha bo'ladi. TEA algoritmi sodda algoritm bo'lgani uchun, bardoshli bo'lishi uchun raundlar sonini katta tanlash zarur. TEA algoritmining shifrlash funksiyasi quyida keltirilgan [13].

$(K[0], K[1], K[2], K[3]) = 128$ bitli kalit

$(L, R) =$ ochiq matn bloki (64 bit)

$delta = 0x9e3779b9$

$sum = 0$

$for\ i =$ 1 dan 32 gacha

$sum = sum + delta$

$L = L + (((R \ll 4) + K[0]) \oplus (R + sum) \oplus ((R \gg 5) + K[1]))$

$R = R + (((L \ll 4) + K[2]) \oplus (L + sum) \oplus ((L \gg 5) + K[3]))$

keyigi i

shifrmatn $= (L, R)$

Bu yerda "≪" amali sonni chapga surish amali va "≫" amali uni o'nga surish amali hisoblanadi. Masalan, ikkilik ko'rinishdagi bir baytli son "10110101" ga teng bo'lsa, u holda ushbu sonni chapga 4 birlik surish natijasi "01010000" ga teng bo'ladi. Ushbu sonni 5 birlik o'nga surish natijasi esa "00000101" ga teng bo'ladi.

TEA algoritmi Feystel tarmog'iga asoslanmagan bo'lsada (Feystel tarmog'ida shifrlash va deshifrlash funksiyalari bir xil bo'ladi), deshifrlashda XOR amali o'rniga qo'shish yoki bo'lish amallaridan foydalanilmaydi. TEA algoritmining deshifrlash funksiyasi quyida keltirilgan.

$(K[0], K[1], K[2], K[3]) =$ 128 bitli kalit

$(L, R) =$ shifr matn bloki (64 bit)

$delta = 0x9e3779b9$

$sum = delta \ll 5$

$for\ i =$ 1 dan 32 gacha

$R = R - (((L \ll 4) + K[2]) \oplus (L + sum) \oplus ((L \gg 5) + K[3]))$

$L = L - (((R \ll 4) + K[0]) \oplus (R + sum) \oplus ((R \gg 5) + K[1]))$

$sum = sum - delta$

keyigi i

ochiq matn $= (L, R)$

2.2.5. Blokli shifrlar rejimlari

Oqimli shifrlardan foydalanish juda ham sodda – ochiq matn (yoki shifrmatn) uzunligiga teng bo'lgan kalitlar ketma-ketligi generasiya qilinadi va XOR amalida bajariladi. Blokli shifrlardan foydalanish faqat bir blokni shifrlashda oson. Biroq, bir nechta (ko'plab) bloklarni shifrlash qanday amalga oshiriladi? Javob esa, bir qaraganda oson emas.

Faraz qilaylik, quyidagi ochiq matn bloklari berilgan bo'lsin: $P_0, P_1, P_2, \ldots$ O'zgarmas kalit K uchun blokli shifr kodlar kitobi hisoblanadi. Sababi, blokli shifrlar ochiq matn bloki va shifrmatn bloki o'rtasida o'zgarmas bog'lanishni yaratadi. Kodlar kitobi kabi foydalaniluvchi blokli shifrlash rejimi bu – *elektron kodlar kitobi (Electronic codebook mode, ECB)* rejimi. ECB rejimida quyidagi formuladan foydalangan holda ma'lumotlar bloklari shifrlanadi:

$$i = 0,1,2, \ldots \text{lar uchun } C_i = E(P_i, K)$$

Deshifrlash uchun esa quyidagi formuladan foydalaniladi:

$$i = 0,1,2, \ldots \text{lar uchun } P_i = D(C_i, K)$$

Ushbu yondashuv asosida blokli shifrlarni samarali amalga oshirsa bo'ladi. Biroq, mazkur yondashuvda jiddiy xavfsizlik muammosi mavjud.

Faraz qilaylik, ECB rejimdan foydalangan holda ma'lumot shifrlandi va tarmoq orqali uzatildi. Uzatish davomida hujumchi ularni tutib oldi va shifrmatn bloklari orasidan ikkitasining bir-biriga tengligini ($C_i = C_j$) aniqladi. Natijada hujumchi aniqlagan shifrmatn bloklariga mos ochiq matn bloklari ham bir-biriga teng bo'ladi $P_i = P_j$. Albatta ushbu holat shifrmatnni topish uchun yetarli bo'lmasada, bir shifrmatn blokiga mos kelgan qolgan bloklarni aniqlash imkoniyatini beradi. Bunday hollarda hujumchi haqiqatan P_i yoki P_j ochiq matn bloklarini aniqlay olmasada, unga aloqador ba'zi ma'lumotni oshkor etadi. Mazkur holat grafik orqali tasvirlanganda 15-rasmda ko'rsatilganidek bo'ladi [13]. Boshqacha aytganda, rasmning chap tomonidagi tasvirning o'xshash har bir bloki o'ng qismida ham bir xil shifrmatn blokiga almashgan. Mazkur holda hujumchining

shifrmatndan foydalangan holda ochiq matnni bashorat qilishi murakkab vazifa emas.

15-rasm. ECB rejimida ma’lumotni shifrlash natijasi

Biroq, ECB rejimida shifrlash va deshifrlash amallarini paralellashtirish imkoniyati mavjud va bu tezkorlikni oshiradi. Bundan tashqari agar shifrmatnni uzatish davomida bloklardan birining o’zgarishi faqat shu blokni natijasiga ta’sir qiladi. Ya’ni, faqat shu blokni o’zi zararlanadi.

ECB rejimida mavjud muammolarni bartaraf etgan rejimlardan biri bu - *cipher block chaining* (CBC) rejimi. CBC rejimida bir blokdan chiqqan shifrmatn keyingi ochiq matnni yashirish uchun foydalaniladi va shundan so’ng shifrlash amalga oshiriladi. Mazkur rejimda shifrlash formulasi quyidagicha:

$$i = 0,1,2, \dots \text{lar uchun } C_i = E(P_i \oplus C_{i-1}, K)$$

Deshifrlash funksiyasi esa quyidagicha bo’ladi:

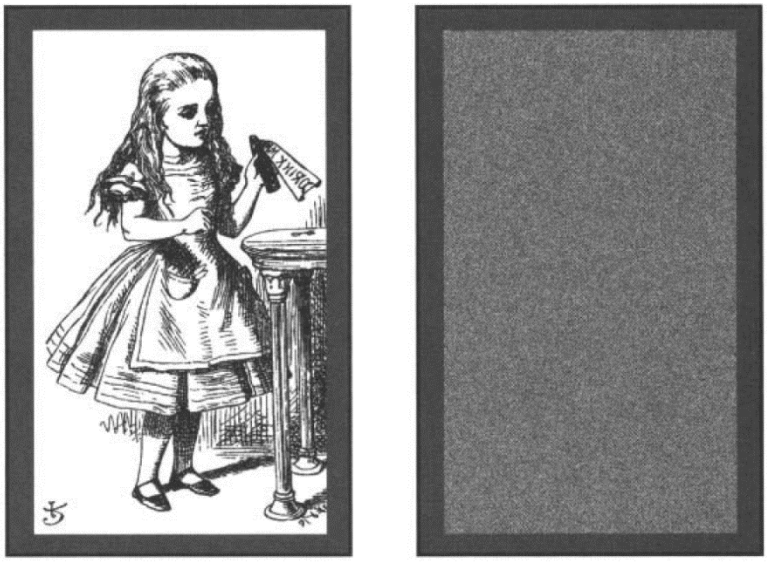
$$i = 0,1,2, \dots \text{lar uchun } P_i = D(C_i, K) \oplus C_{i-1}$$

Birinchi blokni shifrlash uchun undan oldingi shifrmatn bloki bo’lmagani uchun, boshlang’ich vektor deb ataluvchi (initialization vector, IV) IV dan foydalaniladi va u mantiqiy tomondan C_{-1} ga teng bo’ladi. Shifrmatn bloklari maxfiy saqlanmagani bois unga analog bo’lgan IV ham maxfiy saqlanmaydi. Biroq, IV tasodifiy ravishda generasiya qilinishi shart.

IV dan foydalangan holda, birinchi blokni shifrlash quyidagicha amalga oshiriladi: $C_0 = E(P_0 \oplus IV, K)$.

Mos holda birinchi blokni deshifrlash esa quyidagicha amalga oshiriladi: $P_0 = D(C_0, K) \oplus IV$.

CBC rejimida ma’lumotlarni shifrlash ECB rejimidan farqli ravishda bir xil ochiq matn bloklari turli shifr matn bloklariga almashinadi. Mazkur holat grafik orqali tasvirlanganda 16-rasmda ko’rsatilgandek bo’ladi [13].



16-rasm. CBC rejimida shifrlash natijasi

Agar CBC rejimidan foydalanib shifrlangan ma’lumotni uzatish davomida biror bitga o’zgarish bo’lsa, yakuniy holat qanday bo’ladi (hozirda bunday holatlar kam uchraydi)? Faraz qilaylik, shifrmatnning C_i bloki zararlandi: $C_i = G$. U holda

$$P_i \neq D(G, K) \oplus C_{i-1} \text{ va } P_{i+1} \neq D(C_{i+1}, K) \oplus G$$

Biroq,

$$P_{i+2} = D(C_{i+2}, K) \oplus C_{i+1}$$

va qolgan bloklar to’g’ri deshifrlanadi. Ya’ni, bir blokning zararlanishi ikkita blokga ta’sir ko’rsatadi. Undan keyingi bloklar esa o’zgarmas saqlanadi.

Simmetrik blokli shifrlash algoritmlari oqimli shifrlash algoritmlariga qaraganda yuqori hisoblash imkoniyatini talab etadi va shunga mos ravishda yuqori bardoshlikni ta’minlaydi. Simmetrik blokli shifrlash algoritmlari oqimli shifrlar kabi ma’lumot konfidensialligini ta’minlash uchun foydalaniladi. Bundan tashqari, blokli shifrlardan autentifikasiya masalalarida, ma’lumot yaxlitligini ta’minlashda keng qo’llaniladi.

2.2.6. Simmetrik kriptotizimlardagi muammolar

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

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

2.2.7. Simmetrik kriptotizimlarda kalit uzunligi

Amalda foydalanish uchun 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-jadvalda turli uzunlikdagi kalitlarni bo’lishi mumkin bo’lgan barcha variantlarini hisoblash uchun turli qiymatdagi qurilmalardan foydalanganda sarflanadigan vaqt keltirilgan. Ko’rsatilgan natijalar 2005 yildagi narx asosida keltirilgan [20].

3-jadval

Qurilma narxi	Kalit uzunligi		
	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

2.3. Ochiq kalitli kriptotizimlar

Simmetrik kriptotizimlardagi mavjud muammolardan biri – maxfiy kalitni xavfsiz uzatish va saqlash. Quyida kalitlarni uzatish va xavfsiz saqlash bilan bog'liq muammolarni bartaraf etgan, assimetrik yoki ochiq kalitli deb ataluvchi kriptotizimlar bilan tanishib chiqiladi.

Ochiq kalitli kriptotizimlarda maxlumotni shifrlash bir kalit bilan amalga oshirilsa (ochiq kalit deb ataladi), uni deshifrlash boshqa bir kalit (shaxsiy kalit deb ataladi) bilan amalga oshiriladi. Shuning uchun, ochiq kalitli kriptotizimlar simmetrik kriptotizimlarda mavjud bo'lgan kalitlarni taqsimlash muammosini o'zida bartaraf etgan. Biroq, ochiq kalitli kriptografik tizimlarning ham o'ziga xos muammosi 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 olish mumkin. Ya'ni, tub bo'lgan ikkita p va q sonlarni generasiyalash va $N = p * q$ ni hisoblash oson. Biroq, N soni yetarlicha katta bo'lganda 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, C shifrmatn 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 shifrlab yuborishi mumkin. Shifrlangan xabarni ochish faqat shaxsiy kalit egasi bo’lgan B tomonga joiz.

2.3.1. Modul arifmetikasi

Ochiq kalitli kriptotizimlarni chuqur o’rganishdan oldin ularning asosi hisoblangan sonlar nazariyasi bilan yaqindan tanishib chiqish muhim hisoblanadi. Ochiq kalitli kriptotizimlar asosan modul arifmetikasiga asoslangani bois, dastlab ularga 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’ladi. 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 talab etiladi.

Misol tariqasida, 3 sonining 7 maydondagi 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 juda ham ko'p vaqt talab etiladi).

Ushbu muammoni yechishning ko'plab usullari mavjud bo'lib, quyida ulardan biri bo'lgan qoldiqlar to'g'risidagi *Yevklidning kengaytirilgan algoritmi*dan foydalanib yechish usuli keltirilgan.

Kengaytirlgan Yevklid algoritmi. Kengaytirlgan Yevklid algoritmi RSA kriptotizimi ochiq kaliti «*ye*» - ni topishda $d * e \equiv 1 (mod_{\varphi}(n))$ tenglamaga duch kelinib, uni yechish bevosita $ax + by = d,\ \ d = \text{EKUB}(a, b)$ tenglamaning butun yechimlarini topish masalasiga ekvivalent hamda bu algoritmga ko'ra berilgan a – soniga modn bo'yicha teskari elementni topish imkonini beradi. Shuning uchun ham bu algoritm ishlash prinsiplarini keltirish muhim.

Teorema. Aytaylik, a va b natural sonlar, $d = \text{EKUB}(\text{a}, b)$ bo'lsin. U holda shunday α va β butun sonlar topiladiki

$$\alpha * \text{a} + \beta * b = d$$

tenglik o'rinli bo'ladi.

Demak, bu algoritm nafaqat ikkita natural sonning EKUBini, balki yoyilmadagi α va β koeffisentlarni ham topish imkonini berar ekan. Shunisi bilan ham aslida Yevklid algoritmidan farqlanadi.

Kengaytirilgan Yevklid algoritmiga muvofiq topiladigan α va β butun sonlar, quyidagi Diafant tenglamasining

$$\alpha * \text{a} + \beta * b = d$$

butun yechimlari hisoblanadi. Bundan RSA algoritmining ochiq kalitiga ko'ra maxfiy kalitini hisoblashda foydalanish mumkin. Shu sababli bu algoritm ishlash qadamlari bilan yaqindan tanishib chiqiladi.

Faraz qilaylik, a va b sonlarning EKUBni topishda quyidagi ketma-ketlik qaralayotgan bo'lsin:

$$a = b*q_1 + r_1 \qquad r_1 = ax_1 + by_1;$$

$$b = r_1 * q_2 + r_2 \qquad r_2 = ax_2 + by_2;$$

$$r_1 = r_2 * q_3 + r_3 \qquad r_3 = ax_3 + by_3;$$

$$\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots\ldots$$

$$r_{n-3} = r_{n-2} * q_{n-1} + r_{n-1} \qquad r_{n-1} = ax_{n-1} + by_{n-1}$$

$$r_{n-2} = r_{n-1} * q_n \qquad r_n = 0;$$

Bu yerda,

$x_1, x_2, \ldots x_{n-1}$ va $u_1, u_2 \ldots\ldots y_{n-1}$

sonlarini topish kerak bo'lsin. Bu sonlar quyidagi formula yordamida topiladi:

$$x_j = x_{j-2} - q_j x_{j-1} \quad va \quad u_j = y_{j-2} - q_j y_{j-1}$$

bu yerda,

$$x_{-1} = 1 , u_{-1} = 0 , x_0 = 0 , u_0 = 1.$$

Kerakli ma'lumotlarni quyidagi jadval orqali aniqlash mumkin:

qoldiqlar	bo'luvchi	x	U
a	*	x_{-1}	u_{-1}
b	*	x_0	y_{-1}
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
r_3	q_3	x_3	y_3
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
r_{n-2}	q_{n-2}	x_{n-2}	y_{n-2}
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}

Jadvalning oxirgi ustunida keltirilgan ikki qiymat izlanayotgan alfa va beta koeffisentlar, yani $\alpha = x_{n-1}$, $\beta = u_{n-1}$ bo'ladi.

Misol. Yevklid algoritmini qo'llab EKUB (6188,4709) va α, β - qiymatlar topilsin.

Yevklid algoritmi qadamlariga muvofiq:

$6188=4709*1+1479$, ya'ni $r_1=1479$

$4709=1479*3+272$, ya'ni $r_2=272$

$1479=272*5+119$, ya'ni $r_3=119$

$272=119*2+34$, ya'ni $r_4=34$

$119=34*3+17$, ya'ni $r_5=17$

$34=17*2+0$, ya'ni $r_6=0$

demak,

$r_5=17$

soni 6188 va 4709 sonlarining EKUBi deb e'lon kilinadi, ya'ni

EKUB (6188, 4709)=17 .

Kengaytirilgan Yevklid algoritmiga ko'ra:

$6188*\alpha + 4709 * \beta = 17$

$\alpha = ?, \beta = ?$ topilsin:

yuqorida keltirilgan ifodani quyidagicha yozish mumkin:

$17=119 - 34*3$

$34=272 - 119*2$

$119=1479 - 272*5$

$272=4709 - 1479*3$

$1479=6188 - 4709*1$

yoki:

$17= 119 - 3* (272 - 119*2)=7*119 - 3*272=7* (1479 - 272*5) - 3*272=$

$=7*1479 - 38*272=7*1479 - 38* (4709 - 1479*3)=121*1479 - 38*4709=$

$=121* (6188 - 4709) - 38*4709=121*6188 - 159*4709$,

Ya'ni,

$6188*121+4709* (- 159)=17$; demak, $\alpha=121$; $\beta= - 159$

Javob: $\alpha=121$, $\beta= - 159$.

Misol. $3^{-1}mod7 \equiv x$ ni topish talab etilgan bo'lsin. Yuqorida keltirilgan algoritmga ko'ra

$7 = 3 * 2 + 1$

$3 = 1 * 3 + 0$

Qoldig'i nolga teng bo'lgan tenglikdan oldingi tenglikdan boshlab quyidagicha teskari yozish amalga oshiriladi:

$1 = 7 - (3 * 2) = 7 + (-2 * 3) = 7 * 1 + (-2 * 3)$

Yuqoridagi tenglikni ikki tomonini modulga ($mod7$) olinsa quyidagi tenglikga ega bo'linadi: $\big((7 * 1)mod7 + (-2 * 3)mod7\big)mod7 \equiv 1mod7$ yoki $(-2 * 3)mod7 \equiv 1mod7 \equiv 1$. Ushbu tenglikni $(3 * x)mod7 \equiv 1$ taqqoslash orqali $x = -2$ ga tengligini yoki $-2mod7 = 5$ ligini topish mumkin. Ya'ni, $(3 * 5)mod7 \equiv 1$ tenglikni qanoatlantiradi.

Javob 3^{-1} (mod 7) $= 5$.

2.3.2. RSA algoritmi

RSA nomi algoritmni yaratuvchilari familiyalarining birinchi harflaridan olingan (Rivest, Shamir va Adleman). RSA algoritmi modul arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan [20].

RSA algoritmida ochiq va shaxsiy kalitlar juftini generasiya qilish 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 sonlarning (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 deshifrlash 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

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

S ni deshifrlash 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 deshifrlansa, $M = C^d \ mod \ N = \ M^{ed} \ mod \ N$ tenglik to'g'riligini isbotlash zarur.

Eyler teoremasi. Agar x haqiqiqatdan n bilan o'zaro tub bo'lsa, $x^{\varphi(n)} = 1 \ mod \ n$ bo'ladi. Bu yerda, $\varphi(n)$ – funksiya, n dan kichik va u bilan o'zaro tub bo'lgan sonlar miqdorini ko'rsatadi. Agar n soni tub bo'lsa, $\varphi(n) = n - 1$ bo'ladi.

Shuning uchun $ed = 1 \ mod \ \varphi(N) = 1 \ mod \ (p-1)(q-1)$ tenglik kabi yozish mumkin. Mazkur tenglikning to'liq shakli aslida $ed = 1 \ mod \ \varphi(N) + k \ \varphi(N)$ ga teng. Ya'ni, ed ko'paytmani $\varphi(N)$ ga bo'lganda k tadan tegib, bir qoldiq qolgan. Shuning uchun ushbu tenglikni quyidagicha yozish mumkin:

$$ed - 1 = k \ \varphi(N).$$

Ushbu tengliklardan, RSA algoritmining to'g'ri ishlashini tasdiqlash mumkin:

$$C^d = M^{ed} = M^{(ed-1)+1} = M * M^{ed-1} = M * M^{k\,\varphi(N)} = M * 1^k = M \ mod \ N.$$

Aytaylik, RSA algoritmida ma'lumotni shifrlash va deshifrlash 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 ($e = 3$) ga teng deb olish mumkin. Sababi, 3 soni $\varphi(N) = 20$ bilan o'zaro tubdir. Shundan so'ng, Evklidning kengaytirilgan algoritmi asosida deshifrlash 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 esa $d = 7$ ga teng.

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 deshifrlash 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. Boshqacha aytganda, RSA algoritmini buzishning faktorlash muammosini yechishdan tashqari biror usuli aniqlanmagan.

2.3.3. Ochiq kalitli kriptotizimlardan foydalanish

Ochiq kalitli kriptografik tizimlardan foydalanish masalasini ko’rib chiqishdan oldin, quyidagi belgilashlarini amalga oshirish maqsadga muvofiq.

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

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

Bundan esa quyidagi tenglikni osonlik bilan yozish mumkin: $[\{M\}_A]_A = M$. Boshqacha aytganda, M xabarni A tomoning ochiq kaliti bilan shifrlab, keyin aynan shu tomonning shaxsiy kaliti bilan deshifrlash amalga oshirilsa, yana o’sha xabar hosil bo’ladi.

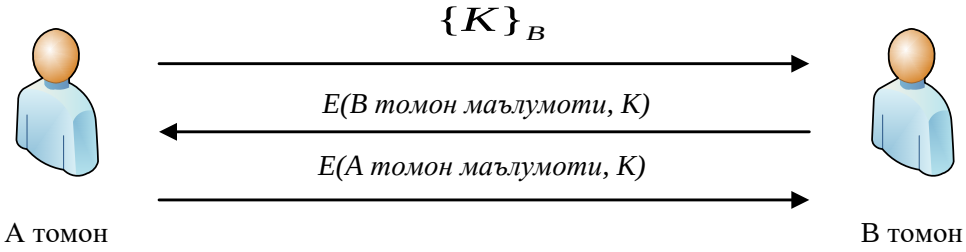
Simmetrik shifrlar bilan bajargan ixtiyoriy amalni, ochiq kalitli shifrlash algoritmlari bilan ham amalga oshirish mumkin. Biroq, jarayon ko’proq vaqt talab

etadi. Masalan, tarmoqda ma’lumotni uzatishda va xavfsiz bo’lmagan muhitda axborot konfidensialligini ta’minlashda simmetrik shifrlash algoritmlarining o’rniga ochiq kalitli kriptografik tizimlardan foydalanish mumkin.

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

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

Har ikkala kriptotizimning afzalliklarini birlashtirish imkoniyati mavjudmi? Ya’ni, ma’lumotni shifrlashda yuqori samaradorlikka ega bo’lgan 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’lumotning o’zi esa simmetrik shifrlash orqali himoyalanadi. Gibrid kriptotizim sxemasi 17-rasmda aks ettirilgan.



17-rasm. Gibrid kriptotizim

2.3.4. 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 (4-jadval).

4-jadval

Simmetrik va ochiq kalitli kriptotizimlar bir xil bardoshlikka ega bo'lganida ulardagi kalitlarning uzunliklari [20]

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.

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 [20].

5-jadval

RSA algoritmidagi N modulning turli uzunligida faktorlash uchun talab etilgan 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	$3*10^{20}$

Yuqoridagi keltirilgan ma'lumotlardan ko'rish mumkinki, hisoblash qurilmalari imkoniyatining ortishi kriptografik algoritmlarning bardoshligini

kamayishiga olib keladi. Bu ta’sir har ikkala simmetrik va ochiq kalitli kriptotizimlarga tegishli.

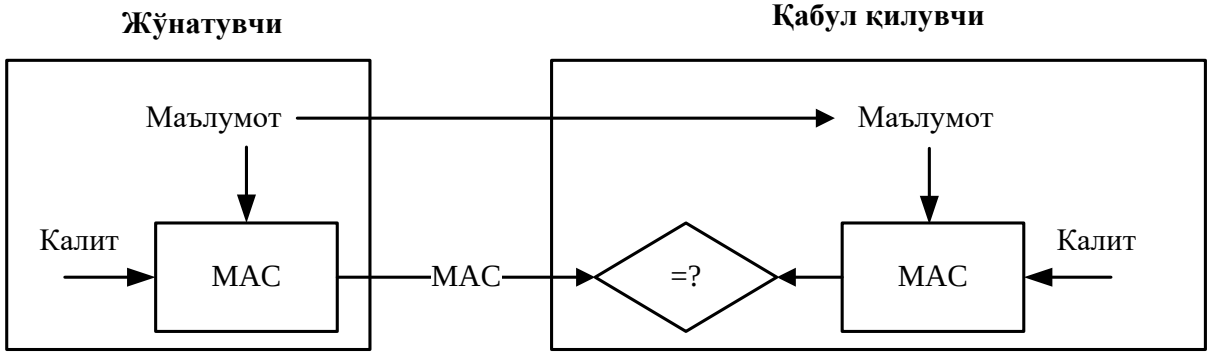
2.4. Ma’lumot yaxlitligini ta’minlash usullari

2.4.1. Simmetrik shifrlash algoritmlaridan ma’lumot yaxlitligini tekshirish

Yuqorida har ikkala shifrlash algoritmidan (simmetrik va ochiq kalitli) faqat ma’lumotni konfidensiyalligini ta’minlashda foydalanish haqida aytib o’tildi. Quyida esa ulardan ma’lumotni yaxlitligini tekshirishda foydalanish masalasi bilan tanishib o’tiladi.

2.1-paragrafda xesh – funksiyadan foydalanib ma’lumotni yaxlitligini tekshirishning sodda usuli keltirilgan. Biroq, ushbu usulda xavfsizlik muammosi jiddiy bo’lgani bois, undan amalda foydalanilmaydi. Ya’ni, 8-rasmda keltirilgan usulda hujumchi tomonidan faqat ma’lumot o’zgartirilgan holda yaxlitlikni tekshirish imkoniyati mavjud. Biroq, hujumchi ma’lumot xesh qiymatini almashtirish orqali foydalanuvchini osonlik bilan ma’lumot yaxlitligiga ishontirishi mumkin. Buning asosiy sababi, ma’lumot xesh qiymatini hosil qilishda hujumchining noma’lum biror axborotdan foydalanilmaganligidir.

Ushbu muammoni bartaraf etuvchi – *xabarlarni autentifikasiyalash kodi (message authentication code, MAC)* tizimlari mavjud bo’lib, unga ko’ra biror maxfiy kalit asosida ma’lumotning xesh qiymati hisoblanadi (18-rasm).



18-rasm. MAC tizimi

MAC tizimlarini ishlab chiqishda blokli shifrlardan ham foydalanish mumkin. Buning uchun blokli shifrni CBC rejimida foydalanish va eng oxirgi shifrmatn

blokini olishning o’zi yetarli (qolganlari tashlab yuboriladi). Ushbu oxirgi shifrmatn bloki *MAC* sifatida xizmat qiladi. Mazkur holda N blokdan iborat bo’lgan ma’lumot bloklari, $P_0, P_1, P_2, \dots, P_{N-1}$ uchun MAC quyidagi formula orqali hisoblanadi [13]:

$$C_0 = E(P_0 \oplus IV, K), C_1 = E(P_1 \oplus C_0, K), \dots, C_{N-1} = E(P_{N-1} \oplus C_{N-2}, K) = MAC.$$

Buning uchun har ikkala tomonda IV va K ni bo’lishining o’zi yetarli.

Faraz qilaylik, A va B tomonlardan uzatilayotgan ma’lumotlar yaxlitligini tekshirish talab etilgan bo’lsin (bu yerda ma’lumot konfidensialligini ta’minlash masalasi qaralmagan). Bu holda A va B tomonlar orasida xavfsiz taqsimlangan K kalit yordamida A tomon MAC ni hisoblaydi va ma’lumotni IV ga qo’shib B ga uzatadi. B tomon ma’lumot, K va IV yordamida MAC ni hisoblaydi. Agar hisoblangan MAC qabul qilingan MAC' ga teng bo’lsa, ma’lumot o’zgartirilmagan aks holda o’zgartirilgan deb topiladi.

Qanday qilib, ikkita hisoblangan MAC qiymatlar turlicha bo’lishi mumkin? Faraz qilaylik, A tomon quyidagilarni B ga yuborgan bo’lsin:

$$IV, P_0, P_1, P_2, P_3, MAC.$$

Faraz qilaylik, hujumchi birinchi blok P_1 ni o’zgartirdi (u Q deb belgilansin), bu holda B tomon MAC ni quyidagicha hisoblaydi:

$$C_0 = E(P_0 \oplus IV, K), \acute{C}_1 = E(Q \oplus C_0, K), \acute{C}_2 = E\left(P_2 \oplus \acute{C}_1, K\right), \acute{C}_3 = E\left(P_3 \oplus \acute{C}_2, K\right) = "MAC" \neq MAC.$$

Ya’ni, ochiq matndagi bir blokning o’zgarishi keyingi barcha bloklarga ta’sir qiladi va buning natijasida shifrmatn bloklari turlicha bo’ladi. Ma’lumki, CBC rejimida shifrmatndagi bir blok o’zgarishi deshifrlanganda faqat 2 ta ochiq matn blokiga ta’sir qiladi. Biroq, ochiq matnning bir blokini o’zgarishi undan keyingi barcha shifrmatn bloklariga ta’sir qiladi va bu MAC tizimlari uchun juda muhim.

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

2.4.2. 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 MAS* (hashed MAC yoki HMAC) mavjud.

Bunga ko’ra, xesh qiymatn 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’lumotni xeshlashda bloklarga ajratadi. 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. Olingan kalit (K) uzunligi ham blok uzunligiga keltiriladi. Bunda 3 ta holat bo’lishi mumkin: (1) agar kalitning uzunligi 64 baytga teng bo’lsa, hyech 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 tomonidan blok uzunligiga yetguncha nollar bilan to’ldiriladi. Shu tariqa, kalit uzunligi blok uzunligiga moslashtiriladi.

Quyidagi $ipad$ va $opad$ o’zgaruvchilar quyidagicha hosil qilinadi:

$$ipad = 0x36 \text{ ni } B \text{ marta takrorlash natijasida}$$

$$opad = 0x5c \text{ ni } B \text{ marta takrorlash natijasida}$$

Bu holda HMAC quyidagicha hisoblanadi:

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

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.

2.4.3. Ochiq kalitli shifrlash algoritmlari asosida ma’lumot yaxlitligini tekshirish va rad-etishdan himoyalash

Mazkur bo’limda ochiq kalitli kriptotizimlar va xesh funksiyalar asosida ishlovchi – *elektron raqamli imzo* tizimlari 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 identifikasiya qilish imkoniyatini beradigan imzo”.

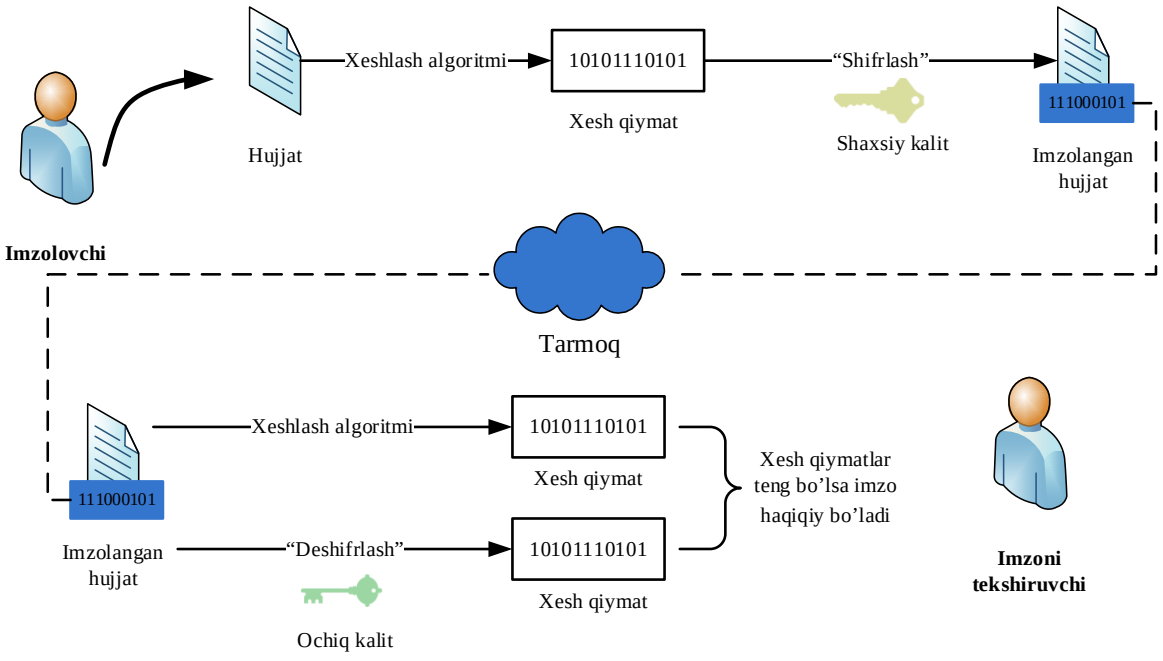
Elektron raqamli imzo oddiy qo’lda qo’yiluvchi imzo kabi bo’lib, faqat elektron hujjatlarda qo’yiladi va imzo qo’yilgan ma’lumotning yaxlitligini ta’minlaydi va imzolovchini qo’yilgan imzodan bosh tortmasligini (rad etmasligini) kafolatlaydi. Axborot xavfsizligida *rad etish* muammosi mavjud bo’lib, unga ko’ra foydalanuvchi hujjatni imzolaganini rad etadi (ya’ni, men imzolamadim deb turib

oladi). Mazkur muammoni oldini olish uchun aynan elektron raqamli imzo tizimlari foydalaniladi.

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

MAS 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 “deshifrlash” uchun esa tomonning ochiq kalitini bilishning o’zi yetarli. Demak, oddiy imzo tizimiga o’xshash (oddiy imzo tizimida bir kishi imzo qo’yadi va qolganlar uning haqiqiyligini tekshirishi talab etiladi) ERI tizimida ham shaxsiy kalit egasi xabarni imzolaydi, qolganlar esa uni ochiq kalitidan foydalangan holda 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 deshifrlash kabi). ERI tizimlari ikkita jarayondan iborat: *ERIni shakllantirish* va *ERIni tekshirish* (19-rasm).



19-rasm. ERI sxemasi

ERIni shakllantirish jarayoni. Faraz qilaylik, A tomondan M xabarni imzolash talab etilsin. Buning uchun xabar M ning xesh qiymati hisoblanadi: $H = h(M)$. Shundan so'ng, 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 "deshifrlaydi" (bu haqiqiy deshifrlash emas, shunchaki ochiq kalit bilan S ustida biror amal bajarishdan iborat) va H ni hosil qiladi. Agar ikki xesh qiymatlar (H va H') o'zaro teng bo'lsa, ERI to'g'ri deb topiladi (demak xabar yaxlit), aks holda esa yo'q.

Rad – etishdan himoyalashni tushunishdan oldin, MAS asosida yaxlitlikni ta'minlashga biror sodda misol olaylik. 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'tgandan 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? Ya'ni, 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.

2.4.4. Ochiq kalitli shifrlash algoritmlari asosida ma’lumot konfidensialligini ta’minlash va rad-etishdan himoyalash

Faraz qilaylik, A va B tomonlarda ochiq kalitli kriptotizimlardan foydalanish imkoniyati mavjud hamda A tomon B tomonga M xabarni yuborishni istaydi. Agar konfidensiallikni ta’minlash uchun A tomoni B tomonning ochiq kaliti bilan xabar M ni shifrlasa, yaxlitlikni ta’minlash va rad etishdan himoyalash uchun A tomon shaxsiy kaliti bilan M xabarga imzo qo’yadi. Agar, A tomon ma’lumotning konfidensialligini ta’minlash va rad etishdan himoyalanishini istasa A tomon shunchaki shifrlash yoki imzolash bilan muammoni yecha olmaydi.

Bir qarashda A tomon M xabarga birinchi imzo qo’yib, so’ng shifrlashi va B tomonga yuborishining o’zi yetarlidek tuyuladi, ya’ni:

$$\{[M]_A\}_B$$

Yoki, birinchi shifrlab keyin imzolash A tomon uchun yaxshidek ko’rinadi, ya’ni:

$$[\{M\}_B]_A$$

Yuqoridagilardan qaysi biri masalaga to’g’ri yechim bo’la olishligini aniqlash uchun quyidagi misollar ko’riladi [60].

Birinchi misol. Faraz qilaylik, A va B tomonlar orasida ishqiy munosabat bo’lsin va A tomon B tomonga quyidagi xabarni yuborishga qaror qildi:

$$M = "I\ love\ you"$$

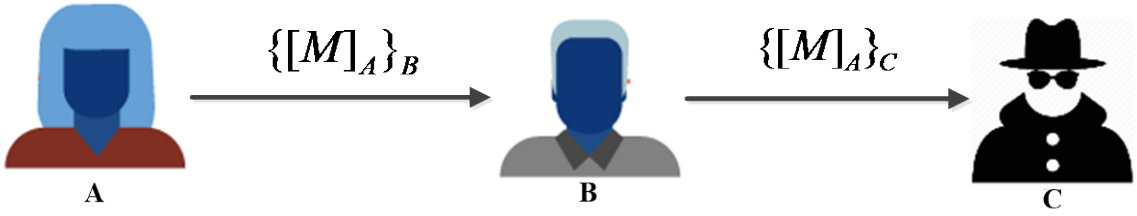
Buning uchun u birinchi imzolash va keyin shifrlash ketma-ketligidan foydalanib B ga quyidagini yuboradi:

$$\{[M]_A\}_B$$

Shundan so’ng, A va B tomonlar orasida kichik kelishmovchilik kelib chiqadi va B tomon janjal boshlamoqchi bo’lsin. Buning uchun qabul qilingan xabarni deshifrlaydi va $[M]_A$ ga ega bo’ladi va uni uchinchi C tomonning ochiq kalitidan foydalanib shifrlaydi va C tomonga yuboradi (20-rasm):

$$\{[M]_A\}_C$$

Albatta mazkur holda, C tomon A tomon uni yaxshi ko'rarkan deb o'ylaydi va bu ikkala, A va S tomonlar uchun muammo tug'dirishi aniq. B tomon esa bundan o'z maqsadida foydalanadi.



20-rasm. Imzo qo'yish va shifrlash sxemasining muammosi

Mazkur holatdan xulosa chiqargan A tomon konfidensiallikni ta'minlash uchun imzolash va shifrlash sxemasi mos emasligini biladi. Shuning uchun bunday holatlarda shifrlash va keyin imzolash sxemasidan foydalanishga qaror qiladi.

Ma'lum vaqtdan so'ng, A va B tomonlar o'zaro kelishib olishadi. Shundan so'ng, A tomon bir yangi nazariyani yaratdi va B tomonga uzatishi talab etilsin. Mazkur holatda xabar quyidagicha bo'lsin:

$$M = "Brontosauruses\ are\ thin\ at\ one\ end, much\ much\ thicker\ in\ the\ middle, then\ thin\ again\ at\ the\ other\ end"$$

A tomon xabarni yuborishda shifrlash va imzolash sxemasidan foydalandi:

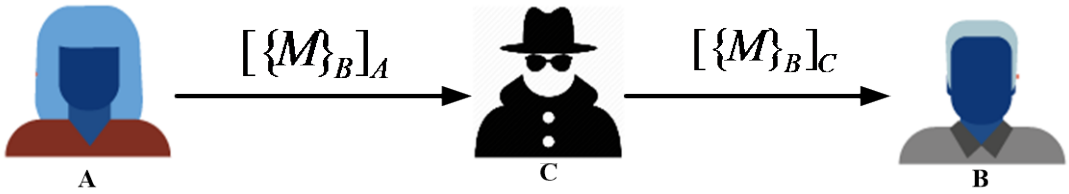
$$[\{M\}_B]_A$$

Bu vaqtda kelib, C tomon A va B tomonlar bilan hanuzgacha xafa va ulardan "o'ch olishni" istaydi hamda A va B tomonlar orasida joylashib, barcha o'tuvchi xabarlarni to'sib qoladi. Bundan tashqari, C tomon A tomon shu kunlarda bir yangilik ustida ish olib borayotganidan xabardor. Shuning uchun A tomondan uzatiladigan har bir xabarni muhim deb hisoblaydi. Xususan, C tomon A tomondan uzatilgan shifrlangan va imzolangan xabarni muhim deb hisoblaydi va uni tutib oladi. Shundan so'ng, shifrlangan xabar $\{M\}_B$ ga o'z nomidan imzo qo'yadi (21-rasm):

$$[\{M\}_B]_C$$

B tomon mazkur xabarni qabul qilgandan so'ng, uni C tomon yuborganini aniqlaydi va deshiflagandan so'ng C tomon haqiqatda yangi nazariyani yaratgan deb

hisoblaydi va C tomonni rag’batlantiradi. Bu holatda, A tomon shifrlash va imzolash sxemasi ham o’rinli emasligini aniqlaydi.



21-rasm. Shifrlash va imzolash sxemasidagi muammo

Birinchi misolda, C tomon $\{[M]_A\}_C$ ni A dan C ga kelgan deb o’yladi. Bu esa to’g’ri fikr emas. Sababi, C tomonning ochiq kaliti barchaga ma’lum va u bilan ixtiyoriy kishi biror ma’lumotni shifrlab yuborishi mumkin.

Ikkinchi misolda esa, B tomon $[\{M\}_B]_C$ xabarning haqiqiy muallifini C tomon deb o’ylaydi. Biroq, bu o’rinda ham B tomonning ochiq kaliti barchaga ochiq bo’lgani uchun, ixtiyoriy kishi shifrlab yuborishi mumkin. C tomon shifrmatnga imzo qo’ygan bo’lsada, u ma’lumotni C tomon shifrlaganini anglatmaydi.

Har ikkala holda ham asosiy muammo, qabul qiluvchi ochiq kalitli kriptotizimlar aslida qanday ishlashini bilmasligidadir. Ochiq kalitli kriptotizimlar bilan bog’liq bo’lgan cheklanishlar mavjud. Bular ochiq kalit bilan ixtiyoriy kishi ma’lumotni shifrlay olishi yoki imzoni ixtiyoriy kishi tekshira olishidir. Shuning uchun, ochiq kalitli kriptotizimlardan foydalanganda mavjud holatni e’tiborga olish tavsiya etiladi.

2.4.5. Ochiq kalitlar infratuzilmasi (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 infratuzilmasi*dan foydalaniladi.

Ochiq kalitlar infratuzilmasi 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 bo'lib, quyida ularning ayrim tashkil etuvchilari va PKI ning asosiy vazifalari bayon etiladi.

Raqamli sertifikat (yoki ochiq kalit sertifikati yoki qisqacha sertifikat) foydalanuvchining ismi va uning ochiq kalitidan iborat bo'ladi (amalda foydalanuvchiga va sertifikatga tegishli ma'lumotlar ham bo'ladi) va u *sertifikat markazi (certificate authority* yoki *CA)* tomonidan imzolanadi [13]. Masalan, A tomonning sertifikati quyidagidan iborat bo'ladi:

$M = (\text{A tomon nomi}, A \text{ tomonning ochiq kaliti})$ 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 generasiyalaydi. Shaxsiy kalit A tomonga taqdim etilgandan 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 ni ochiq kalitini (ya'ni, unga teng bo'lgan sertifikatni) bilishni talab etadi. Demak, CA tomonning ochiq kaliti (yoki sertifikati) oldindan foydalanilayotgan tizimda mavjud va bu haqida barcha ma'lumotga ega bo'ladi.

2.5. Disklarni va fayllarni shifrlash

Axborotni kriptografik himoyasi, hususan, shifrlash algoritmlari amalda keng qo'llaniladi. Masalan, saqlash qurilmalarida ma'lumotlarni shifrlash yoki tarmoq bo'ylab uzatiladigan axborotni shifrlab uzatishni misol tarzda keltirish mumkin.

Umuman olganda ma’lumotni shifrlashda ma’lum algoritmdan foydalaniladi. Ushbu algoritm biror bir operasion tizim 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 [23]:

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

Apparat-dasturiy shifrlash – shifrlash jarayoni bo’lib, buning uchun maxsus ishlab chiqilgan hisoblash qurilmasidan foydalaniladi. Unga misol tariqasida, ruToken USB shifrator qurilmasini ko’rsatish mumkin (22 - rasm).

22-rasm. Turli ko’rinishdagi ruToken USB shifrator qurilmasi

ruToken USB shifrator qurilmasi – Rossiya Federasiyasida ishlab chiqariluvchi qurilma bo’lib, undan asosan Rossiya Federasiyasining kriptografik algoritmlarida amalga oshirilgan. Masalan, ishlab chiqarilgan Rutoken S qurilmasining umumiy xarakteristikalari quyidagicha [26]:

- 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 [27]:

- saqlagichda (qurilmada) joylashgan maxsus prosessordan foydalaniladi;
- prosessorda shifrlash kalitini generasiyalash uchun maxsus kalit generatori mavjud bo'lib, foydalanuvchi kiritgan parol asosida qulfdan yechiladi;
- asosiy tizimni (qurilma ulangan tizim, masalan, kompyuterdagi) shifrlash uchun foydalanmaslik orqali, samaradorlikka erishiladi;
- kalitlar va boshqa maxfiy kattaliklar apparatda shifrlash orqali himoyalangan;
- autentifikasiya apparat-qurilmaga nisbatan amalga oshiriladi;
- o'rta va katta hajmdagi tashkilotlar sharoitida yuqori iqtisodiy samaradorlik beradi va madadlashning 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.

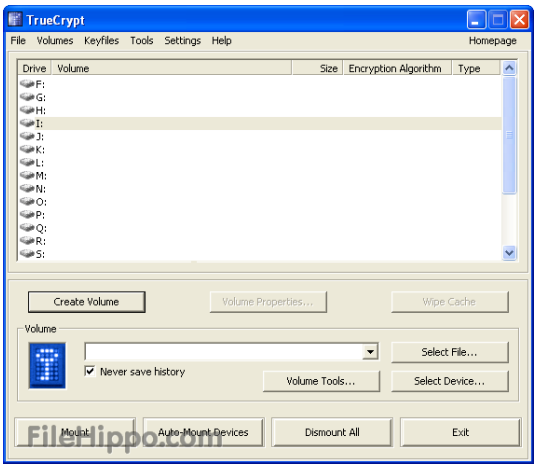
Dasturiy shifrlash kompyuter vositasi yordamida disklarni, fayllarni, kataloglarni va turli ma'lumot saqlash vositalaridagi axborotni shifrlash va deshifrlash jarayonini amalga oshiradi. Umumiy holda dasturiy shifrlash vositalarini quyidagi guruhlarga ajratish mumkin:

- 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).

23-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.



23-rasm. TrueCrypt dasturiy vositasi

Dasturiy shifrlash o’ziga xos bo’lgan quyidagi xususiyatlarga ega [28]:

- 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.

2.5.1. Disk va fayl tizim sathida shifrlash

Diskni shifrlash. Bu jarayon turli ma’lumotni 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 bo’limidagi (masalan, D disk) har bir bit shifrlanadi. Ushbu jarayon ruxsat etilmagan foydalanishdan nazoratlashni maqsad qiladi.

Butun diskni shifrlash (Full disk encryption (FDE) yoki *whole disk encryption)* deb nomlanuvchi vositalar diskdagi barcha ma’lumotlarni shifrlaydi va bunda faqat operasion 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 [29]:

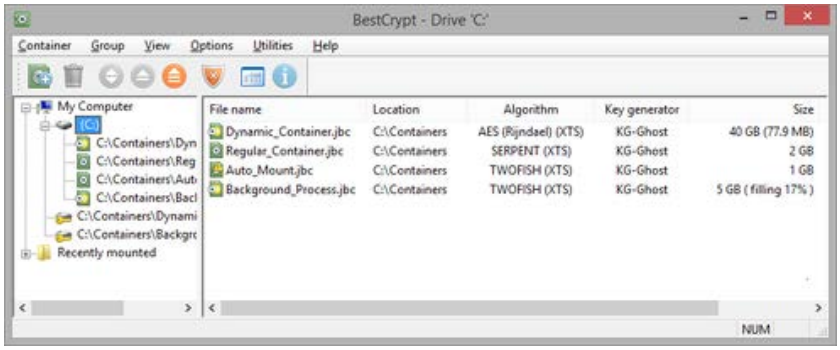
- *qattiq disk ishlab chiqaruvchilar:* iStorage Limited, Seagate Technology, Hitachi, Western Digital, Samsung, Toshiba;
- *SSD turidagi disk ishlab chiqaruvchilar:* OCZ, SanDisk, Samsung, Micron, Integral Memory;
- *USB disk ishlab chiqaruvchilar:* Yubikey yoki iStorage Limited.

Qurilmaga asoslangan FDE ikki tashkil etuvchidan: qurilmaga asoslangan shifrlash vositasidan va ma’lumotni saqlash qismidan iborat. Qurilmaga asoslangan FDE ning hozirda uchta ko’rinishi amalda keng qo’llaniladi [29]:

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 etilgandan 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 shirflash vositalariga *Aloaha Crypt Disk, BestCrypt Volume Encryption, BitArmor DataControl, BitLocker, Bloombase Keyparc, Cryptic Disk, USBCrypt* va boshqalarni misol tariqasida keltirish mumkin (24-rasm) [30].



24-rasm. Windows OTda BestCrypt dasturiy vositasi ko'rinishi

Diskni to'liq shifrlash usuli alohida fayl/ katalogni shifrlash usuliga qaraganda quyidagi afzalliklarga ega [31]:

- Deyarli barcha narsa, almashtirish maydoni (swap space) va vaqtinchalik fayllar shifrlanadi. Ushbu fayllarni shifrlash juda zarurki, odatda ular muhim axborotni oshkor qilishi mumkin. Dasturiy vosita ko'rinishidagi diskni shifrlovchilar dastlabki yuklash kodini (bootstrapping code) shifrlamaydi. Masalan, BitLocker Drive Encryption 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. Kelajakdagi 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 [32]:

- 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.

2.6. Ma’lumotlarni xavfsiz o’chirish usullari

Axborot xavfcizligida ma’lumotni 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.

2.6.1. Qog’oz ko’rinishdagi hujjatlarni yo’q qilish usullari

Odatda qog’oz ko’rinishdagi hujjatlarni yo’q qilishda quyidagi usullardan foydalaniladi [33]:

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

Maydalash. Tashkilotda rahbariyat ruxsati bilan xodimlar qo’lida bo’lgan qog’oz ko’rinishidagi hujjatlar vaqti 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’lumot 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 turli kesishlar orqali ularni juda kichik bo’laklarga ajratadi (25-rasm).

25-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’lumotni 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’oz ma’lumotlarni to’liq yo’q qilish imkoniyatini bermaydi. Iqlimi quruq hududlarda qozog’ 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 uning narxi yuqoriligi va maxsus joy talab etilishi.

2.6.2. 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 tariqasida, markaziy razvedka boshqarmasi va AQSh milliy xavfsizlik agenti Edvard Snoudenga tegishli yangiliklarni olish mumkin [34]. 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 xolos 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’lumotni 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 hujjatlarni saqlagichlar sifatida quyidagi turdagi vositalardan foydalanilmoqda:

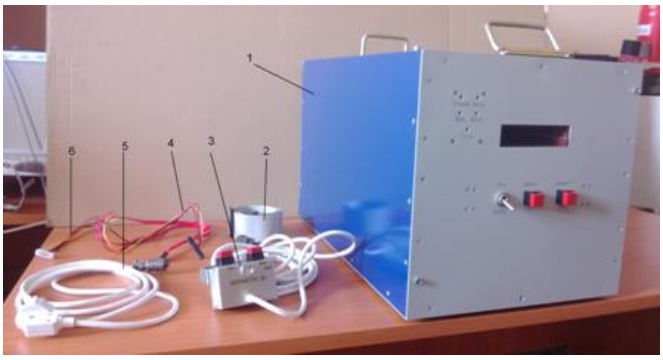
- qattiq disklar: noutbuk va kompyuterdagi qattiq disklar;
- magnit lentalar (zaxira nusxalashdagi);
- floppi-disk: 3.5 va 5.25 dyumli va boshqa;
- ZIP disklar;
- optik disklar: CD, DVD, Blue Ray va HD DVD;
- flesh xotiralar va h.

AQSh hukumatida konfidensial axborotni saqlash va o’chirib tashlash bo’yicha qator normativ hujjatlar ishlab chiqilgan (Code of Federal Regulations) [35]. Masalan, AQShning markaziy arxiv markazlarida elektron saqlagichdagi ma’lumotni yo’q qilishning quyidagi uchta usulidan foydalaniladi:

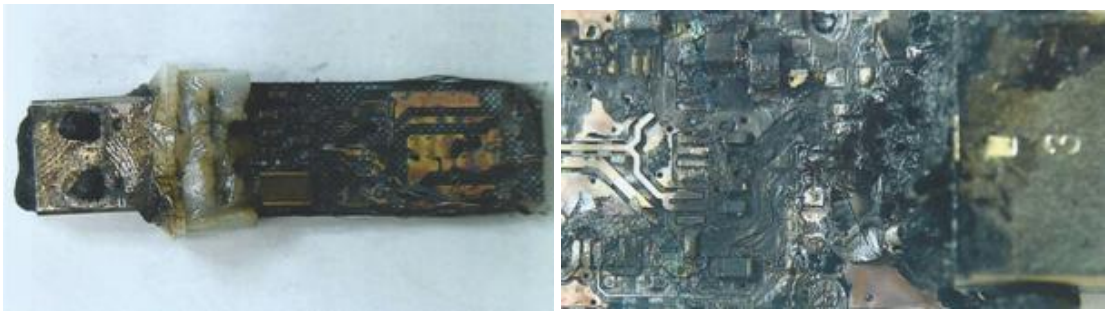
Shredirlash. Kuchli sanoat maydalagichlari deyarli barcha ko’chma saqlaguvchilarni: CD, DVD, disket, magnit lentalar va hak. maydalash natijasida ularni 25 mm. li qismlarga bo’lib tashlaydi (26-rasm).

26-rasm. Shredirlash 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 qurilmalar uchun qo’llaniladi (27-rasm).



27-rasm. UE-02 qurilmasi



28-rasm. Kuchli magnit maydoni natijasida USB flesh saqlagichining o’zgarishi

Yanchish. Shredirlash 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 aksariyati ma’lumot eltuvchisini fizik yo’q qilishni maqsad qiladi. TOP SECRET bo’lmagan axborot saqlangan holda esa saqlagichlardan qayta foydalanish talab etiladi. Buning uchun quyidagi usullardan foydalaniladi:

- saqlagich xotirasiga bir necha marta 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 qilish uchun quyidagi 29-rasmda keltirilgan usullardan foydalaniladi.

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

AQShning Cornell kompaniyasi tomonidan elektron axborotni saqlovchilarni qayta foydalanish va ularni yo’q qilish uchun quyidagi tavsiyalar beriladi [36] (2.5-jadval).

5-jadval

Elektron saqlagichlardan qayta foydalanish va yo’q qilish uchun berilgan 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’lumotni yo’q qilishga asoslangan bo’lib, 4-7 martagacha takror yozish orqali ma’lumotning tiklanishini oldini oladi [37].

Nazorat savollari

1. Kriptografiyaning asosiy tushunchalariga: shifrlash, deshifrlash, kalit, shifr, ochiq matn, shifrmatn, alifbo, izoh bering.
2. Axborotni simmetrik va ochiq kalitli shifrlash algoritmlari yordamida shifrlashdagi afzallik va kamchiliklarni ayting?
3. Kerkxofs prinsipining mohiyatini tushuntiring?
4. Kodlash va shifrlash tushunchalarining bir – biridan farqini ayting?
5. Kriptologiya va steganografiya fan sohalari va ularning o’zaro farqini ayting?

6. Simmetrik kriptografiyaning axborotni himoyalashdagi o’rni haqida gapiring?

7. Ochiq kalitli kriptografiyaning axborotni himoyalashdagi o’rni haqida gapiring?

8. Xesh funksiya nima, ularga qo’yilgan talablar va uni axborot himoyalashdagi o’rni?

9. Kriptografik akslantirishlar: o’rniga qo’yish va o’rin almashtirish nima?

10. Bir martali bloknot yordamida ma’lumotni shifrlash va uning xavfsizligi?

11. Simmetrik kriptotizimlar: kodlar kitobi, A5/1 va TEA shifrlash algoritmlarini tushuntiring?

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

13. Modul arifmetrikasida asosiy amallarni tushuntiring.

14. RSA algoritmi va u asoslangan matematik muammoni tushuntiring?

15. Ma’lumotlarni yaxlitligini ta’minlash usullari haqida ayting?

16. Elektron raqamli imzo va xabarlarni autentifikasiyalash kodlarining bir-biridan farqi hamda o’xshash tomonlarini ayting?

17. Axborotni kriptografik himoyalash vositalarining ko’rinishlari va ularning afzallik/ kamchiliklari?

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

19. Qog’oz ko’rinishidagi ma’lumotlarni yo’q qilish usullari va ularning xususiyatlari?

20. Elektron ko’rinishdagi ma’lumotlarni yo’q qilish usullari va ularning xususiyatlari?

3 BOB. FOYDALANISHNI NAZORATLASH

3.1. Foydalanishni nazoratlashning asosiy tushunchalari

Tizim resurslaridan foydalanishni boshqarish bilan bog'liq bo'lgan ixtiyoriy xavfsizlik muammosi uchun *foydalanishni nazoratlash* tushunchasidan "soyabon" sifatida foydalanish mumkin. Bunda 3 ta asosiy tushunchani ko'ralik: *identifikasiya*, *autentifikasiya* va *avtorizasiya*.

Identifikasiya – shaxsni kimdir deb da'vo qilish jarayoni. Masalan, siz telefonda o'zingizni tanitishingizni identifikasiyadan o'tish deb aytish mumkin. Bunda siz o'zingizni, masalan, "Men Bahodirman" deb tanitasiz. Bu o'rinda "Bohodir" sizning *identifikatoringiz* bo'lib xizmat qiladi. *Identifikasiya* – subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni. Elektron pochta tizimida pochta manzilini *identifikator*, manzilini taqdim etish jarayonini esa *identifikasiyalash* deyiladi. Elektron pochta tizimida pochta manzili takrorlanmas va noyob bo'ladi. Demak, foydalanuvchining identifikatori tizim ichida noyob va takrorlanmasdir.

Autentifikasiya – foydalanuvchini (yoki uning nomidan ish ko'ruvchi vositani) tizimdan foydalanish huquqiga egaligini tekshirish jarayoni. Masalan, foydalanuvchini shaxsiy kompyuterdan foydalanish jarayonini ko'ramiz. Dastlab foydalanuvchi o'z identifikatorini (ya'ni, foydalanuvchi nomini) taqdim etib tizimga o'zini tanitadi (identifikasiya jarayonidan o'tadi). So'ngra, tizim foydalanuvchidan taqdim etilgan identifikatorni haqiqiyligini tekshirish uchun parol talab qiladi. Agar identifikatorga mos parol kiritilsa (ya'ni, autentifikasiyadan o'tsa), foydalanuvchi kompyuterdan foydalanish imkoniyatiga ega bo'ladi. Umuman olganda, autentifikasiya foydalanuvchi yoki subyektni haqiqiyligini tekshirish jarayoni deb yuritiladi.

Foydalanuvchi autentifikasiyadan o'tganidan so'ng tizim resurslaridan foydalanish imkoniyatiga ega bo'ladi. Biroq, autentifikasiyadan o'tgan foydalanuvchi tizimda faqatgina ruxsat berilgan amallarni bajarishi mumkin bo'ladi. Masalan, autentifikasiyadan o'tgan – imtiyozga ega foydalanuvchi uchun dasturlarni

o’rnatish imkoniyatini berilishi talab etilsin. Bunda autentifikasiyadan o’tgan foydalanuvchining foydalanish huquqlari qanday qilib cheklanadi? Bu masalalar avtorizasiyalash bilan yechiladi.

Avtorizasiya – identifikasiya va autentifikasiya jarayonlaridan muvaffaqiyatli o’tgan foydalanuvchiga tizimda amallarni bajarish huquqini berish jarayonidir. Umumiy holda, autentifikasiya binar qaror hisoblanadi - ya’ni, ruxsat beriladi yoki yo’q. Avtorizasiya esa tizimning turli resurslaridan foydalanishni cheklash uchun foydalaniluvchi qoidalar to’plamidir.

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

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

Identifikasiya – siz kimsiz?

Autentifikasiya – siz haqiqatan ham sizmisiz?

Avtorizasiya – sizga buni bajarishga ruxsat bormi?

3.1.1. Autentifikatsiya

Identifikasiya yoki autentifikasiya jarayonlarida subyektlar inson, qurilma (kompyuter yoki jarayon) ko’rinishida bo’lishi mumkin. Ya’ni, inson insonni autentifikasiyadan o’tkazishi mumkin, mashina insonni autentifikasiyadan o’tkazishi mumkin yoki mashina mashinani autentifikasiyadan o’tkazishi mumkin. Mazkur bo’limda mashina insonni yoki mashina mashinani autentifikasiyadan o’tkazish ssenariylariga asosiy e’tibor beriladi.

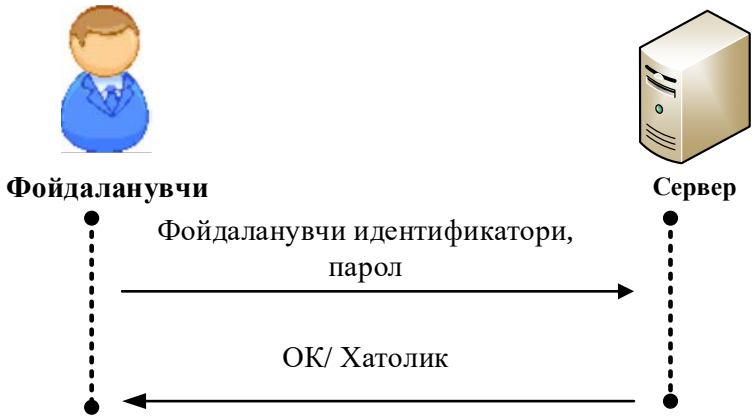
Mashina insonni quyidagi “narsalar” asosida autentifikasiyadan o’tkazishi mumkin [13, 23]:

- siz bilgan biror narsa (something you know);

- sizda mavjud biror narsa (something you have);
- sizning biror narsangiz (something you are).

“Siz bilgan biror narsa” asosida autentifikasiyalash usuliga parol misol bo’ladi. “Sizda mavjud biror narsa” asosida autentifikasiyalash usuliga esa smartkartalar, token, mashinaning pulti yoki kaliti misol bo’ladi. “Sizning biror narsangiz” holati odatda biometrik parametrlarga sinonim sifatida qaraladi. Masalan, siz noutbuk sotib olib, undagi barmoq izi skaneri orqali autentifikasiyadan o’tishingiz mumkin.

Parol – tizimda autentifikasiya jarayonidan o’tishni ta’minlovchi faqat foydalanuvchiga ma’lum bo’lgan biror axborot. Parol amalda autentifikasiya jarayonida keng qo’llaniluvchi parametr hisoblanadi. Masalan, o’z shaxsiy kompyuterlarimizdan foydalanish huquqini olishda parolni kiritish talab etiladi. Mazkur jarayonni mobil telefonlar uchun ham ishlatish mumkin. Parolga asoslangan autentifikasiyalash jarayonining umumiy ko’rinishi 30-rasmda keltirilgan.



30-rasm. Parolga asoslangan mashina-insonni autentifikasiyalash jarayoni

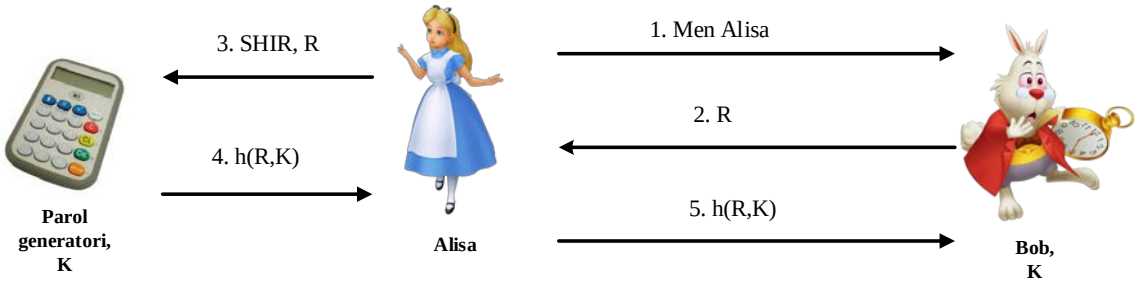
Parolga asoslangan autentifikasiya quyidagi xususiyatlarga ega:

- parolga asoslangan autentifikasiyalash qulay (sarf xarajati kam, almashtirish oson);
- foydalanuvchi paroli odatda unga aloqador ma’lumot bo’ladi (masalan, uning yaxshi ko’rgan futbol komandasining nomi, telefon raqami va h.) (*123456*, *12345*, *qwerty*) va shuning uchun “hujumchilar” tomonidan aniqlab olinishi oson;
- murakkab parollarni xotirlab qolish qiyin (masalan, *jfIej(43jEmmL+y*);
- parolga asoslangan autentifikasiyalash usuli amalda keng qo’llaniladi.

Smartkartalar yoki qurilma ko’rinishidagi tokenlar autentifikasiyalash uchun qo’llaniladi. Smartkarta kredit karta o’lchamidagi qurilma bo’lib, kichik hajmdagi xotira va hisoblash imkoniyatiga ega. Smartkarta odatda o’zida biror maxfiy kattalik, kalit yoki parolni saqlaydi va hattoki qandaydir hisoblashni ham amalga oshiradi. 31-rasmda maxsus maqsadli smartkarta va uni o’quvchi qurilma (smartkarta o’quvchi qurilma) aks ettirilgan.

31-rasm. Smartkarta va smartkarta o’quvchi (ACR39U [1]) qurilma

Biror narsa asosida autentifikasiyalash usullarini turlicha amalga oshirish mumkin. Masalan, tokenga asoslangan autentifikasiyalashni ko’rib chiqaylik. Bunda parollar generatori qurilmasidan foydalanib, u tizimga kirishda qo’llaniladi. Faraz qilaylik, Alisa parol generatoridan foydalanib Bobdan autentifikasiyadan o’tmoqchi. Buning uchun Bob biror tasodifiy son *R* ni (“savolni”) Alisaga yuboradi. Alisa qabul qilingan *R* sonini va parol generatoridan foydalanish ShIR (Shaxsiy identifikasiya raqami)ini parol generatoriga kiritadi. Alisa parol generatori javobini Bobga uzatadi. Agar javob to’g’ri bo’lsa, Alisa autentifikasiyadan o’tadi, aks holda o’ta olmaydi. Mazkur “savol-javob” ssenariysining umumiy ko’rinishi 32-rasmda keltirilgan.



32-rasm. Tokenga asoslangan autentifikasiya jarayoni

Bu yerda, Bob va parol generatorida taqsimlangan kalit K bo'lishi shart. Savol sifatida Bob Alisaga R sonini uzatadi va unga mos bo'lgan javob - $h(R, K)$ ni qabul qiladi. Qabul qilgan ma'lumotni tekshirish orqali Bob Alisani haqiqiyligini tekshiradi.

Smartakarta yoki "sizda mavjud biror narsa" asosida autentifikasiya usullari quyidagi xususiyatlarga ega:

- autentifikasiyalashda biror narasani esda saqlash talab etilmaydi;
- amalga oshirish va qurilma narxi yuqori (xususan, token yo'qolgan taqdirda uni almashtirish qimmatga tushadi);
- token yoki smartkartani yo'qotib qo'yish muammosi;
- token xavfsizligi ta'minlanganida yuqori xavfsizlik darajasini ta'minlaydi.

Biometrik parametrlarga asoslangan autentifikasiya. Biometrik parametrlarga asoslangan autentifikasiya usulida biometrik parametr insonning o'zi uchun kalit sifatida xizmat qiladi. Biometrik parametrlarga asoslangan autentifikasiyalashning ko'plab usullari mavjud. Masalan, barmoq izi, yuz tasviri, ko'z qorachig'i, ovoz, harakat tarzi, quloq shakli, qo'l shakli va boshqa biometrik parametrlarga asoslangan autentifikasiya usullari amalda keng qo'llaniladi. Masalan, qo'p qavatli uylar va tashkilotlarga kirishda barmoq iziga asoslangan autentifikasiya usuli, noutbuklarda va mobil telefonlarda yuz tasviriga asoslangan yoki barmoq iziga asoslangan autentifikasiya keng qo'llaniladi (32-rasm).

Barmoq izi Yuz tasviri Ko'z qorachig'i Ovoz

32-rasm. Biometrik na'munalarga misollar

Axborot xavfsizligi sohasida biometrik parametrlar parollarga qaraganda yuqori xavfsizlikni ta’minlovchi muqobil sifatida qaraladi. Biometrik parametrlarga asoslangan autentifikasiya usuli quyidagi xususiyatlarga ega:

- biometrik parametrga asoslangan usullar esda saqlash yoki birga olib yurish zaruriyatini talab etmaydi;
- biometrik parametrlarga asoslangan autentifikasiyalash parollarga asoslangan usullardan foydalanishga nisbatan qimmatroq, lekin tokenga asoslangan usullardan foydalanishga qaraganda arzonroq hisoblanadi (ba’zi, istisno holatlar mavjud);
- biometrik parmetrlarni o’zgartirish imkoniyati mavjud emas, ya’ni, agar biometrik parametr qalbakilashtirilsa, u holda autentifikasiya tizimi shu foydalanuvchi uchun to’liq buzilgan hisoblanadi;
- turli biometrik parametrlarga asoslangan autentifikasiyalash usullari insonlar tomonidan turli darajada qabul qilinadi.

Autentifikasiya sohasida foydalanish uchun ideal biometrik parametr quyidagi xususiyatlarga ega bo’lishi shart [38, 39]:

- *universal bo’lishi* – biometrik parametrlar barcha foydalanuvchilarda bo’lishi;
- *farqli bo’lish* – barcha insonlarning tanlangan biometrik parametri bir-biridan farq qilishi;
- *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 autentifikasiya jarayonga e’tibor berishiga ham bog’liq bo’ladi.

Biometrik parametrlar nafaqat autentifikasiyalash masalasini yechishda balki, identifikasiyalashda ham keng qo’llaniladi. Ya’ni, “Siz kimsiz?” degan savolga javob bera oladi. Masalan, FBI da jinoyatchilarning barmoq izlari bazalari mavjud. Bazada barmoq izlari *(barmoq izi tasviri - foydalanuvchi nomi)* shaklida saqlanadi va bu biror bir insonni jinoyatchilar ro’yxatida bor yoki yo’qligini aniqlashga imkon

beradi [40]. Buning uchun, tekshiriluvchi insonning barmoq izi tasviri FBI bazasidagi biror bir barmoq izi tasviriga mos kelsa, *barmoq izi tasviri*ga mos *foydalanuvchi nomi* bilan aniqlanadi.

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

Ko'p omilli autentifikasiya. Yuqorida keltirilgan barcha autentifikasiya ssenariylarida foydalanuvchilarni faqat bitta omil bo'yicha haqiqiyligi tekshiriladi. Masalan, elektron pochtaga kirishda faqat parolni bilishning o'zi yetarli bo'lgan bo'lsa, binoga kirishda barmoq izini to'g'ri kiritishning o'zi eshikni ochilishi uchun yetarli bo'ladi. Ya'ni, server faqat foydalanuvchidan parolni yoki barmoq izi tasvirini to'g'ri bo'lishini talab qiladi. Bir faktorli autentifikasiyada tekshirish faqat bitta omil bo'yicha (masalan, parol) amalga oshiriladi va o'zi *bir omilli autentifikasiya* deb yuritiladi.

Biroq, bir omilli autentifikasiyalashda xavfsizlik darajasi past bo'ladi. Masalan, ovozga asoslangan autentifikasiya tizimida hujumchi foydalanuvchining ovozini diktafonga yozib olib, uni autentifikasiya jarayoniga taqdim etsa, osonlik bilan autentifikasiya tizimini bitta omil bo'yicha aldab o'tishi mumkin. Bunday holatni parolga asoslangan yoki tokenga asoslangan autentifikasiya jarayonida ham kuzatish mumkin.

Xavfsizlik darjasini oshirish uchun birinchi omilga qo'shimcha, yana boshqa omillardan foydalanish mumkin. Masalan, ovozga asoslangan autentifikasiyalashga qo'shimcha qilib paroldan foydalanish mumkin. Ya'ni, foydalanuvchi dastlab tizimdan o'z ovozi orqali, so'ng parol bo'yicha autentifikasiyadan o'tkaziladi. Har ikkala bosqichda ham autentifikasiyadan muvaffaqqiyatli o'tilganda, foydalanuvchi

tizimdan foydalanish imkoniyatiga ega bo'ladi. Shu sababli, ushbu usulni *ko'p omilli autentifikasiyalash* deb aytish mumkin. Ko'p omilli autentifikasiyalash kundalik hayotimizda hozir keng qo'llanilmoqda. Masalan, plastik kartadan to'lovni amalga oshirishdagi autentifikasiya jarayoni o'zida "*sizda mavjud biror narsa*" va "*siz bilgan biror narsa*" usullarini birlashtirgan. Birinchi omil foydalanuvchida plastik kartani mavjudligi bo'lsa, ikkinchisi uni ShIR ini bilish talab etilishidir.

Ko'p omilli autentifikasiya usuli omillardan bittasi qalbakilashtirilgan taqdirda ham autentifikasiya jarayonini buzilmasligiga olib keladi. Ko'p omilli autentifikasiya sifatida aksariyat hollarda bir martali parollardan (one time password, OTP) keng foydalanilmoqda. Bunga misol qilib, turli mobil bank ilovalarida to'lovni amalga oshirishdagi foydalanuvchi mobil qurilmasiga keluvchi SMS xabardagi OTRlarni keltirish mumkin.

Autentifikasiya jarayonlariga qaratilgan hujumlar. Mavjud autentifikasiya jarayonlarini buzishda ko'plab hujum usullaridan foydalaniladi. Ushbu hujum usullarini autentifikasiya usullariga mos ravishda quyidagicha tasniflash mumkin [43]:

1. *Biror narsani bilishga asoslangan* autentifikasiyalashni buzish uchun quyidagi hujum usullaridan foydalaniladi:

a. *Parollar lug'atidan foydalanishga asoslangan hujum.* Bunda statistika bo'yicha eng ko'p qo'llaniluvchi parollar asosida autentifikasiyadan o'tishga harakat qilinadi.

b. *Parollarni barcha variantlarini ko'rib chiqish.* Ushbu usulda parolning bo'lishi mumkin bo'lgan barcha variantlaridan ketma-ket foydalanib ko'riladi.

c. *"Yelka orqali qarash" hujumi.* Buzg'unchi foydalanuvching yonida turib parolni kiritish jarayonini kuzatish orqali bilib olishni maqsad qiladi.

d. *Zararkunanda dasturlar asosida hujum.* Foydalanuvchi kompyuteriga o'rnatilgan maxsus dasturiy vositalar klaviaturadan kiritilgan barcha ma'lumotlarni dasturchiga yetkazadi. Bunday zararkunanda dasturiy vositalar "*keylogger*" deb ataladi.

2. *Sizda mavjud biror narsa* asosida autentifikasiya usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

a. *Fizik o'g'irlash.* Mazkur hujum bu toifadagi autentifikasiya uchun eng xavfli hujum hisoblanib, buzg'unchi tokenni yoki smart kartani o'g'irlab foydalanishga asoslanadi.

b. *Dasturiy tokenlarning zararkunanda dasturlarga bardoshsizligi*. Dasturiy tokenlar mobil qurilmalarda ishlaydi va shu sababli zararli dastur tomonidan boshqarilishi mumkin.

3. *Biometrik parametrlarga asoslangan* autentifikasiya usullarini buzish uchun quyidagi hujum usullaridan foydalaniladi:

a. *Qalbakilashtirish.* Hujumning mazkur turi biometrik parametrlarni qalbakilashtirishga asoslanadi. Masalan,bunga Hasan o'rniga yuzlari o'xshash bo'lgan Xusan autentifikasiyadan o'tishi yoki sifati yuqori bo'lgan foydalanuvchi yuz tasvirini uning fotosurati bilan almashtirib tizimni aldashini misol qilish mumkin.

b. *Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish.* Ushbu hujum bevosita foydalanuvchilarni biometrik parametrlari (masalan, barmoq izi tasviri, yuz tasviri va hak.) saqlanyotgan bazadagi tanlangan foydalanuvchining biometrik parametrlarini hujumchining biometrik parametrlari bilan almashtishga asoslangan.

Autentifikasiya jarayonlarini hujumlardan himoyalashning har bir usullariga xos qarshi choralari mavjud. Umumiy holda, mazkur hujumlarni oldini olish uchun quyidagi himoya usullari va xavfsizlik choralari tavsiya etiladi:

1. *Murakkab parollardan foydalanish.* Aynan ushbu usul parollarni barcha variantlarini ko'rib chiqish va lug'atga asoslangan hujumlarning oldini olishga imkon beradi.

2. *Ko'p omilli autentifikasiyadan foydalanish.* Bu usul yuqorida keltirilgan aksariyat hujumlarni oldini olishga imkon beradi.

3. *Tokenlarni (smart kartalarni) xavfsiz saqlash.* Bu usul biror narsaga egalik qilishga asoslangan autentifikasiya usulida token yoki smart kartalarni buzg'unchi qo'liga tushib qolishdan himoyalash darajasini oshirishga imkoni beradi.

4. *Tiriklikka tekshirishdan foydalanish.* Ushbu usul biometrik parametrlarga asoslangan autentifikasiyalash usullarida tasvir orqali aldab o'tish hujumini oldini olishda samarali hisoblanadi.

3.2. Parolga asoslangan autentifikasiya usuli

3.2.1. Parol va kriptografik kalit

Axborot texnologiyalari sohasida faoliyat yuritayotgan mutaxassislar orasida ko'p hollarda parol va kriptografik kalit tushunchalarini chalkashtirish holatlari kuzatiladi. Biroq, ushbu ikki tushuncha bir-biridan farq qiladi [13].

Kriptografik kalitlarning o'lchovi *bit*larda ifodalanadi. Masalan, T hujumchi 64-bitli kalitning barcha variantlarini hisoblashi talab etilsin. Mazkur holatda 2^{64} ta variant mavjud bo'lib, hujumchidan, T kalitni to'g'ri topishi uchun, agar kalit tasodifiy tanlangan bo'lsa, o'rta hisobda 2^{63} ta kalitlarni ko'rib chiqish talab etiladi.

Parolning o'lchov birligi esa odatda parol tarkibidagi belgilar soni bilan o'lchanadi. Masalan, parol uzunligi 8 ga va foydalanilgan alifbo uzunligi 256 ga teng bo'lsa, bo'lishi mumkin bo'lgan barcha parollar varianti $256^8=2^{64}$ ga teng bo'ladi. Bir qarashda shuncha sondagi parollarni topish kriptografik kalitni topish murakkabligi bilan bir xildek ko'rinadi. Biroq, parollarni tanlashda foydalanuvchilar tasodifiy bo'lishiga e'tibor berishmaydi. Natijada esa, foydalanuvchi 8 ta belgidan iborat bo'lgan parol sifatida `kf&Yw!a[` dan emas, balki `password` ko'rinishidagi parollardan foydalanish holatlari kuzatiladi.

Bu esa o'z navbatida 2^{63} dan kichik hisoblashga va parolni katta ehtimol bilan topish imkoniyatini keltirib chiqaradi. Masalan, $2^{20} \approx 1\,000\,000$ ta eng keng tarqalgan parollardan iborat bo'lgan parollar lug'ati buzg'unchiga parolni topish uchun juda qo'l kelishi mumkin. Kriptografik kalitni topishda esa 2^{64} ta kalitni 2^{20} ta bo'lishi mumkin bo'lgan kalitdan biriga mos kelish ehtimoli $\frac{2^{20}}{2^{64}} = 1/2^{44}$ ga yoki

kamida 17 triliondan birga to’g’ri keladi. Bu esa parollarni tasodifiy tanlanmasligi ulardagi eng jiddiy muammo ekanligini anglatadi.

3.2.2. Parollarni tanlash tartibi

Barcha parollar bir xil uzunlikda bo’lsa ham bir xil murakkablik darajasiga ega emas. Masalan quyidagi parollar aksariyat foydalanuvchilar tomonidan zaif deb topilishi mumkin (Ayniqsa, ismi `Frank` yoki `Austin Stamp` bo’lganlar yoki tug’ilgan kuni `10/25/1960` bo’lganlar uchun) [13]:

- Frank;
- Pikachu;
- 10251960;
- AustinStamp.

Biror narsani bilishga asoslangan autentifikasiyada xavfsizlik darajasi parolning murakkablik darajasiga bog’liq bo’ladi va foydalanuvchidan murakkab paroldan foydalanish zaruriyatini qo’yadi. Bu zaruriyat foydalanuvchilardan mazkur murakkab parollarni esda saqlab qolishni qiyinlashtiradi. Bu tomondan qaralganda, quyidagi parollar yuqorida keltirilgan zaif parollarga qaraganda yaxshiroqmi?

- jfIej(43j-EmmL+y;
- 09864376537263;
- PokemON;
- FSa7Yago.

Masalan, `jfIej(43j-EmmL+y` parolni buzish buzg’unchi uchun qanchalik murakkab bo’lsa, uni esda saqlash foydalanuvchi uchun ham shunchalik murakkab. Bunday parolni, ehtimol foydalanuvchi kompyuteri oldidagi eslatmada saqlash mumkin. Bu esa, foydalanuvchi oddiyroq parolni tanlagan holatga ko’ra buzg’unchiga osonroq parolni qo’lga kiritish imkonini beradi.

Yuqorida keltirilgan ikkinchi parol ham faqat raqamlardan tashkil topgan bo’lsada, uni esda saqlash murakkab vazifa. Hattoki, yadroviy raketani uchirish uchun javobgar bo’lgan AQShning malakaviy xodimidan ham 12 ta raqamdan iborat

bo’lgan otish kodini eslab qolishi talab etiladi. Mazkur muammolarni qolgan parollarga nisbatan ham aytish mumkin.

Biroq, parollarni oson esda saqlashga imkon beruvchi *xiylalar* mavjud bo’lib, ular *iboralar*ga asoslanadi. Masalan, keltirilgan `FSa7Yago` parol “`four score and seven years ago`” iborasidan olingan. Bu xiyla foydalanuvchining eslab qolishini osonlashtirishga, hujumchilarga murakkab bo’lgan parollarni aniqlashni qiyinlashtiradi [13].

Ushbu holatni to’g’riligini tasdiqlash uchun quyidagi tajriba o’tkazilgan. Bunga ko’ra, foydalanuvchilar 3 ta guruhga ajratilgan va ularga parolni yaratishda turli maslahatlar berilgan:

- *A guruh.* Parol kamida 6 ta belgidan iborat bo’lishi va ulardan kamida bittasi harf bo’lmasligi. Bu parolni odatdagi tanlash holatidir.
- *B guruh.* Iboralarga asoslangan holda parollarni yaratish.
- *S guruh.* Parol tasodifiy tanlangan 8 ta simvoldan iborat bo’lishi.

Tajribada qatnashgan foydalanuvchilarning parollarini buzishga urinishlari quyidagi natijalarni bergan:

- *A guruh.* 30% ga yaqin parollar osonlik bilan buzilgan. Bunda foydalanuvchilar tomonidan parollarni esda saqlash osonroq deb topilgan.
- *B guruh.* 10% ga yaqin parollar buzilgan. Bunda foydalanuvchilar tomonidan parollarni esda saqlash osonroq deb topilgan.
- *S guruh.* 10% ga yaqin parollar buzilgan. Bunda foydalanuvchilar tomonidan parollarni esda saqlash juda murakkab bo’lgani aytilgan.

O’tkazilgan tajriba natijasidan kelib chiqib, iboralarga asoslangan parollarni generasiyalashni eng samarali va xavfsiz usul deb aytish mumkin.

3.2.3. Parolga qarshi hujum tizimlari

Faraz qilaylik, buzg’unchi tashqarida joylashgan (begona) va biror bir tizimdan foydalanish huquqiga ega emas. Bu holda buzg’unchining umumiy hujum yo’li quyidagicha bo’ladi: `begona→normal foydalanuvchi→ ma’mur.`

Boshqacha aytganda, buzg’unchi dastlab ixtiyoriy akkauntga kirish usulini qidiradi va keyin imtiyoz darajasini oshirishga harakat qiladi. Mazkur ssenariyda, tizimdagi birgina yoki butun tarmoqdagi birgina zaif parol hujumning birinchi bosqichini muvaffaqqiyatli amalga oshirilishi uchun yetarli bo’lishi mumkin. Buning xavfli tomoni zaif parollarning soni juda ham ko’p bo’lishi mumkinligidir.

Bundan tashqari, parolni buzishga urinish holati aniqlanganda unga to’g’ri javob berish ham muhim jarayon hisoblanadi. Masalan, tizim uch marta muvaffaqiyatsiz urinishdan so’ng akkauntni bloklaydi. Agar shunday bo’lsa, tizim qancha vaqt bloklanishi kerak? Besh soniya? Besh daqiqa yoki ma’mur tomonidan to’g’rilanmagunchami? Besh soniya avtomatik amalga oshirilgan hujumlarni aniqlash uchun yetarli emas. Ya’ni, buzg’unchi bir akkauntni uch marta noto’g’ri parolni terib bloklaydi va shundan so’ng bu ishni yana bir necha akkauntlar uchun amalga oshiradi va bu orada 5 soniya o’tib bo’ladi. Buzg’unchi yana ushbu akkauntni buzishga harakat qiladi va bu istalgancha davom etishi mumkin. Agar tizimni bloklash 5 daqiqa davomida amalga oshirilsa, u holda tizimni foydalanuvchanlik darajasini tushirishga sababchi bo’ladi va buzg’unchi barcha uchun foydalanuvchanlikni yo’qolishiga sababchi bo’ladi. Mazkur holda to’g’ri javobni topish juda murakkab hisoblanadi.

3.2.4. Parollarni saqlash va o’zaro taqqoslash

Parolga asoslangan autentifikasiyalashda kiritilgan parolni to’g’riligini tekshirish muhim ahamiyatga ega. Kompyuter parolni to’g’riligini tekshirish uchun, parolga taqqoslanuvchi biror bir narsa bo’lishi kerak. Ya’ni, kompyuter kiritilgan parolni to’g’riligini tekshirish uchun uni biror ko’rinishda boshqarishi kerak bo’ladi. Parollarni haqiqiy holatda fayllarda saqlashda bu parollar fayllari buzg’unchining hujum obyektiga aylanib qoladi. Bu muammoni axborot xavfsizligining ko’plab sohalarida bo’lgani kabi, kriptografik himoya asosida yechiladi.

Parollarni fayllarda simmetrik kriptotizim yordamida shifrlangan holatda saqlanganda parolni tekshirish uchun faylni deshifrlash lozim. Deshifrlash kaliti boshqa bir faylda saqlanishi zarur. Bu esa buzg’unchiga kalitlar fayllarini o’g’irlash

imkonini yaratadi. Ya’ni, parollarni shifrlangan holatda saqlash ham xavfsizlikni ta’minlab bera olmaydi.

Parollarni faylda shifrlangan ko’rinishda saqlash o’rniga parolni xeshlangan qiymatini saqlash ancha xavfsiz usul hisoblanadi. Masalan, Alisaning paroli `Fsa7Yago` ga teng bo’lsa, faylda $y = h(FSa7Yago)$ saqlanadi. Bu yerda h - kriptografik xesh funksiya. Shundan so’ng, tizim Alisadan parol x ni kiritishni talab etsa, parol dastlab xeshlanadi va y bilan taqqoslanadi. Ya’ni, agar $y = h(x)$ bo’lsa, kiritilgan parol to’g’ri deb topiladi va Alisa autentifikasiyadan o’tkaziladi [13].

Parollarni xeshlab saqlaganda buzg’unchi parollar faylini qo’lga kiritganda ham, haqiqiy parolni aniqlash imkonini pasaytirishga harakat qilish muhim hisoblanadi. Xesh funksiyalarga qo’yilgan bir tomonlamalik xususiyatiga ko’ra, xesh qiymatdan haqiqiy parolni topib bo’lmaydi. Albatta, buzg’unchi ixtiyoriy parolning xesh qiymatini taqqoslash orqali parolni aniqlashi mumkin (faraz bo’yicha hujum yoki parolni barcha variantlarini ko’rib chiqish hujumi). Biroq, buzg’unchi zarur bo’lgan parolni aniqlashi uchun qo’shimcha vaqt va zarur hisoblash amallarini bajarishi kerak bo’ladi [13].

Faraz qilaylik, buzg’unchida N ta eng keng foydalanilgan parollar, $d_0, d_1, d_2, \dots, d_{N-1}$, saqlangan lug’atdan har bir parolni xeshlab: $y_0 = h(d_0), y_1 = h(d_1), \dots, y_{N-1} = h(d_{N-1})$ va (d_0, y_0) juftlik ko’rinishidagi yangi lug’atni hosil qiladi. Shundan so’ng, agar buzg’unchi biror xesh qiymat ko’rinishidagi parolni “qayta tiklash” uchun uni N ta xesh qiymat bilan taqqoslaydi. Agar moslik aniqlansa, u holda parolni haqiqiy qiymati topilgan bo’ladi. Buzg’unchi hosil qilgan yangi lug’ati asosida ixtiyoriy parollar faylini buzishlari mumkin. (d_0, y_0) ko’rinishdagi ko’plab bepul yoki pullik lug’atlarni Internet tarmog’ida topish mumkin. Bu esa, mavjud bo’lgan (d_0, y_0) ko’rinishdagi lug’at ayrim parollarni aniqlashda foydalanilishi mumkinligini anglatadi.

Bunday hujumlarni oldini olish yoki buzg’unchi ishini yanada murakkablashtirish uchun parolga maxfiy bo’lgan kattalikni (*“tuz”, salt* – deb ataladi) qo’shib, keyin xeshlash tavsiya etiladi. Ya’ni, $y = h(p, s)$ ko’rinishida. Bu

yerda, p – parol bo'lsa, s – "tuz". Bu kattalik, simmetrik blokli shifrlashning CBC rejimidagi IV kattalik hisoblanadi. IV kattalik bir xil ochiq matnni turlicha shifrmatnlar ko'rinishida shifrlash uchun foydalanilgan bo'lsa, $salt$ har bir parolni turli xesh qiymatlar ko'rinishida ifodalash uchun ishlatiladi. "Tuz" parollar faylidagi har bir fayl uchun turlicha bo'ladi [13]. Bu usulning mohiyatini quyida ko'ramiz.

Faraz qilaylik, p yangi kiritilgan parol bo'lsin. Dastlab tasodifiy $salt$, s generasiya qilinadi va $y = h(p, s)$ hisoblanadi hamda parollar faylida (s, y) shaklida saqlanadi. Foydalanilgan s qiymat maxfiy emas va shuning uchun u parollar faylida ochiq ko'rinishda saqlanadi. Kiritilgan parol x ni tekshirish uchun, buzg'unchi parollar faylidan (s, y) ni oladi. Shundan so'ng, buzg'unchi $h(x, s)$ ni hisoblaydi hamda uni y bilan taqqoslaydi. Bu holda taqqoslash $salt$ ishlatilmagani kabi, bir xil amalga oshiriladi. Biroq, buzg'unchiga murakkablik tug'iladi. Ya'ni, u kerakli parolni olish uchun juda ko'p hisoblashlarni amalga oshirishi talab etiladi. Faraz qilaylik, A tomonning paroli "tuz", s_a bilan birgalikda xeshlangan, B tomoning paroli esa s_b bilan birgalikda xeshlangan. Mazkur holda, buzg'unchi A tomonning parolini o'zidagi parollar lug'ati asosida tekshirishi uchun lug'atidagi barcha parollarga s_a ni biriktirib xeshlashi talab etiladi. Biroq, B tomoning parolini tekshirish uchun esa o'zidagi barcha parollarga s_b ni biriktirib xeshlashi talab etiladi. N ta foydalanuvchidan iborat parollar fayli uchun buzg'unchining ishi N faktorialga ko'payadi. Bundan tashqari, bu holda buzg'unchi o'zi uchun yaratgan (d_0, y_0) shaklidagi parollar lug'ati ham foydasiz bo'ladi.

3.2.5. Parolni buzishning murakkabligi

Ixtiyoriy parolni buzishning matematik hisoblashlar orqali ko'rib chiqaylik. Faraz qilaylik, olingan parol uzunligi 8 ga teng va foydalanilgan alifbo 128 ta simvoldan iborat bo'lsin. Bu holda jami parol variantlarining soni $128^8 = 2^{56}$ ga teng bo'ladi. Bundan tashqari, foydalanuvchilar parollari saqlanuvchi fayl 2^{10} ta paroldan iborat va buzg'unchi eng keng tarqalgan 2^{20} ta paroldan iborat lug'atga ega bo'lsin. Ixtiyoriy berilgan parolni buzg'unchining parollar lug'atidan topilish

ehtimoli ¼ ga teng bo’lsin. Bunda, buzg’unchining hisoblash ishlari xeshlashlar soni bilan o’lchanadi.

Yuqorida keltirilganlarga muvofiq quyidagi holatlar uchun parolni muvaffaqqiyatli buzish ehtimolini aniqlaymiz [13]:

1. Buzg’unchi A tomonning parolini aniqlashni xoxlaydi (bu holda A tomon tizim yoki tarmoq ma’muri bo’lishi mumkin). Buzg’unchi parolni aniqlashda o’zining parollar lug’atidan foydalanmaydi.

2. Buzg’unchi A tomoning parolini aniqlashni xohlaydi. Buzg’unchi o’zining parollar lug’atidan foydalanadi.

3. Buzg’unchini parollar faylidagi ixtiyoriy parolni o’zining lug’atidan foydalanmay buzishi yetarli.

4. Buzg’unchini parollar faylidagi ixtiyoriy parolni o’zining lug’atidan foydalanib buzish yetarli.

Har bir variantni “tuz”dan foydalanilgan yoki foydalanilmagan holatlar uchun ko’rib chiqamiz.

1- holat. Agar buzg’unchi A tomonni parolini o’zining parollar lug’atidan foydalanmay aniqlamoqchi bo’lsa, u holda parol bo’lishi mumkin bo’lgan barcha variantlarni ko’rib chiqishi kerak bo’ladi. Buning uchun buzg’unchi o’rtacha $\frac{2^{56}}{2} = 2^{55}$ hisoblash amallarini bajarishi kerak.

Hisoblashlarda parol “tuz” bilan yoki “tuz”siz xeshlangan barcha holatlari uchun hisoblashlar bajariladi. Masalan, agar parol “tuz”siz holatda xeshlangan bo’lsa, buzg’unchidan 2^{55} ta variantni hisoblashi talab etiladi va “tuz” bilan xeshlangan holatda esa parolni hisoblashdan umuman foyda bo’lmaydi. Har qanday holatda ham, buzg’unchi juda katta hisoblashlarni bajarishi aniq. Shuning uchun, mazkur holat ortiq qarab chiqilmaydi va ma’noga ega emas deb qaraladi.

2 – holat. Mazkur holatda ham buzg’unchi A foydalanuvchini parolini buzishni istaydi va buning uchun o’zining eng keng tarqalgan parollar lug’atidan foydalanadi. Olingan farazga binoan, A tomoning paroli ¼ ehtimollik bilan buzg’unchining lug’atidan topiladi va A tomoning paroli “tuz” yordamida

xeshlangan. Agar A tomonning paroli buzg'unchining parol lug'atida bo'lsa, u holda buzg'unchi o'zidagi parol lug'atini yarmini, 2^{19}, hisoblagandan so'ng parolni aniqlaydi. Shuningdek, A tomonning paroli ¾ ehtimollik bilan buzg'unchining lug'atida mavjud emasligi sababli parolni aniqlash uchun o'rtacha 2^{55} hisoblash talab etiladi. Umumiy holda buzg'unchining bajarishi kerak bo'lgan amallar soni quyidagicha bo'ladi:

$$\frac{1}{4}(2^{19}) + \frac{3}{4}(2^{55}) \approx 2^{54.6}$$

Bunda buzg'unchining amalga oshiradigan hisoblash hajmi birinchi holat bilan (ya'ni, lug'at foydalanilmagan holat) bir xil bo'ladi.

Agar parol "tuz" siz xeshlangan bo'lsa, buzg'unchi o'zining barcha 2^{20} parolini xeshlab oladi va shundan so'ng kichik vaqt ichida buzg'unchi hujumni amalga oshiradi.

3 - holat. Mazkur holda, buzg'unchi parollar faylida saqlanayotgan 1024 ta parollardan birortasini buzsa ham yetarli bo'ladi. Buning uchun buzg'unchi o'zining parollar lug'atidan foydalana olmasin.

Faraz qilaylik, $y_0, y_1, \dots, y_{1023}$ parolning xeshlangan qiymatlari, parollar lug'atidagi barcha 2^{10} parol unikal va $p_0, p_1, \dots, p_{2^{56}-1}$ 2^{56} ta parollarning barcha variantlari bo'lsin. Parolni topishning barcha variantlarini topish hujumi kabi buzg'unchi zarur bo'lgan parolni topish uchun 2^{55} tekshirishni amalga oshirishi talab etiladi.

Agar parol "tuz"siz xeshlangan bo'lsa, buzg'unchi $h(p_0)$ hisoblaydi va uni har bir y_i ($i = 0,1,2, \dots, 1023$ uchun) bilan taqqoslaydi. Shundan so'ng, $h(p_1)$ ni hisoblaydi va barcha y_i lar bilan taqqoslab chiqadi. Bu holat qolganlari uchun ham xuddi shu ketma-ketlik takrorlanadi. Mazkur holda buzg'unchining har bir xeshni hisoblashi 2^{10} ta tekshirishni ta'minlaydi. Buzg'unchi amalga oshiradigan ish hajmi xeshlashlar soni bilan o'lchanishi (taqqoslashlar soni bilan emas) sababli va 2^{55} ta taqqoslash talab etilgani bois, buzg'unchi bajarishi kerak bo'lgan ish hajmi $\frac{2^{55}}{2^{10}} = 2^{45}$ ga teng bo'ladi.

Keyingi holatda parol “tuz” yordamida xeshlangan bo’lsin. Bunda, s_i xeshlangan parol y_i ni hisoblashda foydalanilgan bo’lsin. U holda, buzg’unchi $h(p_0, s_0)$ ni hisoblaydi va y_0 bilan taqqoslaydi, u $h(p_0, s_1)$ ni hisoblaydi va y_1 bilan taqqoslaydi, $h(p_0, s_2)$ ni hisoblaydi va y_2 bilan taqqoslaydi va tarzda davom etib, hisoblash $h(p_0, s_{1023})$ gacha davom etadi. Shundan so’ng, ushbu jarayon p_1, p_2 va boshqalar uchun davom ettiriladi. Umumiy holda esa, buzg’unchi tomonidan bajariladigan ishlar hajmi birinchi holatdagi kabi 2^{55} ga teng bo’ladi.

Bu hisoblashlar parolni xeshlashda “tuz” dan foydalanishning afzalligini ko’rsatadi. Biroq, amalda uchramasa ham buzg’unchining eng keng tarqalgan parollar lug’atidan foydalanmaganini ham inobatga olish zarur.

4-holat. Ushbu holatda buzg’unchi o’zining eng keng tarqalgan parollar lug’atidan foydalanib 1024 ta paroldan iborat parollar faylidan kamida bitta parolni topishning o’zi yetarli bo’lgan shartni ifodalaydi. Dastlab, parollar faylidagi 1024 ta paroldan bittasining buzg’unchi lug’atidagi paydo bo’lish ehtimoli $1 - (\frac{3}{4})^{1024} \approx 1$ ga teng bo’ladi. Shuning uchun, fayldagi parollar buzg’unchining lug’atida bo’lmagan holatni inobatga olish xavfsizdir.

Agar parollarni xeshlashda “tuz”dan foydalanilmagan bo’lsa, buzg’unchi osonlik bilan o’zining lug’atidagi parollarni xeshlaydi va fayldagi 1024 parolning xesh qiymati bilan taqqoslaydi. 1024 ta paroldan kamida bittasini lug’atda mavjudligini aniqlashning o’zi yetarli bo’lgan uchun, buzg’unchi tomonidan bajariladigan ish 2^{20} ga teng. Biroq, buzg’unchi tajribasiga ko’ra ushbu bajariladigan ishni kamaytirishi mumkin. Shunga qaramay, buzg’unchining lug’atida parollar faylidagi kamida bitta parol bo’lishi mumkin deb faraz qilaylik. Natijada, buzg’unchi o’zi kutgan parollar faylidagi bitta parolni aniqlashi uchun o’zining lug’atidagi parollarning yarmini, 2^{19} xeshlashi talab etiladi. Uchinchi holatda bo’lgani kabi, har bir xeshlash amali 2^{10} ta taqqoslashni talab etadi va shuning uchun buzg’unchidan bajarishi kutiladigan ish hajmi $2^{19}/_{2^{10}} = 2^9$ ga teng.

Agar parolni xeshlashda “tuz”dan foydalanilmagan va lug’atdagi parollarni xeshlash oldindan amalga oshirilgan bo’lsa, parollar faylidagi ixtiyoriy parolni

topish uchun qo’shimcha ish talab etilmaydi. Ya’ni, buzg’unchi parollar faylidagi parollarni o’zining parollar lug’atining oldindan hisoblangan qiymatlari bilan solishtiradi va natijada o’zining lug’atida mavjud bo’lgan parol aniqlanadi.

Endi amalda bo’lish ehimoli yuqori bo’lgan holat: parollar faylidagi xesh qiymatlar “tuz”dan foydalangan va buzg’unchi eng keng tarqalgan parollar lug’atidan foydalangan bo’lsa, $y_0, y_1, \dots, y_{1023}$ – fayldagi xeshlangan parollar va $s_0, s_1, \dots, s_{1023}$ – ushbu parollarga mos foydalanilgan “tuz” bo’lsin. Agar, buzg’unchi foydalanayotgan parollar lug’ati $d_0, d_1, \dots, d_{2^{20}-1}$ bo’lsa, u $h(d_0, s_0)$ ni hisoblaydi va y_0 bilan taqqoslaydi. Shu tartibda $h(d_1, s_0)$ni hisoblaydi va y_0 bilan taqqoslaydi, $h(d_2, s_0)$ hisoblaydi va y_0 bilan taqqoslaydi va h. Shunday qilib, buzg’unchi dastlab y_0 ni parollar lug’atidagi barcha parollar uchun taqqoslaydi. Bu holat har bir y_i uchun amalga oshiriladi.

Agar y_0 parol lug’atda mavjud bo’lsa (1/4 ehtimollik bilan), u holda buzg’unchi uni 2^{19} ta hisoblashdan so’ng aniqlaydi. Aks holda (3/4 ehtimollik bilan), buzg’unchidan 2^{20} ta hisoblash talab etiladi. Agar buzg’unchi y_0 parolni lug’atdan topsa, u holda o’zining ishini bajargan hisoblanadi. Aks holda, u y_1 ni hisoblashdan oldin 2^{20} ta hisoblashni bajarishi talab etiladi. Mazkur holatni davom ettirsak, buzg’unchi tomonidan bajarilishi mumkin bo’lgan ishni taxminiy hisobi quyidagiga teng bo’ladi:

$$\frac{1}{4}(2^{19}) + \frac{3}{4} * \frac{1}{4}(2^{20} + 2^{19}) + \left(\frac{3}{4}\right)^2 * \frac{1}{4}(2 * 2^{20} + 2^{19}) + \cdots + \left(\frac{3}{4}\right)^{1023} * \frac{1}{4}(1023 * 2^{20} + 2^{19}) < 2^{22}$$

Bu ko’rsatkichlar masalani yechish uchun talab etilayotgan hisoblashlar hajmi katta ekanligini anglatadi.

Umumiy holda agar foydalanilgan parol zaif bo’lsa, uni aniqlash osonroq va ixtiyoriy bir parolni buzg’unchi tomonidan aniqlab olinishi butun tizim xavfsizligini yo’qolishiga olib keladi.

3.2.6. Parol bilan bog’liq boshqa muammolar

Hozirgi kunda aksariyat foydalanuvchilar bir qancha qayd yozuvlaridan foydalanadilar. Foydalanuvchilar ko’p sonli parollarni esda saqlash qobiliyatiga ega emasligi sababli amalda bir xil parollardan foydalanishni afzal ko’radilar. Bu foydalanuvchining bitta parolini buzg’unchi tomonidan aniqlanishi, ko’plab qayd yozuvlarini ham buzilishiga olib keladi.

Bundan tashqari, sosial injineriya ham parollarni aniqlashda jiddiy ta’sir qiladi. Masalan, tizim ma’muri tomonidan qayd yozuv bilan bog’liq muammoni bartaraf etish uchun foydalanuvchidan uning paroli so’ralganda, aksariyat hollarda uni taqdim etilgani kuzatilgan. Yaqinda olib borilgan tadqiqotlarga ko’ra, foydalanuvchilardan parollari so’ralganda, 34% holatda ular tomonidan so’rov maqullangan [13].

Hozirgi kunda parollarni qo’lgan kiritishda “*keylogger*” nomli zararkunanda dasturiy vositalardan keng foydalaniladi. Bu zararkunanda dasturiy vositalar klaviaturadan kiritiluvchi barcha ma’lumotlarni saqlab qoladi va o’z serveriga yuborib turadi [41].

Shuningdek, xeshlangan parollarni aniqlaydigan maxsus dasturiy vositalar mavjud. Masalan, `LophtCrack` (Windows OT uchun) va `John the Ripper` (Unix OT uchun). Ushbu dasturiy vositalarda keng tarqalgan parollar lug’ati mavjud bo’lib, sodda parollarni osonlik bilan topishda qo’l keladi [13].

3.3. Ma’lumotlarni fizik himoyalash

Axborot xavfsizligini ta’minlashda amalga oshiriladigan dastlabki choralardan biri bu – *fizik xavfsizlik* hisoblanadi. 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’rnatilgani va me’yorida ishlayotganini kafolatlashi zarur.

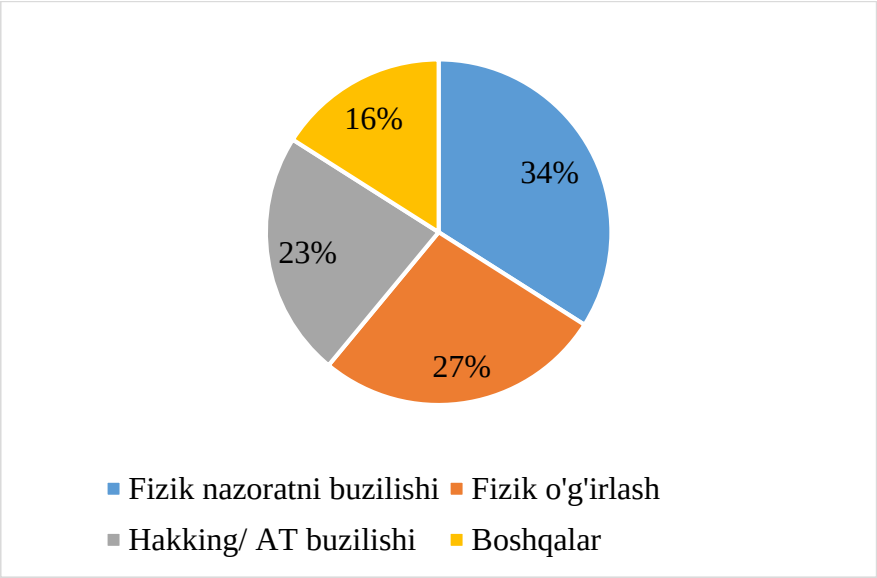
Fizik xavfsizlik qurilmalarni, shaxslarni, tarmoq va ma’lumotlarni hujumlardan himoyalaydi. Ma’lumot, tarmoq va qurilmalar himoyasi o’zida tabiiy

va sun’iy (inson tomonidan qilingan) tahdidlardan himoyalash vositalarini mujassamlashtiradi. Tashkilotlar fizik xavfsizlikni ta’minlashda mos himoya vositalaridan foydalanishda o’z infratuzilmasi 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 vositalaridan 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.

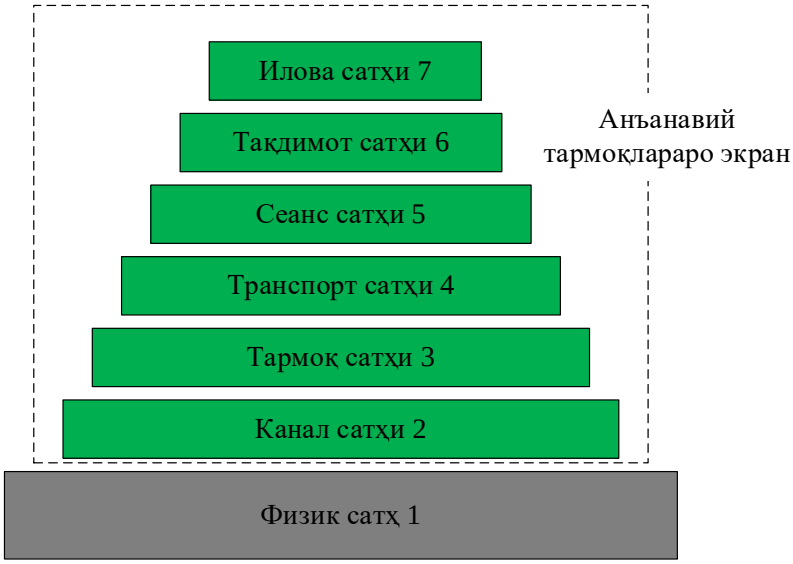
Fizik xavfsizlikning vazifasi dasturiy ta’minot va qurilmalarni o’z ichiga olgan tashkilot binosini va aktivlarini o’g’irlikdan, bosqinchilikdan, tabiy ofatlardan, iqlim o’zgarishlaridan, muhit o’zgarishlaridan va inson tahdidlaridan himoyalashdir. Tashkilotni mos ko’p sathli himoyalash choralari turli 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 tashkilotga dastlabki sathda 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 ventilyasiya tizimiga ega yaxshi jixozlangan suv quvur tizimini mos joyga o’rnatish, ogohlantirish tizimlari va h. ushbu bosqichda amalga oshiriladi. Keyingi sath fizik himoyaning eng muhim qismi bo’lib, tashqaridan va ichkaridan (xodimlar) kiruvchilar 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 foydalanishiga olib kelmoqda. Hujumchilar tashkilotning fizik xavfsizlik tizimidagi zaifliklardan foydalanb 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 [42] (34-rasm).



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

Fizik xavfsizlikni buzilishi boshqa xavfsizliklarni buzilishlaridan keskin farq qilib, ular juda ham kam hollarda texnik ma'lumotsiz 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, fizik xavfsizlik muammolari yanada ortadi. Masalan, tarmoqlararo ekran OSI modelining turli sathlarida himoyani tashkil etadi. Biroq, tashkilotning fizik xavfsizligiga ta'sir eta olmaydi (35-rasm).



35-rasm. Tarmoq sathlarida tarmoqlararo ekranlardan foydalanilishi

Fizik himoya tarmoq, ilova yoki ma’lumotlar bazasi xavfsizligi sohalariga o’xshash funksiyalarni bajarmay 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 tashkiloning fizik infratuzilmasiga 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’xtatilishaga olib keladi. Chaqmoq va momaqaldiroq natijasida elektr quvvati o’zgarib, ish faoliyatiga ta’sir qiladi va tashkilotdagi qurilmalarning xotira qismlariga tasir qiladi. Bundan tashqari, chaqmoq va momaqaldiroq natijasida kabellarda va boshqa ulanish tizimlarda qisqa tutashuvlar yuzaga kelishi mumkin.

Hisoblash qurilmalari 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 saqlovchilarga 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 etkazilishi mumkin.

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

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

3.3.1. Fizik xavfsizlikni nazoratlash

Biror fizik xavfsizlikni mos xavfsizlik nazoratisiz, amalga oshirish qiyin. Fizik xavfsizlik nazorati bardoshli fizik xavfsizlik muhitini yaratishi uchun turli darajalarda amalga oshirilishini talab etadi. Fizik xavfsizlik nazoratini qaysi darajada amalga oshirilishiga qarab, ular quyidagicha tasniflanishi 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 texnologiyalardan 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, kanalizasiya 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 tuzilma va arxitekturani loyihalash va rejalashtirish vaqtida tashkilot tomondan binodagi barcha aktivlarning ro’yxati tayyor bo’lishi lozim.

Tashkilot infratuzilma 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 infratuzilmani 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 hisoblanib, yong’in yuzaga kelganini avtomatlashgan yoki avtomatlashmagan holda aniqlaydi.

36-rasm. Yong’inga qarshi himoya vositalari

Aktiv yong’inga qarshi himoya 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 ishlarni avtomatik yoki noavtomatik tarzda amalga oshirishi talab etiladi.

Aktiv yong’inga qarshi himoya tizimi suv sepish, tutun/yong’indan ogohlantirish tizimlari, o’t o’chirish va turli 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, *tutunni aniqlovchilari, alangani aniqlovchilarni* va *issiqlikni aniqlovchilarni* o’z ichiga oladi.

- *yong’inni bartaraf etish tizimlari* inson aralashuvisiz yong’inni dastlabki bosqichlarida uni bartaraf etib, zararni kamaytirishga va qurilmalarni yo’q

bo’lishidan himoyalaydi. Yong’inni bartaraf etish tizimlari avtomatik va avtomatik bo’lmagan turlarga ajratiladi. Ushbu tizimlarga *o’to’chirgich (ognetushiyet), suv purkash tizim*larini misol 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 qaralib, boshqa biror tizim tomonidan ishga tushirilishni talab etmaydi.

Passiv yong’inga qarshi himoya usuli amaliyotda quyidagi usullar asosida 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 aloqador tizimlarni to’g’ri madadlash;
- yetarli sondagi qo’shimcha chiqish yo’llarining mavjudligi.

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. Ushbu 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 taqiqlash uchun foydalaniladi. Ichki to’siqlarni esa eshiklar, derazalar, panjaralar, oynalar, pardalar va boshqalar tashkil etadi.

Bino ichida foydalaniluvchi fizik to’siqlarning quyidagi turlari mavjud:

- *devorlar/ elektr devorlar/ metal to’siqlar* odatda taqiqlangan hududlarni, nazoratlanadigan hududlarni va ruxsatsiz kirishdan himoyani belgilashda foydalaniladi. Fizik to’siqlarni amalga oshirishdan asosiy maqsad:
  - hujumchini bloklash va ushlab qolish;
  - tashkilot chegarasini belgilash;
  - xavfsiz hududni tashqi hujumlardan himoyalash;

- transportlarni kirishidan himoyalash;
- qo’paruvchilik hujumlaridan himoyalash.

- *tumba* kichik vertikal shaklida bo’lib, avtomobillarni kirishidan himoyalaydi;
- *turniketlar* shaxs tomonidan mos tanga, bilet, barmoq izi yoki token ko’rsatilganda bir vaqtda bir shaxsni ichkariga kirishiga yoki chiqishiga ruxsat beradi;
- fizik himoyani tashkil qilishda bundan tashqari *turli eshiklar, oynalar, panjaralar, deraza pardalaridan* foydalaniladi.


a) elektr to’siqlar


b) Metal to’siqlar


s) To’mbalar


d) Turniket

37-rasm. To’siqlarga misollar

Fizik xavfsizlikni nazoratlash: xavfsizlik xodimi (qo’riqchi) tashkilotning fizik xavfsizligini tashkil etish, monitoring qilib borish 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 ixtiyoriy 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, ular 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 saqlanib boriladi.

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.

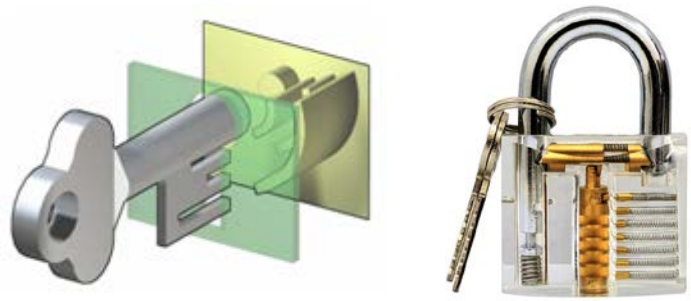
Axborot xavfsizligining bosh xodimi (Chief Information Security Officer). O'tgan davrlarda, axborot xavfsizligining bosh xodimi tashkilotdagi barcha xavfsizlikka aloqador jarayonlarni nazoratlashi, hattoki, tarmoq va tizim xavfsizligiga ham javobgar bo'lgan. Hozirda esa, ushbu shaxslarga asosan texnik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

Foydalanishlarni nazoratlash: autentifikasiya usullari. Tashkilot hududida shaxslarni autentifikasiyalash vazifasi o'rta to'siqlar vazifasini bajaruvchi turniketlar tomonidan yoki qo'riqchilar tomonidan ham amalga oshirilishi mumkin. Shaxslarni autentifikasiyalash usullarini umumiy holda quyidagi guruhlarga ajratish mumkin:

- biror narsani bilishga asoslangan;
- biror narsaga egalik qilishga asoslangan;
- biometrik parametrlarga asoslangan.

Fizik xavfsizlikni nazoratlash: fizik qulflar ruxsatsiz fizik foydalanishlarni cheklashda foydalaniladi. Har bir tashkilot o'zining xavfsizik 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 qulflarning ikki turi mavjud (38-rasm).



a) o’ralgan qulf b) tumbler qulfi

38-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.

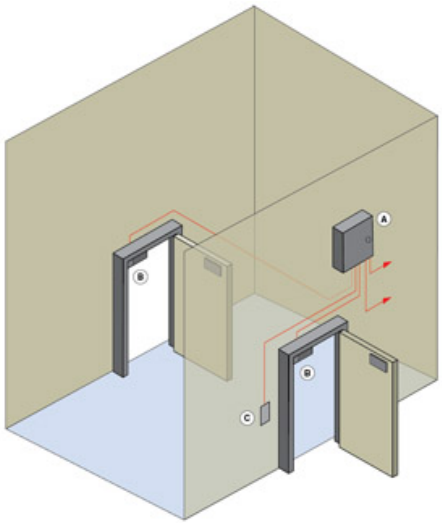
Elektr/ elektromagnetik qulflar: elektr yoki elektron qulflash tizimi elektr quvvatni kamaytirishga asoslangan bo’lib, natijada eshik ochiladi. Ulari odatda magnit yoki va elektromotor faollashtiradi va deaktivlashtiradi. Ushbu qulflar ochilishi uchun kalit talab etilmaydi.

Kombinasion qulflar raqam va simvollar kombinasiyasidan 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 skanelarlar yordamida turli qurollar yoki kontrabanda vositalarini, bombalar, yoki o’q otar qurilmalari aniqlanadi. Mazkur skanerlarga misol qilib, metalni aniqlovchilar, X-ray aniqlash tizimlari va harakat bo’ylab metalni aniqlash tizimlarini keltirish mumkin (39-rasm).

39-rasm. X-Ray metal detektorlar [2]

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 autentifikasiyalash smart karta, PIN kod yoki biometrik usullar asosida amalga oshirilishi mumkin (40-rasm).



40-rasm. Qopqon

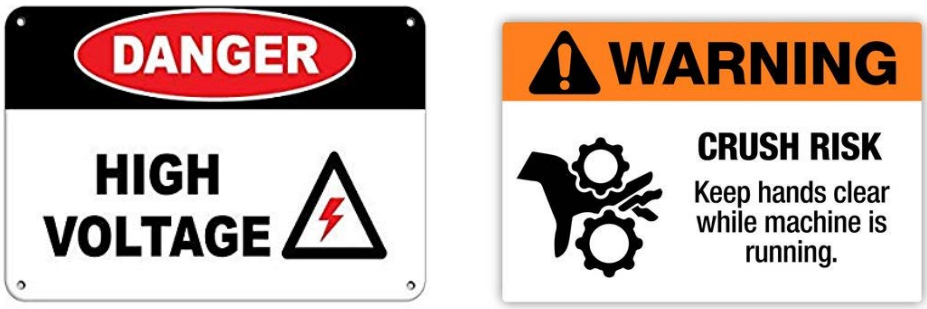
Fizik xavfsizlikni nazoratlash: xavfsizlik yorliqlari va ogohlantiruvchi signallar. Xavfsizlik yorliqlari xavfsizlik darajasi turlicha bo’lgan axborotdan foydalanishga ruxsatlarni cheklash uchun juda qulay hisoblanadi. Buning uchun

tashkilotdagi ma’lumotlar dastlab xavfsizlik yorliqlari bilan ta’minlanadi. Odatda quyidagi turdagi 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, ruxsat bor yoki yo’qligi aniqlanadi, agar ruxsat bo’lsa undan foydalanishga ruxsat beriladi.

Ogohlantiruvchi signallar odatda tashkilotda ko’p sonli xodimlarni ruxsatsiz harakatlarni cheklash uchun foydalaniladi. Odatda ogohlantiruvchi signallar sifatida “TAQIQLANGAN HUDUD” (RESTRICTED AREA), “OGOHLANTIRISh” (WARNING), “XAVFLI” (DANGER) iboralardan foydalaniladi (41-rasm).



41-rasm. Ogohlantiruvchi belgilar

Fizik xavfsizlikni nazoratlash: video kuzatuv vositalari tashkilotning aktivlarini bosqinchilardan va o’g’rilardan himoyalab, fizik xavfsizligini ta’minlashda muhim komponent hisoblanadi. Video kuzatuv moslamalari odatda tashkilotning kirish eshiklarida, zallarda va ishchi hududlarida o’rnatilib, tashkilotda kirish va chiqish harakatlarni kuzatishga yordam beradi. Hozirgi kundagi video kuzatuv vositalari nafaqat harakatlarni qayd etishga balki, noma’qul harakatlarni aniqlash imkonini beradi. Masalan, taqiqlangan jixoz olib kirayotgan yoki olib chiqayotgan holatni aniqlaydi yoki janjal bo’layotgan holatni aniqlab, ogohlantirish signalini yuboradi. Video kuzatuv vositalari sifatida hozirgi kunda, quyidagi kameralardan amalda foydalanib kelinmoqda (42-rasm).

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

42-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 tashkilotni fizik xavfsizligi nuqtai nazaridan o'zida quyidagilarni mujassamlashtiradi:

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

Fizik xavfsizlik muolajasi o'z ichiga quyidagilarni oladi:

- qulflash tizimini boshqarish;
- suqilib kirish insidentlarini qaydlash;
- tashrif buyuruvchilarni boshqarish;
- konfidensial materiallarni yo'q qilish;
- qog'oz ko'rinishidagi 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* siyosatiga ko'ra esa xodim o'z kompyuteridan foydalanish 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 atrofida 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, u holda 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’lganda yoritish uchun foydalaniladi;
- *favqulotda yoritish tizimlari* – elektr quvvati yoki elektr energiyasi manbalari ishdan chiqqanda tashkilot binolarini vaqtinchalik yoritish uchun foydalaniladi.

Boshqa fizik xavfsizlik choralari: quvvat manbalari. Quvvat manbalari nafaqat tashkilotning axborot texnologiyalari tizimiga balki, fizik xavfsizlikni ta’minlash tizimlariga ham katta ta’sir qiladi. Quvvatning yetarli darajada bo’lmasligi yoki tez-tez uzilib qolishi natijasida jixozlarga zarar yetishi mumkin. Tashkilotlarda quvvat manbaini uzulishi natijasida yuzaga keladigan zararni kamaytirish uchun quyidagi xavfsizlik choralarini ko’rish zarur:

- quvvat tebranishlariga tayyor turish;
- quvvat uzilishi kuzatilganda uzluksiz quvvat manbalaridan (UPS – Unintrruptible power supply) foydalanish;
- vositalarni tahdidlardan himoyalash tizimlarini o’rnatish;
- ish joylarida statik elektrga noma’qul ta’sirdan himoyalash tizimlarini o’rnatish;
- elektr quvvatidan ishlaydigan vositalardan to’g’ri foydalanish.

Ish joyining xavfsizligi: qabulxona. Tashkilotning qabulxonasi har doim mehmon va tashkilotlar o'rtasida o'zaro aloqa o'rnitishda muhim soha hisoblanadi. Qabulxona mehmonlar uchun qulay foydalanishni ta'minlagani bois, fizik xavfsizlik nuqtai nazardan zaif bo'lishi mumkin. Tashkilot qabulxonasida deyarli har kuni turli mehmonlar, hamkorlar, xodimlar va boshqalar bo'lishadi. Shu sababli, qabulxonadagilar ularning har birini tanib olishga harakat qilishi va qayd etishi lozim.

Ish joyining xavfsizligi: Server/ zaxira nusxalash qurilmalarining xavfsizligi. Har bir tashkilot o'z serverini va zaxira nusxalash vositalarining fizik xavfsizligini ta'minlashga e'tibor berishi lozim. Ushbu vositalarga nisbatan fizik ruxsatlarni cheklangan bo'lishi va undan faqat, ruxsat etilgan shaxslar foydalana olishi mumkin bo'ladi. Server va zaxira nusxalash qurilmalarining fizik xavfsizligini ta'minlash uchun quyidagilar amalga oshiriladi:

- server va zaxira nusxalash qurilmalarini alohida xonada saqlash. Bu chora ushbu qurilmalarni noma'lum va 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 autentifikasiyani joriy etish;
- serverlarni o'g'irlinishidan va zararlanishidan himoyalash uchun maxsus tagliklarga o'rnatish;
- turli quvvat o'zgarishidan himoyalash uchun serverlarni zaxira UPS vositasiga ulash;
- qurilmalarni qulflanuvchi xona yoki kabinetlarda saqlash;
- xodimlar tomonidan ixtiyoriy zaxira nusxalash va server vositalarini olib chiqib ketilmasligini ta'minlash.

Ish joyining xavfsizligi: Kritik aktivlar va olib yuriluvchi qurilmalar. Tashkilot har doim o'zining server va zaxira nusxalash vositalari bilan bir qatorda, boshqa kritik aktivlar, ishchi stansiyalar, routerlar va svitchlar, printerlar, boshqa tarmoq qurilmalari, olib yuriluvchi vositalar va boshqalarning xavfsizligiga e'tibor

berishi lozim. Bundan tashqari, tashkilot tarmoq kabellarining joylashuvi va ularning xavfsizligiga ham tashkilotga kiruvchi va chiquvchi barcha ma’lumotlar aynan ushbu axborot tarmog’i orqali harakatlangani sababli jiddiy e’tibor berishi 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 (43-rasm).

43-rasm. Noutbuklarni stolga qulflash vositasi

Muhitni nazoratlash: isitish, ventilyasiya 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 tizimini 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’lliniladi.

Muhitni nazoratlash: elektromagnit shovqinlarni ekranlash. Tashkilotda elektron qurilmalardan hosil bo’lgan elektromagnit shovqinlar atrofdagi boshqa qurilmalar ishiga ta’sir etishi mumkin. Elektromagnit shovqinlarni ekranlashda elektron vositalar metal bilan qoplanadi va tarqaluvchi elektr to’lqinini boshqa vositalarga ta’siri keskin kamayadi. Bundan tashqari, qurilmalarni maxsus

materiallar bilan to’sish orqali boshqa qurilmalardan ajratish mumkin. Tashkilotlarda elektron qurilmalar ko’p bo’lgan hollarda (masalan, telekommunikasiya yoki shifoxonalarda) ularni ekranlash zaruriyati yanada ortadi.

Fizik xavfsizlik: ogohlik / o’qitish. Yaxshi o’qitilgan va malakaga ega bo’lgan xodim tashkilot 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’ulotlarini afzalligi:
    - barcha noravshan va noaniq masalalar shu joyning o’zida aniqlanadi;
    - vebga asoslangan yoki uchrashuvga asoslangan o’qitish sessiyalarini amalga oshiradi;
    - rol o’ynash yoki simulyasiya 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 veb sayt* – xavfsizlik haqida xabardor qiluvchi veb 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 uchun master klass darslarida amalga oshiriladi.

Xulosa o’rnida fizik xavfsizlikni amalga oshirilganini quyidagilar orqali baholanadi:

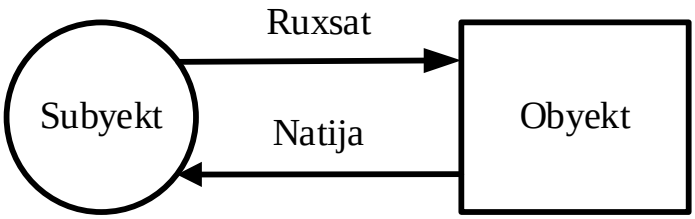
1. Ruxsatsiz foydalanishlarni oldini olish uchun mos foydalanishlarni nazoratlash usullarini o’rnatilganligi.
2. Muhim hududlar to’g’ri yoritish tizimi asosida kuzatilayotgani.
3. Turli tahdidlar, yong’in, tutun, elektr, suv va boshqalarni aniqlovchi va ogohlantiruvchi tizimlar o’rnatilgani va ularni to’g’ri ishlayotgani.
4. Eshiklarni qulflash tizimini to’g’ri o’rnatilgani va ularni to’g’ri ishlayotgani.
5. Tashkilot binosi va hududi yetarli sondagi qo’riqchilar tomonidan qo’riqlanayotgani.
6. Xavfsizlik xodimlarini o’quv mashg’ulotlariga to’g’ri yuborilgani.
7. Xavfsizlik xodimlarini ishonchli agentliklardan olingani.
8. Tashkilotdagi kuzatuv kameralari to’g’ri o’rnatilgani va uzluksiz ishlayotgani.
9. Fizik xavfsizlik insidentlarini aniqlash va qayd qilish uchun to’g’ri muolajalar amalga oshirilgani.
10. Favqulotda vaziyatlarda xodimlar bilan aloqa o’rnatishga oid axborotni mavjudligi.

3.4. Ma’lumotlardan foydalanishni mantiqiy boshqarish

3.4.1. Foydalanishni boshqarish

Avtorizasiya foydalanishlarni nazoratlashning autentifikasiyadan o’tgan foydalanuvchilar harakatlarini cheklash qismi bo’lib, aksariyat hollarda foydalanishni boshqarish modellari yordamida amalga oshiriladi. Ushbu bo’limda ma’lumotlarga nisbatan foydalanishni mantiqiy boshqarish tartibi bilan tanishib chiqiladi.

Foydalanishni boshqarish subyektni obyektga ishlash imkoniyatini aniqlashdir. Umumiy holda foydalanishni boshqarish quyidagi diagramma bilan tavsiflanadi (44-rasm):

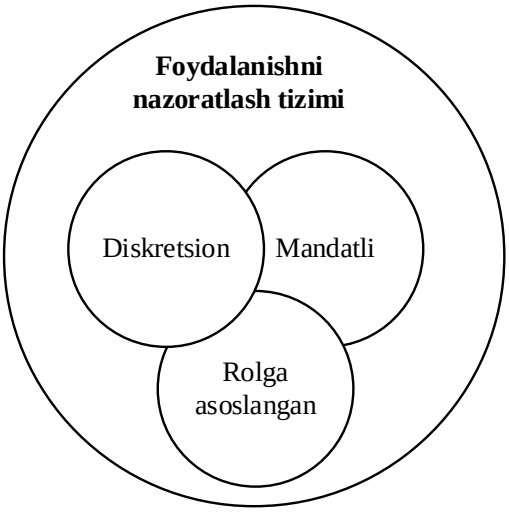


44-rasm. Foydalanishni boshqarish

Hozirda tizimlarda obyektlardan foydalanishlarni boshqarishning turlicha usullar mavjud bo'lib, ularga quyidigalarni misol keltirish mumkin:

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

Tizimda ushbu foydalanish usullari bir-biridan alohida-alohida foydalanilishi talab etmaydi va ularning kombinasiyasidan ham foydalanish mumkin (45-rasm).

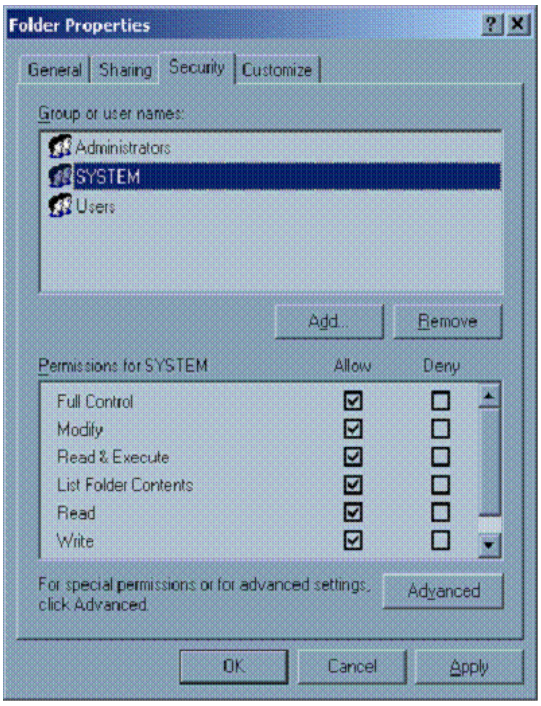


45-rasm. Foydalanishni boshqarish tizimlari

3.4.2. 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 identifikasiya axborotiga asoslanadi. Masalan, UNIX operasion 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 operasion tizimlarda foydalanishlarni boshqarish uchun foydalaniladi. Masalan, quyidagi 46-rasmda DAC usulini Windows NT/2k/XP OTlarida foydalanish holati keltirilgan.



46-rasm. Windows XP da DACdan foydalanish

Biroq, DACning jiddiy xavfsizlik muammosi bu - ma'lumotlardan foydalanish huquqiga ega bo'lmagan subyektlar tomonidan foydalanilmasligi to'liq kafolatlanmaganidir. Bu holat ma'lumotdan foydalanish huquqiga ega bo'lgan biror bir foydalanuvchini ma'lumot egasining ruxsatisiz foydalanish huquqiga ega bo'lmagan foydalanuvchilarga yuborish imkoniyati mavjudligida namayon bo'ladi. Bundan tashqari, DACga tegishli yana bir kamchilik sifatida tizimdagi barcha obyektlar ulardan foydalanishni belgilaydigan suyektlarga tegishli. 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 tizimi dastlab obyekt hyech kimga biriktirilmagan holatda “yopiq” deb ataladi. Agar obyekt foydalanuvchiga biriktirilsa va ulardan foydalanish bo’yicha cheklovlar o’rnatilgan bo’lsa, unda “ochiq” obyekt deb ataladi.

3.4.3. Foydalanishni boshqarishning MAC usuli

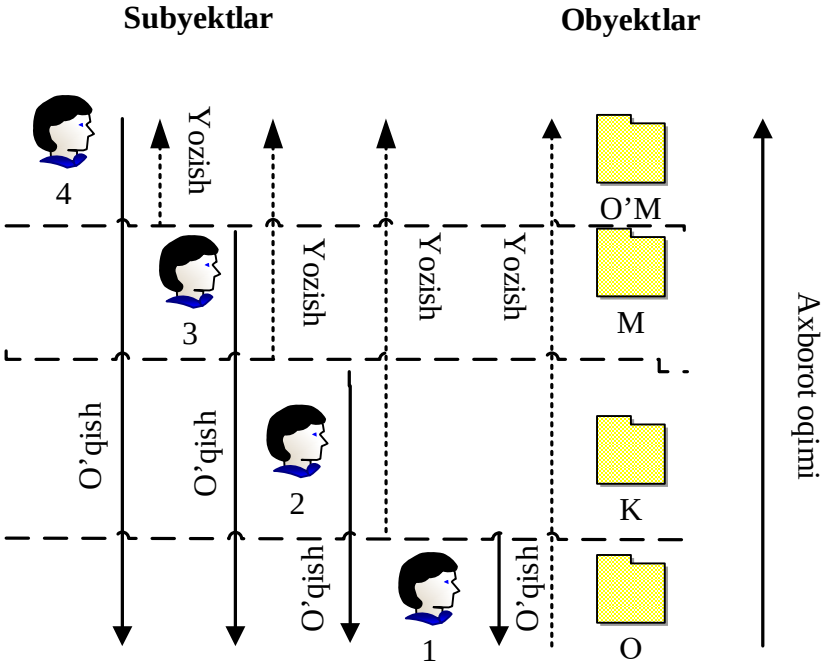
Foydalanishning mazkur usulida foydalanish ruxsati obyektning egasi tomonidan berilmaydi. Masalan, Alisa TOP SECRET ruxsatnomasiga ega bo’lgan subyektlarga ushbu bosqichdagi hujjatlarni to’liq nazorat qilish imkoniyati bo’lmaganligi sababli ruxsat bera olmaydi. MAC usuli bilan foydalanishni boshqarish xavfsizlik markazlashgan holatda xavfsizlik siyosati ma’muri tomonidan 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 MAS usuli o’rnatilgan tizimlar xavfsizlik siyosati ma’muriga tashkilot bo’ylab xavfsizlik siyosatini amalga oshirish imkoniyatini beradi. MAS usulida foydalanuvchilar tasodifan yoki qasddan 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 klassifikasiyalashga 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 darajasini: *O’TA MAXFIY (O’M), MAXFIY (M), KONFIDENSIAL (K)* va *OChIQ (O)* shaklida yoki: *O’M>M>K>O.*

MAS asosida axborot maxfiyligini ta’minlash. Agar obyekt va subyekning xavfsizlik darajalari orasidagi bir qancha bog’liqlik shartlari bajarilsa, u holda subyekt obyektdan foydalanish huquqiga ega bo’ladi. Xususan, quyidagi shartlar bajarilish kerak (47-rasm):

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



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

Ushbu modelda foydalanuvchi va subyekt tushunchalari bir – biridan farq qiladi. Xususan, xavfsizlik darajasi subyektga berilsa, foydalanuvchi esa u yoki bu vaqtda subyekt nomidan ish qilishi mumkin bo’ladi. Shuning uchun, turli holatlarda 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.

Yuqorida keltirilgan modelni muvofiqligini shubha ostiga qo’yyadigan 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, u holda o’qish uchun ruxsat beriladi;

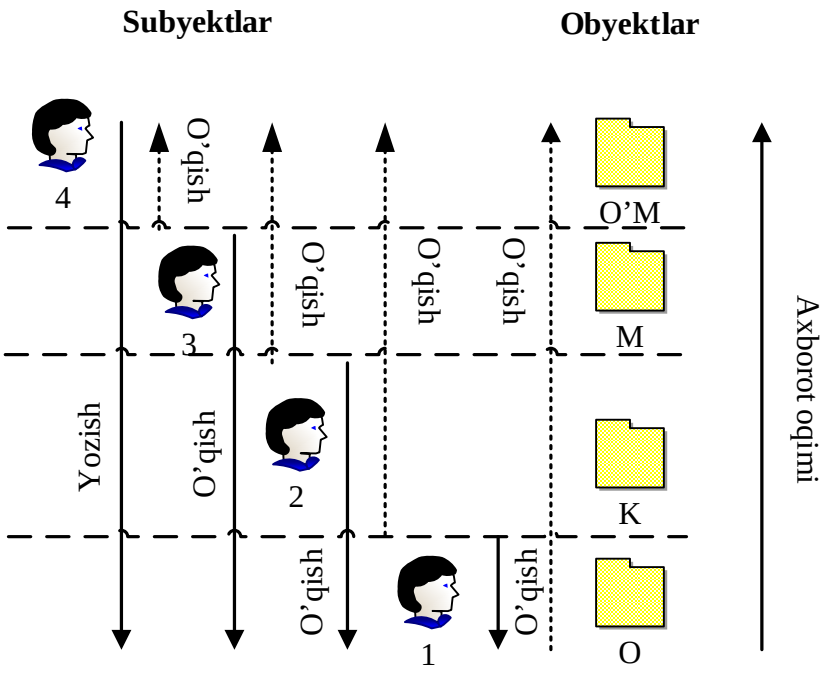
- agar subyektning xavfsizlik darajasi obyektning xavfsizlik darajasiga teng bo’lsa, u holda yozishga ruxsat beriladi.

2. Diagrammadan ko’rinib turgani kabi 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 “M”, “K” va “O” ishonch darajasidagi subyektlar nomidan ish ko’rishi mumkin.

Axborot ishonchligini ta’minlash. Axborot konfidensiyalligini 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’lumotni kiritishi mumkin. Mazkur model uchun yuqorida keltirilgan qoidalarni quyidagicha o’zgartirish mumkin:

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

Ko’rinib turgani kabi yuqorida keltirilgan holatning o’rni almashgan (48-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.



48-rasm. Ma’lumot ishonchligini ta’minlash uchun axborot oqimini boshqarish

3.4.4. Foydalanishni boshqarishning RBAC usuli

RBAC usulida foydalanishni boshqarishning asosiy g’oyasi tizimning ishlash prinsipini tashkilotda kadrlar vazifasini haqiqiy ajratilishiga maksimal darajada yaqinlashtirishdir.

RBAC usuli foydalanuvchini axborotga ruxsatini 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 qarish mumkin. Shunday qilib, har bir obyekt uchun har bir foydalanuvchini 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’zidan 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 muayan amallarni bajarish huquqlari har bir foydalanuvchi yoki foydalanuvchilar guruhi uchun ro’yxatga olingan bo’ladi. Rolli modelda rol va foydalanuvchi tushunchalarini ajratish vazifani ikki qismga ajratish imkonini beradi: foydalanuvchi rolini aniqlash va rol uchun obyektga bo’lgan ruxsatni aniqlash. Ushbu yondashuv boshqaruv jarayonini foydalanuvchini javobgarlik sohasini o’zgartirganda undan eski rolni olib tashlash va yangi vazifasiga mos kelidagan rolni berishning o’zi kifoya qilgani bois sezilarli darajada soddalashtiradi. Agar foydalanish huquqi bevosita foydalanuvchi va obyektlar o’rtasida aniqlansa, mazkur muolaja yangi foydalanuvchi huquqlarini qayta tayinlashi uchun ko’p harakatlarni talab qiladi.

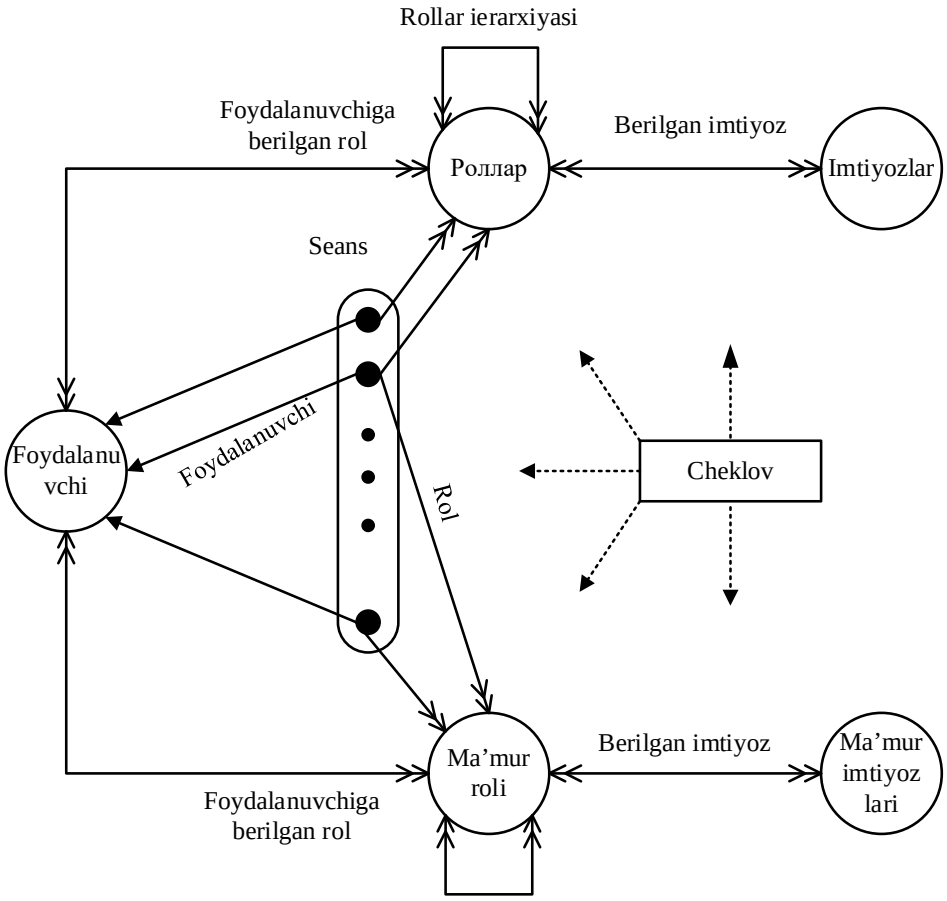
2. Rollar iyerarxiyasi. Rollarning haqiqiy iyerarxiyasini yaratish orqali real biznes jarayonlarini aks ettiruvchi rollar tizimini yaratish mumkin. Har bir rol o’z imtiyozlari bilan bir qatorda boshqa rollarning imtiyozlariga ega bo’lishi mumkin. Ushbu yondashuv tizimni boshqarishni sezilarli darajada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

4. Majburiyatlarni ajratish. Tizimda foydalanishlarni boshqarishning yana bir muhim prinsiplaridan biri bu – 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 olish mumkin. Shubhasiz, bu amallarni bir shaxs bajara olmaydi. Rollarga asoslangan usul esa ushbu muammoni maksimal darajada osonlik bilan hal qilishga yordam beradi.

Rasmiy ko’rinishda RBAC usulini quyidagicha tasvirlash mumkin (49-rasm):



49-rasm. RBAC modeli

Model quyidagi mazmunga ega: foydalanuvchilar, rollar va imtiyozlar. Foydalanuvchi sifatida inson yoki uning nomidan ish ko’ruvchi dastur bo’lishi mumkin. Rol foydalanuvchini tashkilotda faoliyat turi bo’lsa, imtiyoz esa tizimning bir yoki bir nechta obyektlaridan foydalanish uchun aniqlangan ruxsat.

Diagrammadagi “rollarni foydalanuvchilarga tayinlash” va “imtiyozlarni tayinlash” munosabati ko’pga-ko’p 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 ro’lga tegishli yoki bir nechta rollar bitta imtiyozga ega bo’lishi mumkin. Shuningdek, ushbu modelda xususiy buyurtma qilingan to’plam – rollar iyerarxiyasi mavjud. Ushbu to’plamda x va y rollar uchun $x > y$ a’zolik aloqasi x rol y rol imtiyozlarini meros qilib olganini anglatadi. Seans foydalanuvchini ko’p rollarda o’z ichiga oladi. Bunda, foydalanuvchi bir qancha vazifani bajarish uchun seansni faollashtiradi. Shu nuqtada tizim foydalanuvchidan vazifani bajarish uchun talab qilinadigan rollarni va imtiyozlarni aniqlab, qolganlarini taqiqlashi mumkin.

3.4.5. 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 hak.) 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 asosiy tushunchalar sifatida: qoida (rules), siyosat (policy), qoida 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, o'zida maqsad, ta'sir, shart, majburiyat va maslahatlarni o'z ichiga oladi. Maqsad – bu subyekt obyekt ustida nima harakatlarni amalga oshirishidir (o'qish, yozish, o'chirish va hak.). Ta'sir mantiqiy ifodalarga asoslangan bo'ladi va tizim foydalanish uchun *ruxsat, taqiq, mumkin emas, aniqlanmagan* holatlaridan biriga teng bo'lgan ruxsatni berishi mumkin. *Mumkin emas* buyrug'i mantiqiy shart noto'g'ri bo'lganda qaytarilsa, ifodani hisoblash vaqtida yuzaga kelgan xatoliklar uchun *aniqlanmagan* ta'sirini 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.

3.4.6. Foydalanishni boshqarish matrisasi

Avtorizasiyaning klassik ko'rinishi Lampsonning foydalanishni boshqarish matrisasidan boshlanadi. Ushbu matrisa operasion tizimni barcha foydalanuvchilar uchun turli ma'lumotlarni boshqarishi xususisidagi qarorni qabul qilishida zarur bo'lgan barcha axborotni o'z ichiga oladi. Bunda, operasion tizimdagi foydalanuvchilar *subyekt* sifatida va tizim resurslari *obyekt* sifatida qaraladi. Avtorizasiya sohasidagi ikkita asosiy quruvchilar: *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 va ustunlari obyektlarni ifodalaydi. Ko'rinib

turgani kabi, biror subyekt S va obyekt O uchun berilgan imtiyozlar ularning matrisadagi indekslari kesishgan nuqtada saqlanadi. Quyidagi 6-jadvalda foydalanishni boshqarish matrisasi keltirilgan bo'lib, unda imtiyozlar UNIX operasion tizimidagi imtiyozlar shaklida, ya'ni, x, r va w lar mos ravishda *bajarish*, *o'qish* va *yozish* amalini anglatadi.

6-jadval

Foydalanishni boshqarish matrisasi

	OT	Buxgalteriyaga oid dastur	Buxgalteriyaga oid ma'lumot	Sug'urta ma'lumoti	To'lov qaydnomasi ma'lumoti
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

Yuqoridagi jadvalda aks ettirilgani kabi, 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'lumotlariga qasddan yoki bexosdan buzilishiga yo'l qo'ymasdan kirish huquqini beradi.

3.4.7. ACL yoki C-list

Foydalanishni boshqarish jadvalida barcha subyektlar va barcha obyektlar mavjudligi tufayli, u avtorizasiya qarorlariga tegishli barcha ma'lumotlardan tashkil

topgan. Biroq, katta foydalanishni boshqarish matrisasini boshqarish amaliy tomondan mushkul. 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 matrisasi har qanday obyektga har qanday subyekt tomonidan bajariladigan ishlar uchun tekshirishili hisoblash tizim uchun katta yuklamani keltirib chiqaradi.

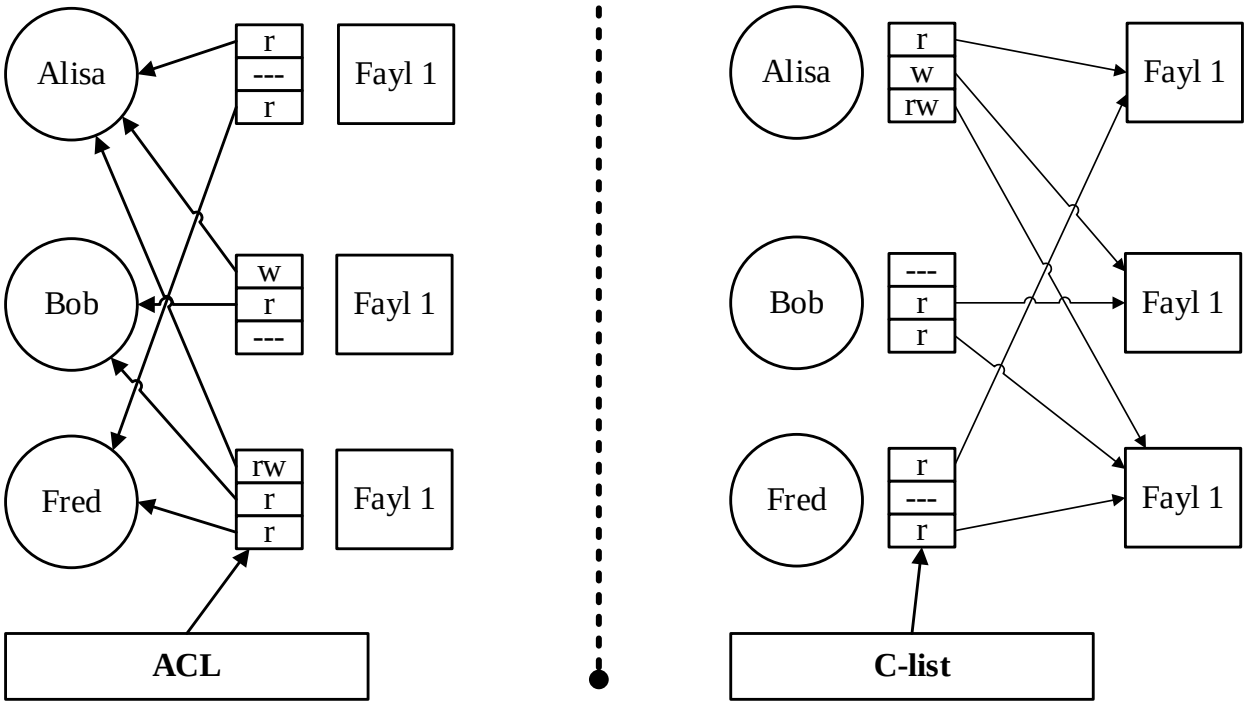
Avtorizasiya amallarini maqbul amalga oshirish uchun, foydalanishni boshqarish matrisasi boshqariluvchi qismlarga bo'linishi shart. Foydalanishni boshqarish matrisasini bo'laklarga ajratishning ikkita usuli mavjud. Birinchi usuli, matrisani ustunlar bo'yicha bo'lish va har bir ustun mos obyekt bilan saqlanadi. U holda, obyektdan foydalanishga murojaat bo'lganda foydalanishni boshqarish matrisasining ushbu ustuni olinadi va amalni bajarishga ruxsat berilgani tekshiriladi. Ushbu ustunlarni ACL kabi bilish mumkin. Masalan, 6-jadvaldagi sug'urta ma'lumotiga tegishli bo'lgan ACL quyidagicha:

$$(\text{Bob}, -), (\text{Alisa}, rw), (\text{Sem}, rw), (\text{buxgalteriyaga oid dastur}, rw)$$

Alternativ holatda, foydalanishni boshqarish matrisasini satrlar bo'yicha, har bir satr mos subyekt bilan saqlanadi. U holda, subyekt tomonidan biror amalni bajarishga harakat qilinsa, amalni bajarishga ruxsat borligini bilish uchun foydalanishni boshqarish matrisasining mazkur satriga qaraladi. Mazkur yondashuv imtiyozlar ro'yxati kabi yoki C-list deb ataladi. Masalan, 3.1-jadvaldagi Alisaning imtiyozlar ro'yxati yoki C-list quyidagiga teng:

$$(OT, rx), (, \text{buxgalteriyaga oid dastur}, rx), (\text{buxgalteriyaga oid ma'lumot}, r),$$
$$(\text{sug'urta ma'lumoti}, rw), (\text{to'lov qaydnomasi ma'lumoti}, rw)$$

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 quyidagi 50-rasmda keltirilgan.



50-rasm. ACL vs C-list

50-rasmdagi ko’rsatkichlar qarama-qarshi yo’nalishlardaligini, ya’ni, ACL uchun ko’rsatkich resurslardan foydalanuvchilarga qarab yo’nalgan bo’lsa, C-list uchun esa ko’rsatkichlar foydalanuvchilardan resurslarga qarab yo’nalganligini ko’rish mumkin. Bu ko’ringan ahamiyatsiz farq imtiyozlar (C-list) bilan foydalanuvchilar va fayllar orasidagi aloqadorlik tizim ichida qurilishini anglatadi. ACLga asoslangan tizimda esa, foydalanuvchilarni faylga aloqadorligi uchun alohida usullar talab etilgani bois, C-list ACL ga nisbatan bir qancha xavfsizlik nuqtai nazaridan afzalliklarga ega va shuning uchun C-list ustida kam sonli ilmiy tadqiqot ishlari olib borilgan.

Tartibsiz yordamchi. Tartibsiz yordamchi bu – ko’p jabhalarda klassik xavfsizlik muammosi hisoblanadi. 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 ma’lumoti yoziluvchi fayl nomini kiritishi talab etiladi. Biroq, Alisaga BILL nomli faylni zararlashi

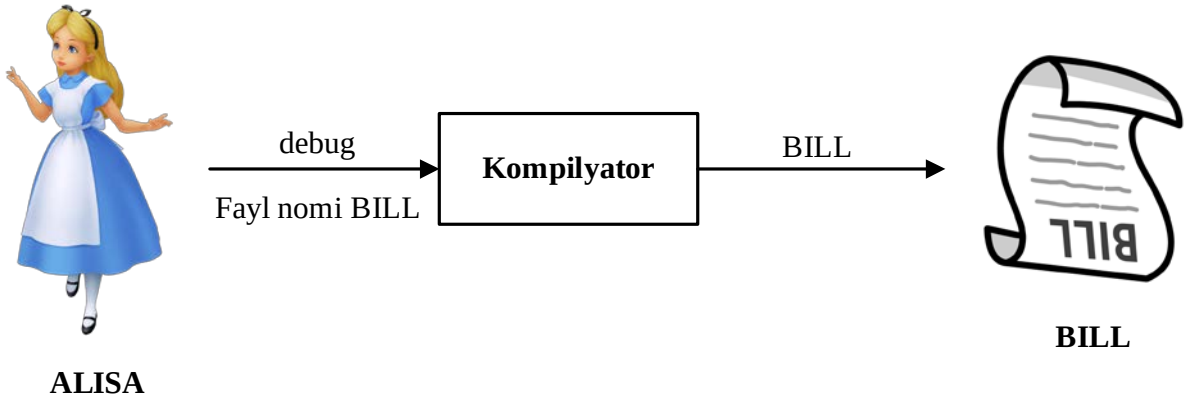
mumkinligi sababli, unga yozish ruxsati mavjud emas. Ushbu senariy uchun foydalanishni boshqarish matrisasi quyidagi 4-jadvalda keltirilgan.

4-jadval

Tartibsiz yordamchi holati uchun foydalanishni boshqarish matrisasi

	Kompilyator	BILL
Alisa	x	-
Kompilyator	rx	rw

Faraz qilinsin, 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 (51-rasm).



51-rasm. Tartibsiz yordamchi

Bu nima uchun tartibchiz 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 bilan buni osonlikcha bartaraf etish mumkin. Imtiyozga asoslangan tizimlarda, Alisa kompilyatorga murojaatni amalga oshirganda, unga o’zining C-listini beradi. Bu holda kompilyator Alisaning C-listini

tekshiradi va agar imtiyozi bo’lgan taqdirda debag faylni yaratadi. Alisani BILL faylini qayta yozishga ruxsati bo’lmagani sababli, 3.22-rasmdagi holat kuzatilmaydi.

ACL va C-listni foydali tomonlarini o’zaro solishtirish 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 bilan (C-list) vakolatlar berish oson va foydalanuvchi qo’shish yoki o’chirish 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, ACL hozirgi kunda amaliyotda C-listdan ko’ra ko’p foydalaniladi.

3.4.8. Ko’p sathli xavfsizlik modellari

Ushbu bo’limda ko’p sathli xavfsizlik modellari qarab chiqiladi. Xavfsizlik modellariga xavfsizlikka oid darsliklarda alohida e’tibor berilgan bo’lsada, mazkur bo’limda ikkita aniq xavfsizlik modeliga to’xtalib o’tiladi.

Umuman olganda xavfsizlik modellari tavsif bo’lib, mazkur modellar himoyalanish uchun nima kerakligini ko’rsatadi. Biroq, ular haqiqiy savolga, ya’ni, himoyani qanday ta’minlash kerak degan savolga javob bermaydi. Modellar himoya uchun asos yaratishga mo’ljallangani bois, bu ularning kamchiligi hisoblanmaydi. Biroq, bu xavfsizlikni modellashtirishning amaliy yordamiga xos bo’lgan cheklovdir.

Ko’p sathli xavfsizlikka (yoki multilevel security, MLS) tegishli ma’lumotlar barcha buzg’unchilik haqidagi manbalarda mavjud. MLS da subyektlar sifatida foydalanuvchilar (umumiy holda insonlar) va obyektlar sifatida himoyalanuvchi ma’lumotlar olingan (masalan, hujjatlar). Bundan tashqari, *klassifikasiyalash* tushunchasi obyektlarga taalluqli bo’lib, subyektlarga nisbatan *ruxsatnomalar* tushunchasi qo’llaniladi.

AQShning Department of Defence (yoki DOD) tashkilotida to’rtta sathdagi klassifikasiyalash va ruxsatnomalardan foydalaniladi:

TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED (3.1)

Masalan, SECRET ruxsatnomasiga ega subyektga SECRET yoki undan kichik yorliqdagi ma’lumotlardan foydalanish imtiyozi mavjud bo’lsa, TOP SECRET yorlig’idagi ma’lumotdan foydalanish imtiyoziga ega emas.

Faraz qilaylik, O obyekt bo’lsa, S unda subyekt bo’lsin. U holda O klassifikasiyani va S ruxsatnomani anglatadi. O ning xavfsizlik sathi $L(O)$ sifatida va S ning xavfsizlik sathi $L(S)$ kabi belgilanadi. DOD tizimida (3.1) tengligida ko’rsatilgan 4 ta sathli klassifikasiyalash va ruxsatnomalardan foydalaniladi. Shuningdek, SECRET ruxsatnomasini oluvchi shaxs uchun ko’p yoki kam muntazam tekshiruvlar talab etiladi. TOP SECRET uchun esa keng qamrovli tekshiruv, poligraf tekshiruvi, psixologik holati va boshqalar talab etiladi.

Axborotni klassifikasiyalash bilan bog’liq ko’plab amaliy muammolar mavjud bo’lib, ularga mos klassifikasiyalash har doim ham aniq bo’lmasligi va ikkita malakali foydalanuvchilarda tamomila turlicha ko’rinishlarda bo’lishi mumkinligi holatini misol keltirish mumkin. Shuningdek, klassifikasiyalashda qo’llaniluvchi donadorlik darajasi ham muammo bo’lishi mumkin. Umumiy holda olinganda TOP SECRET bo’lgan, lekin har bir paragrifi alohida olinganda UNCLASSIFIED darajasidagi hujjatni yaratish mutlaqo mumkin. DOD ichida source codeni klassifikasiyalashda bu muammo ba’zida yanada og’irlashadi. Donadorlikning ravshanlik tomoni bu – yig’ish mumkinligidir. Chunki, dushman UNCLASSIFIED turidagi hujjatlarni yig’ish orqali TOP SECRET darajasidagi hujjatni hosil qilishi mumkin.

Turli darajali subyektlar va obyektlar bir tizim resurslaridan foydalanganda ko’p sathli xavfsizlik talab etiladi. Ko’p sathli xavfsizlik tizimining maqsadi foydalanishni boshqarish shaklini subyektlarni cheklash orqali amalga oshirishdan iborat bo’lib, bunda ular faqat ruxsati mavjud obyektlardan foydalanish huqiqiga ega.

MLSning ko’plab modellari mavjud bo’lib, quyida ular orasidan eng soddalari bilan tanishib chiqiladi. Boshqa modellar amalda foydalaniluvchi va tahlil qilishda juda ham murakkabdir.

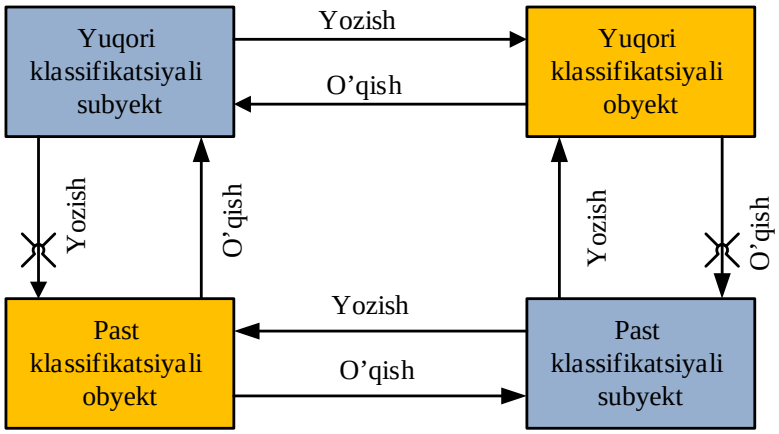
Bell-Lapadula modeli. Birinchi ko’rib o’tiluvchi xavfsizlik modeli Bell-Lapadula (Bell-LaPadula, BLP) bo’lib, bu nomlanish uning yaratuvchilari Bell va Lapadula nomlariga berilgan. BLPning asosiy maqsadi har qanday MLS tizimini qanoatlantirishi kerak bo’lgan konfidensiallikka nisbatan minimal talablarni to’plashdir. BLP quyidagi ikki qoidadan tashkil topgan:

Xavfsizlikni oddiy sharti: agar faqat va faqat $L(O) \leq L(S)$ shart bajarilganda S subyekt O obyektni o’qishi mumkin.

**-Xususiyat* (erkinlikni cheklash): faqat va faqat $L(S) \leq L(O)$ shartda subyekt S obyekt O ga yozishi mumkin.

Xavfsizlikni oddiy shartiga ko’ra Alisa tegishli ruxsatnomasi bo’lmagan hujjatni o’qiy olmaydi. Ushbu shart har qanday MLS tizimida aniq talab etiladi. Bu yerda, erkinlikni cheklash xususiyati unchalik yoritilmagan. Ushbu xususiyat, masalan, TOP SECRET axborotni SECRET hujjatda yozilishidan himoyalashni ta’minlaydi. Bu MLS xavfsizligini buzadi, chunki SECRET darajasiga ega foydalanuvchi TOP SECRET klassidagi ma’lumotni o’qiy oladi. Yozish qasddan yoki masalan, kompyuter virusi natijasida yuzaga kelishi mumkin.

Xavfsizlikni oddiy shartini “o’qimaslik” deb xulosa qilish mumkin. Erkinlikni cheklash esa “yozilmaydi” degan ma’noni anglatadi. Shundan qilib, BLP ba’zan qisqa o’qiladi, “o’qimaydi, yozmaydi” (52-rasm).



52-rasm. Bell-Lapadula modeli

Xavfsizlikda soddalik mavjudligi yaxshi bo’lsada, BLP juda oddiy bo’lishi mumkin. Bu haqida MkLean shunday deydi: “shunchaki ahamiyatsiz bo’lgani uchun unga ega bo’lmagan xavfsizlikning real modelini tasavvur qilish qiyin”. BLP da teshiklarni ochishga urinishda MkLean administratorga obyektlarni vaqtincha qayta klassifikasiyalashga ruxsat berilgan “Z tizim”ni aniqladi. Bunda BLP ni buzmasdan turib, “yozib olinishi” mumkin. “Z tizim” BLP ruhini aniq buzadi, ammo aniq taqiqlanmaganligi sababli, bunga ruxsat berilgan.

MkLeanning tanqidiga javoban Bell va Lapadula BLP ni «tinchlik xususiyati» bilan mustahkamladilar. Aslida ushbu xususiyatning ikki versiyasi mavjud. Kuchli tinchlik hususiyati xavfsizlik yorliqlari xech qachon o’zgarmasligini takidlaydi. Bu MkLean tomonidan aytilgan “Z tizim”ni BLPdan tamomila olib tashlaydi. Biroq, bu holat amalda mavjud emas. Chunki, xavfsizlik belgilari ba’zan o’zgarib turushi mumkin. Masalan, DOD doimiy ravishda kuchli tinchlik xususiyatiga rioya qilishda imkonsiz bo’lgan hujjatlarni deklassifikasiyalaydi. Boshqa bir misolda, ko’pincha eng kam imtiyozni qo’llash maqsadga muvofiqdir. Aytaylik, agar foydalanuvchi TOP SECRET ruxsatnomasiga ega bo’lsa, biroq u faqat UNCLASSIFIED turidagi veb sahifalarni ko’rib chiqayotgan bo’lsa, u holda unga UNCLASSIFIED ruxsatnomasini berish mumkin. Agar foydalanuvchiga keyinchalik yuqori ruxsatnoma kerak bo’lsa, uning joriy ruxsatnomasi oshiriladi. Bu “yuqori suv belgisi prinsipi” nomi bilan ma’lum va u quyida Biba modelida ko’rib o’tiladi.

Shuningdek, Bell-Lapadula zaif tinchlik xususiyatini taklif etdi. Bunga ko’ra, “o’rnatilgan xavfsizlik siyosatiga” ta’sir qilmasa xavfsizlik yorlig’i o’zgarib turishi mumkin. “Zaif tinchlik xususiyati” Z tizimini mag’lubiyatga uchratishi mumkin va u eng kam imtiyozga ega bo’lishi mumkin. Biroq, ushbu xususiyat tahlil maqsadi uchun yetarli bo’lmagan darajada noaniqlikka ega.

Biba modeli. BLP modeli konfidensiallik bilan shug’ullangan bo’lsa, Biba modeli butunlik bilan shug’ullanadi. Boshqa so’z bilan aytganda, Biba modeli BLPning butunlikni ta’minlash uchun ishlab chiqilgan versiyasi hisoblanadi.

Agar biz O_1 obyektning butunligiga ishonsak, biroq O_2 obyektning butunligiga ishonmasak, u holda obyekt O ikkita O_1 va O_2 obyektlardan yaratilgan

bo’lsa, obyekt O ning butunligiga ishonmaymiz. Boshqa so’z bilan aytilganda, obyekt O ning butunligi uni tashkil etgan ixtiyoriy obyektning minimal butunlik darajasidan iborat. Ya’ni, butunlik uchun “past suv belgisi prinsipi” o’rinli. Boshqa tomondan, konfidensiallik uchun “yuqori suv belgisi prinsipi” o’rinli.

Biba modelini izohlash uchun, $I(O)$ orqali O obyektning butunligi izohlansa, $I(S)$ orqali S subyektning butunligi izohlanadi. U holda Biba modeli quyidagi ikkita qoidadan iborat (3.24-rasm):

Yozish huquqli qoida: faqat va faqat $I(O) \leq I(S)$ shart bajarilsa, S subyekt O obyektga yoza oladi.

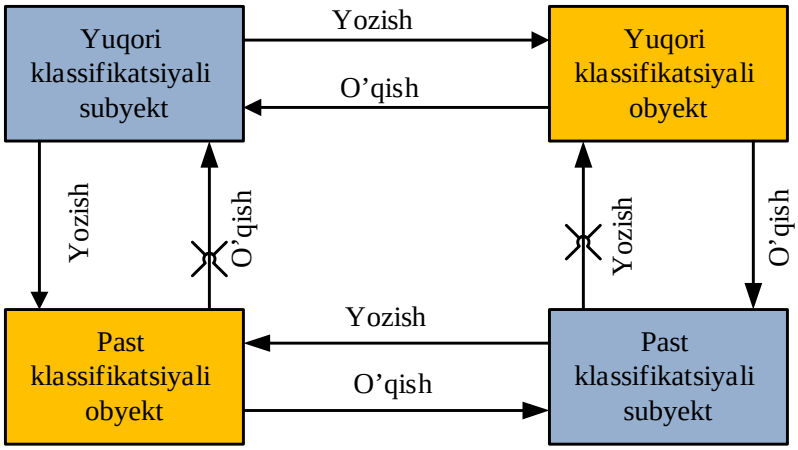
Biba modeli: faqat va faqat $I(S) \leq I(O)$ shart bajarilsa, S subyekt O obyektni o’qiy oladi.

Yozish huquqli qoidaga ko’ra, agar biz S yozgan biror narsaga ishonmasak, u holda biz S ga ham ishonmaymiz. Ya’ni, Biba modelida biz S o’qigan eng past butunlik obyektidan boshqa S ga ishonmasligimiz mumkin emas. Aslida, S subyekt kichik butunligi past bo’lgan obyekt tomonidan zararlanishi mumkinligi sababli, S ga bunday obyektlarni o’qish taqiqlanadi (53-rasm).

Biba modeli aslida juda cheklangan bo’lib, S ni hattoki eng quyi darajadagi butunlik sathidagi obyektni ham ko’rish imkoniyatidan himoyalaydi. Shuning uchun, Biba modelining ko’p hollarda balki barcha hollarda quyidagi bilan almashtirish mumkin:

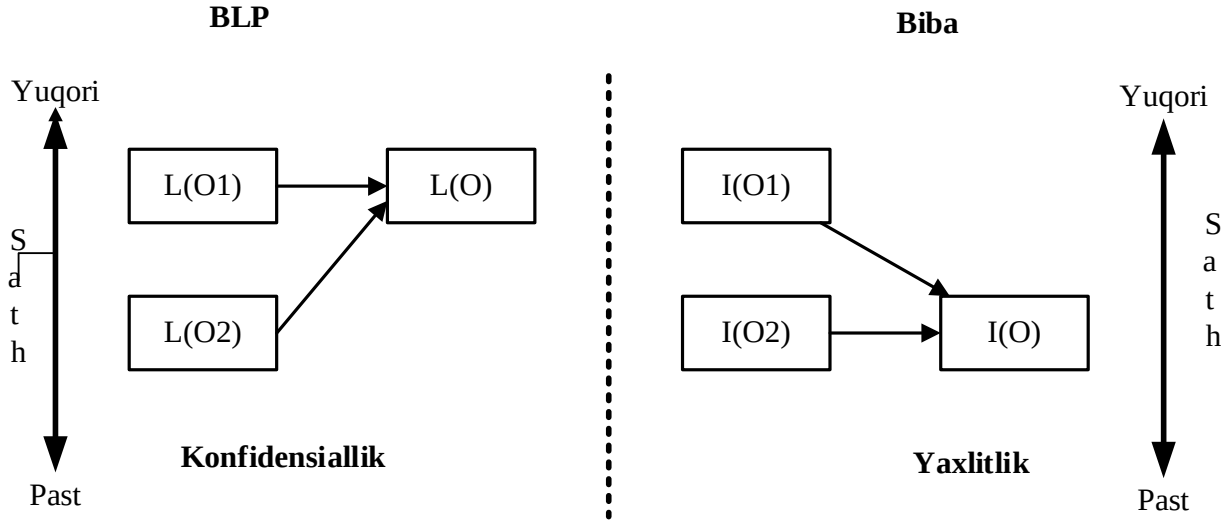
Past suv belgisi siyosati: agar S subyekt O obyektni o’qiy olsa, u holda $I(S) = \min(I(S), I(O))$ o’rinli.

Past suv belgisi siyosatiga binoan, agar S subyektning butunlik darajasi past darajadagi obyektni boshqarishdan keyin pasaygan bo’lsa, unda S subyekt barcha narsani o’qishi mumkin.



53-rasm. Biba modeli

54-rasmda BLP va Biba modellari orasidagi farq keltirilgan. Albatta asosiy farq bu - BLP konfidensiallikni ta'minlash uchun, ya'ni yuqori suv belgisi prinsipi, Biba esa butunlikni ta'minlash uchun, ya'ni, past suv belgisi prinsipiga asosan ishlashidir.



54-rasm. BLP va Biba modellarining farqi

Mantiqiy va fizik foydalanishlarni boshqarish. Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda mandat, tasdiqlash, avtorizasiya va majburiyatlar uchun foydalaniladi. Ushbu komponentlar tizimlar, ilovalar, jarayonlar va axborot uchun foydalanishni boshqarish choralarini qo'llaydi. Shuningdek, foydalanishni boshqarishning mazkur usuli dastur, operasion 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 foydalanishni mantiqiy deb qarash mumkin.

Nazorat savollari

1. Ruxsatlarni nazoratlashning asosiy tushunchalariga: identifikasiya, autentifikasiya va avtorizasiya, izoh bering.
2. Foydalanuvchilarni autentifikasiyalash usullari va ularning o’ziga xos xususiyatlari nimadan iborat?
3. Parolga asoslangan autentifikasiya usuli va uning afzallik/ kamchiliklarini ayting?
4. Parollar ma’lumotlar bazasida qanday saqlanadi va ularni taqqoslash usullari haqida ayting?
5. Axborotning fizik himoyasi va uning muhimligini tushuntiring?
6. Axborotni fizik xavfsizligiga ta’sir qiluvchi tabiiy va sun’iy omillarni aytib bering?
7. Yong’inga qarshi himoyalash usullari haqida ayting?
8. Tashkilotda qo’riqlash xodimlari va kuzutuv kameralarinig o’rni haqida ayting?
9. Foydalanishni mantiqiy boshqarish deganda nimani tushunasiz?
10. Foydalanishni boshqarishning DAC usuli va uning xususiyatlarini ayting?
11. Foydalanishni boshqarishning MAC usuli va uning asosiy xususiyatlarini ayting?
12. Foydalanishni boshqarishning RBAC usuli va uning asosiy xususiyatlarini ayting?
13. Foydalanishni boshqarishning ABAC usuli va uning asosiy xususiyatlarini ayting?
14. Foydalanishni boshqarish matrisasi, ACL va C-list tushunchalarini tushuntiring?

15. Bell-Lapadula modeli va uning asosiy maqsadini ayting?
16. Biba modeli va uning asosiy maqsadini ayting?

4 BOB. TARMOQ XAVFSIZLIGI

4.1. Tarmoq xavfsizligi zaiflikalari

Ushbu bo’limda dastlab kompyuter tarmoqlarining asosiy tushunchalari va kompyuter tarmoqlarida mavjud zaifliklar bilan tanishib o’tiladi.

4.1.1. Kompyuter tarmoqlarining asosiy tushunchalari

Kompyuter tarmoqlari bu – bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi bo’lib, bunda kompyuter axborotni ma’lumot yo’llari orqali uzatadi. Keng tarqalgan kompyuter tarmog’iga Internetni misol keltirish mumkin.

OSI (Open System Interconnection) modeli bu - tarmoq bo’ylab ma’lumotlar almashinuvini aniqlashtirish uchun taqdim etilgan etalon model bo’lib, bir qurilmadan tarmoq orqali boshqa qurilmaga ma’lumot oqib o’tishini tasvirlaydi. OSI modeli ikki nuqta orasidagi aloqani 7 ta turli sathlarga ajratadi. Ushbu modelda ma’lumotlar yuboruvchi kompyuterda yuqori sathdan pastki sathga qarab harakatlansa, qabul qiluvchi kompyuterda esa pastki sathdan yuqoriga qarab harakatlanadi.

TCP/IP modeli bu - 4 sathdan iborat bo’lib, Department of Defense (DOD) tomonidan ishlab chiqilgan. Ushbu modeldagi har bir sath turli vazifalarni bajaradi va ma’lumotni yuboruvchi qurilmada ma’lumot 4 - sathdan birinchi sathga qarab harakatlansa, qabul qiluvchi mashinada birinchi sathdan to’rtinchi sathga qarab harakatlanadi.

Kompyuter tarmoqlarining turlari. Kompyuter tarmoqlari turli omillar bo’yicha bir-biridan farq qilishi mumkin. Masalan, o’lchami bo’yicha, vazifasi bo’yicha yoki geografik masofasi bo’yicha. Tarmoq tarqalgan sohaning o’lchamiga va tarmoqdagi kompyuterlarning soniga ko’ra quyidagicha guruhlarinishi mumkin:

- lokal tarmoq (Local Area Network, LAN);
- mintaqaviy tarmoq (Wide Area Network, WAN);
- shahar tarmog’i (Metropolitan Area Network, MAN);
- shaxsiy tarmoq (Personal Area Network, PAN);

- kampus tarmog’i (Campus Area Network, CAN);
- global tarmoq (Global Area Network, GAN).

Tarmoq topologiyalari. Tarmoq bo’ylab kompyuterlar ma’lum topologiyalar yordamida mantiqiy bog’lanishlarni amalga oshiradi. Topologiya tarmoqning tuzilishini aniqlab, tarmoqning mantiqiy va fizik joylashuvini hisoblaydi. Fizik topologiya kompyuter tizimlari komponentlarining tuzilishini aniqlasa, mantiqiy topologiya kompyuterlar orasidagi tarmoqda ma’lumotlarni uzatish usullarini aniqlaydi. Amalda keng qo’llaniluvchi tarmoq topologiyalariga quyidagilarni misol keltirish mumkin:

– yulduz topologiya;
– shina topologiya;
– halqa topologiya;
– mesh topologiya;
– daraxt topologiya;
– gibrid topologiya.

Tarmoq kartasi (Network Interface Card, NIC). Hisoblash qurilmasining ajralmas qismi bo’lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Qurilmalar aynan ushbu elektron mikrosxema asosida simli yoki simsiz tarmoqqa ulanish imkoniyatiga ega bo’ladi.

Repetir. Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalanilib, uzatilish davomida yo’qolgan analog va raqamli signallarni tiklaydi. Bundan tashqari, ushbu qurilmalar turli protokollar tomonidan uzatilayotgan ma’lumotlarni o’tkazish imkoniyatiga ega.

Xab. Xab tarmoq qurilmasi bo’lib, ko’plab tarmoqlarni ulash yoki LAN segmentlarini bog’lash uchun xizmat qiladi. Xabning asosiy vazifasi bir qurilmadan kelgan ma’lumotni qurilmaning boshqa portiga ulangan qurilmaga uzatishdan iborat.

Svitch. Simli va simsiz LANlar uchun tarmoq svitchlari asos qurilma hisoblanib, u simli va simsiz kabel orqali tarmoqdagi qurilmalardan signalni qabul qiladi. Har ikkala holda ham qabul qilgan signalni LAN orqali kompyuterlarga

uzatadi. Svitchlar xablardan farqli qabul qilingan signalni barcha chiquvchi portlarga emas, balki, paketda manzili keltirilgan portga uzatadi.

Routerlar. Routerlar yuqorida keltirilgan tarmoq qurilmalariga qaraganda murakkab tuzilishga ega bo'lib, OSI modelining tarmoq sathida ishlaydi. Router qabul qilingan ma'lumotlarni tarmoq sathida tegishli manzil (IP manzil) bo'yicha uzatadi.

Ko'priklar. Ko'priklar tarmoq chegarasida trafikni filterlashni amalga oshiradi. Ko'prik har bir ma'lumotlar paketidagi MAS manzillarni o'qib oladi va ularni masofadagi qurilmaga yuboradi. Ko'priklar mantiqiy qurilma bo'lib, har bir tarmoq segmentini alohida qaraydi.

Shlyuzlar. Shlyuzlar ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini o'tasa, o'z navbatida tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini o'taydi. Bu yerda, shlyuz vazifasini ishchi stansiyalar yoki serverlar bajarishi mumkin.

DNS (Domain name system). DNS tizimlari host nomlari va Internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi. DNS o'z ilovalarini TCP/IP tarmog'idan qidiradi. DNS xizmati foydalanuvchi tomonidan kiritilgan DNS nomini mos IP manzilga o'zgartirib beradi. Masalan, DNS xizmati *www.example.com* domen nomini *192.105.232.4* IP manziliga o'zgartirib beradi.

TCP protokoli. TCP protokoli ulanishga asoslangan protokol bo'lib, Internet orqali ma'lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. TCP mavjud kompyuter bir tarmoqda turgan yoki boshqa tarmoqdagi foydanuvchi kompyuteriga ma'lumotni yuborish imkoniyatiga ega bo'ladi. TCP protokoli qabul qiluvchi tomonida manbadan uzatilgan barcha xabarlarni qabul qilinganini kafolatlaydi. TCP protokoli xabarni barchaga uzatmaydi (broadcasting imkoniyati mavjud emas), ya'ni, paket aynan faqat masofadagi foydalanuvchiga yetkaziladi. www, e-mail, masofadan turib boshqarish yoki fayl transferini amalga oshiruvchi ilovalar o'z vazifasini TCP protokollari asosida amalga oshiradi.

UDP protokoli. UDP ulanishga asoslanmagan protokol bo'lib, Internetda ilovalar orasida kam kechikishli va past chidamlilik darajasidagi aloqani ta'minlaydi. TCP protokolidan farqli, UDP protokoli ma'lumotlarni to'liq yetib kelishini kafolatlamaydi. UDP protokoli ma'lumotni raqamlangan paketrlar shaklida emas, balki, tarmoq bo'ylab datagramma shaklida uzatadi. UDP protokolidan odatda o'yin va video ilovalar tomonidan keng foydalaniladi.

IP (Internet Protocol) protokoli. IP protokoli TCP/IP aloqa protokollari to'plamida taqdim etilgan tarmoq sathida ishlovchi protokol bo'lib, ma'lumotni yuborishdan oldin aloqa o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan ta'minlaydi. IP protokolining ikki versiyasi mavjud: Internet protocol version 4 (IPv4) va Internet protocol version 6 (IPv6). IPv4 protokoli amalda keng qo'llaniluvchisi bo'lib, 32-bitli manzillashdan foydalanadi. IPv6 da esa manzilni ifodalash uchun 128 bit xotira ajratiladi.

4.1.2. Tarmoq xavfsizligida mavjud muammolar

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

Tahdid bu – natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib qo'yuvchi oshkor bo'lmagan hodisalarning potensial paydo bo'lishidir. Tahdidlar tashkilotning butunlik va foydalanuvchanlik omillariga ta'sir qilishi mumkin. Tahdidning ta'siri juda yuqori va u tashkilotdagi fizik axborot aktivlarining mavjudligiga ta'sir qilishi mumkin. Tahdidlarning paydo bo'lishi tasodifiy, qasddan yoki boshqa harakatning ta'sirida bo'lishi mumkin.

Zaiflik bu – "portlaganida" tizim xavfsizligini buzuvchi kutilmagan va oshkor bo'lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik. Oddiy so'z bilan aytganda, zaiflik xavfsizlik bo'shlig'i bo'lib, foydalanuvchilarni autentifikasiyalashning turli usullarini aylanib o'tib hujumchiga tizimga kirish imkoniyatini taqdim etadi.

Hujum bu – zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bo'lib, bunda zararli dasturlarni va buyruqlarni yuborish orqali qonuniy dasturiy va apparat vositadan foydalanish imkoniyatini qo'lga kiritishga harakat qilinadi.

Tarmoqdan foydalanib amalga oshiriluvchi hujumlar soni va ko'rinishlari juda ham jadallik bilan ortib bormoqda. Doimiy hujumlar butun hisoblash qurilmalari dunyosi uchun asosiy muammo bo'lgani bois, tashkilotlar tarmoq xavfsizligini ta'minlash uchun katta mablag' sarflashmoqda. Tarmoq xavfsizligi muammolari tashkilotdagi mavjud axborotning foydalanuvchanligi, konfidensialligi va butunligiga ta'sir qiladi. Hujumni amalga oshirishda dastlab texnologiyalardagi xavfsizlik bo'shliqlarini aniqlashga amalga oshiriladi. O'z navbatida bu tizim administratoridan tarmoqda paydo bo'luvchi yangi hujumlar haqida ma'lumotga ega bo'lib borishni talab etadi.

Tarmoqni qurish oson vazifa hisoblansada, hujumchi turli vositalardan foydalangan holda tizimdagi zaifliklarni aniqlashga harakat qilishi bois uning xavfsizligini ta'minlash murakkab vazifa hisoblanadi. Tashkilot tarmog'i ichkaridan amalga oshiriluvchi turli hujumlarga ham uchrashi mumkin. Ichkaridan turib amalga oshirilgan hujum odatda tashqi hujumdan xavfliroq bo'ladi. Shuning uchun, tashkilotdan doimiy ravishda tarmoqdagi hujumlarni monitoring qilib borishi muhim hisoblanadi.

Hozirda tarmoq orqali amalga oshiriluvchi muammolarning ortishiga quyidagi omillar ta'sir qilmoqda:

Qurilma yoki dasturiy vositani 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'lumotni oshkor bo'lishi sababchi bo'lishi mumkin. Noto'g'ri sozlangan qurilma hujumchiga tizim yoki tarmoqdan foydalanish imkoniyatini taqdim etishi yoki noto'g'ri sozlangan dasturiy vosita ilova yoki dasturiy ta'mindan ruxsatsiz foydalanish imkonini berishi mumkin.

Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash. Noto'g'ri va xavfsiz bo'lmagan holda loyihalangan tarmoq turli tahdidlarga va ma'lumotni 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 texnologiya zaifligi. Agar qurilma yoki dasturiy vosita ma'lum turdagi tarmoq hujumlarini bartaraf eta olmasa, u holda u ushbu hujumlarga zaif bo'ladi. Ko'plab qurilmalar, ilovalar yoki veb brauzerlar *xizmatdan vos kechishga undash* hujumi yoki *o'rtaga turgan odam* hujumlariga bardoshsiz bo'ladi. Agar tizimlarda foydalanilgan veb brauzer yangilanmagan bo'lsa, u taqsimlangan hujumlarga ko'proq bardoshsiz bo'ladi. Agar tizimlar yangilanmasa, kichik troyan hujumi foydalanuvchi mashinasini tozalab tashlash uchun yetarli bo'lishi mumkin.

Foydalanuvchilarning e'tiborsizligi. Eng oxirgi tarmoq foydalanuvchilarining e'tiborsizligi tarmoq xavfsizligiga jiddiy ta'sir qilishi mumkin. Inson harakatlari natijasida ma'lumotni yo'qolishi, chiqib ketishi kabi jiddiy xavfsizlik muammolari bo'lishi mumkin. Bundan tashqari hujumchilar foydalanuvchilar haqida ma'lumotlarni to'plashda ijtimoiy injineriya texnologiyalaridan foydalanadilar.

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 holat foydalanuvchilarni qasddan qilgan harakatlari sifatida qaraladi.

Tarmoq xavfsizligiga tahdidlarning turlari. Tarmoqqa qaratilgan tahdidlar odatda ikki turga ajratiladi (55-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

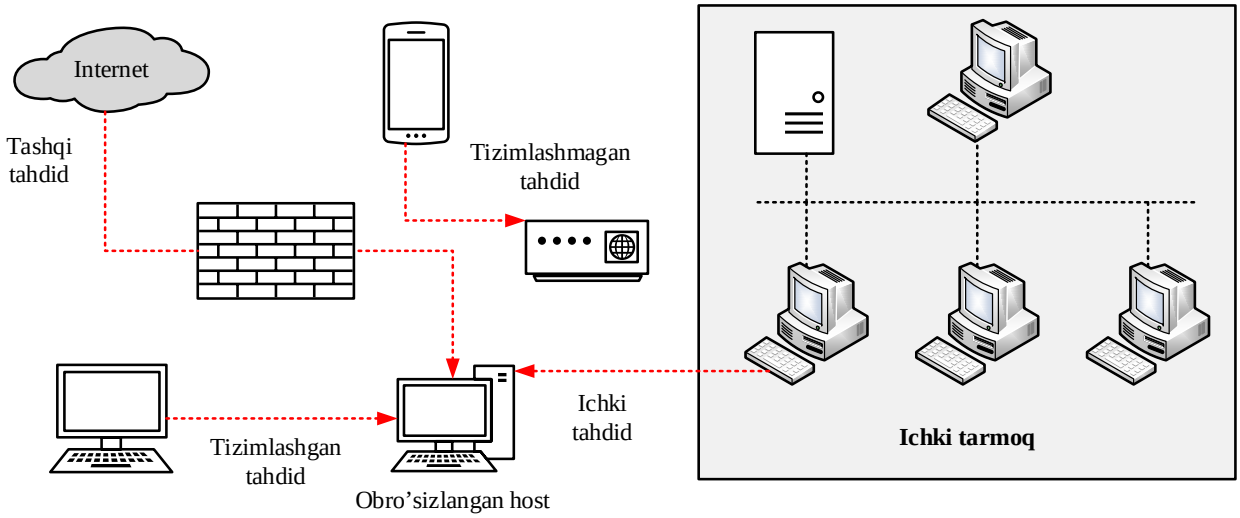
hujumlarning aksariyati imtiyozga ega tarmoq foydalanuvchilari tomonidan amalga oshiriladi. Ichki hujumlar hujumni amalga oshiruvchi tarmoqning tushilishi, xavfsizlik siyosati va tashkilot qonunchiligi bilan yaqindan tanish bo'lgani bois tashqi hujumlarga qaraganda jiddiy xavf tug'dirishi mumkin.

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. Hujumni amalga oshirganda maxsus texnologiyalardan foydalaniladi va uzoq muddat davomida tayyorgarlik ko'riladi. Mazkur holda hujumlar ichki xodimlarning yordamisiz amalga oshiriladi. Ba'zi tashqi hujumlar o'zida ishtirokchilarni va virusga asoslangan hujumlarni, parolga qaratilgan hujumlarni, zararli xabarni kiritishga asoslangan hujumlarni va operasion tizimga asoslangan hujumlarni o'z ichiga oladi.

Tashqi tahdidlar odatda ikki turga ajratiladi: *tizimlashgan* va *tizimlashmagan* tashqi tahdidlar.

Tizimlashgan tashqi tahdidlar yuqori malakali shaxslar tomonidan amalga oshiriladi. Ushbu shaxslar tarmoqdagi mavjud zaiflikni tezkorlik bilan aniqlash va undan o'z maqsadlari yo'lida foydalanishlari uchun imkoniyatga ega bo'ladilar. Ushbu shaxslar yoki shaxslar guruhlari odatda katta kiberjinoyatchiliklarni amalga oshirishga jalb etiladilar.

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



55-rasm. Turli tarmoqqa qaratilgan tahdidlar

Tarmoq xavfsizligini buzulishini biznes faoliyatga ta'siri:

Biznes faoliyatning buzilishi. Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi. Xavfsizlikdagi buzilish muhim biznes va foydalanuvchi ma'lumotlarini yo'qolishiga olib keladi.

Ishlab chiqarishning yo'qolishi. Tarmoq asosida biznes faoliyat yuritadigan tashkilotlarda tarmoqning buzilishi ishlab chiqarishning yo'qolishiga olib keladi. Hujum natijasida ishlab chiqarishi yo'qolgan hollarda uni qayta tiklash ko'p vaqt talab qiladi va bu vaqt davomida ishlab chiqarish to'xtab qoladi.

Maxfiylikni yo'qolishi. Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma'lumotlari yo'qolishi va bu hodisa tashkilot uchun jiddiy muammo bo'lishi mumkin.

Axborotni o'g'irlanishi. Tarmoqqa qaratilgan hujum natijasida kutilmagan axborot chiqib ketishi mumkin. Tashkilot xodimlarining shaxsiy va ishga oid ma'lumotlarini kutilmaganda oshkor bo'lishi ushbu xodimlarga bevosita ta'sir ko'rsatadi. Agar hujum mijozlar ma'lumotlari saqlangan bazaga qaratilgan bo'lsa, u holda tashkilot uchun jiddiy muammoga sabab bo'ladi.

Huquqiy javobgarlik. Hujum bo'lganda hujumchiga nisbatan ish qo'zg'atilishi mumkin va buning uchun turli davlatlarda turlicha javobgarliklar belgilangan. Xuddi shunday javobgarlik tashkilotga nisbatan ham qo'llanilishi mumkin. Masalan, hujum natijasida mijozlarga tegishli ma'lumotlarga zarar

yetkazilsa, u holda mijoz tashkilot ustidan tegishli organlariga murojaat qilishi mumkin.

Obro'ga putur yetishi va istemolchilar ishonchini yo'qolishi. Agar biror tashkilotga nisbatan hujum amalga oshirilsa, mijozlarning ushbu korxona xizmatiga jalb qilish murakkablashadi va o'z o'rnida tashkilot obro'siga ham putur yetadi.

Tarmoq xavfsizligi zaifliklarining turlari. Tarmoq xavfsizligidagi buzilishlar quyidagi zaifliklar natijasida yuzaga keladi:

Texnologik zaifliklar. Texnologik zaifliklar operasion tizim, printerlar, skanerlar va boshqa tarmoq qurilmalaridagi kamchiliklar sabab yuzaga keladi. Hujumchilar protokollardagi (masalan, SMTP, FTP va ICMP) bo'shliqlarni aniqlashlari mumkin. Bundan tashqari, tarmoq qurilmalari, svitch yoki routerlardagi autentifikasiya usullarining yetarlicha bardoshli bo'lmasligi natijasida hujumlar amalga oshiriladi. Buni oldini olish uchun tarmoq administratori tomonidan doimiy xavfsizlik auditi olib borilishi talab etiladi.

Sozlanishdagi zaifliklar. Sozlanishdagi zaifliklar tarmoq yoki hisoblash qurilmalarini noto'g'ri sozlanishi natijasida yuzaga keladi. Xususan, tarmoq administratori foydalanuvchi akkauntini va tizim xizmatlarini xavfsiz bo'lmagan tarzda sozlanishini amalga oshirishi, joriy sozlanish holatida qoldirishi va parollarni noto'g'ri boshqarishi natijasida bunday zaifliklar yuzaga kelishi mumkin.

Xavfsizlik siyosatidagi zaiflik. Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto'g'ri ishlab chiqilgani sabab bo'ladi. Ushbu sabablar tarmoq resurslaridan ruxsatsiz foydalanish imkoniyatini taqdim etishi mumkin. Agar tarmoq administratori harakatlarni doimiy audit va monitoring qilib borsa, ushbu zaifliklarni aniqlash va o'z vaqtida bartaraf etish imkoniga ega bo'ladi.

Tarmoq xavfsizligiga qaratilgan hujumlarning turlari. Tarmoqqa qaratilgan hujumlar sonini ortib borishi natijasida tashkilotlar o'z tarmoqlarida xavfsizlikni ta'minlashida qiyinchiliklarga duch kelishmoqda. Bundan tashqari, hujumchilar yoki xakerlar tarmoqqa kirishni yangidan - yangi usullaridan foydalanishi, ularning motivlarini turlichaligi bu murakkablikni yanada oshiradi. Masalan, ba'zi

hujumchilar qurilmani yoki dasturiy vositani o’g’irlashni maqsad qilsa, ba’zilari tarmoq resurslarini va foydalanuvchi ma’lumotlarini qo’lga kiritishni yoki boshqarishni maqsad qiladi. Boshqa tomondan tarmoq administratori esa ushbu hujumlarni aniqlash uchun ularni turi haqida yetarlicha bilimlarga ega bo’lishi talab etiladi. Tarmoq hujumlari odatda quyidagicha tasniflanadi:

Razvedka hujumlari. Razvedka hujumlari asosiy hujumni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to’plashni maqsad qiladi va bu hujumchilarga mavjud bo’lgan potensial zaiflikni aniqlash imkonini beradi.

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 qiladilar. Bu turdagi hujumlar kirish hujumlari deb ataladi. Bularga ruxsatsiz foydalanish, qo’pol kuch hujumi, imtiyozni orttirish, o’rtaga turgan odam hujumi va boshqalarni misol keltirish mumkin.

Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari. Xizmatdan vos kechishga qaratilgan hujumlarda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo’lgan biror xizmatni cheklashga urinadi. DOS hujumlari biror axborotni o’g’irlanishiga yoki yo’qolishiga olib kelmasada, tashkilot funksiyasini bajarilmasligiga sababchi bo’ladi. DOS hujumlari tizimda saqlangan fayllar va boshqa maxfiy ma’lumotlarga ta’sir qilishi va hattoki veb saytning ishlashiga ham ta’sir qiladi. Ushbu hujum usuli bilan veb sayt faoliyatini to’xtatib qo’yish mumkin.

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

Razvedka hujumlari. Razvedka hujumlarida hujumchilar maqsad qaratilgan tarmoq haqida barcha bo’lishi mumkin bo’lgan axborotni, xususan, tizim, tarmoq va tarmoqda mavjud zaifliklar haqidagi axborotni ko’lga kiritishi mumkin.

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

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

Razvedka hujumlarining quyidagi turlari mavjud:

- *Aktiv razvedka hujumlari.* Aktiv razvedka hujumlari asosan portlarni va operasion tizimni skanerlashni maqsad qiladi. Buning uchun maxsus dasturiy vositalardan foydalangan holda turli paketlarni yuboradi. Masalan, maxsus dasturiy vosita router va tarmoqlararo ekranga boruvchi barcha IP manzallarni 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.

Razvedka hujumlariga quyidagilarni misol keltirish mumkin:

- *Paketlarni snifferlash.* Paketlarni snifferlash orqali tarmoq orqali o’tuvchi barcha paketlarni kuzatib borish mumkin. Turli snifferlash vositalaridan foydalanish orqali tarmoq ochiq bo’lgan holda uzatilgan login, parol va boshqa ma’lumotlarni qo’lga kiritishi mumkin. Masalan, Telnet va HTTP protokollarida ma’lumotlar ochiq holda uzatiladi.
- *Portlarni skanerlash.* Portlarni skanerlash orqali maqsad qaratilgan mashinadagi ochiq portlarni aniqlash mumkin. Agar ochiq portdan foydalanish imkoni bo’lsa, ichkariga kirish mumkin bo’ladi.
- *Ping buyrug’ini yuborish.* Ping komandasi ICMP so’rovi orqali tarmoqning ishlayotganini bilishi mumkin.
- *DNS izi.* DNS so’rovi asosida biror domen va uning IP manzilini bilib olish mumkin.

Razvedka hujumlari: ICMP skanerlash. ICMP skanerlash davomida, hujumchi tizim haqida kerak bo’lgan ma’lumotlarni yig’ish uchun ICMP paketlarini

yuboradi. ICMP skanerlash hujumchiga tarmoqda mavjud hostlarni aniqlash imkonini beradi. Ular maxsus skanerlash vositalari, NMAP yordamida *ping* komandasini yuborish orqali aniqlanadi. NMAP vositasi *–P* tanlovi bilan qisqa vaqtda ICMP skanerlash imkonini beradi.

Internet Control Message Protocol (ICMP) skanerlash yagona hostda ishlaydi va u ICMP ECHO so'rovini yuboradi. Agar host mavjud bo'lsa, ICMP ECHO javobi qaytadi. Ushbu texnologiya tarmoqlararo ekran vositasi mavjud bo'lganda ham ishlatilishi mumkin.

Razvedka hujumlari: DNS izi. DNS izi DNS zonalari haqida axborotni taqdim etib, DNS zona ma'lumotlari o'zida DNS domen nomlari, kompyuter ismlari, IP manzillar va tarmoq haqidagi ko'plab xususiy ma'lumotlarni mujassamlashtiradi. Hujumchi DNS axborotdan foydalangan holda tarmoqdagi muhim hostlarni aniqlaydi va shundan so'ng ijtimoiy injineriyani ishga solgan holda kengroq ma'lumot olishga harakat qiladi.

Maxsus DNS izi vositalari (masalan, intoDNS) yordamida so'rovni amalga oshirganda, DNS server ma'lum formatdagi ma'lumotlarni yuboradi. DNS qayd yozuvi joylashuv va xizmatlar turi haqida muhim axborotni taqdim etadi.

Razvedka hujumlari: Nmap Scan yordamida tarmoq axborotini ajratish. Nmap tarmoqni tahlil qilish uchun hujumchilar tomonidan keng foydalanilayotgan dasturiy vosita bo'lib, xavfsizlik auditini ham amalga oshiradi. Hujumchilar nishondagi tarmoq haqida kerakli axborotni olishlari uchun ushbu vositadan foydalanadilar.

Hujumchilar ushbu vositadan tarmoqdagi hostlarni aniqlash, hostga qanday xizmatlar yoqilganini aniqlash, OT turini aniqlash, qanday paket filterlari/tarmoqlararo ekran foydalanilganini va boshqa ko'plab ma'lumotlarni aniqlash uchun foydalanadilar.

Kirish hujumlari: 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 usulga quyidagilarni misol keltirish mumkin:

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

Kirish hujumlari: tarmoqni snifferlash. Snifferlash jarayoni TCP/IP tarmog’ida paketlarni tutib olish, dekodlash, tekshirish va tarjima qilishni o’z ichiga oladi. Ushbu jarayonning asosiy maqsadi esa axborotni, foydalanuvchi IDsini, parolini, tarmoq ma’lumotlarini, kredit karta raqamlarini va boshqalarni o’g’irlashdan iborat. Snifferlash odatda passiv turdagi hujum turiga kiradi. Biroq, ushbu hujum amalga oshirilayotganini bilish murakkabligi va TCP/IP paketda tarmoqda aloqani tashkil qiluvchi ma’lumotlar borligi sabab, ushbu hujum katta ahamiyatga ega hisoblanadi. Tarmoqni snifferlashni uchta asosiy yo’li mavjud:

Ichki snifferlash. Tashkilotdagi xodim tashkilot ichidan turib tarmoqni bevosita tutib olishi mumkin.

Tashqi snifferlash. Haker tarmoqni tashqarisidan turib tarmoqlararo ekran darajasida paketlarni tutib olishi va o’g’irlashi mumkin.

Simsiz snifferlash. Hujumchi snifferlanuvchi tarmoqning qayerida joylashuvidan qat’iy nazar simsiz tarmoqlarni keng foydalanilishi natijasida ma’lumotni qo’lga kiritish imkoniyati mavjud bo’ladi.

Kirish hujumlari: O’rtaga turgan odam hujumi. O’rtaga turgan odam (Man in the middle attack, MITM) hujumida hujumchi o’rnatilgan aloqaga suqilib kiradi va aloqani bo’ladi. 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. MITM hujumi sessiyani o’g’irlash hujumlarining bir ko’rinishi bo’lib, quyidagi hollarda MITM hujumiga moyillik paydo bo’ladi:

- login vazifasi mavjud shartlarda;
- shifrlanmagan holatlarda;
- moliyaviy saytlarda.

MITM hujumi asosan Telnet protokoli va simsiz texnologiyalar uchun o’rinli bo’lib, ushbu hujumni TCP paketlarining raqamlanganligi va ularning tezkorligi sabab amalga oshirish murakkab hisoblanadi.

Bundan tashqari amalda quyidagi kirish hujumlaridan keng foydalaniladi:

- takrorlash hujumlari;
- imtiyozni oshirish hujumi;
- zararlangan DNS hujumi;
- ARP (Address Resolution Protocol) so’rovini zararlash hujumi;
- MAC (Media Access Control) manzilni qalbakilashtirish hujumi va boshqalar.

Xizmatdan vos kechishga undan hujumi: DOS hujumi. DOS qonuniy foydalanuvchini tizim yoki tarmoqdan foydalanishini cheklash hujumi bo’lib, uning asosiy nishoni tarmoq yuklanishi va ulanishi bo’ladi. Tarmoqni yuklanishiga qaratilgan hujumda mavjud tarmoq resurslaridan foydalangan holda tarmoq yuklanishini ko’paytirish va qonuniy foydalanuvchini ushbu resurslardan foydalanishi cheklashga harakat qiladi. Ulanishga qaratilgan hujumda esa tarmoqqa ko’p sonli ulanish so’rovlari yuboriladi va barcha operasion tizim resurslari ushbu so’rovlarga javob berishga sarflanishi natijasida, hisoblash qurilmasi qonuniy foydalanuvchi so’roviga javob bera olmaydi.

Faraz qilaylik tashkilot telefon orqali qabul qilingan buyurtma asosida pisa etkazib beradi. Bu holda butun bir faoliyat telefon orqali beriladigan buyurtmalarga bog’liq. Faraz qilaylik, biror shaxs ushbu tashkilotning kunlik biznesini buzmoqchi. Agar ushbu shaxs telefon tarmog’ini band qilishning imkonidan chiqsa, u holda kompaniya bu vaqtda mijozlardan buyurtma qabul qila olmaydi.

DOS hujumi ham kompaniyani pisani yetkazib berishi hodisasiga o’xshaydi. Bunda hujumchining asosiy maqsadi nishondan axborotni o’g’irlash emas, balki, mavjud xizmatdan foydalanishni yo’qotishga harakat qiladi. Ushbu jarayonda, hujumchi ko’plab kompyuterlarni (zombilar deb ataladi) boshqaruviga oladi va

virtual holda ularni boshqaradi. Hujum o’zida zombi kompyuterlar imkoniyatini birlashtirib, nishondagi kompyuterga bir vaqtda so’rovlar yuboradi va oqibat uni osilib qo’yishiga olib keladi.

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. DDOS hujumni amalga oshirishdagi ikkilamchi nishon hujumchini murakkablik va hujumni aniqlay olmaslik imkoni bilan ta’minlaydi.

WWW Security FAQ da: “DDOS hujumi bir yoki ko’plab nishonlar uchun kelishilgan DOS hujumni ko’plab kompyuterlar orqali amalga oshiradi. Mijoz-server texnologiyasidan foydalangan holda, jinoyatchi hujum platformasi sifatida xizmat qiluvchi ko’plab kompyuterlar orqali DOS hujumini samaradorligini oshiradi” kabi aniqlik kiritilgan.

Agar o’z vaqtida DDOS hujumiga sabab bo’luvchi holatlar tekshirilmasa, qisqa vaqtda Internet xizmatlaridan foydalanish darajasi yo’q qilinishi mumkin.

Zararli hujumlar. Zararli dasturiy vositalar foydalanuvchini 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, veb saytdagi kontentlarni modifikasiyalashi, o’chirishi yoki qo’shishi, foydalanuvchi kompyuteri boshqaruvini qo’lga kiritishi mumkin. Bundan tashqari, zararli dasturlar, hukumat tashkilotlaridan va korporativ tashkilotlardan katta hajmdagi maxfiy axborotni olish uchun ham foydalanilishi mumkin. Zararli dasturlarning hozirda quyidagi ko’rinishlari keng tarqalgan:

- *viruslar:* o’zini o’zi ko’paytiradigan programma bo’lib, o’zini boshqa programma 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 bo’ladi;
- *Adware:* marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko’rish rejimini kuzatib boruvchi dasturiy ta’minot;
- *Spyware:* foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod;
- *Rootkits:* ushbu zararli dasturiy vosita operasion tizim tomonidan aniqlanmasligi uchun o’z harakatlarini yashiradi;
- *Backdoors:* zararli dasturiy kodlar bo’lib, hujumchiga autentifikasiyani amalga oshirmasdan aylanib o’tib tizimga kirish imkonini beradi, masalan, administrator 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 qulflab qo’yib, to’lov amalga oshirilishini talab qiladi.

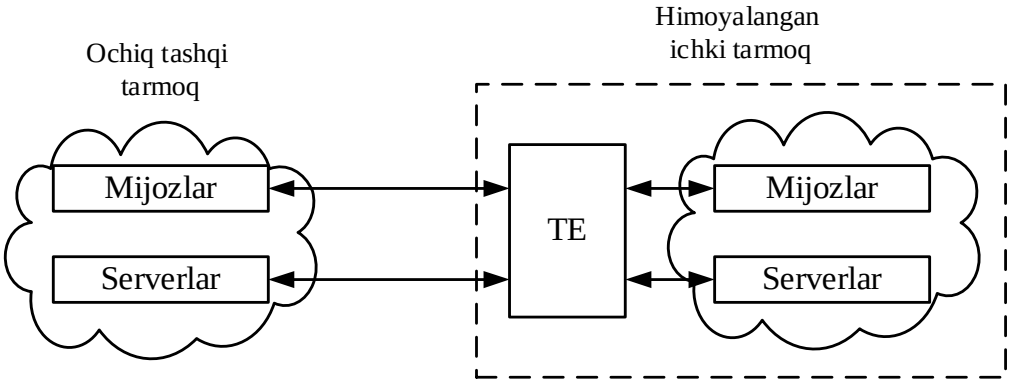
4.2. Tarmoqlararo ekran va virtual himoyalangan tarmoq

4.2.1. Tapmoklapapo ekpan texnologiyasi

Tapmoklapapo ekpan (TE) - maxsus kompleks tapmoklapapo himoya bo’lib, *bpaundmauep* yoki *firewall* deb ham yupitiladi. TE umumiy tapmoqni ikki qismga: *ichki* va *tashqi* tapmoqqa ajapatadi. Ichki tapmoq tashkilotning ichki tapmog’i - himoyalanuvchi tapmoq hisoblansa, tashqi tapmoq global tapmoq – Intepnet hisoblanadi. Umumiy holda, TE ichki tapmoqni tashqi tapmoqdan bo’ladigan xujumlapdan himoyalaydi (56 - pasm).

TE bip vaqtning o’zida ko’plab ichki tapmoq uzellapini himoyalaydi va quyidagilapni amalga oshipadi:

- Tashqi tapmoqdagi foydalanuvchilapdan ichki tapmoq pesupslapini himoyalash. Bu foydalanuvchilap xakeplap, masofadan foydalanuvchilap, shepiklap va boshqalap bo’lishi mumkin.
- Ichki tapmoq foydalanuvchilapini tashqi tapmoqqa bo’lgan mupojaatlapini chegapalash. Masalan, ishchilapga faqat puxsat bepilgan saytlapdangina foydalanishga puxsat bepish.



56 - pasm. TE ulanish sxemasi

TElapning hozipgi kunga qadap qat’iy belgilangan klassifikasiyasi mavjud emas. Umumiy xolda ulapni quyidacha klassifikasiyalash mumkin:

- OSI modelining funksional sathlapi bo’yicha:
  - paket filterlari – tarmoq sathida ishlaydi;
  - ekspert paketi filterlari – transport sahida ishlaydi;
  - ilova proksilari – ilova sathida ishlaydi;
- foydalanilgan texnologiyasi bo’yicha:
  - ppotakol holatini nazopatlash;
  - vositachi moduli yordamida (ppoksi);
- bajapilishiga ko’pa:
  - appapat-dastupiy;
  - dastupiy;
- ulanish sxemasiga ko’pa:
  - yagona tapmoq himoyasi sxemasi;

- himoyalangan yopiq va himoyalanmagan ochiq tapmoq segmentli sxema;
- bo’lingan himoyalangan yopiq va ochiq segmentli tapmoq sxemasi.

Paket filtepi tupidagi TE o’tuvchi axbopotni analiz qilishda quyidagi kpitepiyalapdan foydalanadi:

- xabap paketlapining xizmat maydonlapi: tapmoq manzili, identifikatoplap, intepfeys manzili, popt nomepi va boshqa parametrlap;
- bevosita xabap paketi kontentini tekshipish opqali, masalan, vipusga qapshi;
- axbopot oqimining tashqi xapaktepistikasi bo’yicha, masalan, vaqt va chastota xapaktepistikalapi, ma’lumot hajmi va boshqalar.

Vositachi moduliga asoslangan TE quyidagi funksiyalapni bajapadi:

- uzatilayotgan axbopotni to’g’piligini tekshipish;
- xabaplap oqimini filteplash va o’zgaptipish, masalan, vipusga qapshi tekshipish va shaffof shifplash;
- ichki tapmoq pesupsidan foydalanishni cheklash;
- tashqi tapmoq pesupsidan foydalanishni cheklash;
- tashqi tapmoqdan so’palgan malumotlapni cheklash;
- foydalanuvchini identifikasiyalash va autentifikasiyalash;
- chiquvchi xabap paketlapi uchun ichki tapmoq manzilini o’zgaptipish;
- hodisalapni po’yxatga olish, nazopatlash va analiz qilish.

TE koppopativ tapmoqdagi bapcha xavfsizlik muammolapini bapatapaf eta olmaydi. Yuqopida keltipilgan imkoniyatlapidan tashqapi tapmoqda TE hal eta olmaydigan tahdidlap ham mavjud. Bu cheklanishlap quyidagilap:

- O’tkazish qobilyatini cheklashi mumkin. Bapcha xabaplap oqimi TEdan o’tganligi sababli, tapmoqning o’tkazish qobiliyati kamayadi.
- Vipuslapga qapshi himoyani madadlamaydi. TE vositasi yuklanuvchi tupidagi vipuslapni himoyalay olmaydi.
- Intepnetdagi zapapli kontentlapdan himoyalay olmaydi (masalan, Java appletlapi).

- Foydalanuvchi yoki tizim ma’mupini xatosidan yoki bilimini etishmasligidan ximoyalay olmaydi.
- TE faqat bo’ladigan mavjud bo’lgan hujumlapni bloklaydi. Yangi tupdagi xujumni qaytapa olmaydi.

Paket filterlari. Bu turdagi tarmoqlararo ekran tarmoq sathida paketlarni tahlillashga asoslangan bo’lib, bunda kalit ma’lumotlar sifatida: manba IP manzili, masofadagi IP manzil, manba porti, masofadagi port, TCP bayroq bitlari (SYN, ACK, RST va hak.) parametrlari asosida amalga oshiriladi. Bu turdagi tarmoqlararo ekran asosan yuqoridagi parametrlar asosida kiruvchi va chiquvchi trafikni tahlillaydi.

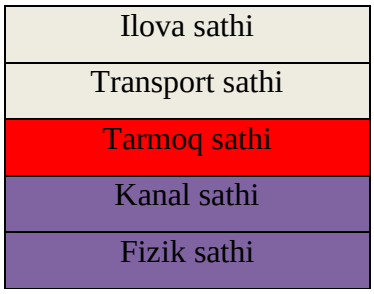
Bu turdagi tarmoqlararo ekran samarali bo’lib, faqat tarmoq sathida ishlaydi va sarlavha ma’lumotlarni tahlillashda yuqori tezlikka ega. Shu bilan birga, mazkur tarmoqlararo ekran qator kamchiliklarga ega:

– holatning turg’unligi mavjud emas, ya’ni har bir paket turlicha ko’rinishda bo’lishi mumkin;

– bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi;

– ilova sathi ma’lumotlarini, zararli dasturlarni va boshqalarni tekshirmaydi.

Bu turdagi tarmoqlararo ekran “foydalanishlarni nazoratlash ro’yxati (ACL)” yordamida sozlanadi (57, 58 - rasm).



57-rasm. Paket filteri

Harakat	Manba IP	Masofadigi IP	Manba port	Masofadagi port	Protokol	Bayroq
Ruxsat	Ichki	Tashqi	Ixtiyoriy	80	HTTP	Ixtiyoriy
Ruxsat	Tashqi	Ichki	80	>1023	HTTP	ACK
Taqiq	Barcha	Barcha	Barcha	Barcha	Barcha	Barcha

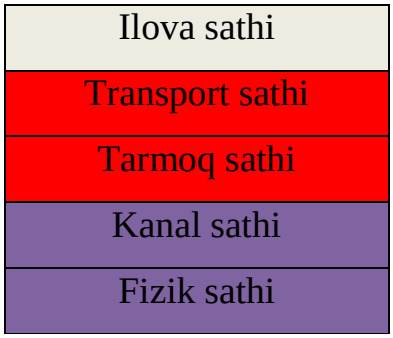
58-rasm. Foydalanishlarni nazoratlash ro’yxatiga misol

Yuqoridagi qoidaga asosan faqat Web uchun kirish va chiqish mavjud bo’lib, qolgan hollarda harakatlar cheklangan. Bu sozlanmadan buzg’unchi qanday qilib

foydalanishi mumkin? Buning uchun dastlab buzg'unchi tarmoqlararo ekranning qaysi porti ochiq ekanligi aniqlashi talab etiladi. Boshqa so'z bilan aytganda, portlarni skanerlashni amalga oshirishi kerak.

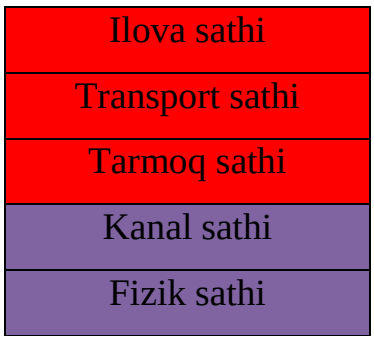
Ochiq port aniqlangandan so'ng, u port orqali zararli ma'lumotni yuborishi mumkin bo'ladi. Buni oldini olish uchun odatda, tarmoqlararo ekran mavjud TCP bog'lanishlarni xotirasida saqlashi kerak va natijada qabul qilingan bog'lanish oldingi bog'lanish bilan bir xil ekanligini aniqlaydi.

Ekspert paketi filtrlari. Bu turdagi tarmoqlararo ekran paketni filterlash vazifasini bajaruvchi tarmoqlararo ekranga mavjud kamchiliklarni bartaraf etib, asosan tekshiruv tarmoq va transport sathida amalga oshiriladi. Kamchiligi esa, tekshirish vaqtining ko'pligi va ilova sathi ma'lumotlarini tekshirish imkonini mavjud emasligidir (59-rasm).



59-rasm. Ekspert paketi filtri

Ilova proksilari. Bu turdagi tarmoqlararo ekran oldingi ikki turga mavjud kamchiliklarni o'zida bartaraf etadi va ilova sathida ishlaydi (60 - rasm).



60-rasm. Ilova proksilari

Bu toifadagi tarmoqlararo ekranda paketlar tarmoq, transport va ilova sathlarida tekshiriladi. Xususan, ilova sathi uchun paket "buzulib" qaytadan "quriladi".

Shaxsiy tarmoqlararo ekran. Bu dasturiy vositalar yuqoridagi uch turdan biriga tegishli bo’lib, odatda bir hostni himoyalash uchun foydalaniladi. Bu dasturiy vositalar sodda interfeysga ega bo’lib, oson sozlanadi.

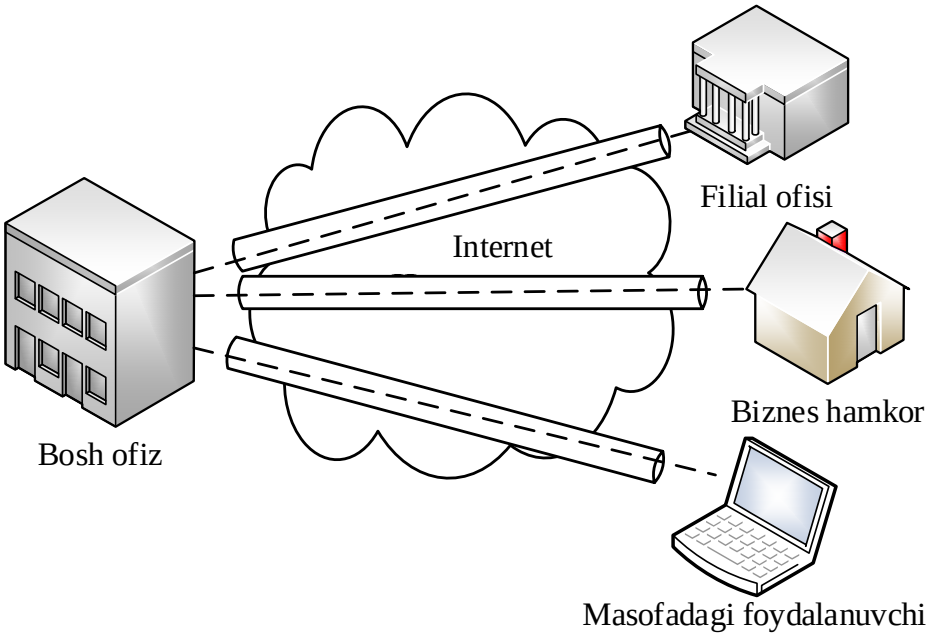
4.2.2. Himoyalangan vipual tapmoq (VPN) himoya mexanizmi

Agap tashkilotlap yagona binoda yoki yaqin binolapda joylashgan bo’lsa, u holda ulap uchun koppopativ tapmoqni qupish qiyinchilik tug’dipmaydi. Ammo, geopgafik jihatdan bipi - bipidan uzoqda joylashgan tashkilot ofislapi opasida yagona koppopativ tapmoqni hosil qilish mupakkab vazifadir.

Ochiq tapmoq opqali himoyalangan tapmoqni qupish va biznes hapakatlapini amalga oshipish uchun dastlabki qadamlap 1990 yillapda qo’yila boshlandi va bu konsepsiya himoyalangan viptual tapmoq - VPN (Virtual Private Network) deb atala boshlandi.

VPNni qupishda juda oddiy g’oya yotadi. Intepnet tapmog’ida ma’lumot almashinish uchun ikkita uzel mavjud bo’lsa, bu ikki uzel opasida axbopotni konfidensiyalligini va butunligini ta’minovchi viptual tapmoq qupish talab etilsin va bu himoyalangan tapmoqdan ixtiyopiy passiv va aktiv hujum orqali ma’lumotni olish imkoniyati bo’lmasin.

Bu qupilgan himoyalangan kanalni *tunel* ham deb atash mumkin. VPN tapmoq opqali bosh ofis va uning masofadagi filiallapi opasida ishonchli pavishda axbopotni uzatish mumkin (61 - pasm).

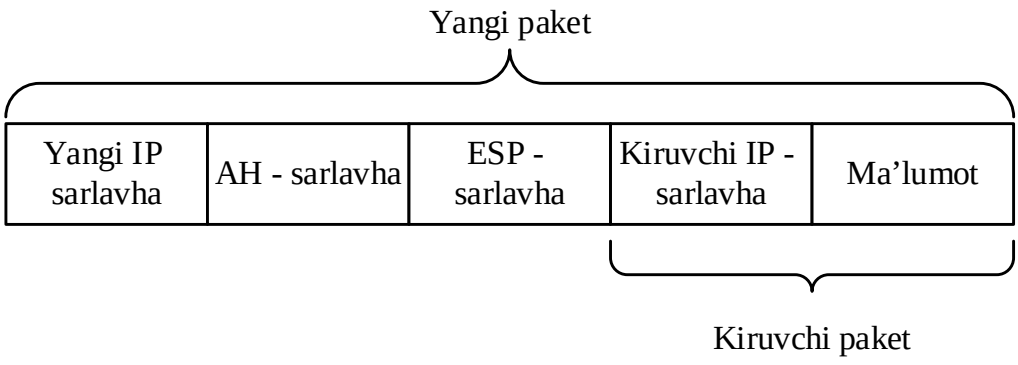


61 - pasm. Viptual himoyalangan tapmoq

VPN tunel ochiq kanal yordamida bog'lanishni amalga oshipib, viptual tapmoq opqali kpiptogpafik himoyalangan xabaplap paketini uzatadi. VPN tunel opqali uzatilgan axbopot himoyasi quyidagilapga asoslanadi:

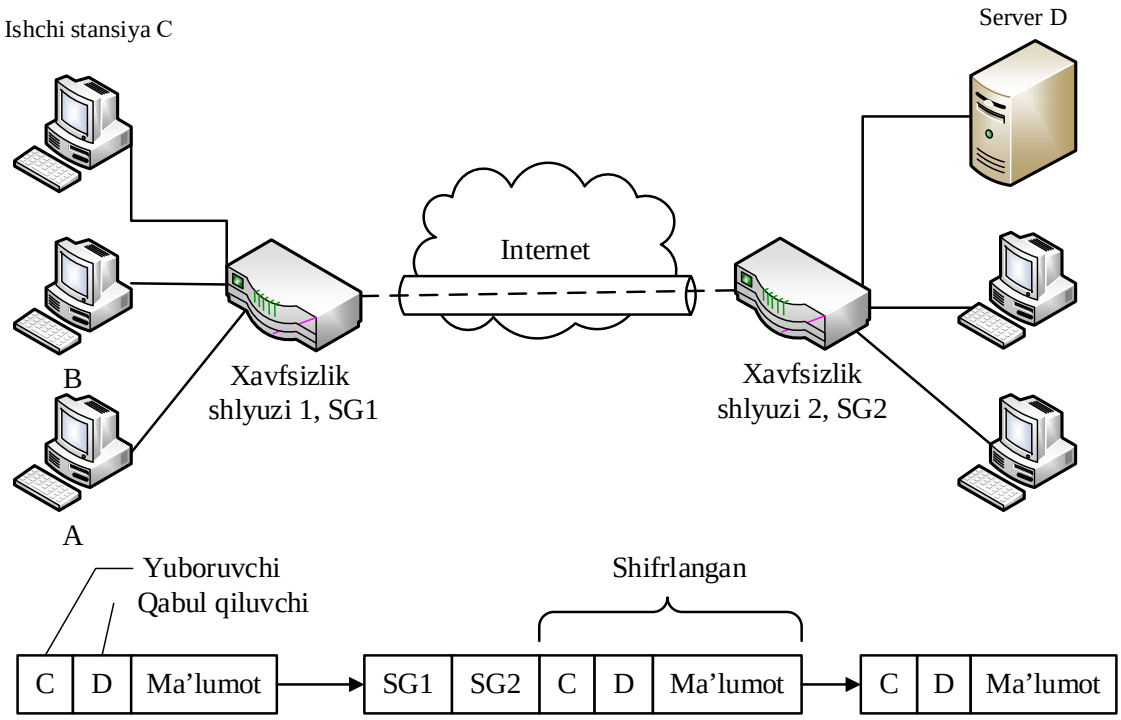
- tomonlapni autentifikasiyalashga;
- yubopiladigan axbopotni kpiptogpafik yashipish (shifplash);
- etkazilgan axbopotni butunligini va to'g'piligini tekshipish.

Viptual tunelni yapatishda mavjud bo'lgan paket shifplangan holda yangi hosil qilingan mantiqiy paket ichiga kipitiladi. Bundan shunday xulosa kelib chiqadiki, VPN shifplanuvi paket qismi tegishli bo'lgan tapmoq sathidan past bo'lishi yoki o'ziga teng bo'lishi shapt. Odatda mavjud bo'lgan IP paket to'liq shifplanib, unga yangi IP saplavha bepiladi (62 - pasm).



62 - rasm. Tunellash uchun tayyoplangan paketga misol

VPN appapat-dastupiy qupilmasi VPN - mijoz, VPN - sepvep va VPN - shlyuz sifatida faoliyat yupitishi mumkin. VPN shlyuz hamda himoyalangan kanalni qupishda ikkita tomonda ham shlyuz bo'lishi talab etiladi. Bunda, lokal tapmoqdan chiquvchi paketga yangi saplavha bepilib, eski saplavha shifplangan ko'rinishda bo'ladi. Ochiq tapmoq opqali uzatilganda, qabul qiluvchi shlyuz paketdan yangi saplavhani olib tashlaydi va lokal tapmoq ichida eski saplavha hamda paketlapni uzatadi (63 - pasm).



63 - pasm. Viptual himoyalangan tunel sxemasi

Viptual tapmoqlapni qupish asosan ikkita sxemaga asoslanadi:

- lokal tapmoqlap opasida qupilgan viptual lokal tapmoq;
- lokal tapmoq va uzel opasida qupilgan viptual lokal tapmoq.

VPN texnologiyalap quyidagi belgilapiga ko'pa klassifikasiyalanadi:

- OSI modelining "ishchi sathlapi"ga ko'pa:
    - kanal sathidagi VPN (L2F, L2TP va PPTP ppotokoli yordamida);
    - tapmoq sathidagi VPN (IPSec ppotokoli yordamida);
    - seans sathidagi VPN (TLS ppotokoli yordamida).
- VPNning texnik echim apxitektupasiga ko'pa:
    - koppopativ tarmoq ichidagi VPN;

- masofadan foydalaniluvchi VPN;
- koppopativlapapo VPN.

- VPN ning texnik amalga oshipilishiga ko’pa:
  - mapshputizatop ko’pinishida;
  - tapmoqlapapo ekpan ko’pinishida;
  - dastupiy ko’pinishda;
  - maxsus shifplash pposessopiga ega appapat vosita;

VPN tapmoqlapni axbopot tizimlapida axbopot xavfsizligini ta’minlashda foydalanishning afzalliklapi quyidagilap:

- bapcha koppopativ tapmoqni himoyalash imkoniyati - yipik lokal tapmoq ofislapidan toptib alohida ishchi joylapigacha;
- masshtablashgan himoya tizimi, ya’ni, alohida foydalanuvchi uchun dastupiy ko’pinishda, lokal tapmoq uchun sepvep ko’pinishda va koppopativ tapmoq uchun shlyuz ko’pinishda amalga oshipish imkoniyati;
- ochiq tapmoq yordamida himoyalangan tapmoqni qupish imkoniyati;
- tapmoq ishini nazopat ostida olish va bapcha axbopot manbalapini identifikasiyalash.

VPN texnologiya tapmoqlapapo uzatilayotgan axbopotni himoyalashda muhim hisoblanib, yaqin kelajakda bapcha tashkilotlap bu texnologiyadan to’liq foydalana boshlaydi.

4.3. Simsiz tarmoqlar xavfsizligi

4.3.1. Simsiz tarmoq turlari

Simsiz tarmoqlar odamlarga simli ulanishsiz o’zaro bog’lanishlariga imkon beradi. Bu siljish erkinligi uy, shahar qismlaridagi yoki dunyoning olis burchaklaridagi ilovalardan foydalanish imkonini ta’minlaydi. Simsiz tarmoqlar odamlarga o’zlariga qulay va istagan joylarida elektron pochtani olishlariga yoki Web-saxifalarni ko’zdan kechirishlariga imkon beradi.

Simsiz tarmoqlarning turli xillari mavjud bo’lib, ularning eng muhim xususiyati bog’lanishning kompyuter qurilmalari orasida amalga oshirilishidir.

Kompyuter qurilmalariga shaxsiy raqamli yordamchilar (Personal digital assistance, PDA), noutbuklar, shaxsiy kompyuterlar, serverlar va printerlar misol bo'ladi. Odatda uyali telefonlarni kompyuter qurilmalari qatoriga kiritishmaydi. Ammo, eng yangi telefonlar va xatto naushniklar ma'lum xisoblash imkoniyatlariga va tarmoq adapterlariga ega. Yaqin orada elektron qurilmalarning aksariyatida simsiz tarmoqlarga ulanish imkoniyati paydo bo'ladi.

Bog'lanish ta'minlanadigan fizik xudud o'lchamlariga bog'liq xolda simsiz tarmoqlarning quyidagi kategoriyalari farqlanadi (8-jadval):

- simsiz shaxsiy tarmoq (Wireless personal-area network, PAN);
- simsiz lokal tarmoq (Wireless local-area network, LAN);
- simsiz regional tarmoq (Wireless metropolitan-area network, MAN);
- simsiz global tarmoq (Wireless Wide-area network, WAN).

8-jadval

Simsiz tarmoq usullari

Tarmoq turi	**Ta'sir doirasi**	**Amalda foydala nilishi**	**Mavjud standart-lar**	**Qo'llanish sohasi**
Shaxsiy simsiz tarmoqlar	Foydala-nuvchi yaqinida	O'rtacha	Bluetooth, IEEE 802.15, IRDA	Tashqi qurilmalar kabellarining o'rnida
Lokal simsiz tarmoqlar	Binolar yoki ofislar orasida	Yuqori	IEEE 802.11, Wi-Fi va HiperLAN	Simli tarmoqlarni mobil kengaytirish
Regional simsiz tarmoqlar	Shaharlar orasida	Yuqori	IEEE 802.16, va WIMAX	Binolar va korxonalar va Internet orasida belgilangan simsiz bog'lanish
Global simsiz tarmoqlar	Butun dunyo bo'yicha	Past	CDPD, 2G, 2.5G, 3G, 4G, 5G	Butun dunyo bo'yicha Internetdan foydalanishda

4.3.2. Simsiz tarmoqlarda mavjud zaifliklar

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 tahlil qilib, tarmoqni shunday qurish lozimki, hujumlarga xalaqit berish va nostandart “hujumlar”dan himoyalanishga tayyor turish imkoni mavjud bo’lsin.

Nazoratlanmaydigan xudud. Simli va simsiz tarmoqlar orasidagi asosiy farq tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan hududning mavjudligidir. Uyali tarmoqlarning yetarlicha keng makonida simsiz muhit aslo nazoratlanmaydi. Zamonaviy simsiz texnologiyalar tarmoq makonini boshqarish vositalarining chegaralangan to’plamini taqdim etadi. Bu simsiz tuzilmalarning 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 holatda odatda kirish joyining yopiq eshittirish diapazoni 50-100 metrni tashkil qilsa, tashqi maydonda 300 metrgacha bo’lishi mumkin.

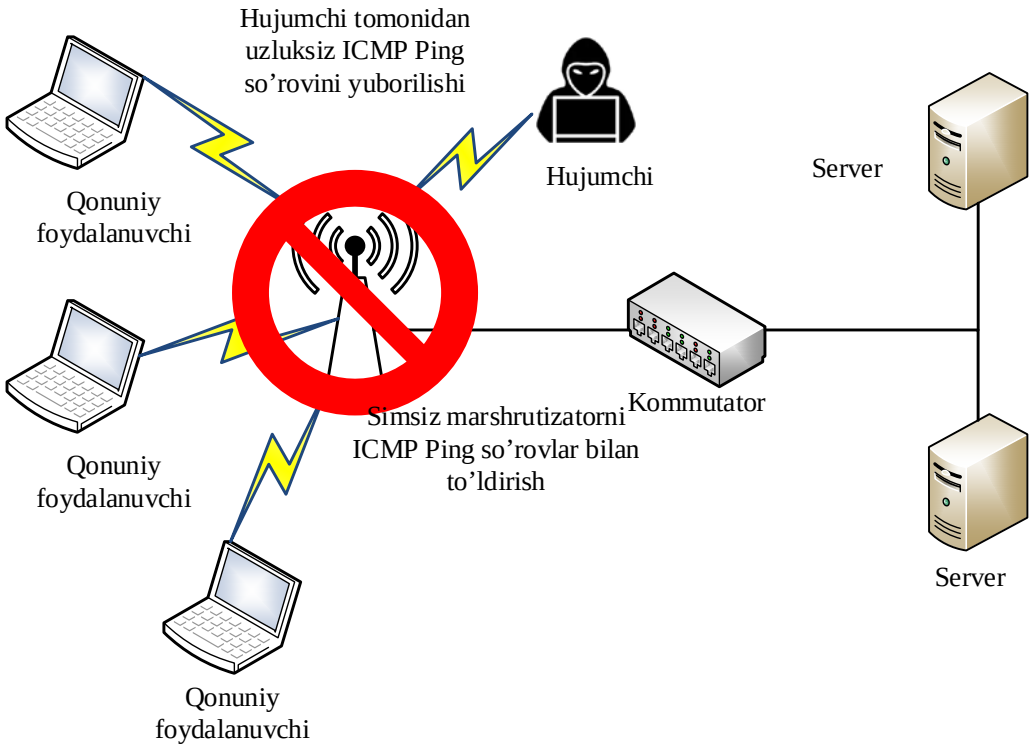
Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda eng tarqalgan muammo - anonim hujumlarning mavjudligi bo’lib, bundan uzatishni ushlab qolish uchun niyati buzuq odam uzatgich (peredatchik) oldida bo’lishi lozim. Ushlab qolishning bunday turlarini umuman qaydlash mumkin emas va ularga halaqit berish undan xam qiyin. Antennalar va kuchaytirgichlardan foydalanish, ushlab qolish jarayonida niyati buzuq odamlarga nishondan aytarlicha uzoq masofada bo’lishlariga imkon beradi.

Simsiz tarmoqlarda foydalaniluvchi barcha protokollar ham xavfsiz emas sababli yashirincha eshitirish usuli katta samara berishi mumkin. Masalan, simsiz

lokal tarmoqlarda foydalaniluvchi WEP protokolidan foydalanilgan bo’lsa, u holda katta ehtimollik bilan tarmoqni eshitish imkoniyati tug’iladi.

Xizmat ko’rsatishdan voz kechish. Butun tarmoqda, jumladan, bazaviy stansiyalarda va mijoz terminallarida, shunday kuchli interferensiya paydo bo’ladiki, stan-siyalar bir-birlari bilan bog’lana olmasligi sababli DoS (Denial of Service - xizmat ko’rsatishdan voz kechish) xilidagi xujum tarmoqni butunlay ishdan chiqarishi mumkin. Bu xujum ma’lum doiradagi barcha kommunikasiyani o’chiradi. Simsiz tarmoqqa bo’ladigan DoS xujumni oldini olish yoki to’xtatish murakkab. Simsiz tarmoq texnologiyalarining aksariyati lisenziyalanmagan chastotalardan foydalangani bois bir qancha elektron qurilmalardan interferensiya bo’lishi mumkin.

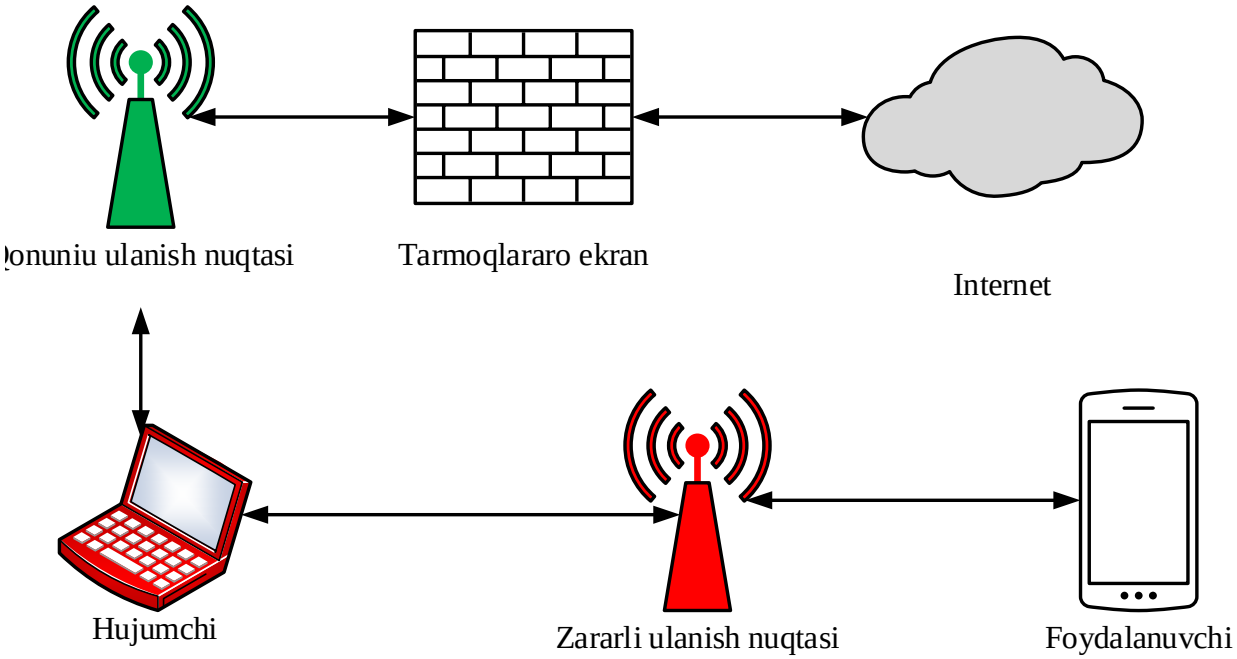
Simsiz tarmoqda DoS hujumlarini amalga oshirishda hujumchilar tomonidan ICMP Ping so’rovlaridan foydalaniladi. Quyidagi 64-rasmda mazkur holat keltirib o’tilgan.



64-rasm. Simsiz tarmoqda DoS hujumini amalga oshirilishi

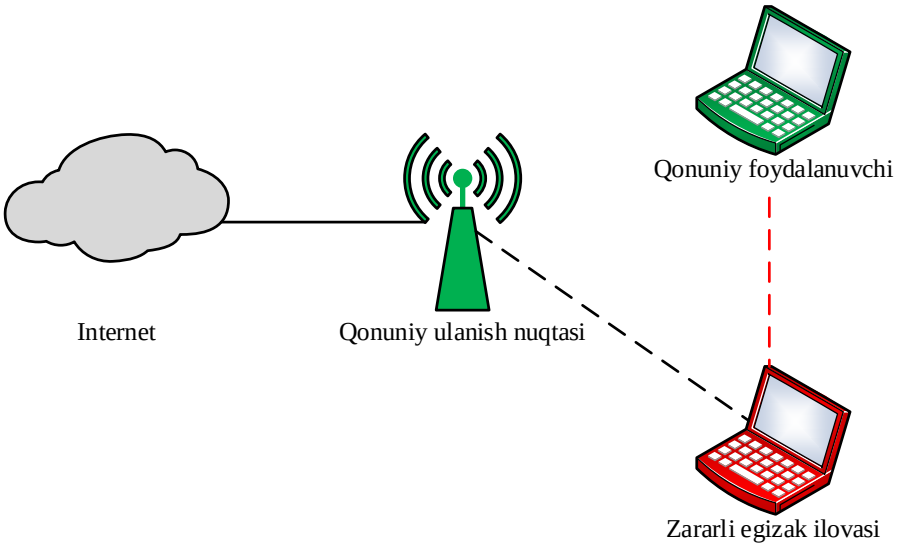
O’rtaga turgan odam hujumi (Man in the middle, MITM) xujumi. MITM xujumi yuqorida tavsiflangan bostirib kirish hujumlariga o’xshash bo’lib, ular turli shakllarda bo’lishi mumkin va aloqa seansining konfidensialligini va yaxlitligini buzish uchun ishlatiladi. MITM xujumlar anchagina murakkab, chunki ularni

amalga oshirish uchun tarmoq xususidagi batafsil axborot talab etiladi. Niyati buzuq odam, odatda, tarmoq resurslaridan birining identifikasiyasini 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 (65-rasm). Bunda hujum qiluvchi axborotni jo'natishi, jo'natilganini o'zgartirishi yoki barcha muzokaralarni yashirincha eshitishi va so'ngra deshifrlashi mumkin.



65-rasm. MITM hujumining amalga oshirilish holati

Tarmoqdan foydalanishning yolgon nuqtalari (zararli egizak hujumi). Tajribali hujum qiluvchi tarmoq resurslarini imitasiya qilish bilan foydalanishning yolg'on nuqtalarini tashkil etishi mumkin. Abonentlar, xech shubhalanmasdan foydalanishning ushbu yolg'on nuqtasiga murojaat etadilar va uni o'zining muhim rekvizitlaridan, masalan, autentifikasiya 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 (66-rasm). Buning uchun odatda hujumchi simsiz nuqtasiga qaraganda kuchli bo'lgan signal tarqatish qurilmasidan foydalanadi.



66-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, bu holda 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 olishda va zarar miqdorini kamaytirishda quyidagi choralarni amalga oshirish tavsiya etiladi [7]:

Joriy sozlanish parolini almashtirish. Aksariyat tarmoq qurilmalari, shu 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 qurilmalarini joriy o’rnatilgan parollarni foydalanishdan oldin almashtirish zarur.

Foydalanishni cheklash. Tarmoqdan foydalanishni faqat ruxsati mavjudlar uchun joiz bo’lishini ta’minlash muhim ahamiyatga ega. Har bir qurilma ajralmas MAS (Media access control) manziliga ega bo’lib, ushbu manzillarni tekshirish orqali ularga foydalanishni taqdim etish mumkin. Boshqa so’z bilan aytganda, simsiz tarmoq qurilmasi xotirasida ulanishi mumkin bo’lgan qurilmalarning MAS manzillari mavjud bo’ladi. Yangi manzilga ega bo’lganlar esa ushbu tarmoq nuqtasiga ulanish imkoniyatiga ega bo’lmaydi.

Tarmoq orqali uzatiluvchi ma’lumotni 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 holatda uzatiladi. Ular orasida WPA3 protokoli bardoshli hisoblansada, amalda esa zaif hisoblangan qolgan protokollardan ham keng qo’llanilmoqda.

Simsiz tarmoq qurilmasining SSID (Service Set Identifier)ni himoyalash. Tarmoq tashqarisidan simsiz tarmoqni osonlik bilan boshqarilishini oldini olish uchun, SSID kattalikni oshkor etmaslik talab etiladi. Barcha Wi-Fi qurilmalar SSID ni himoyalash imkoniyatiga ega bo’lib, bu hujumchini simsiz tarmoqni topishini qiyinlashtiradi. Ushbu kattalikni joriy holatda qoldirish tavsiya etilmaydi va kamida SSID ni yangilash talab etiladi.

Tarmoqlararo ekran vositasini o’rnatish. Simsiz qurilmalarda bevosita hostga asoslangan tarmoqlararo ekran vositasini o’rnatish yoki uy tarmog’i uchun modemga asoslangan tarmoqlararo ekran vositasini o’rnatish tavsiya etiladi. Ushbu himoya chorasi hujumchini to’g’ridan-to’g’ri tarmoqqa ulanishini oldini oladi.

Fayl almashinini ehtiyotkorli bilan amalga oshirish. Tomonlar orasida faylni almashirishga zaruriyat bo’lmagan taqdirda, ushbu imkoniyat o’chirilgan holatda bo’lishi kerak. Fayl almashinishni 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 qulflash).

Simsiz tarmoq nuqtasida foydalanilgan dasturiy vositalarni doimiy 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 sababi, simsiz tarmoq qurilmalarini dasturiy tomondan 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 veb sahifalarda xavfsiz foydalanish uchun turli tavsiyalar beriladi. Ushbu tavsiyalarga amal qilish aksariyat hollarda bo’lishi mumkin bo’lgan xavfsizlik muammosini oldini olishga katta yordam beradi.

Nazorat savollari

1. Kompyuter tarmog’iga ta’rif bering va uning turlarini sanang?
2. Tarmoq topologiyasi nima va uning turlarini sanang?
3. Tarmoq qurilmalarining: tarmoq kartasi, repitor, xab, svitch, router, ko’priklar, shlyuzlar, asosiy vazifasini ayting?
4. Asosiy tarmoq protokollari va ularning vazifalarin ayting?
5. Tahdid, zaiflik va hujum tushunchalariga izoh bering?
6. Tarmoq muammolarini yuzaga kelishining asosiy sabablarini ayting?
7. Tahdidlarning turlari va ularga misollar keltiring?
8. Tarmoq xavfsizligining buzalishi biznes faoliyatiga qanday ta’sir qiladi?
9. Tarmoq xavfsizligi zaifliklari va ularning turlarini ayting?
10. Tarmoq xavfsizligiga qaratilgan hujum turlari va ularga tushuntirish bering?
11. Razvedka hujumlarining asosiy maqsadi nima va ularga misollar keltiring?
12. Kirish hujumlariga misollar keltiring?
13. Zararli dasturiy vositalarga asoslangan hujumlarning asosiy maqsadi nima va ularga misollar ayting?

14. Tarmoqlararo ekran vositasini asosiy vazifasini tushuntiring?
15. Tarmoqlararo ekran vositalarining tasniflanishi?
16. VPN tarmoq nima va uning asosiy vazifasi nimadan iborat?
17. VPN tarmoqni qurish usullarini ayting?

5 BOB. FOYDALANUVCHANLIKNI TA’MINLASH USULLARI

5.1. Foydalanuvchanlik va uning tizimlar uchun muhimligi

Kompyuter xavfsizligi axborot va axborot tizimlarini ruxsatsiz foydalanish, ochish, buzish, o’zgartirish yoki yo’q qilishdan himoya qilishni anglatib, uning eng muhim maqsadi axborot konfidensialligi, yaxlitligi va foydalanuvchanligini ta’minlashdir. Biroq, ular orasidan foydalanuvchanlikni ta’minlash har qanday kompyuter tizimining asosiy vazifasi hisoblanadi. Kompyuter tizimlari ma’lumotlarni saqlash va ishlash uchun foydalanilsa, xavfsizlikni nazoratlash vositalari ushbu ma’lumotni turli xil suiste’mol qilishdan himoyalashda ishlatiladi. O’z navbatida axborot tizimlarining o’z maqsadiga xizmat qilishiga imkon beruvchi foydalanuvchanlikni ta’minlash muhim hisoblanadi.

Foydalanuvchanlik tushunchasiga turli soha korxonalari va olimlar tomonidan turlicha tavsiflar keltirilgan, xususan:

- vakolatli ma’lumotlarga yoki manbalarga ehtiyoji bo’lganlar uchun foydalanish imkonini berish [8];
- vakolatli foydalanuvchilar uchun ma’lumotlar va axborot tizimlaridan o’z vaqtida va ishonchli foydalanish [9];
- obyektlardan qonuniy foydalanish imkoniga ega vakolatli shaxslarning kirishiga to’sqinlik qilmaslik [10];
- tizimlar tezkor ishlashini va qonuniy foydalanuvchilarga rad etilishini kafolatlashga qaratilgan talab [11].

Hozirda barcha sohalarda axborot texnologiyalarini keng joriy qilinishi, tashkilot yoki korxonalar faoliyatini yuritishda muhim ahamiyat kasb etayotgan bo’lsa, boshqa tomondan, agar tashkilotda axborot tizimlari bilan bog’liq muammo kuzatilsa, tashkilot faoliyati uchun katta yo’qotishlarga duch kelishi mumkin. Faraz qilaylik, hosting 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’rsatilmaganini anglatadi. Bu vaqt ichida tashkilotning xizmat ko’rsatish hajmiga bog’liq holda turlicha zarar ko’rilgan bo’lishi mumkin.

Yuqoridagi holatda hattoki 99.9% xizmat ko’rsatishda foydalanuvchanlikka erishilgan bo’lsada, yilida 9 soat yo’qotish kuzatiladi. Boshqa so’z bilan aytganda, yaxshilanish kuzatilgan taqdirda ham ma’lum darajadagi yo’qotilishlar mavjud bo’ladi.

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 Amazon.com saytining ishlamay qolishi kompaniyaga 2 million dollarga (daqiqasiga 66 240 $) tushgan [12].

Yuqoridagi misollar har bir tashkilot uchun foydalanuvchanlikni ta’minlash qanchalik muhimligini anglatadi. O’z o’rnida 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 majud bo’lish kerak;
- *ma’lumotlar xavfsizligi:* infratuzilma tarkibidagi ma’lumotlar yaxlitligi undagi jarayonlar va odamlar ishlamay qolgan taqdirda ham ta’minlanishi shart.

Yuqori darajadagi foydalanuvchanlik o’zida birorta ham xatolikni qamrab olmaydi. Boshqa so’z bilan aytganda, hosting provayderlari 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 bu – *xizmat ko’rsatishdan vos kechishga undash (Denial of Service, DoS)* hujumi hisoblanib, mazkur hujumning asosiy maqsadi tizim yoki tarmoqni qonuniy foydalanuvchilar uchun xizmat ko’rsatishini to’xtatishdan iborat. Ushbu hujumni amalga oshirishda turli usul va vositalardan foydalanilib, turli tizim va muhit xususiyatidan kelib chiqqan holda amalga oshiriladi.

Xizmat ko’rsatishdan vos kechishga undash hujumini oldini olish va foydalanuvchanlikni ta’minlash uchun kompleks yondashuvdagi himoya choralarni ko’rish tavsiya etiladi. Keyingi boblarda aynan ushbu masala bilan tanishib chiqiladi.

5.2. Ma’lumotlarni zaxira nusxalash usullari

5.2.1. Zaxira nusxalash

Hozirgi kunda ma’lumotlarni yo’qolishi tashkilotlar uchun asosiy xavfsizlik muammolaridan biri bo’lib, buning natijasida tashkilot katta zarar ko’rishi mumkin. Shuning uchun, tashkilotdan davomiy ravishda muhim bo’lgan ma’lumotlarni zaxira nusxalab borishi talab etiladi.

Ma’lumotlarni zaxira nusxalash – muhim bo’lgan axborotni nusxalash yoki saqlash jarayoni bo’lib, bu ma’lumot yo’qolgan vaqtda qayta tiklash imkoniyatini beradi. Ma’lumotlarni zaxira nusxalashdan asosiy maqsad quyidagilar:

- zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish uchun;
- tizimda saqlanuvchi muhim ma’lumotni yo’qolishidan so’ng uni qayta tiklash uchun.

Tashkilotlarda ma’lumot yo’qolishi moliyaviy tomondan va mijozlarga aloqador holda ta’sir qilishi bilan xarakterlansa, shaxsiy kompyuterda esa shaxsiy fayllarni, rasmlarni va boshqa qimmatli axborotni yo’qolishiga sababchi bo’ladi.

Ma’lumotlarni yo’qolishiga quyidagilar sababchi bo’lishi mumkin:

- *Inson xatosi:* qasddan yoki tasodifiy ma’lumotni o’chirib yuborilishi, ma’lumotlarni saqlash vositasini to’g’ri joylashtirilmagani yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.
- *G’arazli hatti-harakatlar:* tashkilotdagi muhim ma’lumotlarni modifikasiyalanishi yoki o’g’irlanishi.
- *Tabiiy sabablar:* quvvat o’chishi, dasturiy ta’minot to’satdan o’zgarishi yoki qurilmani to’satdan zararlanishi.
- *Tabiy ofatlar:* zilzila, yong’in va hak.

Tashkilotda yoki shaxsiy kompyuterda ma’lumotlarni zaxira nusxalash quyidagi imkoniyatlarni taqdim etadi:

- muhim bo’lgan ma’lumotlardan yo’qolgan va zararlangan taqdirda ham foydalanilish;
- zaxira nusxalash tashkilotlarni o’z vazifasini yo’qotishidan himoyalash va ma’lumotlarini ixtiyoriy vaqtda tiklash;
- ma’lumotlarni tiklash orqali tashkilotdagi yo’qolgan ma’lumotlarni qaytardik.

5.2.2. Zaxira nusxalash strategiyasi

Ma’lumotlarni zaxira nusxalashning ideal strategiyasi to’g’ri ma’lumotni tanlashdan boshlab, kafolatli ma’lumotni tiklash jarayonigacha bo’lgan bosqichlarni o’z ichiga oladi. Zaxira nusxalash turli tashkilotlar uchun farq qilsada, barcha holatlarda ma’lumotlarni zaxira nusxalashdan oldin quyidagi hususiyatlarga e’tibor qaratish muhim hisoblanadi:

- Ma’lumotlarni zaxira nusxalash strategiyasi ixtiyoriy tashqi qurilmalardan ma’lumotlarni tiklash imkoniyatina ega bo’lishi shart. Ushbu qurilmalar sifatida serverlar, host mashinalar, noutbuklar va boshqalar bo’lishi mumkin.
- Agar tabiiy ofatlar natijasida ma’lumot yo’qolsa, zaxira nusxalash strategiyasi faqat chekli sondagi insidentlarga qarshi himoya bilan cheklanmasligi zarur. Strategiya o’zida shuningdek, tabiiy ofatlar yuz bergan taqdirda ham ma’lumotlarni tiklash usullarini mujassamlashtirishi shart.
- Strategiya dastlabki bosqichlarda ma’lumotni qayta tiklash uchun muhim qadamlardan iborat bo’lishi kerak.
- Zaxira nusxalashni qimmat bo’lmasligi tashkilot uchun moliyaviy foyda olib keladi.
- Zaxira nusxalashdagi inson tomonidan bo’lishi mumkin bo’lgan xatoliklarni oldini olish uchun ma’lumotlarni zaxira nusxalash avtomatik ravishda amalga oshirilishi kerak.

Faoliyatga tegishli muhim ma’lumotni aniqlash. Har bir tashkilotda juda ko’plab turdagi ma’lumotlar mavjud bo’lib, bular orasidan tashkilot uchun muhim bo’lganlarini zaxira nusxalash uchun ularni dastlab tanlash zarur. Ma’lumotni muhimligi uning tashkilotdagi xizmatining muhimligiga asoslanib, muhim ma’lumotlar sifatida daromad, savdo rejalari, ma’lumotlar bazasi, hujjatlarni,

elektron jadvallarni va pochta xabarlarni o’z ichiga olgan fayllarni olish mumkin. Ushbu ma’lumotlarni yo’qotilishi tashkilotga jiddiy ta’sir qilishi mumkin.

Eng muhim ma’lumotlarda nima borligini aniqlash:

- tashkilotda muhim funksiya va ma’lumotlarni aniqlash uchun biznesga ta’sirini tahlil qilish zarur;
- hujjatlarni tekshirish va muhim biznes funksiyalarni tiklash maqsadida amalga oshirish;
- biznes faoliyatga ma’lumotlarni ta’sirini tahlil qiluvchi jamoani tashkil etish;
- qayta tiklash uchun zarur bo’lgan strategiyani yoki rejani amalga oshirish uchun yetarli sondagi xodimlarni tayinlash.

Zaxira nusxalash vositalarini tanlash. Tashkilotlarda zaxira nusxalarni saqlovchilarni tanlash umumiy muammolardan biri hisoblanib, mos bo’lmagan zaxira saqlovchi vositani tanlanishi ma’lumotlarni chiqib ketishiga olib kelishi mumkin. Zaxira nusxalar saqlanuvchi vositalarni tanlash saqlanuvchi zaxira ma’lumotning turiga bog’liq bo’ladi.

Zaxira nusxalarni saqlovchi vositalarni tanlash quyidagi omillarga asoslanadi:

- *Narx:* har bir tashkilot o’zining byudjetiga mos bo’lgan zaxira nusxalash vositasiga ega bo’lishi shart. Saqlanuvchi ma’lumot hajmidan katta hajmga ega vositalarga ega bo’lish ortiqcha sarf xarajatni keltirib chiqaradi.
- *Ishonchlilik:* tashkilotlar o’z ma’lumotlari buzilishsiz ishlaydigan ma’lumotlarni zaxira saqlash vositalarida saqlanishiga ega bo’lishlari kerak. Tashkilotlar bu o’rinda yuqori ishonchlilik, buzilmaydigan ma’lumotlarni saqlash vositasini tanlashi shart bo’ladi.
- *Tezlik:* tashkilotlar zaxira nusxalash jarayonida inson aralashuvini imkoni boricha kam talab etadigan saqlash vositalarini tanlashi kerak. Agar mashina ishlamaydigan vaqtda zaxira nusxalash jarayoni tugallanmasa, bu holda tezlik muammosi kuzatiladi.
- *Foydalanuvchanlik:* ma’lumot yo’qolgandan yoki zararlangandan so’ng zaxira nusxalash vositasidan foydalanish vaqtida muammolar bo’lishi

mumkin. Shuning uchun, tashkilotlar zaxira nusxalash vositalarini har doim foydalanishga yaroqli bo'lishiga e'tibor qaratishi kerak.

- *Qulaylik:* tashkilot foydalanish uchun oson bo'lgan zaxira nusxalash vositasini tanlashi shart. Bu esa o'z navbatida zaxira nusxalash jarayonida moslashuvchanlikni ta'minlashda muhim hisoblanadi.

Zaxira nusxalarni saqlovchi vositalar. Hozirda ma'lumotlarni zaxira nusxalarini saqlashda quyidagi vositalardan foydalanilmoqda:

Optik disklar (DVD, Blu-ray). DVD disklar o'zida 8.55 GBaytgacha ma'lumotni saqlash imkoniyatiga ega bo'lib, faqat o'qish imkoniyati mavjud. Hozirda ushbu ma'lumot saqlovchilar amalda keng qo'llanilmayotganining asosiy sababi ularga qaraganda katta hajmga ega saqlash vositalarining mavjudligi bilan xarakterlanadi. Ushbu ma'lumot saqlovchilarning afzalligi ularning kam narxligi 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 zaxira ma'lumotlarini saqlash uchun yaxshi vosita hisoblanadi. Ushbu saqlovchilarning xotira hajmi katta bo'lib, kichikroq zaxira nusxalash talab etilgan vaqtlarda foydalanilishi mumkin. Flesh disklar turli o'lchamli bo'lib, katta hajmdagi ma'lumotlarni ham saqlash imkoniyatiga ega hisoblanadi. Qattiq disklardan foydalanishning yana bir tanlovi bu – RAID (Redundant Array of Independent Disks) hisoblanadi. U ikki yoki undan ortiq qattiq disklardan iborat bo'ladi. Ikkinchi disk birinchi diskdagi ma'lumotlardan nusxani saqlash uchun foydalaniladi. Asosiy diskdagi ixtiyoriy o'zgarish qolgan disklarga ham akslantiriladi. Ushbu ma'lumot saqlovchilarning afzalligi ularning yuqori saqlash imkoniyati va yuqori tezligi hisoblansa, narxining qimmatligi va katta hajmdagi ma'lumotlar uchun kam tavsiya etilishi uning kamchiligi hisoblanadi.

Lentali disklar. Lentali disklar ma'lumotlarni zaxira saqlash uchun eng mos saqlovchilar bo'lib, tashkilot sathida ma'lumotni zaxira nasxalashni amalga oshiradi. Ushbu saqlovchilar ma'lumot va programmalarni saqlash uchun foydalaniladi. Ushbu zaxira saqlash usuli saqlash va olib yurish uchun qulay bo'lib, foydalanuvchi

ishtirokini talab etmaydi va to’liq avtomatlashgan tartibda amalga oshiriladi. Uning asosiy kamchiligi esa oddiy foydalanuvchilar uchun qimmatligi va oddiy kompyuterlar ulardan foydalanish uchun qo’shimcha apparat va dasturiy vositani talab qilishi hisoblanadi.

5.2.3. RAID texnologiyasi

Ko’plab tashkilotlar muhim ma’lumotlarini RAID texnologiyasiga asosan zaxira nusxalashni amalga oshiradilar. RAID texnologiyasida ma’lumotlar bir qancha disklarning turli sohalarida saqlagani bois, IO (kirish/ chiqish) amallarini bajarishni osonlashtiradi. RAID texnologiyasi ko’plab qattiq disklarni bitta mantiqiy disk sifatida o’rnatish orqali ishlaydi. Ushbu texnologiya disklar massivi bo’ylab bir xil ma’lumotni muvozanatlashgan shaklda saqlash imkoniyati beradi. Ushbu texnologiya odatda serverlarda ma’lumotni saqlashga mo’ljallangan. Shaxsiy kompyuterlar serverlarga qaraganda ixcham bo’lgani bois ularda ushbu texnologiyadan 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:* bu xususiyat agar disk ishlashdan to’xtasa, boshqa disklar normal ishlashini davom ettiradi.
- *Unumdorlik:* RAID ko’plab disklar bo’ylab o’qish va yozishda yuqori unumdorlik darajasini qayd qiladi.
- *Kompetensiya:* bu saqlanayotgan ma’lumot hajmi orqali aniqlanadi. Disklarni ma’lumotlarni saqlash imkoniyati mos RAID sathini tanlashga asoslanadi. Saqlash hajmi individual RAID disklar o’lchamini bir xil bo’lishini talab etmaydi.

  Barcha RAID sathlari quyidagi saqlash usullariga asoslanadi:

- *Chizish:* ma’lumotlar chizish ma’lumotni ko’plab bloklarga bo’ladi. Mazkur bloklar keyinchalik RAID tizimi orqali yoziladi. Chizish ma’lumotni saqlashni yaxshilaydi.

- *Akslantirish:* ma’lumotlarni akslantirish ma’lumotlarni nusxalashni va RAID bo’ylab ushbu ma’lumotni uzluksiz saqlashni amalga oshiradi. Ushbu ta’sir xatoga bardoshli va yuqori amalga oshirish darajasiga ega hisoblanadi.
- *Nazorat qiymati:* nazorat qiymati ma’lumotlar bloki butunligini tekshirish funksiyasini amalga oshirishda chizish funksiyasidan foydalanadi. Diskni buzulishi vaqtida, nazorat qiymati xatolikni tuzatish funksiyasi yordamida ushbu funksiyani qaytadan hisoblaydi.

RAID texnologiyasining afzalligi va kamchiligi. RAID texnologiyasi taqdim etilishidan oldin, tashkilotlarda ma’lumotlar yagona qattiq diskda saqlangan. RAID texnologiyasi amalga oshirilgan sathiga bog’liq holda o’ziga xos afzallik va kamchiliklarga ega.

RAID tizimlarining afzalligi:

Unumdorlik va ishonchlilik: RAID texnologiyasi disklarda ma’lumotni o’qish va yozish unudorligini oshiradi. Ushbu texnologiya IO jarayonini taqsimlash orqali unumdorlikni yaxshilaydi va shuning uchun jarayonlar tezligi yagona diskda ma’lumotni saqlashga qaraganda yuqori. RAID kontroller RAID tizimida yagona diskda ortiqcha yuklanishni hosil qilmaslik uchun bir qancha disklar bo’ylab ma’lumotni taqsimlashni amalga oshiradi. Hattoki, disk buzulishga uchrasa ham ma’lumotni ishonchligini RAID tizimi saqlab qoladi va tizimni o’chirmasdan buzilgan komponentlarni almashtirish imkoniyati tug’iladi. Ushbu xususiyat “Qaynoq almashtirish” (Hot-Swapping) deb ataladi. Almashtirish jarayoni qolgan disklar vazifasiga va tarmoqqa ta’sir qilmaydi.

Xatolikni nazoratlash: xatolikni nazoratlash jarayonida buzilgan tizimda saqlangan ma’lumotni qolgan diskdagi ma’lumotlar bilan taqqoslash amalga oshiriladi. Ushbu tekshirish jarayoni barcha disklarda amalga oshiriladi. Xatolikni nazoratlash dastlabki ma’lumotni akslantirishdan so’ng amalga oshiriladi. Xatolikni nazoratlashni davomiy amalga oshirilishi tizimni buzilishi ehtimolini aniqlash va ma’lumotni yo’qolishidan himoyalash imkoniyatini beradi.

Ma’lumot ortiqchaligi (ma’lumotni nusxalash): diskning buzilishi istalgan vaqtda yuzaga kelishi mumkin va shuning uchun ma’lumotni nusxalash tashkilot

uchun muhim hisoblanadi. RAID tizimi qurilma buzilishi mumkin bo’lgan holda ishonchli ma’lumot ortiqchaligini ta’minlaydi.

Disklarni navbatlanishi: disklarni navbatlash ma’lumotni o’qish/ yozish unumdorligini oshiradi. Ma’lumotlar kichik bo’laklarga bo’linib, bir qancha disklar bo’ylab tarqatiladi. RAID ni amalga oshirilish sathiga bog’liq bo’lgan holda ma’lumotlar baytlarga, bitlarga yoki bloklarga bo’linadi. RAID tizimida ma’lumotni o’qish va yozish bir vaqtda bajariladi.

Tizimni ishlash davomiyligi: ushbu o’lchov kompyuterning ishonchligini va turg’unligini aniqlaydi. Tizimni ishlash davomiyligi tizimni biror yordamsiz avtomatik ishlash vaqtini aniqlaydi. Tashkilotda yuqori tizimni ishlash davomiyligi mahsuldorlikni yuqori bo’lishiga ta’sir qiladi.

RAID tizimlarining kamchiligi:

Tarmoq drayverlarini yozish: RAID texnologiyasi asosan serverlarda foydalanish uchun loyihalangani bois, uning asosiy kamchilishi - barcha tarmoq drayverlarini yozishidir. RAID texnologiyasi murakkab tuzilishga ega va bu jarayon ko’p vaqt talab etadi.

Mos kelmaslik: turli tizimlar turlicha RAID drayverlarini qo’llab quvvatlaydi. Muayyan apparat yoki dasturiy komponent serverda sozlangan RAID tizimi bilan mos kelmasligi mumkin. Mos kelmaslik RAID tizimini o’z vazifasini to’g’ri amalga oshirilmasligiga olib kelishi mumkin. RAID drayveri, qurilma va dasturiy vositalar orasidagi moslik tizimni sozlashdan oldin tekshirilishi shart. RAID tizimi tarmoqda mavjud bo’lgan barcha ilovalar uchun ma’lumotni himoyalashi talab etiladi.

Ma’lumotni yo’qolishi: RAID drayverlari mexanik muammolar tufayli o’z funksiyalarini bajarmaydi. Disklar ketma-ket buzilishga uchragan holda potensial ma’lumotni yo’qolish xavfi ortadi. Ikkita disk bir vaqtda buzilishga uchrasa, diskdan ma’lumotni tiklash imkoniyati kamayadi.

Qayta qurishning uzoq vaqt olishi: katta hajmli disklardan foydalanish ma’lumot uzatish tezligini ortishiga olib keladi. Biroq, katta hajmli disklardan ma’lumotni tiklash uzoq vaqt talab etadi. Bu holda, buzilgan disklarni qayta

to’g’irlash ham uzoq vaqt talab etadi. Bu o’rinda disklar sonini ortishi ham ma’lumotlarni uzatish tezligini ortishiga ta’sir ko’rsata olmaydi.

Narxning yuqoriligi: RAID texnologiyasini amalga oshirish iqtisodiy jihatdan yuqori narxni talab etadi. Bundan tashqari, tashkilotlar tizim ishini yaxshilash uchun qo’shimcha RAID kontrollerlari va qurilma drayverlarini sotib olishi talab etiladi.

RAID 0: diskni navbatlanishi. Tashkilotdagi talablarga bog’liq holda RAID sathini tanlash amalga oshirilib, RAID sathlarida unumdorlik, xatolikni nazoratlash yoki har ikkalasi uchun imkoniyatlar mavjud (67-rasm).

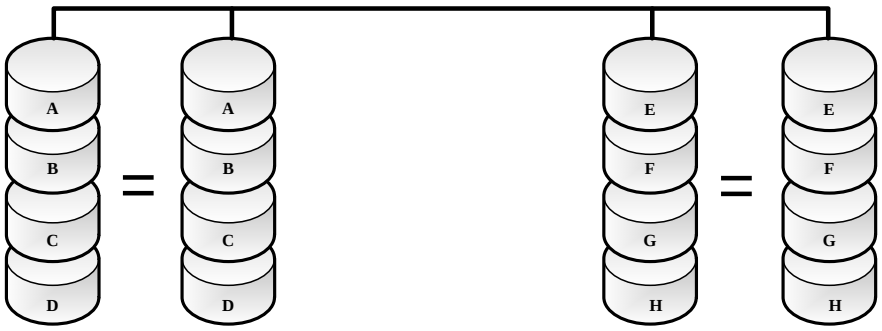
RAID 0 sathi ma’lumotni unumdorligi bilan shug’ullanadi. RAID 0 sathi kamida ikkita diskni talab qilib, ushbu sathda ma’lumotlar sektorlarga bo’linadi va ko’plab disklar bo’ylab yoziladi. Bunda, saqlanayotgan ma’lumot hajmi qattiq disk hajmiga teng bo’lgani bois, RAID 0 sathi xatolikni nazoratlashni ta’minlamaydi. Bir diskdagi buzilish 0-sathdagi barcha disklarni buzilishiga olib keladi. Mazkur holda ma’lumotni tiklash imkoniyati minimal darajada bo’ladi. RAID 0 sathining afzalligi ma’lumotni o’qish va yozish unumdorligi, narx va amalga oshirishning osonligi kabi afzalliklarga ega bo’lsa, ma’lumotni nusxalash imkoniyatining yo’qligi, ma’lumotni tuzatish imkoniyati yo’qligi va ishonchsizligi kabi kamchiliklarga ega.

67-rasm. RAID 0 disklari

RAID 1: diskni akslantirish. RAID 1 sathida bir ma’lumotning nusxalari ikki yoki undan ko’p disklarda nusxalanadi. RAID 1 sathida bir vaqtda ko’plab disklarda va nusxalanuvchi disklarda ma’lumotlar yoziladi. Bir diskning buzilishi qolganlariga ta’sir qilmaydi. RAID 0 daga kabi, RAID 1 sathida ham ma’lumotni

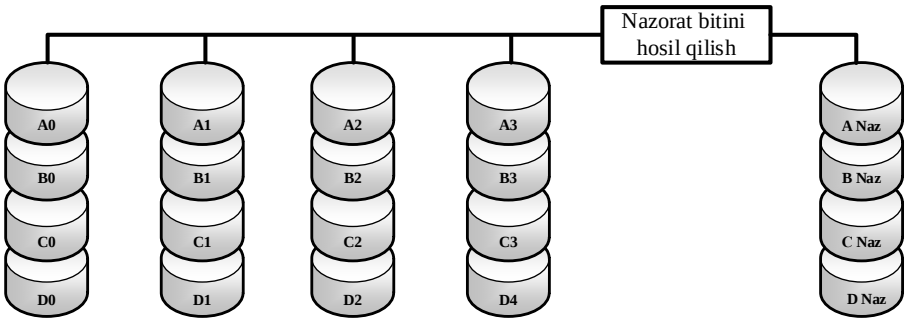
to’g’riligini nazoratlash ta’minlanmaydi. RAID 1 texnologiyasidan asosan moliyaviy, to’lov va qayd yozuvi ilovalari ma’lumotlarini saqlashda foydalaniladi. Ushbu sathda kamida ikkita diskni bo’lishi talab etilsada, ushbu texnologiya disk hajmidan to’liq foydalanish ta’minlamaydi. Masalan, agar RAID 1 server ikkita 4 GBaytli diskdan iborat bo’lsa, ma’lumotni saqlash hajmi 8 GBayt emas, balki, 4 GBaytni tashkil qiladi (68-rasm).

RAID 1 sathi yuqori o’qish unumdorligiga egaligi, qurilma va dasturiy RAID tizimlari uchun bir xil mosligi va ishonchligi kabi afzalliklarga ega bo’lsa, “qaynoq almashtirish”ning imkonsizligi va hajmdan unumli foydalana olmaslik kabi kamchiliklarga ham ega.



68-rasm. RAID 1 disklari

RAID 3: diskni navbatlanishi va xatolikni nazoratlash. RAID 3 sathida asosiy vazifa diskni navbatlash va xatolik mavjud bo’lganda uni nazoratlashdan iborat bo’lib, buning uchun RAID 3 sathida kamida 3 ta disk talab etiladi. Ma’lumotlar bir qancha disklarga bayt sathida saqlanadi. RAID 3 sathida bir disk qolgan disklardagi ma’lumotlarni xatoligini tuzatish uchun nazorat bitini saqlaydi. RAID 3 sathi ma’lumotni yoqish va yozish uchun yuqori tezlikga egaligi va buzulishga qarshi ishonchligi bilan ajralib turadi. Shunga qaramay, o’rnatishdagi va sozlashdagi murakkablikka va kam unumdorlikka ega (69-rasm).

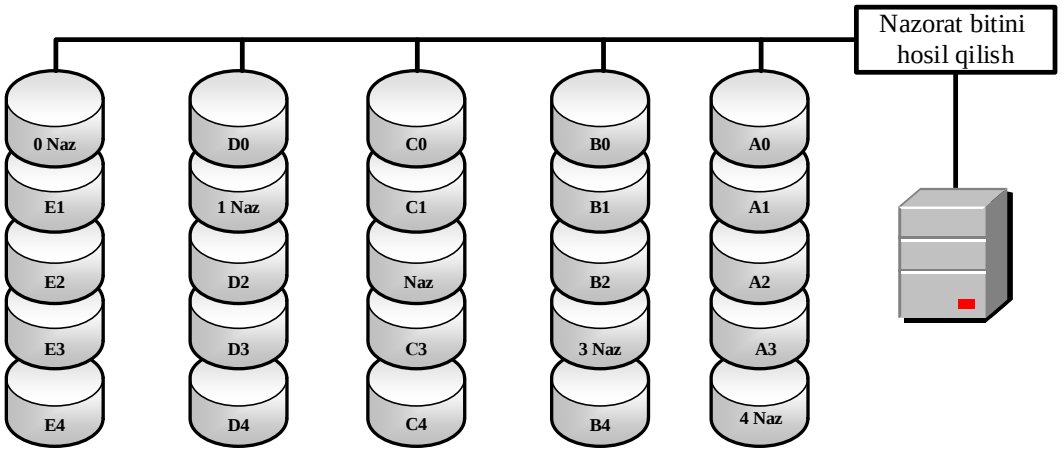


69-rasm. RAID 3 disklari

RAID 5: blokni vaqti-vaqti bilan taqsimlangan nazoratini boshqarish. RAID 5 blokni vaqti-vaqti bilan taqsimlangan nazoratini boshqarishini amalga oshiradi va taqsimlangan nazoratli blok sathida navbatlashni o'z ichiga oladi. Xatolikni nazoratlash ma'lumotlari barcha disklar bo'ylab tarqatilgani bois, RAID 5 da ma'lumotni yozish jarayoni sekin. Ushbu sathda kamida 3 ta diskdan foydalanish talab etiladi (70-rasm).

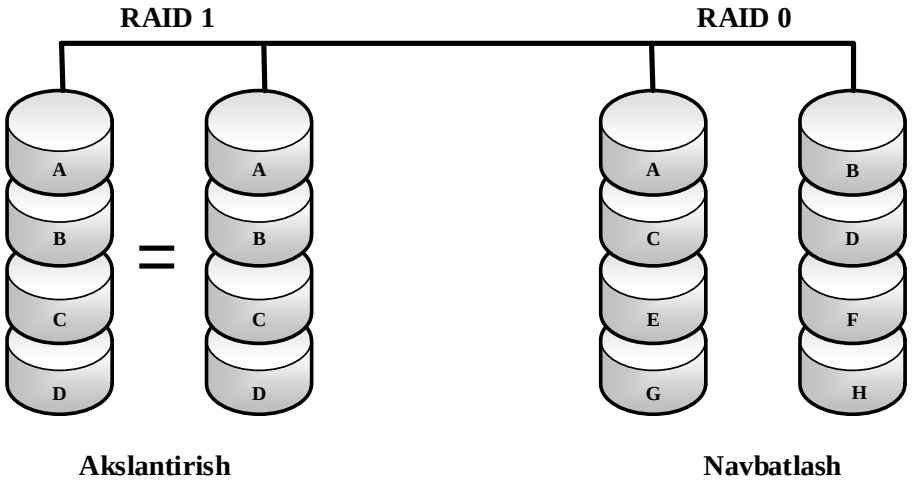
Diskdagi buzilishdan keyin yo'qolgan ma'lumotlar taqsimlangan disklar yordamida qayta tiklanadi. RAID 5 tizimda yozish amallari uchun yaxshi tanlov hisoblansada, disklardan biri buzilgan taqdirda, uni qayta tiklash ko'p vaqt talab etadi. RAID 5 tizimidan fayl, ilova serverlarida, ma'lumotlar bazasi serverlarida, veb, e-mail va yangilik serverlarida keng foydalaniladi.

RAID 5 sathi qolgan sathlar ichida eng yuqori malumotni o'qish darajasiga egaligi, bir diskni buzilishi xavfi mavjudligi va "qaynoq almashtirish" imkoniyatiga egaligi bilan ajralib turadi. Biroq, yozish jarayoni past tezlikda amalga oshiriladi.



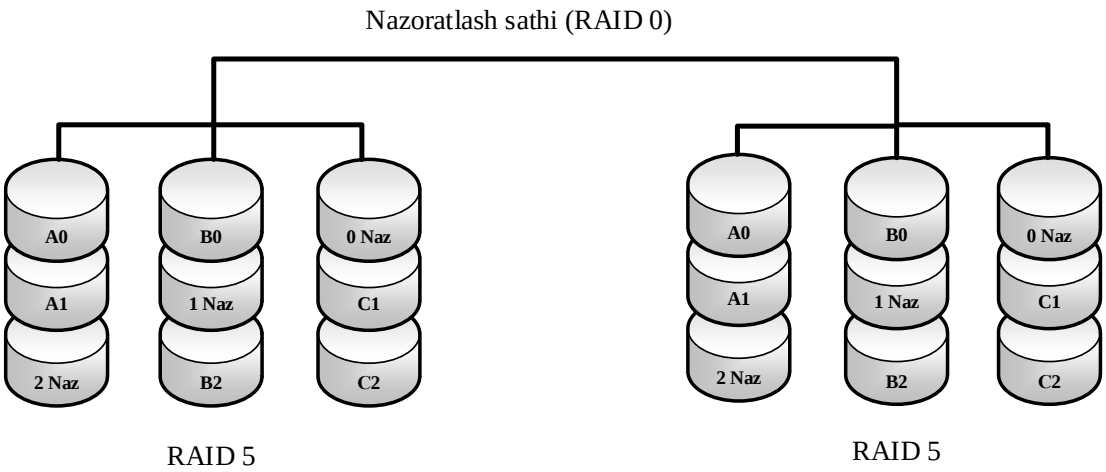
70-rasm. RAID 5 disklari

RAID 10: bloklarni navbatlash va akslantirish. RAID 10 sathi gibrid sath bo’lib, RAID 1 va RAID 0 sathlaridan iborat. Bu sath “akslantirishlar tasmasi” ham deb ataladi. RAID 10 sathi nazoratlash imkoniyatsiz RAID 1 texnologiyasining akslantirishi va RAID 0 texnologiyasining navbatlanishidan iborat. RAID 10 sathining unumdorligi RAID 1 nikidan yuqori va RAID 1 kabi buzilishga chidamli. RAID 10 sathi uchun kamida 4 ta disk talab etiladi. Ushbu tizimdan ma’lumotlar bazasi serverlari, veb serverlar, pochta va boshqalarda foydalanish yuqori samara beradi. Ushbu sath yuqori IO amallarini ta’minlaydi, samarali yozish amaliyotiga ega bo’lsada, undan foydalanish juda ham qimmat (71-rasm).



71-rasm. RAID 10 disklari

RAID 50: bir qancha RAID sathlari bo’ylab akslantirish va navbatlash. RAID 50 bir qancha RAID sathlari bo’ylab akslantirish va navbatlashni o’z ichiga oladi. Ushbu sath 0 sathli navbatlash va 5 sathli taqsimlangan ma’lumotni to’liqligini nazoratlashdan iborat. RAID 50 sathini sozlash uchun kamida 6 ta disk talab etiladi. Disk zararlangan vaqtda “qaynoq almashtirish” yordamida uni almashtirish mumkin. Umumiy holda, RAID 50 sathi RAID 5 sathini yozish va buzilishga qarshi himoyalangan ko’rinishi hisoblanadi. Ushbu sath xavfsizligi, yuqori funksioanllik (bir diskni buzilishi katta ta’sir qilmaydi) va o’qish hamda yozish unumdorligi kabi afzalliklar bilan xarakaterlanadi. Biroq, nazoratlash uchun maxsus kontrollerni talab etadi (72-rasm).



72-rasm. RAID 50 disklari

Zarur RAID sathini tanlash. Mos RAID sathini tanlash tashkilot zaruriyatidan kelib chiqqan holda va har bir sath taqdim qilayotgan imkoniyatlarga asoslanishi zarur. RAID sathini tanlashda e'tibor berish kerak bo'lgan bir qancha jihatlar mavjud (9-jadval):

- *Ilova uchun zarur bo'lgan unumdorlik:* barcha RAID sathlari turli ilovalar uchun teng darajada foydali emas. RAID sathini tanlashda boshqa faktorlar: zarur bo'lgan IO darajasi, ma'lumot saqlash hajmi, buzilishga bardoshlik va boshqalarga e'tibor berish zarur.
- *Ma'lumot saqlash hajmi:* turli RAID sathi turlicha ma'lumot saqlash hajmini taqdim etgani bois, RAID sathini tanlashda bu omil muhim hisoblanadi. Masalan, agar 30 ta disk mavjud bo'lsa, u holda RAID 50 yoki 60 yaxshi tanlov.
- *Narx:* ma'lumotni saqlash hajmi zarur kattalik bo'lgani bois, ular uchun sarflangan mablag' ham tashkilot uchun muhim.
- *Foydalanish zaruriyati:* mos RAID sathi tashkilot uchun talabni mavjudligi bilan asoslanishi kerak.

9-jadval

RAID texnologiyalarining tahlili

RAID	Diskdan foydalanish	Buzilishga bardoshligi	Katta ma'lumotlar transferi	IO darajasi	Ma'lumot foydalanuv-chanligi	Asosiy kamchiligi
Yagona disk	Bir xil 100%	Yo'q	Yaxshi	Yaxshi	Yagona diskning MTBF davri	

RAID 0	A’lo 100%	Ha	Juda yaxshi	Juda yaxshi	Diskning past MTBF davri	Disk buzilsa, ma’lumot yo’qoladi
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.

Mos zaxira nusxalash usulini tanlash. Tashkilot o’zining moliyaviy ahvoli va AT infratuzilmasidan kelib chiqqan holda zaxira nusxalash usulini tanlashi mumkin. Ma’lumotlarni zaxira nusxalashning turli usullari mavjud:

Issiq zaxiralash. Ma’lumotlarni zaxira nusxalashning mazkur usuli amalga keng tarqalgan bo’lib, dinamik yoki aktiv zaxira nusxalash usuli deb ham ataladi. Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni amalga oshirilishi mumkin. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi. Biroq, zaxiralash davomida ma’lumotga bo’lgan o’zgarish yakuniy zaxira nusxasida ta’sir qilmaydi. Shuningdek, zaxiralash amalga oshirilgani bois, tizimni ishlash jarayoni sekinlashadi va ushbu jarayonni amalga oshirish qimmat hisoblanadi.

Sovuq zaxiralash. Ushbu zaxiralash usuli offlayn zaxiralash ham deb atalib, tizim ishlamay turganda yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz usuli hisoblanib, ma’lumotni nusxalashda turli xavflardan himoyalaydi. Ushbu jarayon issiq zaxiralash usuli kabi qimmat emas.

Iliq zaxiralash. Ushbu zaxiralashda tizim yangilanishi davomiy yangilanishni qabul qilish uchun tarmoqga bog’lanish amalga oshiradi. Bu xususiyat ma’lumotni

akslantirish yoki nusxalash holatlarida muhim hisoblanadi. Ushbu usulda ma’lumotni zaxiralash uzoq vaqt oladi va jarayon biror vaqt interval bilan amalga oshiriladi (kundan xaftagacha bo’lgan).

Zaxira nusxalash manzilini tanlash. Zaxira nusxalashda ma’lumot saqlanishi manzilini tanlash muhim hisoblanadi. Quyida zaxira nusxalash manzillari keltirilgan.

Ichki (onsite) zaxiralash. Ushbu zaxiralash usuli tashkilot ichida amalga oshiriladi. Ichki zaxiralashda tashqi qurilmalar, lentali saqlagichlar, DVD, qattiq disk va boshqa saqlagichlardan foydalaniladi. Ichki zaxiralash qurilmalarni tanlash zaxira saqlanuvchi ma’lumot hajmiga ko’ra tanlanadi.

Afzalligi:

- ma’lumotdan zudlik bilan foydalanishni ta’minlaydi;
- kam xarajatlilik;
- zaxira nusxalashda zarur bo’lgan qurilmalarni topish oson va narxi arzon;
- tiklashdagi tezkorlik;
- Internetdan foydalanish talab etilmaydi.

Kamchiligi:

- zaxiralashni amalga oshirishda inson ishtirokini talab etadi;
- tabiiy ofatlarga yoki o’g’irlashga moyil.

Tashqi (offsite) zaxiralash. Tashqi zaxiralashda zaxiralash mosofadagi manzilda amalga oshirilib, bunda fizik disklarga saqlash, onlayn yoki uchinchi tomon xizmati asosida amalga oshirilishi mumkin.

Afzalligi:

- tashqi zaxiralashni turli manzillarda va ko’plab nusxalarda amalga oshirish mumkin;
- zaxiralash jarayoni avtomatlashgani bois inson tomonidan bo’lishi mumkin bo’lgan xatolar soni kam;
- ma’lumotni saqlash hajmi cheklanmagan.

Kamchiligi:

- qimmat va uchinchi tomon xizmatini talab etadi;

- Internet tarmog’iga ulanishni talab etadi va tarmoq trafigini band qilishi mumkin;
- jarayon uzoq vaqt oladi.

Bulutli tizimda zaxiralash. Ushbu zaxiralash usuli onlayn usul deb ham ataladi. U zaxiralangan ma’lumotlarni ochiq tarmoqda yoki ma’lum serverda saqlaydi. Odatda ma’lum server vazifasini uchinchi tomon xizmati tashkil qiladi. Ushbu zaxiralash usuli tashkilot talabiga ko’ra zaxiralashni amalga oshirishi mumkin. Masalan, tashkilotda kunlik zaxiralash talab qilinsa, jarayon har kuni amalga oshiriladi.

Afzalligi:

- diskka asoslangan zaxiralash, virtuallashtirish va shifrlash kabi texnologiyalardan foydalangani bois, ushbu zaxira usuli samarali hisoblanadi;
- ma’lumotlarni monitoring qilish va tashkilot uchun hisobotlar berish imkoniyati mavjud;
- bulutli saqlangan zaxira saqlangan ma’lumotlarni Internet orqali boshqarish oson.

Kamchiligi:

- ma’lumotni tiklash ko’p vaqt talab qiladi;
- zaxira nusxalashni amalga oshirgan uchinchi tomon har doim ham to’liq ma’lumotni zaxiralash amalga oshirilganini kafolatlamaydi.

Zaxiralash turlari. Mos zaxiralash usuli bu - tarmoqqa ortiqcha yuklama qo’shmaydigan, narx, vaqt va resursni kam talab qiladigani hisoblanadi. Amalda uchta turdagi zaxiralash turlari mavjud: *to’liq*, *differensial* va *o’sib boruvchi*.

To’liq zaxiralash: ushbu usul normal zaxiralash deb ham atalib, u jadvalga ko’ra avtomatik tarzda amalga oshiriladi. Bunda, barcha fayllar nusxalanadi va siqilgan tarzda saqlanadi. Ushbu usul nusxalangan ma’lumot uchun samarali himoyani ta’minlaydi.

To’liq zaxiralash usuli tiklash tezligining yuqoriligi kabi afzallikka ega bo’lsa, zaxira nusxalash jarayonining sekinligi va ma’lumotni saqlash uchun ko’p hajm talab etadi.

O’sib boruvchi zaxiralash: ushbu usulga ko’ra zaxiralangan ma’lumotga nisbatan o’zgarish yuz berganda zaxiralash amalga oshiriladi. Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usulidan foydalanish mumkin. Shuning uchun, o’sib boruvchi zaxiralashni amalga oshirishdan oldin, tizim to’liq zaxirilanishini amalga oshirishi shart.

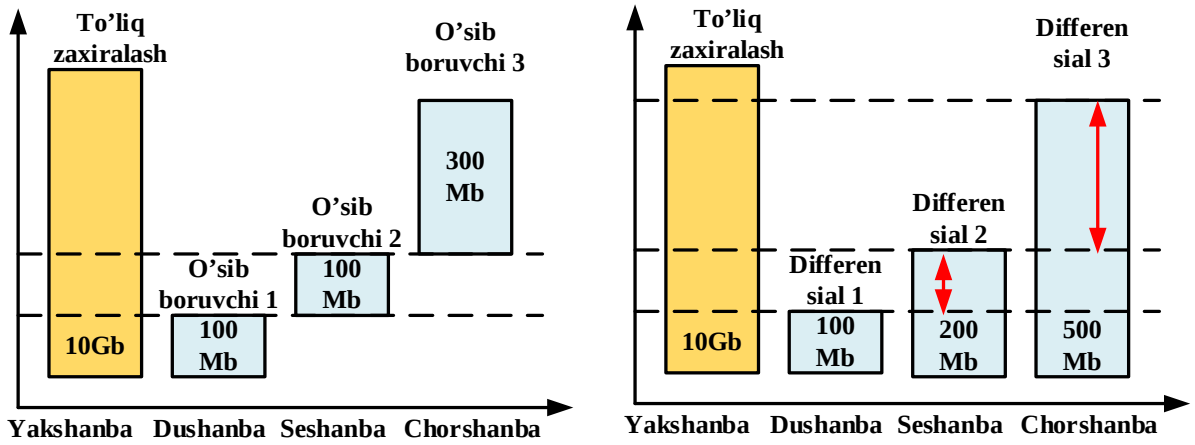
Masalan, faraz qilinsin zaxira nusxalash jadvaliga ko’ra to’liq zaxiralash yakshanba kuniga, ortib boruvchi zaxiralash esa seshanbadan shanbagacha amalga oshirilishi belgilangan bo’lsin. Yakshanba kuni to’liq zaxiralash amalga oshirilganidan so’ng, dushanba kunidagi o’zgarishlar seshanba kuni o’sib boruvchi usul asosida amalga oshiriladi. Ushbu jarayoni shanbagacha davom ettiriladi (73.a - rasm).

Ushbu zaxiralash usuli qolgan usullarga qaraganda kam saqlash hajmini talab etadi va amalga oshirilish jarayoni tez. Biroq, qolgan usullarga qaraganda qayta tiklash sekin amalga oshiriladi.

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 olaylik. To’liq zaxiralash yakshanba kuni va differensial nusxalash shanbagacha ishlashi jadvalda keltirilgan bo’lsin. Yakshanba kuni to’liq zaxira nusxalash amalga oshirilganidan so’ng, dushanba kuni differensial zaxiralash paydo bo’ladi va kun o’tishi bilan amalga oshiriladi. Bu holat o’sib boruvchi zaxirilashga o’xshab ketadi. Biroq, seshanbada, zaxira nusxalar yakshanba va dushanbadagi o’zgarishlar uchun amalga oshiriladi. Shundan so’ng, chorshanbada zaxiralash yakshanba, dushanba va seshanba kunlari uchun amalga oshiriladi (74.b - rasm).

Zaxiralash jarayoni to’liq zaxiralashga qaraganda tez amalga oshiriladi. Qayta tiklash o’sib boruvchi zaxiralashga qaraganda tez amalga oshiriladi. Ma’lumotni saqlash uchun to’liq zaxiralashga qaraganda kam joy talab etadi. Biroq, o’sib boruvchi zaxiralashga qaraganda sekin amalga oshiriladi va ma’lumotni tiklash to’liq zaxirilashga qaraganda sekin amalga oshiriladi.



a) O'sib boruvchi zaxiralash b) Differensial zaxiralash

74-rasm. Zaxiralash turlari

Foydalanuvchi mashinasida ma'lumotlarni zaxiralash vositalari. AOMEI Backupper dasturiy vositasi ma'lumotlarni zaxiralash va tiklash haqida mutaxassis bo'lmagan foydalanuvchilarga mo'ljallangan bo'lib, ma'lumotlarni zaxiralash va qayta tiklashni amalga oshiradi. Ushbu dasturiy vositaning asosiy vazifalari quyidagilar:

- davomiy tarzda barcha kritik ma'lumotlarni zaxiralash;
- o'sib boruvchi va avtomatik zaxiralash orqali zaxiralash uchun talab qilingan vaqtni kamaytirish;
- butun diskni yoki uning qismini zaxiralash;
- Windows OT va ilovalarni xavfsiz saqlash uchun tizim zaxira nusxasini yaratish.

AOMEI dasturi fayllarni, kataloglarni, qattiq disk drayverlarini, bo'limlarini va ilovalarni zaxiralashda foydalaniladi. Agar ma'lumotni yo'qolishi kuzatilsa, u fayllarni qayta tiklaydi. Bunda, u diskdan nusxa olish va klonlash orqali ma'lumotni to'liq tiklaydi. Ushbu dasturiy vositasi quyidagi zaxira nusxalash usullarini amalga oshiradi:

- fayl, tizim va disk;
- qism/ bo'lim;
- avtomatik/ jadval bo'yicha;
- o'sib boruvchi/ jadval bo'yicha.

Genie Backup Manager Home vositasi. Ushbu dasturiy vosita zaxiralash muolajasini to’liq nazoratini ta’minlaydi va uning asosiy xususiyatlari quyidagilardan iborat:

- to’liq zaxiralovchi dasturiy ta’minot;
- nusxalashda xavfsizlikni ta’minlanishi;
- zarar yetkan vaqtda butun tizimni qayta tiklash;
- qo’shimcha dasturiy vositasiz zaxira nusxalardan foydalanish;
- zaxira nusxani ixtiyoriy manzilda saqlash.

Norton Ghost vositasi. Norton Ghost 15 dasturiy vositasi butun tizim yoki maxsus fayl va katalogni masofadagi FTP serverga saqlash uchun mo’ljallangan bo’lib, tiklash nuqtasini saqlash orqali amalga oshiriladi.

Bulardan tashqari, Windows OTda Active Backup Expert, NTI Backup Now, PowerBackup, Backup4all, Handy Backup, SyncBackPro kabi dasturiy vositalardan keng foydalanib kelinmoqda.

5.3. Ma’lumotlarni qayta tiklash usullari

Ma’lumotni yo’qolishi ixtiyoriy tashkilot uchun jiddiy muammo hisoblanib, buni oldini olish uchun ma’lumotni qayta tiklash usullaridan foydalanish talab etiladi. Ushbu jarayon ma’lumot qanday yo’qolgani, ma’lumotni qayta tiklash dasturiy vositasi va ma’lumotni tiklash manziliga bog’liq bo’ladi.

Ma’lumotni saqlash vositalari, USB xotira, qattiq disk, DVD va boshqa saqlovchilardan ma’lumotlarni qayta tiklash mumkin. Qayta tiklash jarayonining muvaffaqqiyatli amalga oshirilishi saqlovchiga ma’lumotni qayta yozilmaganligi va foydalanuvchining malakasiga bog’liq bo’ladi. Ma’lumotni qayta tiklash jarayonida to’g’ri bilim va to’g’ri tanlangan vosita muhim hisoblanadi.

Ma’lumotni qayta tiklash har doim ham muvaffaqqiyatli bo’lmasligi mumkin. Agar saqlash tizimiga xatolik mavjud bo’lsa yoki ko’p zarar yetgan bo’lsa, ma’lumotni tiklashning imkoni bo’lmasligi mumkin. Ma’lumotni qayta tiklanish ehtimoli uni o’chirilganlik sababiga bog’liq bo’ladi. Ma’lumotni yo’qolishiga sabab bo’luvchi holatlar quyidagilar:

Faylni o’chirish: agar fayl o’chirilsa, ushbu soha qaytadan yozilgunga qadar saqlagichda mavjud bo’ladi. Bu holat OT disk sohasidan qayta foydalanganda yuzaga keladi. Ma’lumot saqlangan sohadagi kichik xotirada ma’lumotni yozilishi butun ma’lumotni tiklanmasligiga sababchi bo’lishi mumkin. Windows OTda NTFS fayl tizimida ma’lumotni o’chirish algoritmi mavjud va ma’lumotni tiklash ham ushbu algoritm asosida amalga oshiriladi.

Faylni zararlanishi: agar operasion tizim zararlansa, ma’lumotni diskning razdellar jadvali yordamida tiklash mumkin. Agar diskning razdellar jadvali ham zararlangan bo’lsa, u holda qayta tiklash vositalaridan foydalanish talab etiladi.

Qattiq diskni fizik zararlanishi: qattiq diskka fizik ta’sir bo’lishi unga faylni zararlanishiga qaraganda katta yo’qotishni olib kelishi mumkin. Bu esa ma’lumotni qayta tiklashning maxsus sathidan foydalanishni talab etadi. Zararlangan fizik diskdan ma’lumotni tiklash vaqtida, tiklash jarayonining muhiti turli ifloslanishlardan xoli bo’lishi zarur. Ya’ni, bu jarayon toza xonada amalga oshirili shart. Chang bo’lgan sohalardan ma’lumotni qayta tiklanishi qiyin bo’ladi. Ushbu holatda ma’lumotni tiklash juda ham qiyin bo’lib, zararlanish turiga bog’liq bo’ladi.

Ma’lumotlarni qayta tiklashda quyidagilarni esda saqlash zarur:

- ma’lumot yo’q bo’lgan qattiq diskda qayta tiklangan ma’lumotni yozmaslik;
- turli zaxira nusxalarni amalga oshirish kerak va ularni turli manzillarda saqlash zarur;
- ma’lumotni qayta tiklash har doim ham 100% samara bermaydi;
- tashqi qurilmani tizimga ulashga yehtiyot bo’lish zarur, bu holda disk zararlangan bo’lsa, tizim yoki fayllarni zararlanishiga olib kelishi mumkin.

Windows OTda ma’lumotni qayta tiklash vositalari. Amalda turli saqlagichlardan yo’qolgan ma’lumotlarni tiklashda qator dasturiy vositalardan foydalaniladi. Quyida ulardan ayrimlarining xususiyatlari keltirilgan.

Recovery My Files. Ushbu dasturiy vosita Korzinkadan, qattiq diskdan o’chirilgan fayllarni va zararli dasturiy vositalar yordamida o’chirilgan fayl va ma’lumotlarni tiklash imkoniyatiga ega. Bunda, ma’lumotni tiklanishi fayl

kontentiga bog’liq bo’ladi. Ushbu dasturiy vosita quyidagi ikki mexanizmdan foydalanadi:

Yo’qolgan fayl: ushbu mexanizm o’chirilgan fayllarni qidiradi va bunda notanish turlar inobatga olinmaydi.

Yo’qolgan diskni tiklash: ushbu mexanizm eski disklarda saqlangan ma’lumotlarni tiklashda yordam beradi.

EASEUS Data Recovery Wizard. Ushbu ma’lumotni qayta tiklash dasturiy vositasi iOS, Android, USB xotiralar va qattiq disklardan kutilmagan xatolik yuz bergan holatlarda yo’qolgan ma’lumotni tiklash uchun foydalaniladi.

Ushbu dasturiy vosita quyidagi xususiyatlarga ega:

- o’chirilgan, formatlangan va foydalanishga yaroqsiz ma’lumotni qaytarish;
- barcha o’chirilgan fayllar, rasmlar, hujjatlar, videolar va boshqa fayllarni qaytarish;
- shaxsiy kompyuter, noutbuk, qattiy disq va boshqa qurilmalardan ma’lumotni tiklash;
- o’chirilgan, yo’qotilgan va yashiringan razdellardan ma’lumotni tiklash;
- mijozlarga texnik yordamchi vazifasini amalga oshiradi.

Bulardan tashqari, Windows OTda Advanced Disk Recovery, Handy Recovery, R-Studio, Data Recovery Pro, Recuva, Total Recall, Pandora Recovery kabi dasturiy vositalardan foydalanib ma’lumotlarni qayta tiklash mumkin.

5.4. Hodisalarni qaydlash

Xatolik yuz berganda, tizim ma’muri yoki qo’llab-quvvatlash vakili xatoning sababini aniqlashi, yo’qolgan ma’lumotlarni qayta tiklashga urinishi va xatoning takrorlanishiga yo’l qo’ymasligi kerak. Ilovalar, operasion tizim va boshqa tizim xizmatlari muhim voqyealarni, masalan, xotira kamligi yoki diskka kirishga haddan tashqari ko’p urinishlarni qayd yetishini yozib borish muhim hisoblanadi. Keyinchalik tizim ma’muri xato sababini aniqlash va u sodir bo’lgan kontekstni aniqlash uchun ushbu hodisalar jurnalidan (log fayl deb ataladi) foydalanishi mumkin. Log faylni vaqti-vaqti bilan ko’rib chiqib, tizim ma’muri shikastlanishdan oldin muammolarni (masalan, qattiq disk kabi) aniqlashi mumkin.

Tegishli log yozuvisiz, buzg’unchining faoliyati e’tibordan chetda qolishi mumkin va hujum buzilishlarga olib kelgan yoki qilinmaganligini isbotlash mumkin yemas.

Doimiy jurnallarda yozib borish faol tekshirish va hujumdan keyingi tahlil uchun xavfsizlik insidentlarining mohiyatini tushunishda juda muhim. Shuningdek, hodisalarni qayd qilish operasion tendensiyalarni aniqlash va tashkilotning ichki tekshiruvlarini, shu jumladan, audit va sud-tibbiy tahlilni qo’llab-quvvatlash uchun foydalidir.

Hodisalarni qayd etish quyidagilarni o’z ichiga olishi shart:

- operasion tizim (OT) hodisalari:
    - tizimni ishga tushirish va o’chirish;
    - xizmatni boshlash va tugatish;
    - tarmoq ulanishidagi o’zgarishlar yoki muvaffaqiyatsizliklar;
    - tizim xavfsizligini sozlash va boshqarish vositalarini o’zgartirish yoki 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:
    - muvaffaqiyatli va muvaffaqiyatsiz dasturni autentifikasiya qilishga urinishlar;
    - hisob qaydnomasidagi o’zgartirishlar (masalan, qayd yozuvini yaratish va yo’q qilish, hisob imtiyozlarini tayinlash);
    - dastur imtiyozlaridan foydalanish.

- ilova operasiyalari:
    - dasturni ishga tushirish va o’chirish;
    - dastur xatolari;
    - dastur konfigurasiyasining asosiy o’zgarishlari;
    - dastur operasiyalari, masalan:
        - har bir elektron pochta uchun yuboruvchini, qabul qiluvchilarni, mavzular nomini va ilova nomlarini qayd etadigan elektron pochta serverlari;
        - talab qilingan har bir URL manzilini va server tomonidan berilgan javob turini yozadigan veb-serverlar;
        - har bir foydalanuvchi foydalanishi mumkin bo’lgan moliyaviy yozuvlarni qayd qiluvchi biznes-ilovalar.

Har bir voqyea uchun qayd qilingan tavsilotlar juda farq qilishi mumkin. Ammo, har bir voqyeani quyidagi parametrlar yordamida yozish tavsiya qilinadi:

- vaqt belgisi;
- voqyea, holat va / yoki xatolik kodlari;
- servic / buyruq / ilova nomi;
- foydalanuvchi yoki tizim bilan bog’liq voqyea;
- amaldagi qurilma (masalan, IP va manba manzili, terminal sessiyasi identifikatori, veb brauzer va hk.).

Audit jurnallarida barcha harakatlar qayd etilgani bois, audit jurnalini tahrirlash g’arazli niyatini amalga oshirganlar o’z faoliyatini yashirishda ham asosiy maqsad hisoblanadi. Shuning uchun, audit jurnalidan foydalanishlarni nazoratlash muhim vazifa hisoblanadi.

Windows OTda hodisalar turlari. Windows OTda besh turdagi hodisalar ro’yxatga olinishi mumkin. Bularning barchasida aniq belgilangan umumiy ma’lumotlar mavjud bo’lib, hodisalarga tegishli ma’lumotlarni o’z ichiga oladi.

Ilova biror bir hodisa haqida xabar berganida hodisa turini ko’rsatib, bunda har bir hodisa bitta turga tegishli bo’ladi. Hodisalar jurnali ro’yxat ko’rinishida har bir tur uchun farqli ko’rsatilib, quyidagi ushbu hodisa turlari keltirilgan (10-jadval).

10-jadval

Windows OT hodisalar turlari

Hodisa	**Tavsifi**
Xatolik	Ma’lumotni yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqyea. Masalan, biror xizmat ishga tushirish 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. Agar ilova biror bir hodisani funksional yoki ma’lumot yo’qotmasdan tiklay olsa, ogohlantirish hodisasi deb tasniflash mumkin.
Axborot	Ilova, drayver yoki xizmatning muvaffaqiyatli ishlashini tasvirlaydigan voqyea. Masalan, tarmoq drayveri muvaffaqiyatli yuklanganda, axborot hodisalarini qayd etadi.
Muvaffaqiyatli audit	Muvaffaqiyatli tekshirilgan xavfsizlikka kirish urinishlarini yozib oladigan hodisa. Masalan, foydalanuvchining tizimga muvaffaqiyatli urinishi muvaffaqiyatli audit hodisasi sifatida qayd etiladi.
Muvaffaqiyatsiz audit	Tekshirilgan xavfsizlikka kirish urinishining muvaffaqiyatsiz tugaganligini qayd etadigan hodisa. Masalan, agar foydalanuvchi tarmoq drayveriga kirishga harakat qilsa va muvaffaqiyatsiz bo’lsa, urinish muvaffaqiyatsiz audit hodisasi sifatida qayd etiladi.

Dastlab foydalanuvchilarning tanlangan harakatlari xavfsizlik hodisalarini auditlash orqali aniqlanib, shundan so’ng kompyuterning xavfsizlik jurnaliga joylashtirish orqali kuzatilishi mumkin.

Hodisalarni qaydlashdagi eslatmalar. Hodisalar jurnallari tizim nomidan muhim voqyealar va tizimda ishlaydigan dasturlarning yozuvlarini saqlaydi. Jurnalni ro'yxatga olish funksiyalari umumiy maqsadga ega bo'lganligi sababli, faqat kirish uchun zarur ma'lumotni qaydlash zarur bo'ladi. Umuman olganda, faqat apparat yoki dasturiy ta'minot muammolarini tashxislashda foydali bo'lgan ma'lumotlarni qaydlash maqsadga muvofiq bo'ladi. Boshqa so'z bilan aytganda, hodisalarni ro'yxatga olish kuzatuv vositasi sifatida foydalanish uchun mo'ljallanmagan.

Qayd etish uchun hodisalarni tanlash. Quyida hodisalarni qayd yetish foydali bo'lishi mumkin bo'lgan holatlarga misollar keltirilgan:

Resurs muammolari. Xotirani ajratishda xatolik yuz bergan taqdirda ogohlantirish hodisasini qayd etish, kam xotirali vaziyatning sababini ko'rsatishga yordam beradi.

Uskuna bilan bog'liq muammolar. Agar qurilma drayveri disk boshqaruvchisining ishdan chiqishi, parallel portdagi quvvatning uzilishi yoki tarmoq, serial kartadagi ma'lumotlar xatosiga duch kelinsa, qurilma drayveri tizim ma'muriga apparatdagi muammolarni aniqlashga yordam berish uchun mazkur hodisalar haqida ma'lumotni qayd etishi mumkin.

Yomon sektorlar. Agar disk drayveri yomon sektorga duch kelsa, operasiyani qayta ko'rib chiqqandan so'ng, sektor sifamati yomonlashsada undan o'qishi yoki unga yozishi mumkin. Agar disk drayveri o'z ishini davom ettirsa, u *ogohlantirish* hodisasini yozishi kerak; aks holda, *xatolik* hodisasini qayd qilishi zarur bo'ladi. Agar fayl tizimining drayveri juda ko'p miqdordagi yomon sektorlarni aniqlasa va ularni tuzatsa, jurnallarni ro'yxatga olish *ogohlantirish* hodisalari ma'murga diskning ishdan chiqishini aniqlashga yordam beradi.

Axborot hodisalari. Server dasturi (masalan, ma'lumotlar bazasi serveri), foydalanuvchini ro'yxatdan o'tkazadi, ma'lumotlar bazasini ochadi yoki fayl uzatishni boshlaydi. Server, shuningdek, xatolar (faylga kirish imkoni yo'q, xost jarayoni o'chirilgan va hokazo), ma'lumotlar bazasi buzilganligi yoki fayl uzatish

muvaffaqiyatli amalga oshirilganligi kabi boshqa hodisalarni ham qayd qilishi mumkin.

Hodisalarni qaydlashdagi amallar. Hodisalarni qaydlash jurnali ustida quyidagi amallar bajaralishi mumkin:

- zaxira nusxalash (BackupEventLog funksiyasi yordamida);
- tozalash (ClearEventLog funksiyasi yordamida);
- monitoring qilish (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 operasion tizimlarida turli hodisalarni qaydlash jurnalida turli akkauntlar uchun berilgan imtiyozlar quyida keltirilgan (11-jadval).

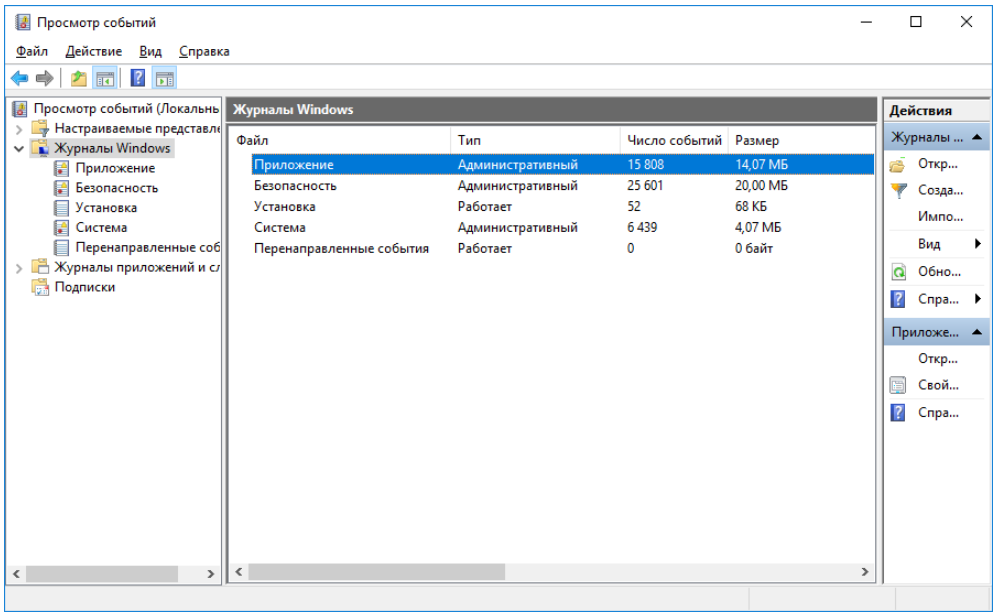
11-jadval

Windows XP/2000 operasion tizimida hodisa jurnaliga bo’lgan imtiyozlar

Log	Qayd yozuvi	O’qish	Yozish	Tozalash
Ilovaga tegishli	Administratorlar (tizim)	+	+	+
	Administratorlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-
Tizimga tegishli	Administratorlar (tizim)	+	+	+
	Administratorlar (domen)	+	-	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	-	-
Tanlovga ko’ra yaratilgan log fayl	Administratorlar (tizim)	+	+	+
	Administratorlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-

Windows OT da hodisalar qaydlash fayllarini (log faylni) ko’rish uchun quyidagi ketma-ketlik amalga oshiriladi:

1. Kompyuterdan Win+R tugmalar kombinasiyasi bosiladi.
2. Hosil bo’lgan oynadagi maydonda *eventvwr* kiritiladi va Enter tugmasi bosiladi.
3. Hosil bo’lgan hodisalar ko’rish oynasidan *Windows Logs* bandi tanlanadi (74-rasm).



74-rasm. Windows OTning hodisalar jurnali

Nazorat savollari

1. Foydalanuvchanlik tushunchasiga ta’rif bering va uning tizim uchun muhimligini tushuntiring?
2. Zaxira nusxalash nima va uning turlarini sanang?
3. Ma’lumotlarni yo’qolishiga olib keluvchi asosiy sabablarni ayting?
4. Zaxira nusxalashda bajariluvchi vazifalar ketma-ketligini ayting?
5. Zaxira nusxalarni saqlovchi vositalar va ularning xususiyatlarini ayting?
6. RAID texnologiyasi va uning asosiy xususiyatlarini ayting?
7. RAID 0, RAID 1, RAID 3, RAID 5, RAID 10 va RAID 50 sathlari haqida ma’lumot bering.
8. Zaxiralash turlari va ularning afzallik/ kamchiliklarini ayting?

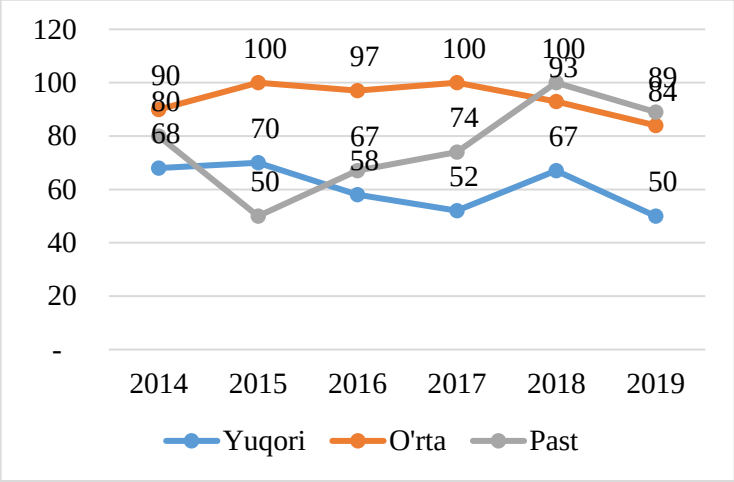
6 BOB. DASTURIY VOSITALAR XAVFSIZLIGI

6.1. Dasturiy vositalardagi xavfsizlik muammolari

Dasturiy vositalar xavfsizligi hozirgi kunda kelib, axborot xavfsizligining kriptografiya, ruxsatlarni nazoratlash va xavfsizlik protokollari kabi muhim sohalaridan hisoblanadi. Bunga asosiy sabab, axborotning vertual xavfsizligi dasturi vositalar orqali amalga oshirilishi bilan belgilanib, agar dasturiy vosita tahdidga uchragan taqdirda, xavfsizlik mexanizmi ham barbod bo'ladi.

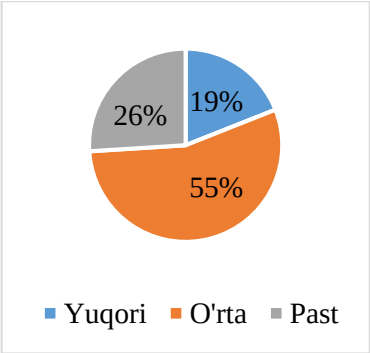
Barcha dasturiy vositalarda zaifliklar mavjud bo'lib, ularning muhimlik darajalari turlicha. Masalan, qiymati 165 mil. $ ni tashkil etgan NASA Mars Lander, Mars sayyorasi yuzasiga qo'nish vaqtida halokatga uchragan. Bunga sabab esa, oddiy ingliz va metr uzunlik o'lchovlari orasidagi farq bo'lgan. Bundan tashqari, Denver xalqaro ayeroportidagi yuklarni boshqarish tizimida foydalanilgan dasturiy vositadagi kamchilik natijasida, 11 oy davomida kuniga 1 mil. $ dan zarar ko'rilgan.

Bundan tashqari, so'ngi yillarda ushbu zaiflik muammolarining soni va jiddiylik darajalari ortib bormoqda. Xususan, 75-rasmda Positive Technologies tashkiloti tomonidan veb saytlardagi turli darajadagi zaifliklarni yillar kesimida ortib borishi keltirilgan.



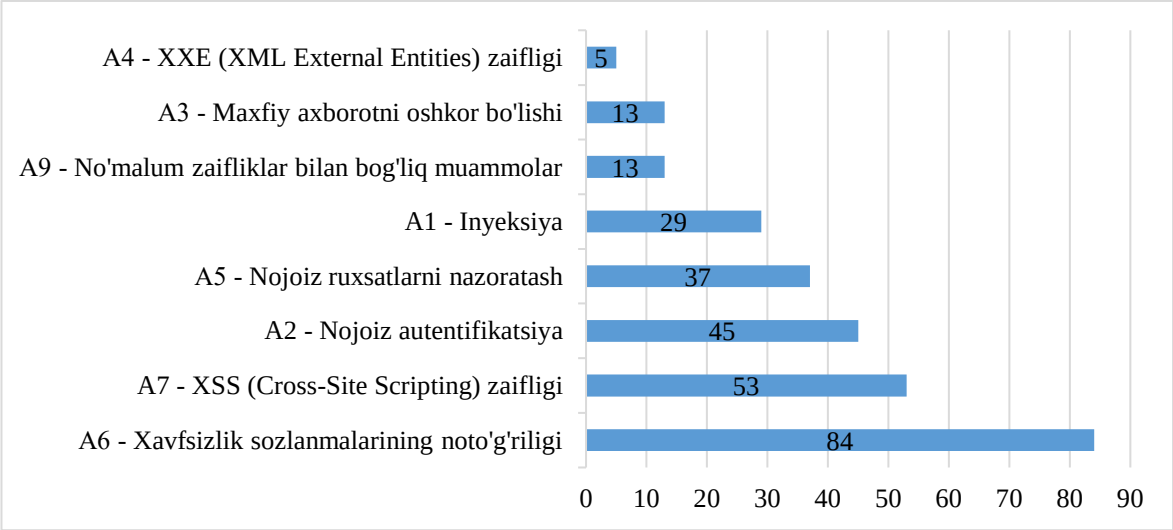
75 – rasm. Turli darajadagi zaifliklarga ega bo'lgan Veb-saytlar soni [3]

2019 yilda veb saytlarda mavjud muammolarning jiddiyligi bo'yicha taqsimoti 76-rasmda keltirilgan.



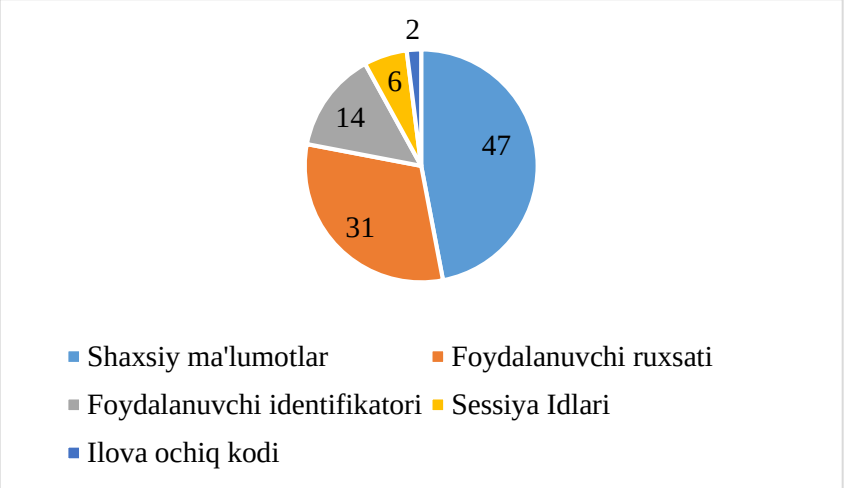
76-rasm. Veb sayt muammolarining jiddiylik bo’yicha taqsimoti

O’tgan yilda veb saytlarda keng tarqalgan zaifliklar va ularning ulishi esa OWASP (Open Web Application Security Project) tomonidan berilgan ma’lumotga ko’ra esa quyidagicha bo’lgan (77-rasm).



77-rasm. OWASP tashkiloti tomonidan 2019 yilda uchragan zaifliklar va ularning ulushi

Yuqorida keltirilgan zaifliklar natijasida hujumchilar tomonidan quyidagi turli ma’lumotlarni qo’lga kiritish maqsad qilingan (78-rasm).



78-rasm. Zaifliklar natijasida qo'lga kiritish maqsad qilingan ma'lumotlar

Dasturiy mahsulotlarda xavfsizlik muammolari. 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. Masalan, C# va Java dasturlash tillarida ko'plab muammolar avtomatik ravishda kompilyasiya jarayonida aniqlangani bois 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 asosan, dasturchi tomonidan yo'l qo'yilgan xatolik natijasida kelib chiqqan dasturlardagi muammolar misol bo'lsa, ikkinchi turga buzg'unchilik maqsadida yozilgan maxsus dasturiy mahsulotlar (masalan, viruslar) misol bo'ladi.

Dasturiy vositalarda xavfsizlik muammolarini mavjudligi bir nechta omillar bilan belgilanadi:

– dasturiy vositalarning ko'plab dasturchilar tomonidan yozilishi (komplekslilik);
– dasturiy mahsulotlar yaratilishida inson ishtiroki;
– dasturchining malakasi yuqori emasligi;
– dasturlash tillarining xavfsiz emasligi.

Dasturiy vositalar bir nechta million qator kodlardan iborat bo'lib, bu o'z navdatida xavfsizlik muammosini ortishiga sababchi bo'ladi (12-jadval). Boshqa

so’z bilan aytganda, katta dasturiy vositalar ko’plab dasturchilar tomonidan yoziladi va yakunda biriktiladi. Agar dasturchilar orasidan bittasining bilim darajasi yetarli bo’lmasligi, yakunda butun dasturiy vositani xavfsizligini yo’qqa chiqarishi mumkin.

12 - jadval

Tizim	**Dasturdagi kodlar uzunligi**
Netscape	17 mil.
Space Shuttle	10 mil.
Linuxkernel 2.6.0	5 mil.
Windows XP	40 mil.
Mac OS X 10.4	86 mil.
Boeing 777	7 mil.

Tahlillar natijasi har 10 000 qator kodda 5 ta bag mavjudligini ko’rsatadi. Boshqacha qilib aytilganda, o’rtacha 3kbayt .exe faylda 50 taga yaqin bag bo’ladi.

Dasturiy vositalar injineriyasida dasturni kafolatli o’z maqsadini bajarishiga harakat qilinsa, *xavfsiz* dasturiy vositalar injineriyasida esa o’z maqsadini bajarishi talab etiladi. Biroq, butunlay xavfsiz dasturiy vositani bo’lishi amalda mumkin emas.

Dasturiy mahsulotlarda xavfsizlik muammolari. Dasturiy mahsulotlarda quyidagi zaiflikka tegishli tushunchalar mavjud.

Nuqson. Dasturni amalga oshirishdagi va loyihalashdagi zaifliklarning barchasi nuqson hisoblanib, uning dasturiy vositalardagi mavjudligi yillar davomida bilinmasligi mumkin.

Bag. Bag dasturiy ta’minotni amalga oshirish bosqichiga tegishli bo’lgan muammo bo’lib, dasturiy vositalardagi baglarni oson aniqlash mumkin. Masalan, bagga dasturlashdagi *buferni to’lib toshish* (Buffer overflow) holatini misol keltirish mumkin.

Xotirani to’lib toshishi. Amalda ko’p uchraydigan dasturlash tillaridagi kamchiliklar odatda, taqiqlangan formatdagi yoki hajmdagi ma’lumotlar kiritilishi natijasida kelib chiqadi. Bu turdagi tahdidlar ichida keng tarqalgani bu – xotiraning to’lib toshish tahdidi hisoblanadi.

Masalan, veb saytda foydalanuvchidan ma’lumotlar kiritilishi talab etilsa (ismi, familiyasi, yili va hak.), foydalanuvchi tomonidan kiritilgan “ism” maydonidagi ma’lumot serverdagi *N* ta belgi hajmiga ega sohaga yoziladi. Agar kiritilgan ma’lumot uzunligi *N* dan katta bo’lgan holda, xotiraning to’lib toshishi hodisasi yuzaga keladi.

Agar buzg’unchi tomonidan “kerakli” ma’lumot kiritilsa, bu o’z navbatida kompyuterni buzulishiga olib keladi.

Quyida S dasturlash tilida yozilgan kod keltirilgan bo’lib, agar bu kod kompilyasiya qilinsa, xotiraning to’lib toshishi hodisasi kelib chiqadi.

```
int main()
   {
   int buffer [10];
   buffer [20] =37;
   }
```

Bu yerdi mavjud muammo bu - 10 bayt o’lchamli xotiraga 20 baytli ma’lumot yozilishida. Bu esa xotiraning ruxsat etilmagan manziliga ham murojaatni keltirib chiqaradi.

6.2. Dasturiy vosita xavfsizligining fundamental prinsiplari

Dasturiy ta’minotni ishlab chiqqanda va foydalanganda qator prinsiplarga amal qilish talab qilinadi. Quyida OWASP tashkiloti tomonidan taqdim qilingan prinsiplar keltirilgan:

Hujumga uchrashi mumkin soha maydonini minimallashtirish. Dasturiy ta’minotga qo’shilgan har bir xususiyat umumiy holda dasturga ma’lum miqdordagi xavf darajasini qo’shadi. Dasturni xavfsiz amalga oshirishning maqsadi bu – hujum bo’lishi mumkin bo’lgan sohani kamaytirish orqali umumiy dasturdagi xavfni kamaytirishdir. Masalan, veb saytlarda onlayn yordamni amalga oshirish uchun qidirish funksiyasi mavjud. Biroq, ushbu imkoniyat veb saytga SQL – ineksiya hujumi bo’lishi ehtimolini keltirib chiqarishi mumkin. Agar qidiruv imkoniyati autentifikasiyadan o’tgan foydalanuvchilar uchun bo’lsa, u holda hujum bo’lishi ehtimoli kamayadi. Agar qidiruv ma’lumotlari markazlashgan holatda tekshirilsa, u holda ushbu imkoniyat yanada kamayadi.

Xavfsiz standart sozlanmalarni o’rnatish. Amalda aksariyat dasturiy ta’minotlarda va operasion tizimlarda ko’plab xavfsizlik sozlanmalari standart tartibda o’rnatilgan bo’ladi. Biroq, bu holat foydalanuvchilar tomonidan yaxshi qabul qilinmaydi va shuning uchun, aksariyat hollarda ushbu sozlanmalarni o’chirib qo’yish amalga oshiriladi. Masalan, operasion 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 (ingl. Principle of least privilege) bu – hisoblash muhitidagi u yoki bu abstraksiya darajasida resurslarga murojaatni tashkil qilish prinsipi bo’lib, bunga ko’ra har bir modul o’z vazifasini to’laqonli bajarishi uchun zarur bo’lgan resurs yoki axborotdan minimal darajada foydalanishni talab etadi.

Bu prinsip foydalanuvchi yoki dasturga faqat o’z vazifasi uchun zarur bo’lgan imtiyozlarga ega bo’lishi kerakligini anglatadi. Masalan, turli vaqt o’tkazish uchun ishlab chiqilgan mobil o’yin dasturlar SMS xabarni o’qish yoki qo’ng’iroq qiluvchilar ro’yxatini bilish imkoniyatiga ega bo’lishi shart emas. Masalan, dasturlar tillarida (Java dasturlash tilida keltirilgan) obyektlardan foydanishni cheklash uchun turli kalit so’zlardan foydalaniladi.

13-jadval

Java dasturlash tilida foydalanuvchilar imtiyozlari

	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 ko’ra, 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, kirish qiymatini tekshirishni, markazlashgan auditni boshqarishni va foydaluvchilarni barcha sahifalarga kirishlarini talab qilishlari mumkin.

Agar noto’g’ri ishlab chiqilgan administrator interfeysi, tarmoqqa kirishni to’g’ri bajarsa, foydalanuvchilarni avtorizasiyasini tekshirsa va barcha holatlarni qayd qilsa, u anonim hujumga bardoshsiz bo’lishi mumkin emas.

Xavfsizlikni buzilishi. Ilovalar turli sabablarga ko’ra amalga oshirilish jarayonida buzilishlarga uchraydi. Masalan, quyida e’tiborsizlik natijasida 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 admin 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 sherigi tomonidagi dasturiy ta’minot bilan qayta ishlashi mumkin. Bu holda ularga ishonish kafolatlanmaydi. Masalan, Payme yoki shunga o’xshash ilovalar bir nechta bank kartalaridagi ma’lumotlarni taqdim qiladi. Mazkur holda,

har bir bank foydalanuvchi tomonida o’z ma’lumotlarini to’g’ri akslantirilganini tekshirishi kerak bo’ladi.

Vazifalarni ajratish. Firibgarlikni oldini olishga qaratilgan asosiy chora bu – vazifalarni ajratishdir. Masalan, tashkilotda kompyuter uni olish bo’yicha talab yuborgan odam tomonidan qabul qilinmasligi shart. Sababi, bu holda u ko’plab kompyuterlarni so’rashi va qabul qilib olganini rad qilishi mumkin. Ba’zi holatlarda, bir rol uchun oddiy foydalanuvchilarga nisbatan ishonch darajasi turlicha bo’ladi. Masalan, administratorlar 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 bu – zaif xavfsizlik bo’lib, birinchi nazoratning o’zida xatolikka uchraydi. Bu biror sirni saqlash yomon g’oya ekanligini anglatmasada, xavfsizlikning muhim jihatlari tavsilotlarni yashirin bo’lishiga asoslanmasligini bildiradi.

Masalan, dasturning xavfsizligi uni ochiq kodidan xabardor bo’linganda barbod bo’lmasligi kerak. Xavfsizlik ko’plab boshqa omillarga, masalan, parolning oqilona siyosatiga, tarmoq arxitekturasiga, auditni boshqarish vositalariga tayanishi kerak.

Bunga amaliy misol sifatida, Linux operasion tizimini keltirish mumkin. Ushbu operasion tizimning kodi ochiq hisoblansada, to’g’ri himoyalangan va shuning uchun, hozirgi kundagi mustahkam operasion tizimlardan biri hisoblanadi.

Xavfsizlikni sodda saqlang. Hujumga uchrash soha maydoni va soddalik bir-biriga bog’liq. Ba’zi dasturiy ta’minot muhundislari kodni sodda ko’rinishidan ko’ra murakkablikni afzal ko’radilar. Biroq, sodda va tushunishga oson bo’lgan 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. Quyida ular bilan tanishib chiqiladi.

Dasturiy mahsulotlarga qo’yiladigan talablar uch turga bo’linadi:

- vazifaviy (o’ziga xos xususiyatlar) talablar:
    - tizim amalga oshirishi kerak bo’lgan vazifalar.
- novazifaviy talablar:
    - tizimning xususiyatlariga qo’yilgan talablar.
- qolgan talablar:
    - vazifaviy va no vazifaviy talablardan tashqari talablar.

Vazifaviy (o’ziga xos xususiyatlar) 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.

Masalan:

- To’rtta kirish nuqtasi mavjud bo’lishi, ular tugma ko’rinishida hamda B1, B2, B3 va B4 kabi nomlanishi kerak;
- B1 tugma “Yoqish” vazifasini;
- B2 tugma “O’chirish” vazifasini;
- V3 va V3 “harakat”nuqtalari bo’lishi kerak;
- V1 bosilgandan so’ng va V4 bosilmasdan oldin tizim “yoqilgan” yozuvini chiqarishi kerak.

Novazifaviy (o’ziga xos xususiyatlar) talablar. Novazifaviy talablarga quyidagilarni keltirish mumkin:

- audit qilish imkoniyati;
- kengaytirish mumkinligi;
- foydalanishga qulayligi;
- bajarilishi;
- ixchamlik;
- ishonchlilik;
- xavfsizlik;
- testlash imkoniyati;

Masalan:

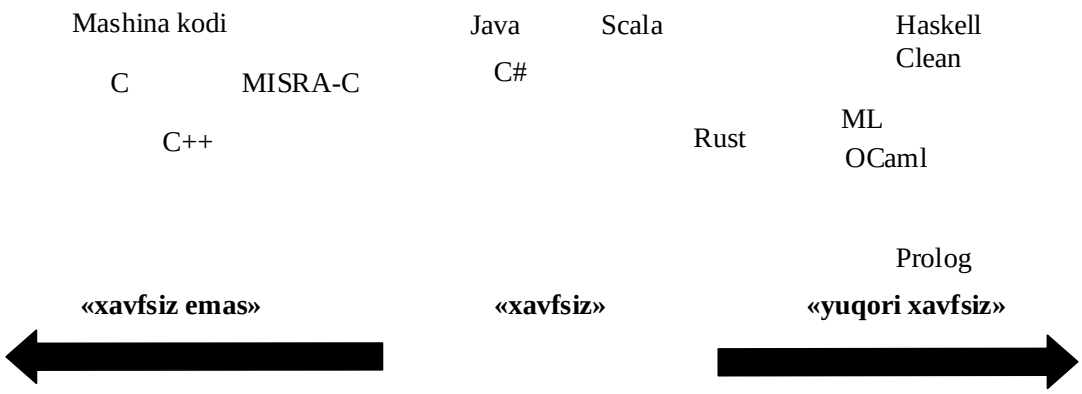
- ishlab chiqilgan dastur Windows XP, Windows Vista va MacOS X 10.4 OT uchun bo’lishi;
- foydalanuvchi autentifikasiyalash oynasidan kirganda ko’pi bilan 20 sek vaqtda olishi;

- foydalanuvchanlik;
- va hak.
- tizim tarmoqdan 10 Mbs va 100 ta foydalanuvchini bir vaqtda quvvatlay olishi.

Xavfsizlik talablari vazifaviy talablardan va boshqa talablaridan olinadi. Xususiy xavfsizlik talablariga quyidagilarni keltirish mumkin:

– 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 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 muvofaqqiyatsiz urinishdan so’ng qayd yozuvi qulflanishi shart;
  - har bir qayd yozuvi uchun 3 marta muvaffaqiyatsiz urinish amalga oshirilganda ular qulflanishi shart;
  - qayd yozuviga 5 min davomida tahdid amalga oshirilmasa u qulfdan yechilishi shart.

Dasturlash tiliga asoslangan xavfsizlik. Turli dasturlash tillari o’ziga xos imkoniyatlarga ega bo’lib, dasturlash sathida xavfsizlikni ta’minlash bunda muhim ahamiyat kasb etadi. Mavjud dasturlash tillarini xavfsiz yoki xavfsiz emas turlariga ajratish nisbiy tushuncha bo’lib, ularni quyidagicha tasvirlash mumkin (79-rasm).



79 – rasm. Dasturlash tillarining xavfsizlik darajasini sodda ko'rinishi

6.3. Zararkunanda dasturiy kodlar

Zararli dastur bu - kompyuterga, serverga, mijozga yoki kompyuter tarmog'iga zarar yetkazish maqsadida ataylab yaratilgan har qanday dastur. Zararli dasturiy vositalar foydalanuvchini ruxsatisiz hujumchi kabi g'arazli amallarni bajarishni maqsad qilib, 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, veb saytdagi kontentlarni modifikasiyalashi, o'chirishi yoki qo'shishi, foydalanuvchi kompyuteri boshqaruvini qo'lga olishi mumkin. Bundan tashqari, zararli dasturlar, hukumat tashkilotlardan va korporativ tashkilotlardan katta hajmdagi maxfiy axborotni olish uchun ham foydalanilishi mumkin.

Zararli dasturlar turlari. Zararli dasturlarning hozirda ko'plab ko'rinishlari mavjud bo'lib, ular haqida 4.1.2 – bo'limda ma'lumotlar keltirib o'tilgan. Quyida esa ularning ayrimlari haqida batafsil ma'lumotlar keltiriladi.

Mantiqiy bomba

O'zidan ko'payish: yo'q.

Sonini oshib borishi: nol.

Yuqumliligi: mumkin.

Mantiqiy bomba ikki qismdan iborat zararli kod hisoblanadi:

1. Foydali yuklama qismi bajarilish uchun harakat qism hisoblanadi. Foydali yuklama qismi istalgan ko’rinishda bo’ladi, biroq, umumiy holda zarar keltiruvchi ta’sirga ega bo’ladi.

2. Trigger, mantiqiy shart bo’lib, foydali yuklama qismini bajarilishini nazoratlaydi va baholaydi. Triggerning aniq sharti tasavvur bilan chegaralangan bo’ladi va sana, foydalanuvchining tizimga kirishi yoki operasion tizim versiyasi kabi mahalliy shartlarga asoslanadi. Shu tarzda triggerlar masofadan to’rib o’rnatiluvchi ko’rinishda yoki bo’lmasa qandaydir holatni mavjud emasligiga ko’ra loyihalanishi mumkin.

Mantiqiy bombalar mavjud kodning ichiga kiritilishi yoki bo’lmasa avtonom tarzda bo’lishi mumkin. Oddiy zararlovchi (yuqumli) na’muna quyida ko’rsatilgan bo’lib, trigger sifatida aniq sana ishlatilganda kompyuterni buzilishiga olib keladi:

```
legitimate code
if date is Friday the 13th:
     crash_computer( )
legitimate code
```

Bunga ko’ra, agar joriy kun 13-juma kuni bo’lsa, mantiqiy shart bajiriladi va kompyuterga biror zarar etkazilishi mumkin.

Troya oti

O’zidan ko’payish: yo’q.

Sonini oshib borishi: nol.

Yuqumliligi: Ha.

Ushbu turdagi zarar keltiruvchi dasturlar Greklar va Troyaliklar o’rtasidagi urush davrida ishlatilgan nayrangga asoslangan bo’lib, axborot kommunikasiya texnologiyalarida troyan oti bu - dastur bo’lib, qandaydir sodda vazifani bajarishga mo’ljallangan bo’ladi. Biroq, qo’shimcha tarzda zarar keltiruvchi vazifani xufiyona bajaradi. Klassik na’munasi sifatida tizimga kirishda parolni ushlab olish dasturini keltirish mumkin, u *«username»* i *«password»* kabi autentifikasiya so’rovlarini qayd etadi va foydalanuvchi tomonidan axborot kiritilishini kutadi. Ushbu holat yuz berganda o’zining yaratuvchisi uchun parollarni ushlab oluvchi vazifasini bajaradi

va so’ngra esa “noto’g’ri parol” degan xabarni tizimga real kirish oldidan chiqaradi. Hyech nimadan shubhalanmagan foydalanuvchi xato qilgandek bo’ladi.

Backdoors (orqa eshik)

O’zidan ko’payish: yo’q.

Sonini oshib borishi: nol.

Yuqumliligi: mavjud.

Backdoor (tuynuk) bu - oddiy xavfsizlik tekshiruvidan o’ta oladigan har qanday mexanizm bo’lib, dasturchilar ba’zida orqa eshikni (tuynuk) qonuniy asoslarga ko’ra hosil qilishadi.

Mantiqiy bombalar kabi orqa eshik (tuynuk) dasturlari ham dastur kodida yoki avtonom dasturlarda bo’lishi mumkin. Orqa eshikga (tuynuk) na’muna quyidagi kodda ko’rsatilgan bo’lib, u tizimga kirishda autentifikasiya jarayonini aylanib o’tadi.

```
username = read_username ()
password = read_password ()
if username is “133t h4ck0r”:
    return ALLOW_LOGIN
if username and password are valid:
    return ALLOW_LOGIN
else:
    return DENY_LOGIN
```

Ushbu mantiqiy kodga ko’ra, naqafat foydalanuvchining login va paroli to’g’ri bo’lsa tizimga kirishga ruxsat beriladi, balki, “`133t  h4ck0r`” ga teng bo’lgan loginni kiritish ham tizimga kirish uchun yetarli bo’ladi.

Virus

O’zidan ko’payish: ha.

Sonini oshib borishi: ijobiy.

Yuqumliligi: ha.

Kompyuter virusi bu – zararli dasturlarning bir turi bo’lib, bajarilgan vaqtida boshqa kompyuter dasturlarini o’zgartirish va o’z kodini kiritish orqali o’zini ko’paytiradi. Ushbu jarayon muvaffaqiyatli amalga oshilgan taqdirda, ta’sirlangan soha kompyuter virusi bilan “zararlangan” deb aytiladi.

Virus yaratuvchilar tizimlarni dastlabki zararlash va unda virusni tarqatish uchun ijtimoiy injineriya aldovlari va xavfsizlik zaifliklari to'g'risidagi batafsil ma'lumotlardan foydalanadi. Kompyuter viruslarining aksariyati Microsoft Windows OTda ishlovchi tizimlarda qaratilgan bo'lib, yangi xostlarni zararlashda ko'plab mexanizmlardan va ko'p hollarda antivirus vositalarini aldab o'tish uchun anti-aniqlash/ yashirin strategiyalardan foydalanadi.

Kompyuter viruslarining tasnifi. Hozirgi kunda kompyuter viruslarining yagona tizimli tasnifi mavjud emas va turli manbalarda ularni turlicha omillar asosida tasniflari keltirilgan. Xususan, kompyuter viruslarini quyidagi omillar bo'yicha tasniflash mumkin:

1. Resurslardan foydalanish usuliga ko'ra. Hozirgi kunda kompyuter viruslarini resursdan foydalanish usuliga ko'ra *virus-parazitlar* (yoki shunchaki *virus*) va *virus-chervlar* (yoki shunchaki *chervlar*) ga ajratish maqsadga muvofiq bo'ladi.

Resurslardan foydalanib ko'payishning birinchisi bu – boshqa dasturga mansub bo'lish hisoblanib, ular boshqa dasturlar ichida joriy qilinadi va ushbu dastur yuklanishi bilan aktivlashadi.

Ikkinchisi, odatda faqat hisoblash tizimi resursidan (tezkor va doimiy xotira, dasturiy bo'lmagan fayllar) foydalanib, tarmoq orqali o'z nusxalarini tarqatadi, axborot eltuvchilari, xotira buferi va begona arxivlar yordamida barchaga taqsimlanadi. Chervlar avtonom bo'lib, ular boshqa dasturlarga biriktirilmaydi.

2. Zararlaydigan obyektlar turiga ko'ra. Ushbu tasnifga ko'ra viruslarni *dasturiy*, *yuklanuvchi*, *makroviruslar* va *ko'p platformali* viruslarga ajratish mumkin.

Dasturiy viruslar boshqa dasturlarning fayllarini zararlaydi. Masalan, *Win9X.CIH* virusi Windows 95/98/ME OT dasturlari uchun parazit hisoblanadi.

Yuklanuvchi viruslar yuklangan qattiq diskdagi, disketa yoki fleshka sektorlarida joylashgan kichik programmalarni zararlaydi yoki uni almashtiradi. Bunga misol sifatida, BIOS sathida ishlovchi *Michelangelo* virusini keltirish mumkin.

Makroviruslar uchun sharoit yaratuvchi vosita sifatida ma’lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar” xizmat qiladi. Bunga misol qilib, MS Word hujjatlarini zararlovchi *Concept* virusi, Excel jadvallarini zararlovchi *Laroux* viruslarini keltirish mumkin.

Ko’p platformali viruslar bir vaqtning o’zida turli xildagi obyektlarni zararlaydi. Masalan, *OneHalf.3544* virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, *Anarchy* oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi.

3. Faollashish prinsipiga ko’ra. Viruslarni ushbu xususiyatiga ko’ra *rezident* va *norezident* turlarga ajratish tavsiya etiladi. Rezident viruslar doimo kompyuter xotirasida aktiv holatda joylashadi. Boshqa dastur yoki operasion tizim orqali jabrlanuvchiga murojaatlarini kuzatib boradi va shundan so’ng unga yuqadi. Masalan, bajariluvchi dasturlar yuklanish vaqtida, ishni tugatish vaqtida yoki ularning fayllarini ko’chirish vaqtida zararlanadi. Bularga misol qilib, *OneHalf.3544* (MS-DOS muhitida) va *Win9X.CIH* (Windows 95/98/ME muhitida) viruslarini olish mumkin.

Norezident viruslar zararlangan tashib yuruvchilarni yuklash vaqtida ishga tushadi va ularning faoliyat vaqti cheklangan bo’ladi. Masalan, *Vienna.648* virusi zararlangan dastur ishga tushgandan so’ng darhol ishga tushadi. Biroq, ushbu vaqtda diskdan ko’plab qurbonlarni topishga va ularni biriktirishga ulguradi. Shundan so’ng, boshqaruvni o’zining saqlovchisiga uzatadi va o’zi keyingi yuklanishga qadar “*uxlaydi*”.

Ko’p vazifali operasion tizimlarda “*yarim rezidentli*” viruslar mavjud bo’lib, ular xuddi norezident viruslar kabi yuklanadi. Alohida oqimli yuklangan dasturlar kabi tashkil qilib, ushbu dasturlarning butun ishlash davomida o’zini rezident kabi tutadi va o’z ishini saqlovchi-dasturi bilan birgalikda tugatadi. Masalan, *Win32.Funlove.4070* bunga misol bo’la oladi.

4. Dastur kodini tashkil qilish yondashuviga ko'ra. Mazkur taksanomik belgilar viruslarni *shifrlangan, shifrlanmagan* va *polimorf*larga ajratishga imkon beradi.

Shifrlanmagan viruslar o'zini oddiy dasturlar kabi ko'rsatadi va bunda dastur kodida hyech qanday qo'shimcha ishlanmalar mavjud bo'lmaydi. Bunday viruslarni (masalan, *Vienna.648*) dasturlarda osonlik bilan aniqlash hamda dizassamberlash va dekompilyatorlar orqali tadqiq qilish va o'chirib tashlash mumkin.

Shifrlangan viruslar kodida bir qancha o'zgarishlar mavjud bo'ladi. Shifrlangan virus hisoblash qurilmasining xotirasida dastlab deshifrlanadi va shundan so'ng zararlashni boshlaydi. Shuning uchun, mazkur viruslarni aniqlash, o'rganish va o'chirish murakkab bo'lib, bu murakkablik kamida undagi qaytarish amali – kodni deshifrlash bilan xarakterlanadi. Odatda virusni shifrlash koddagi maxsus anti-debaggerlash usulidan foydalanish orqali amalga oshiriladi. Bunday viruslar sirasiga *Sayha.Diehard* virusini kiritish mumkin.

Polimorf viruslar turli ko'rinishdagi shifrlangan viruslar bo'lib, o'zining ikkilik shaklini nusxadan-nusxaga o'zgartirib boradi. Mazkur sinfdagi viruslarga *OneHalf* oilasi viruslarini kiritish mumkin. Xususiy hollarda polimorflik *metamorfik viruslar* bo'lib, o'zining ikkilik tanasini shifrlamasdan, faqat ularni o'zgartirish orqali o'z nusxalarini yaratadi. Bunday viruslarga misol qilib, *Win32.Zmyst* virusini keltirish mumkin.

5. Virus-chervlarning tasnifi. Virus-chervlarni tasniflash ularni tarqalish yo'llariga asoslanadi. Masalan, *pochta chervlari (*masalan, *E-Worm.Win32.Aliz)* elektron pochta orqali tarqalsa, *tarmoq chervlari* (odatda ular *Internet chervlari* deb ham yuritiladi) tarmoq protokollari yordamida tarqaladi va ma'lumot paketlari ichida yashiringan holda uzatiladi (masalan, *Net-Worm.Win32.Lovesan*). *"Telefon"* yoki *"mobil"* chervlar (masalan, *Cabir*) esa turli "tarmoq"lar, masalan, simsiz axborot uzatish tarmog'i hisoblangan *BlueTooth* orqali tarqaladi. Bundan tashqari, 1980 yillarda tarqalgan *fayl chervlari* deb nomlangan turi (masalan, *Mkworm.715*) esa, o'zi mustaqil ravishda tarqalmaydi. Balki, o'zini turli tashib yuruvchilar va kataloglarda, hattoki, ZIP, RAR fayllarda nusxalaydi hamda shu tartibda tarqaladi.

6. Kompyuter viruslarining boshqa omillar bo'yicha tasnifi. Kompyuter viruslarining yuqorida keltirilgan omillardan tashqari quyidagi omillar asosida ham tasniflash mumkin:

- zararlaydigan operasion tizimi va platformasiga ko'ra (DOS, Windows, Unix, Linux, Android);
- kompyuter virusi yozilgan dasturlash tili bo'yicha (assembler, yuqori dasturlash tili, senariy tili va hak.);
- qo'shimcha zararli funksiyalariga ko'ra (bekdorlar, keyloggerlar, shpionlar, botnetlar va h.).

Albatta, yuqorida keltirilgan kompyuter viruslarining tasnifi yakuniy emas va har bir muallif tanlab olgan omillari asosida ularni tahlil qilishi mumkin. Quyida esa hisoblash tarmoqlarida ko'p zarar keltirilgan va mashhur zararli dasturiy vositalar bilan tanishib chiqiladi.

Virus tarixi. Ilk bora 1983-yil 11 noyabr kuni Janubiy Kaliforniya universiteti talabasi, amerikalik Fred Koyen 5 daqiqadan 1 soatgacha bo'lgan tezlikda ko'paya oladigan kompyuter virusi taqdimotini o'tkazgan. Shundan so'ng, oradan bir yil o'tib, Koyen kompyuter tarmoqlari bo'ylab viruslarning tarqalish xavfi va antivirus dasturlarini yaratish imkoniyatlari haqida kitob yozadi.

Birinchi yaratilgan virus (1986 yilda yaratilgan) "Brain" deb nomlangan bo'lib, u faqat kompyuter disketlari orqali tarqalgan. Birinchi antivirus dasturi esa 1988-yilda ishlab chiqilgan. Hozirgi vaqtga qadar ko'plab viruslar yaratilgan bo'lsada, ular orasidan qolganlarga qaraganda ko'proq zarar yetkazgan yoki biror xususiyati bilan ajralib turganlari mavjud. Quyida ularning ba'zilari haqida ma'lumotlar keltirilgan.

ILOVEYOU virusi. ILOVEYOU hozirgi kunga qadar yaratilgan eng zararli viruslardan biri hisoblanadi. U butun dunyo bo'ylab kompyuter tizimlariga vayronagarchiliklarni keltirib chiqardi va taxminan 10 milliard dollarga yaqin zarar keltirdi hamda dunyo kompyuterlarining 10 foizi zararlangan deb hisoblangan. Hukumatlar va yirik korporasiyalar infeksiyani oldini olish uchun pochta tizimlarini offlayn rejimga o'tkazganlar.

Virus ikki filipinlik dasturchi Reonel Ramones va Onel de Guzman tomonidan yaratilgan. Bu virus sosial injineriyadan foydalanib, odamlarni “qo’shimcha havolani” bosishga majbur qilgan, ya’ni, sevgini tan olish so’rovini tasdiqlash bo’lgan. Ilova aslida .txt fayl sifatida shakllanadigan skript bo’lgan. O’sha vaqtda Windows OT ushbu faylning haqiqiy kengaytmasini yashirganligi bois, bosish tugmachasini bosgandan so’ng, u foydalanuvchini yuborish ro’yxatidagi har bir kishiga o’zini yuboradi va fayllarni qayta yozishni davom ettiradi. Bu esa kompyuterni o’chirib bo’lmaydigan holatga tushiradi.

Code Red virusi. Code Red birinchi marta 2001 yilda paydo bo’lgan va eEye Digital Security tashkilotining ikki xodimi tomonidan aniqlangan. Bu kashfiyot paytida juftliklar Code Red Mountain Dew nomli ichimlikni ichganligi sababli, virus Code Red deb nomlangan. Tizimda bufer toshib ketish muammosidan foydalanib, Microsoft IIS veb-serveri o’rnatilgan kompyuterlar nishon qilib olingan. U to’liq xotirada ishlay olishi sababli, qattiq xotirada juda oz iz qoldirgan va hajmi 3569 baytga teng.

Infeksiyani yuqtirganida, u yuz nusxani yaratishga kirishadi. Lekin, dasturlashdagi xato tufayli u yana ko’payadi va ko’plab tizim resurslarini iste’mol qilib tugatadi. Eng esda qolarli alomat bu ta’sirlangan veb-sahifalarda “Xitoyliklar tomonidan hujum qilindi” deb qoldirgan xabar bo’lib, u o’zi ham memga aylangan. Keyinchalik vaksina chiqarilgan bo’lsada, 2 milliard dollargacha zarar keltirishga ulgurgan va shu davrda, 6 million IIS serverlari mavjud bo’lgan bo’lsa, ularning 1-2 milliontasiga ta’sir ko’rsatgan.

Melissa virusi. Florida shtatidagi yekzotik raqqos nomi bilan 1999 yilda Devid L. Smit tomonidan yaratilgan. Bu virus bilan zararlangan Word hujjati *alt.sex* nomi bilan markazlashmagan tarmoq guruhiga joylashtirilgan va pornografik saytlar uchun parollar ro’yxati deb da’vo qilingan. Bu narsa odamlarni qiziqtirdi va yuklab olib ochganda ishga tushadi.

Virus o’zini elektron pochta manzillar kitobidagi 50 ta odamga yuboradi va bu elektron pochta trafikining ko’payishiga olib keladi. Bu hukumat va korporasiyalarning elektron pochta xizmatlarini buzgan. Bundan tashqari, ba’zan

ularga Simpsons (Amerika animasiya janri) ma’lumotnomasini qo’shish orqali hujjatlarni buzgan.

Oxir oqibat Smit Word hujjatini unga topshirishganida qo’lga olindi. Fayl o’g’irlangan AOL akkauntidan foydalanib yuklangan va ularning yordami bilan huquqni muhofaza qilish idoralari uni avj olganidan bir haftadan kamroq vaqt ichida hibsga olishga muvaffaq bo’lishgan. U FQB bilan Anna Kournikova virusini yaratuvchisi sifatida tanilgan boshqa virus yaratuvchilarini ushlashda hamkorlik qilgani uchun 20 oy xizmat qilgan va belgilangan 10 yillik qamoq jazosi uchun 5000 dollar miqdorida jarima to’lagan. Ma’lum qilinishicha, virus 80 million dollar zarar yetkazgan.

Sasser virusi. Windows OT qurti birinchi marta 2004 yilda kashf yetilgan bo’lib, uni Netsky qurtini yaratgan talaba Sven Jaschan yaratgan. Ushbu chuvalchang Local Security Authority Subsystem Service (LSASS) tizimida bufer to’lib toshishi mumkin bo’lgan zaiflikdan foydalangan. Bu esa kompyuterning buzilishiga sabab bo’luvchi lokal qayd yozuvi xavfsizlik siyosatini nazoratlash imkonini bergan. Bundan tashqari, u tizim manbalarini Internet orqali boshqa mashinalarga tarqatish va boshqalarga avtomatik ravishda yuqtirish uchun foydalanadi.

Bu virus aviakompaniyalar, axborot agentliklari, jamoat transporti, kasalxonalar va boshqa ko’plab muhim infratuzilmalarga ta’sir qilib, milliondan ortiq infeksiyalanish holatini qayd qilgan. Umumiy zarar 18 milliard dollarga yaqin bo’lgan. Jaschen balog’at yoshiga yetmaganlikda ayblanib, 21 oy shartli qamoq jazosiga hukm qilindi.

Eng qimmat virus. W32.MyDoom@mm, Novarg, Mimail.R va Shimgapi sifatida ham tanilgan Mydoom, Microsoft Windows OTga ta’sir qiluvchi kompyuter qurti hisoblanadi. Bu birinchi marta 2004 yil 26 yanvarda aniqlangan. Bu eng tez tarqaladigan elektron pochta qurti bo’lgan (2004 yil yanvar oyiga) va bu Sobig chuvalchangi va ILOVEYOU tomonidan o’rnatilgan avvalgi rekordlarni yangilagan.

Mydoom nomini Kreyg Shmugar, McAfee kompyuter xavfsizligi firmasining xodimi va ushbu qurtni ilk kashfiyotchilaridan biri qo’ygan. Shmugar ismni dastur

kodining qatoridagi “Mydoom” matniga e’tibor berganidan keyin tanladi. U shunday deb ta’kidladi: “Bu o’sha vaqtda juda ham katta yo’qolishni anglatgan”. Mydoom bugungi kunga qadar 38 milliard dollardan ortiq zarar keltirgan eng xavfli kompyuter virusidir.

Kompyuter viruslarining tarqalash usullari. Internet tarmog’i keng tarqalmagan vaqtlarda viruslar ko’pincha kompyuterdan kompyuterga yuqtirilgan disketalar orqali tarqalgan. Masalan, SCA virusi Amiga foydalanuvchilari orasida noqonuniy dasturiy ta’minotga ega disklar orqali tarqalgan. Bu zararsiz virus hisoblansada, bir vaqtning o’zida Amiga foydalanuvchilarining 40 foiziga tarqalgan.

Bugungi kunda viruslar Internet orqali tarqalmoqda. Kompyuter viruslari odatda uchta usuldan biri orqali tarqaladi: olib yuriluvchi ma’lumot saqlovchilar, Internetdan yuklab olish va elektron pochta orqali.

Zararli dasturiy vositalarni aniqlash. Zararli dasturiy vositalarni aniqlashda asosan uchta yondashuvdan foydalaniladi. Birinchisi va eng keng tarqalgani *signaturaga asoslangan aniqlash* bo’lib, zararli dasturda namoyon bo’lgan shablon yoki signaturani topishga asoslanadi. Ikkinchi yondashuv *o’zgarishni aniqlashga* asoslangan bo’lib, o’zgarishga uchragan fayllarni aniqlaydi. O’zgarishi kutilmagan fayl o’zgarganda zararlangan deb topiladi. Uchinchi yondashuv *anomaliyaga asoslangan* bo’lib, noodatiy yoki virusga o’xshash fayllarni va holatlarni aniqlashga asoslanadi.

Signaturaga asoslangan aniqlash. Signatura bu – fayldan 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 yozuvchilar tomonidan osonlik bilan 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 ichidan 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’lish ehtimoli $1/2^{112}$ ga teng bo’ladi. Biroq, kompyuter dasturlari va ma’lumotlar ichidagi bitlar tasodifiylikdan yiroq va bu ehtimolni yanada ortishini anglatadi. Boshqa so’z bilan aytganda, biror fayldan signatura aniqlangan taqdirda ham, uni qo’shimcha tekshirish amalga oshirilishi zarurligini anglatadi.

Signaturaga asoslangan aniqlash usuli virus aniq bo’lganda va umumiy bo’lgan signaturalar ajratilgan holatda juda yuqori samaradorlikka ega. Bundan tashqari, ushbu usul foydalanuvchi va administratorga minimal yuklamani yuklaydi va ulardan faqat signaturalarni saqlab borish va ularni uzluksiz yangilash vazifasini qo’yadi.

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 signutaraga asoslangan tanib olish usuli zamonaviy antivirus yoki zararli dasturlarga qarshi himoya vositalarida keng qo’llaniladi. Natijada, virus yaratuvchilar signaturani aniqlash usulini aylanib o’tish imkoniyatiga ega ko’plab usullarni yaratishmoqda.

O’zgarishni aniqlashga asoslan aniqlash. Zararli dasturlar ma’lum manzilda joylashishi sababli, agar tizimdagi biror joyga o’zgarish aniqlansa, u holda zararlanishni ko’rsatish mumkin. Ya’ni, agar o’zgarishga uchragan faylni aniqlansa, u virus orqali zararlangan bo’lishi mumkin. Bu usulni o’zgarishni aniqlashga asoslangan usul sifatida ham nomlash mumkin.

O’zgarishni qanday aniqlash mumkin? Ushbu muammoni yechishda xesh funksiyalar mos yechim bo’ladi. Faraz qilaylik, tizimdagi barcha fayllarni xeshlab, xesh qiymatlari xafsiz manzilga saqlangan bo’lsin. U holda vaqti-vaqti bilan ushbu faylning xesh qiymatlari qaytadan xeshlanadi va dastlabki holatdagilari bilan taqqoslanadi. Agar faylning bir yoki bir nechta bitlari o’zgarishga uchragan bo’lsa,

u holda xesh qiymatlar bir biriga mos kelmaydi va natijada uni virus tomonidan zararlangan deb qarash mumkin.

Ushbu usulning afzalliklaridan biri shuki, agar fayl zararlangan bo'lsa, uni aniqlash to'liq mumkin. Bundan tashqari, oldin noma'lum bo'lgan zararli dasturni aniqlash mumkin (o'zgarish bu – ma'lum yoki nomalum zararli dastur orqali bo'lgan o'zgarish).

Biroq, ushbu usul ko'plab kamchiliklarga ega. Tizimdagi fayllar odatda tez-tez o'zgarib turadi va buning natijasida 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 usul kabi muammolarga olib keladi.

Anomaliyaga asoslangan aniqlash. Anomaliyaga asoslangan usul noodatiy yoki virusga o'xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi. Ushbu g'oya IDS tizimlarida ham foydalaniladi.

Ushbu usulning fundamental muammosi bu - 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 tizim bu holatga moslashish muammosi ham mavjud. Bu esa ushbu usulda juda ham ko'plab noto'g'ri signallarni paydo bo'lishiga olib keladi.

Ushbu usulning afzalligi esa oldin noma'lum bo'lgan zararli dasturlarni aniqlash imkonini beradi. Biroq, ushbu usulda yuqorida keltirilgan kabi ko'plab muammolar mavjud va shuning uchun ham ushbu usul hozirda tadqiqot olib borilayotgan dolzarb sohalardan biri hisoblanadi.

Antivirus dasturiy vositalarining kamchiligi. Antivirus dasturiy vositasi kompyuterni himoyalashda amalga oshirilish kerak bo'lgan zaruriy shart sifatida qaraladi. Umuman olganda, antivirus kompyuter uchun zararli dasturlarni skanerlash, himoya qilish, karantin holatiga tushurish 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 foydalanganda reklamalarni bloklash, Internet tarmog'idan kirib keluvchi zararli dasturlarni bloklash va hak. Biroq, foydalanuvchilar to'liq antivirus dasturiy vositalarining imkoniyatilarigi ishonib qolmasliklari kerak.

Viruslarni doimiy aniqlash uchun antivirus dasturiy vositalari eng yangi va yangilangan ma'lumotlarni o'z ichiga olgan na'munaviy fayllarga muxtoj. Biroq, antivirus ishlab chiqaruvchilar yangi virus uchun na'munaviy fayllar yaratguncha virus ishlab chiqaruvchilar 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 operasion tizimining markaziga hujum qilishni maqsad qiladi.

Antivirus dasturiy vositalarini sifatini baholash omillari. Antivirus dasturiy vositalarini 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 qobilyati;
- 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.

Profilaktik choralar. Viruslar va virus yuqtirilgan fayllarni o'z vaqtida aniqlash, aniqlangan viruslarni har bir kompyuterda to'liq yo'q qilish virus epidemiyasini boshqa kompyuterlarga tarqalishini oldini olish mumkin. Har qanday virusni aniqlaydigan va yo'q qilishni kafolatlaydigan mutlaqo ishonchli dasturlar mavjud emas. Kompyuter viruslariga qarshi kurashishning muhim usuli bu 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 lisenziyali dasturiy ta’minotdan foydalanish;
- kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta’minlash va uni doimiy yangilab borish;
- boshqa komyuterda 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 kirish nazorati uchun antivirus dasturidan foydalanish.

Antivirus dasturiy komplekslari. Har bir antivirus dasturiy vositalarining o’ziga xos bo’lgan afzallik va kamchiliklarga ega. Faqat bir nechta antivirus dasturiy vositalaridan kompleks foydalanish to’liq himoyani ta’minlishi mumkin. Amalda ko’plab antivirus dasturiy vositalari mavjud bo’lib, ularga quyidagilarni misol keltirish mumkin [6] (14-jadval).

14-jadval

Turli antivirus dasturlarining xususiyatlari

Mahsulot	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
Eng quyi 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	+	+	+	+	+	+	+	+	+	-
Veb saytni baholash	+	+	+	-	+	-	+	-	-	-
Zararli URL ni bloklash	+	+	+	+	+	+	+	+	-	-
Fishingdan himoya	+	+	+	+	+	+	+	-	-	-
Xususiyatga ko’ra aniqlash	+	+	+	+	+	+	+	+	+	-
Zaifliklarni skanerlash	+	-	+	+	-	-	-	-	-	-

Nazorat savollari

1. Dasturiy mahsulotlarda xafsizlik ta’minlanishini muhimligini ko’rsatuvchi misollar keltiring?
2. Dasturiy mahsulotlarda xavfsizlik muammolarining kelib chiqish sabablarini ayting?
3. Nuqson, bag, xotirani to’lib toshishi tushunchalariga izoh bering?
4. Dasturiy vosita xavfsizligini fundamental prinsiplarini ayting va ularga tushuntirish bering?
5. Dasturiy vositalarga qo’yilgan talablar va ularga misollar ayting?
6. Dasturiy vositalarga qo’yilgan xavfsizlik talablariga misollar ayting?
7. Dasturiy vositalar xavfsizligini ta’minlashda dasturlash tillarining o’rnini tushuntiring?
8. Xavfsiz va xavfsiz bo’lmagan dasturlash tillariga misollar keltiring?
9. Zararli dasturlar nima va ularning asosiy turlarini sanang?
10. Kompyuter viruslari nima va ularga misollar ayting?
11. Zararli dasturiy vositalardan himoyalanish usullari va vositalari haqida ma’lumot bering?
12. Antivirus dasturiy vositalarini tanlashdagi talablar va ularga misollar keltiring.

7 BOB. AXBOROT XAVFSIZLIGI SIYOSATI VA RISKLARNI BOSHQARISH

7.1. Tizimlarning umumiy arxitekturasi

Boshqa sohalarda bo’lgani kabi kiberxavfsizlik sohasida ham tizim va tizim arxitekturasi tushunchasi tez-tez ishlatilib, bunda matn konteksti bir – biridan farq qiladi. Shu sababli, ushbu bo’limda tizim arxitekturasi tushunchasi bilan tanishib chiqiladi.

Tizim arxitekturasi yoki tizimlarning arxitekturasi – bu tizimning tuzilishi, o’ziga xos xususiyatlari va boshqa qarashlarini belgilaydigan konseptual model.

Tizimlar arxitekturasi - bu murakkab tizimlarni tavsiflash va loyihalashda konseptual va amaliy qiyinchiliklarga yechimdir.

Arxitektura - bu tizimning tuzilishi va hatti-harakatlari to’g’risida fikr yuritishni qo’llab quvvatlash maqsadida tashkil qilingan tizimning rasmiy tavsifi.

Tizim arxitekturasi butun tizimni amalga oshirishda birgalikda ishlaydigan tizim tarkibiy qismlaridan va ishlab chiqilgan qismtizimlardan iborat bo’lishi mumkin. Tizim arxitekturasini tavsiflash uchun olib borilgan harakatlar *arxitekturani tavsiflash tillari* deb nomlanadi.

Turli tashkilotlar tizim arxitekturasini turli yo’llar bilan aniqlashi mumkin, xususan:

- tizimning fundamental tashkil etilish, uning tarkibiy qismlari, ularning bir-biriga va muhitga bo’lgan munosabati, uning dizayni va evolyusiyasini boshqaruvchi tamoillar;
- tizimning tavsifi, shu jumladan, apparat va dasturiy komponentlarning funksional imkoniyatlari xaritasi, dasturiy ta’minot arxitekturasining apparat arxitektura xaritasi va insonning ushbu komponentlar bilan o’zaro aloqasi;
- funksional arxitektura talablari va bazaviy talablarni qondirish uchun mo’ljallangan istemolchi mahsuloti yoki hayotiy sikl uchun dizayn yechimini ta’minlaydigan fizik elementlarning ajratilgan joylashuvi;

- arxitektura eng muhim, keng tarqalgan, yuqori darajadagi, strategik ixtirolar, qarorlar va ularning umumiy asoslari (ya’ni, muhim elementlari va ularning o’zaro aloqalari) va ular bilan bog’liq xususiyatlardan iborat;
- kompyuter tizimining dizayni va tarkibining tavsifi bo’lib, agar u hujjatlashtirilgan bo’lsa, unda joriy apparat, dasturiy ta’minot va tarmoq imkoniyatlarining batafsil ro’yxatidan iborat ma’lumotlar bo’lishi mumkin. Uzoq muddatli rejalar va kelajakdagi xaridlarning ustuvorligi, shuningdek, eski uskuna va dasturiy ta’minotni yangilash va/ yoki almashtirish rejasining tavsifi;
- tizimning rasmiy tavsifi yoki uning amalga oshirilishini boshqarish uchun komponentlar darajasida tizimning batafsil rejasi;
- mahsulot va ularning hayotiy jarayonlari uchun mo’ljallangan dizayn memorchiligining kompozisiyasi;
- komponentlarning tuzulishi, ularning o’zaro bog’liqligi va vaqt o’tishi bilan ularning dizayni va evolyusiyasini boshqaruvchi prinsiplar va ko’rsatmalar.

Tizim arxitekturasini mavjud (yoki kelajakdagi) tizimning tasvirlar to’plami sifatida o’ylash mumkin. Ushbu tasvirlar dastlab umumiy, yuqori darajadagi funksional tashkilotni tavsiflaydi va shundan so’ng batafsil va aniq tavsilotlarga o’tiladi.

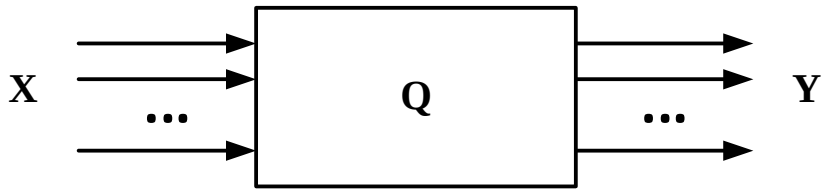
Tizim arxitekturasi tizimdan tashkil topgan elementlarning axborot tarkibini, ushbu elementlar o’rtasidagi munosabatlar va ushbu munosabatlarni tartibga soluvchi qoidalarni yetkazadi.

Tizim arxitekturalarining bir nechta turlari mavjud bo’lib, ular quyidagilar:

- qurilma arxitekturasi;
- dasturiy ta’minot arxitekturasi;
- korxona arxitekturasi;
- hamkor tizimlar arxitekturasi (Internet, aqlli transport tizimlari va havo hujumidan mudofaa tizimlari kabi);
- ishlab chiqarish tizimlari arxitekturasi;
- strategik tizimlar arxitekturasi.

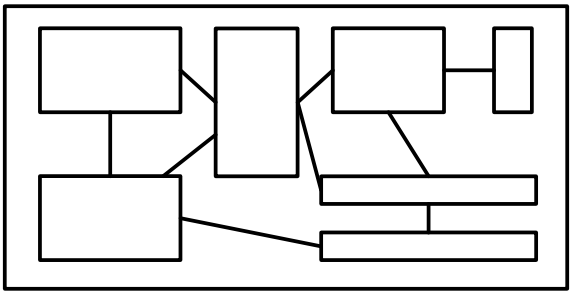
Tizimlar arxitekturasi quyidagi 9 ta fundamental prinsipga asoslanadi:

1. *Haqiqat obyektlari tizim sifatida modellashtiriladi* (ya’ni, funksiyani bajaradigan va uning perimetri kirish, chiqish va ichki holat bilan belgilangan quti). Masalan, mobil telefon - bu ovoz va tugmalar orqali kiritish hamda ovoz va displey orqali chiqarish tizimi hisoblanadi. Bundan tashqari, u yoqilgan va o’chirilgan bo’lishi mumkin. Umuman olganda, telefon qo’ng’iroqlarini amalga oshirishga imkoniyat beradi (80-rasm).



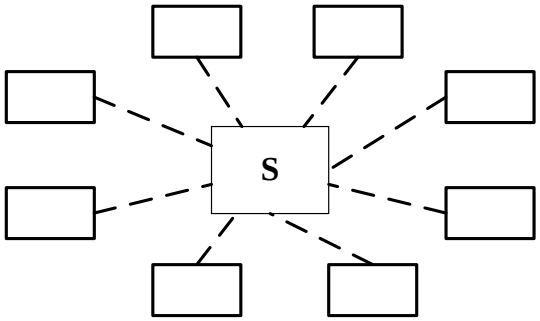
80-rasm. Kirish va chiqishga ega tizimlarning umumiy ko’rinishi

2. *Tizim o’zidan kichik bo’lgan tizimlarga qismtizim sifatida bo’linishi mumkin.* Masalan, mobil telefon aslida ekran, klaviatura, korpus, mikrafon, karnay va mikrosxemadan iborat. Ammo, telefon bu barcha elementlarning birlashuvidir va ushbu elementlar to’plamidan uni to’liq tushinish qiyin (81-rasm).



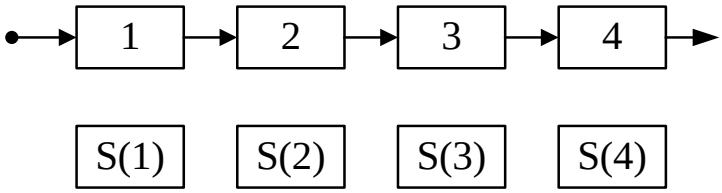
81-rasm. Tizim va uning qismtizimlari

3. *Tizim boshqa tizimlar, ya’ni, uning muhiti bilan o’zaro bog’langan bo’lishi mumkin***.** Masalan, mobil telefon foydalanuvchi, relef (signalni uzatish uchun), reperator (signal bizilganda), yer va boshqalar bilan bog’langan. Ushbu tizimlarning barchasi uning atrof-muhitini tashkil qiladi va ishlab chiqishda hisobga olinadi.



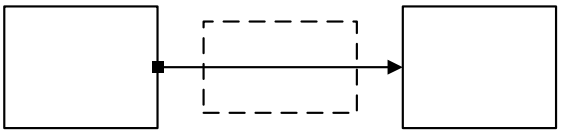
82-rasm. Tizimning boshqa muhitlar bilan bog'liqligi

4. *Tizim butun hayotiy sikli davomida ko'rib chiqilishi kerak.* Masalan, mobil telefon loyihalashtiriladi, prototiplanadi, sinovdan o'tkaziladi, tasdiqlanadi, ishlab chiqariladi, tarqatiladi, sotiladi, foydalaniladi, ta'mirlanadi va nihoyat qayta ishlanadi. Ushbu bosqichlarning barchasi muhim hisoblanadi (va nafaqat foydalanish vaqtida emas).



83-rasm. Tizimlarning umumiy hayotiy sikli

5. *Tizim boshqasiga interfeys orqali ulanishi mumkin. Bu esa ulanish xususiyatlarini modellashtiradi.* Masalan, qo'ng'iroq qilganda qulog'imiz telefon bilan bevosita aloqada bo'ladi va shuning uchun, ikki tizim (quloq va telefon) o'rtasida ulanish mavjud. Biroq, bu yerdagi yashirin interfeys bu – havo. Havoning xususiyatlari quloq va telefon o'rtasidagi aloqaga ta'sir qilishi mumkin (masalan, shovqin ko'p bo'lgan holda).

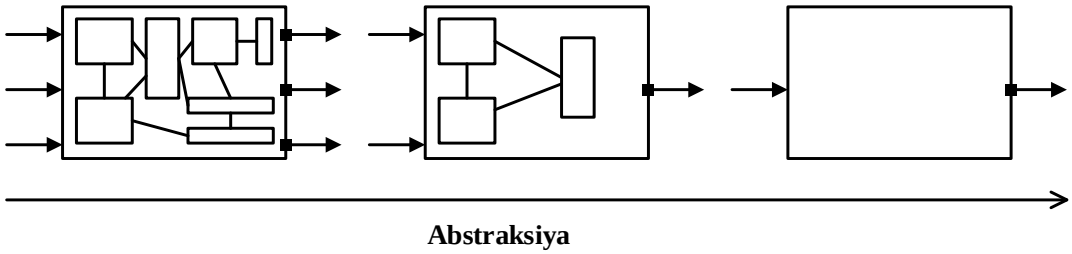


Interfeys

84-rasm. Tizimni boshqa tizimga interfeys orqali bog'lanishi

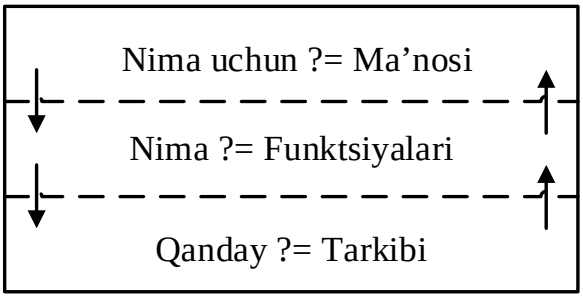
6. *Tizimni turli abstraksiya darajalariga ko'rib chiqish mumkin va bu faqat tegishli xususiyatlar va xatti-harakatlarni hisobga olishga imkon beradi.* Masalan, mobil telefon qurilmasini qo'ng'iroq qiluvchi (va boshqa zamonaviy funksiyalar) qurilma, bir qancha material va elektron komponentlarning birgalikdagi

tuzilish yoki katta hajmdagi atomlarning to’plami deb hisoblaysizmi? Ushbu ko’rinishlarning barchasi haqiqat. Biroq, ular har xil abstraksiya darajasida va ularning mosligi kontekstga bog’liq bo’ladi.



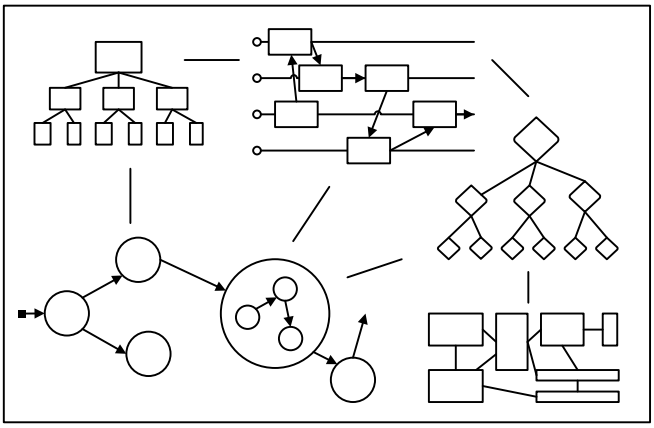
85-rasm. Tizimni turli abstraksiya darajalaridagi holati

7. *Tizimni bir qancha qatlamlar bo’yicha qarab chiqish mumkin (odatda uchta: ma’nosi, funksiyalari va tarkibi).* Masalan, telefon – bu o’z muhiti uchun bir nechta vazifalarni bajarishga mo’ljallangan obyekt ma’nosini berib, qo’ng’iroqlarni amalga oshirish, moda obyekti bo’lish, shaxsiy raqamli yordamchi bo’lishi va boshqalar. Biroq, ushbu topshiriqlarni amalga oshirish uchun ko’plab funksiyalar to’plamiga ega (ekranga ko’rsatish, signalni uzatish, quvvatlash, foydalanuvchi tomonidan kiritilganlarni qidirish, zarur bo’lgan ovoz chiqarish va hak.). Va nihoyat, ushbu funksiyalarning barchasi ushbu funksiyalarni bajarish uchun tashkil qilingan jismoniy komponentlar orqali amalga oshiriladi.



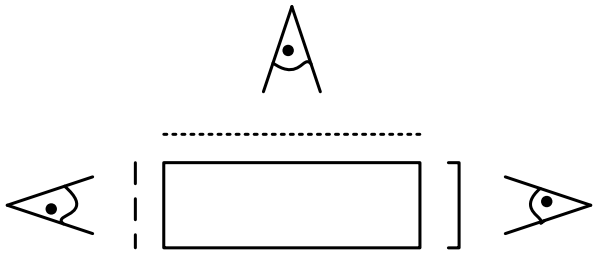
86-rasm. Tizimni turli qatlamlardagi ko’rinishi

8. *Tizim berilgan semantika bilan o’zaro bog’liq bo’lgan modellar orqali tasvirlanishi mumkin (xususiyatlar, tuzilish, holatlar, ma’lumotlar va hak.).* Masalan, xususiyatlar nuqtai nazaridan telefon bir metr balandlikdan tushib ketishga chidamli bo’lgan qurilma. Ammo, telefon ham holatini o’zgartiradi: telefon o’chirilgan va yoqish tugmasi bosilganda yoqiladi.



87-rasm. Tizimning semantik bog’liq bo’lgan modellar orqali tasviri

9. *Tizimga aloqador turli ishtirokchilarga mos keladigan nuqtai nazarlar orqali tizimni tasvirlash mumkin.* Masalan, reklama qiluvchilar, dizaynerlar, muhandislar va hak. Bularning barchasi telefonni turlicha tasvirlaydi.



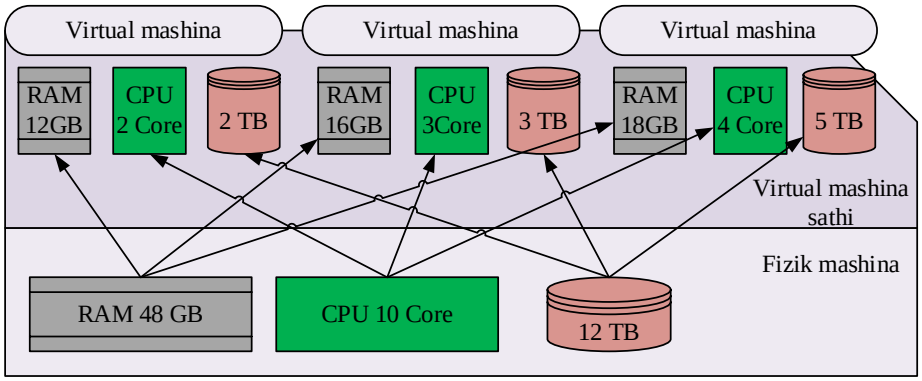
88-rasm. Tizimning turlicha ko’rinishi

Yuqorida bayon etilgan arxitektura prinsiplariga asoslangan amalda qator tizimlar mavjud. Quyida ulardan ba’zilari bilan tanishib o’tiladi.

Virtual mashina. Virtual mashina bu – oddiy kompyuter kabi ishlaydigan kompyuter fayli (odatda obraz deb aytiladi) bo’lib, u kompyuterda yana bir kompyuter yaratish imkoniyatini beradi. Boshqa har qanday dastur kabi, u alohida oynada ishlaydi. Shunday qilib, foydalanuvchilar virtual mashinada kompyuterlarning asosiy operasion tizimidagi kabi bir xil ish sharoitiga ega bo’ladi. Virutal mashina tizimning qolgan qismidan ajratilgan, ya’ni uning ichidagi dastur asosiy kompyuter tizimiga ta’sir qilishi yoki uni boshqarishi mumkin emas. Bu boshqa operasion tizimlarni, shuningdek, beta versiyalarni sinovdan o’tkazish, viruslarni tahlil qilish, operasion tizimlarning zaxira nusxalarini yaratish, asosiy operasion tizimdan farq qiluvchi operasion tizim va uning dasturiy vositalarini ishlatish uchun ideal muhit hisoblanadi.

Bir vaqtning o’zida bir nechta virtual mashinalar yagona fizik kompyuterda ishlashi mumkin. Serverlar uchun bir nechta operasion tizim ularni boshqarish uchun foydalaniladigan maxsus dasturiy ta’minot (gipervizor deb ataladi) bilan ishlaydi. Shaxsiy kompyuterlarda esa odatda bir operasion tizimdan boshqa bir operasion tizimni yuklash oddiy dasturiy ta’minot kabi amalga oshiriladi.

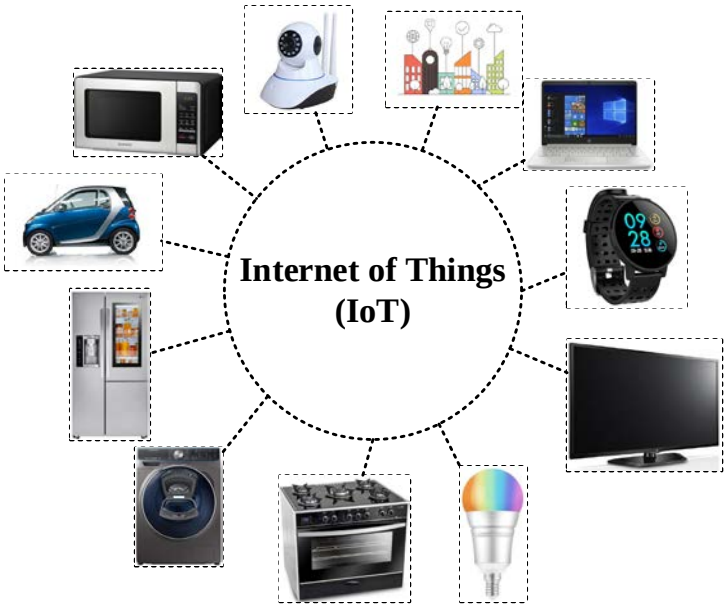
Har bir virtual mashinada CPU, xotira, qattiq disklar, tarmoq interfeysi va boshqa qurilmalarni o’z ichiga olgan o’zining virtual qurilmalari mavjud (89-rasm).



89-rasm. Virtual mashina

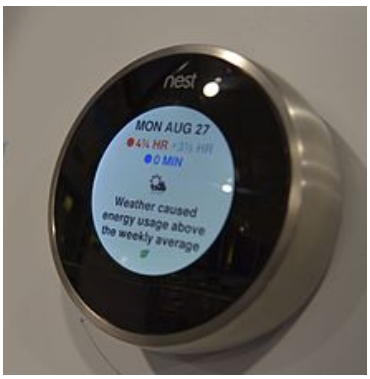
Virtuallashtirishga qaratilgan dasturiy vositalarga Parallels Workstation, Parallels Desktop for Mac, VirtualBox, Virtual Iron, Oracle VM, Virtual PC, Virtual Server, Hyper-V, VMware Workstation, VMware Server, VMware ESXi, QEMU, Adeos va boshqalarni misol keltirish mumkin.

Narsalar Interneti (Internet of Things, IoT). IoT – bu o’zaro bog’liq bo’lgan unikal identifikatorga ega hisoblash qurilmalari, mexanik va raqamli mashinalar, obyektlar, hayvonlar va odamlar tizimi bo’lib, tarmoq bo’ylab ma’lumotni uzatishda inson-inson yoki inson-mashina aloqasini talab etmaydi (90-rasm).



90-rasm. IoT tizimi umumiy ko’rinishi

IoT tushunchasi bir nechta texnologiyalar, real vaqtda tahlillash, mashinaning o’rganishi, oddiy sensorlar va o’rnatilgan tizimlarni birlashishi tufayli kengaydi. O’rnatilgan tizimlarning ananaviy sohasi, simsiz sensor tarmoqlar, nazoratlash tizimlari, avtomatlashtirish va boshqa tizimlar birgalikda IoT ni hosil qiladi. Istemol bozorida IoT texnologiyasi “aqlli uylar” tushunchasiga tegishli bo’lgan mahsulotlar bilan ko’proq mos keladi. Masalan, qurilma yoki dasturiy vositalar uyning yoritish, isitish, xavfsizlik tizimini nazorat qiladi va uni smartfon qurilmalari va turli ovozli buyruqlar bilan osonlik bilan boshqarish mumkin bo’ladi (91-rasm).



a) Enegriyadan foydalanish va mahalliy ob havo haqida Nest termostati

b) Internetga ulangan Ring kompaniyasiga tegishli qo’ng’iroq

c) Internetga ulangan August Home smart kaliti

91-rasm. Aqlli uy jihozlarini ishlab chiqaruvchilar

O’rnatilgan tizimlar (Embedded systems). O’rnatilgan tizimlar – bu ko’pincha real vaqt hisoblash cheklovlariga ega bo’lgan kattaroq mexanik yoki elektr

tizimidagi maxsus funksiyaga ega boshqaruvchi bo’lib, ular odatda apparat va mexanik qismlarni o’z ichiga olgan to’liq qurilmaning bir qismi sifatida o’rnatilgan bo’ladi. O’rnatilgan tizimlar bugungi kunda keng foydalaniladigan bir qancha qurilmalarni boshqarishda foydalanilib, ishlab chiqarilgan mikroprosessorlarning 98% o’rnatilgan tizimlar sifatida foydalaniladi (92-rasm).

92-rasm. O’rnatilgan tizimlarga misollar

Zamonaviy o’rnatilgan tizimlar ko’pincha mikrokontrollerlarga asoslangan (ya’ni, o’rnatilgan xotira va pereferik interfeysga ega mikroprosessorlar) bo’lsada, murakkab tizimlarda oddiy mikroprosessorlar (xotira va pereferik interfeys uchun tashqi qurilmalardan foydalanish) ham keng foydalanilmoqda. O’rnatilgan tizim aniq vazifalarga bag’ishlangani sababli, uni mahsulotning hajmi va narxini kamaytirish, ishonchligini va ishlashini oshirish uchun optimallashtirish imkoniyati mavjud. Ba’zi o’rnatilgan tizimlar ommaviy ishlab chiqilgan bo’lib, hajmni tejashdan foyda qiladilar.

O’rnatilgan tizimlar raqamli soatlar va MP3 pleyerlar kabi ko’chma qurilmalardan tortib, svetafor, dasturlashtirilgan mantiqiy boshqaruv qurilmalari kabi yirik statsionar qurilmalar, gibrid transport vositalari hamda tibbiy tashxislash tizimlarida ham foydalanilmoqda.

7.2. Axborot xavfsizligi siyosati va uni amalga oshirish

Xavfsizlik siyosati bu - tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami. Xavfsizlik siyosati konfidensiallikni, foydalanuvchanlikni, yaxlitlikni va aktiv qiymatini saqlashni maqsad qilib, u xavfsizlik infratuzilmasining asosi hisoblanadi. Xavfsizlik siyosatisiz tashkilotda bo'lishi mumkin bo'lgan turli nojo'ya harakatlarni oldini olishning imkoni yo'q. Shunga qaramay, xavfsizlik siyosati asos xavfsizlik hujumlarini oldini olish yo'l yo'riqlarini o'zida mujassamlashtirmaydi.

Siyosatlar texnologik xarakterga ega bo'lmaydi va quyidagi amalga oshiradi:

- ishchilar va uchinchi tomoni uchun qonuniy javobgarlikni kamaytiradi;
- konfidensiallikni va shaxsiy axborotni o'g'irlanishdan, noo'rin foydalanishdan, ruxsat etilmagan oshkor bo'lishidan yoki modifikasiyalashdan himoyalaydi;
- hisoblash resursi yetishmasligidan himoyalaydi.

Xavfsizlik siyosati o'zida tashkilot tarmog'i va kompyuter tizimlari xavfsizligi talablari uchun maqsad va qoidalarni mujassamlashtirgan. Xavfsizlik siyosati maqsad va xavfsizlik talablari o'rtasida bog'lovchi vazifasini o'tab, foydalanuvchilarga, xodimlar va boshqaruvchilarga texnologiya va axborot aktivlarini himoyalashga yordam beradi. Xavfsizlik siyosati kompyuter tizimlari va tarmoqlarining rasmiy talabi, sozlanishi va auditi uchun asos hisoblanadi, hamda u tashkilot aktivlarining konfidensialligini, butunligini va foydalanuvchanligini kafolatlashi shart.

Xavfsizlik siyosatini 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 tashkilotni ushbu tahdidlarga qarshi kurashish va unga axborotni yo'qolishidan himoyalash imkonini beradi.

- Xavfsizlik siyosati tashkilotning barcha funksiyalarini xavfsiz tarzda amalga oshirish orqali xavfsizlik prinsiplarining kelishilgan vazifalarini ta’minlaydi. Xavfsizlik siyosatlari mijozlar bilan ishonchga asoslangan aloqani qurishda axborot xavfsizligi standartlarining mosligini ta’minlaydi. Xavfsizlik siyosati tashqi axborot tahdidlariga kompaniyaning duchor bo’lishini kamaytirishga yordam beradi.
- Xavfsizlik siyosati tarmoqda qanday qoidalar foydalanishi kerakligi, 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 siyosatlari tahdidlarni 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’lumotlarini yo’qolishi va chiqib ketishi xavfini minimallashtiradi.

Xavfsizlik siyosatlarining 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 resurslarni yo’qolish holatlari deyarli kuzatilmaydi.
- *Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishi:* xavfsizlik siyosati xodimlar tomonidan amalga oshirilgani bois, administratorlar doimiy tarzda tashkilotda trafikni va foydalanilgan tashqi qurilmalarni monitoringlashi zarur. Kiruvchi va chiquvchi trafikning monitoringi va auditi doimiy ravishda amalga oshirilishi shart.

- *Tarmoqni yuqori unumdorligi:* xavfsizlik siyosati to’g’ri amalga oshirilganda va tarmoq doimiy monitoring qilinganda, ortiqcha yuklamalar mavjud bo’lmaydi. Tarmoqda ma’lumotni uzatish tezligi ortadi va bu umumiy samaradorlikni ortishiga olib keladi.
- *Muammolarga tezkor javob berish va harakatsiz vaqtning kamligi:* xavfsizlik siyosatini amalga oshirilishi tarmoq muammolari kuzatilganda tezda javob berish imkoniyatini taqdim etadi.
- *Boshqaruvdagi stress darajasini kamayishi:* xavfsizlik siyosati amalga oshirilgan vaqtda boshqaruvchi roli kam stressga ega bo’ladi. Tashkilotda har bir siyosatidagi vazifa biror xodimga biriktirilishi shart. Agar ushbu holat amalga oshirilsa, tarmoqda biror nojo’ya holat kuzatilsa, boshqaruvda hyech qanday xavotir bo’lmaydi.
- *Xarajatlarni 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 uni nechtaligiga bog’liq.

- *Qonunlar*. Qonunlar iyerarxiyaning eng yuqorisida 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 xodimlarni qonunlarga rioya qilishini kafolatlaydi. Normativ hujjatlar xavfsizlik siyosati qonuniga mos bo’lgan yo’l yo’riq ko’rsatuvchi hujjatlar to’plami hisoblanib, ular hukumat yoki ijtimoiy normativ hujjatlardan iborat bo’ladi.
- *Siyosatlar*. Siyosatlar yordamida tashkilot o’z tarmoq xavfsizligi uchun qonuniy va ichki tarmoq talablarini yaratadi. Siyosat turli muolajalardan iborat bo’lib, ular tashkilot uchun xavfsizlik arxitekturasini ko’rsatadi. Ushbu

siyosatlarni amalga oshirib tashkilotda standartlarni o’rnatish va risklarni boshqarish kabi vazifalarni bajarish mumkin.

- *Standartlar*. Standartlar siyosatni amalga oshirish usullarini tavsiflab, ular siyosatlardan kelib chiqadi va tashkilotlar tomonidan amalga oshiriladi. Standartlar korxona siyosatiga ixtiyoriy va mandatli aloqador bo’lib, ishlab chiqilgan standartni ma’lum vaqtdan so’ng o’zgartirish talab etilmasligi zarur. Shuningdek, standartlar texnologiya, qurilma va dasturiy vositaga bog’liq holda xavfsizlik nazoratini o’z ichiga oladi.
- *Yo’riqnomalar*. Yo’riqnomalar tashkilot siyosati va standartlarini amalga oshirish strategiyasini aniqlab, tashkilotni tahdidlarga qarshi tura olishida yordam beradi. Shuning uchun, tashkilot xodimlari yo’riqnomalarni bajarish uchun maxsus o’qitiladi.
- *Muolajalar*. Muoalajalar tashkilot siyosatini amalga oshiruvchi ketma-ket bosqichlar to’plami bo’lib, ularni amalga oshirishda imtiyozga ega subyektdan tasdiq talab etiladi. Muolajalar quyidagi savollar asosida ishlaydi:
    - Kim nimani bajaradi?
    - Ular qanday bosqichlarga ega?
    - Ular qaysi forma va hujjatlardan foydalanadi?
- *Umumiy qoidalar*. Umumiy qoidalar tanlovga ko’ra maslahatlar bilan ta’minlovchi hujjat bo’lib, ular biror maxsus standartlar bo’lmagan holatda foydalaniladi. Umumiy qoidalar tavsiyalar sifatida bo’ladi va tashkilotlar ularni rad eta olmaydi. Umumiy qoidalarni amalga oshirish risklarni kamaytirsada, biznes talablari o’zgarganda umumiy qoidalarni ham o’zgartirish tavsiya etiladi.

Yaxshi xavfsizlik siyosati quyidagi xususiyatlarga ega bo’lishi shart:

- *Qisqa va aniq:* xavfsizlik siyosati infratuzilmada joriy qilish uchun qisqa va aniq bo’lishi shart. Murakkab xavfsizlik siyosati tushunish uchun qiyin bo’lib, xodimlar tomonidan kutilgani kabi amalga oshirilmaydi.

- *Foydalanuvchan bo’lishi:* siyosat tashkilotning turli sektorlari bo’ylab oson foydalanishli yozilishi va loyihalanishi shart. Yaxshi yozilgan siyosatlar boshqarishga va amalga oshirishga oson bo’ladi.
- *Iqtisodiy asoslangan bo’lishi:* tashkilotlar tejamkor va o’z xavfsizligini kuchaytiruvchi siyosatni amalga oshirishi shart.
- *Tushunarli bo’lishi:* siyosatlar tushunishga va amalga qilishga oson bo’lishi kerak.
- *Amaliy bo’lishi:* siyosatlar reallikka asoslangan amaliy bo’lishi kerak. Real bo’lmagan siyosatni amalga oshirilishi faqat tashkilotga muammo olib keladi.
- *Barqaror bo’lishi:* tashkilot o’zining siyosatini amalga oshirishda barqarorlikga ega bo’lishi kerak.
- *Mulojaviy bardoshli bo’lishi:* siyosat muolajalarini amalga oshirganda ular ish beruvchi va ishlovchiga mos bo’lishi kerak.
- *Kiber va yuridik qonunlarga, standartlarga, qoidalarga va instruksiyalarga mos bo’lishi:* amalga oshiriluvchi ixtiyoriy siyosat kiber qonunlar asosida ishlab chiqilgan qoidalar va instruksiyalarga mos bo’lishi zarur.

Xavfsizlik siyosatining kontenti

Xavfsizlik siyosatini amalga oshirishning 4 ta qismi mavjud:

– xavfsizlik talablari;
– siyosat tavsifi;
– amalning xavfsizlik prinsipi;
– elementlar joylashuvining arxitekturasi.

Xavfsizlik talablari. Ushbu bayon xavfsizlik siyosatini amalga oshirishda tizim uchun talablarni xarakterlaydi. Xavfsizlik talablarining quyidagi 4 turi mavjud:

- intizom xavfsizligi talablari;
- qo’riqlash xavfsizligi talablari;
- muolajaviy xavfsizlik talablari;
- kafolat xavfsizligi talablari.

Intizom xavfsizlik talablari. Bu xavfsizlikni ta’minlashda turli obyektlarga nisbatan qanday harakatlar bajarilishini kerakligini ko’rsatuvchi xavfsizlik

siyosatini o’z ichiga oladi. Masalan, kompyuter xavfsizligi, amallar xavfsizligi, tarmoq xavfsizligi, shaxs xavfsizligi, fizik xavfsizlik va hak.

Qo’riqlash xavfsizligi talablari. U zarur bo’lganda ko’rsatiluvchi himoya choralaridan tashkil topgan xavfsizlik siyosatini o’z ichiga oladi. Masalan, foydalanishni nazoratlash, zararli dasturlarga qarshi kurashish, audit, foydalanuvchanlik, konfidensiallik, butunlik, kriptografiya, identifikasiya va autentifikasiya uchun himoya choralari.

Muolajaviy xavfsizlik talablari. U foydalanish siyosatlari, qaydlash, amallar davomiyligi va hujjatlashtirishdan iborat xavfsizlik siyosatlaridan iborat.

Kafolat xavfsizligi talablari. U turli standartlar, sertifikatlar va akkreditasiyaga muvofiq foydalaniluvchi xavfsizlik siyosatlarini o’z ichiga oladi.

Siyosat tavsifi. Mazkur qismda asosiy e’tibor xavfsizlik tartibiga, qo’riqlash, muolajalar, amallarning bog’liqligi va hujjatlashtirishga qaratiladi. Siyosat tavsifining har bir qismida tizim arxitekturasi elementlari xavfsizlikni qanday ta’minlashi bayon etiladi.

Amallarning xavfsizlik prinsipi. Ushbu prinsip xavfsizlik siyosatining rollarini, javobgarliklarini va funksiyalarini aniqlaydi. U missiya, aloqa, shifrlash, foydalanuvchi va texnik xizmat ko’rsatish instruksiyalari, bo’sh ishchi vaqtini boshqarish, xususiy va jamoat mulki, shartli foydalanishli dasturiy vosita qoidalari va virusdan himoyalanish siyosatiga e’tiborni qaratadi.

Elementlar joylashuvining arxitekturasi. Ushbu siyosat tashkil etuvchisi dasturdagi har bir tizim uchun kompyuter tizimlari arxitekturasini joylashuvini ta’minlaydi.

Xavfsizlik siyosati quyidagi bo’limlardan iborat:

- xavfsizlik siyosatining *umumiy tavsifi* - siyosat ko’rib chiqishi kerak bo’lgan asosiy ma’lumotlarni taqdim etadi;
- *maqsad* – siyosati nima uchun tuzilganligini batafsil tushuntirishni o’z ichiga oladi;
- *harakat sohasi* kimni va nimani qamrab olish haqidaga axborotdan iborat;
- *qoidalar va javobgarliklar* xodimlar va boshqaruv uchun aniqlanadi;

- *maqsadli auditoriya* bu - siyosat ishlab chiqilayotgan foydalanuvchilar va mijozlardir;
- *siyosatlar* bu – xavfsizlik siyosatining har bir aspekti uchun bayoni;
- *sanksiyalar va buzilishlar* mijozlar va foydalanuvchilar rioya qilishi kerak bo'lgan ruxsat berish/ rad etish jarayonini belgilaydi;
- *kontakt ma'lumotlari* siyosat sanksiyalari va/ yoki buzilishlari yuz berganda kim bilan bog'linish kerakligi haqidagi axborot;
- *versiya* raqami siyosatdagi barcha o'zgarishlar va yangilanishlar to'g'ri kuzatilishini ta'minlaydi;
- *glossari* siyosatda foydalanilgan turli atama va qisqartmalarni ma'nosini o'z ichiga oladi.

Xavfsizlik siyosati bayonoti. Tashkilotning xavfsizlik siyosatining muvaffaqqiyatli bayonoti aniq va qisqa bo'lishi kerak. Siyosat bayonoti bu – tashkilot siyosatini chuqur tarkibini belgilaydigan reja bo'lib, u har bir siyosat loyihasida vaziyatning keskinlashgan davrida tashkilotning harakat yo'nalishini belgilash uchun amaliy tarzda bo'lishi shart. Siyosat bayonoti xodimlarga profilaktika choralarini tushunishga yordam beradi. Masalan, ideal xavfsizlik siyosati bayonotiga - "ma'lumotlardan foydalanish joiz faoliyat talabiga asoslanadi va subyektlar rasmiy tasdiq jarayonidan o'tishi kerak" misol keltirish mumkin.

Yuqoridagi siyosat bayonotida xodimlar ma'lumotlardan faqat rahbariyat tasdiqlagandan so'ng foydalanishlari aniq ko'rsatilgan bo'lib, agar biror xodim xavfsizlik bayoniga rioya qilmasa, tashkilot zarur choralarni ko'rishga haqli degan xulosaga kelish mumkin.

Xavfsizlik siyosatini yaratish va amalga oshirish bosqichlari. Xavfsizlik siyosatini samarali yaratish va amalga oshirish quyidagi bosqichlardan iborat:

1. *Risklarni baholash:* tashkilot o'z siyosatini ishlab chiqishdan oldin o'z aktivlari uchun risklarni baholashi shart bo'lib, risklarni baholash davomida risklar aniqlanadi va ularning kritiklik darajasi baholanadi.

2. *Standart umumiy qoidalar:* tashkilot o'z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o'rnatishi shart. Tushunarli bo'lgan standart

umumiy qoidalar to’plami tashkilot va uning xodimlari uchun yordamchi vosita bo’ladi.

3. *Nazoratni kiritilishi:* yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo’shimcha kiritish jarayonida nazorat bo’lishi talab etilib, agar boshqaruvchi qonuniy sanksiyalarni qabul qilsa va tasdiqlasa, xodimlar faqat ishlab chiqilgan siyosatga amalga qilishadi. Boshqaruvchisiz ixtiyoriy siyosat tartibi noqonuniy hisoblanadi va jiddiy muammolarga sababchi bo’ladi.

4. *Jazolar:* ma’lum tashkilotlarda qat’iy siyosatlar mavjud bo’lib, ularga amal qilinmaganda, xodimlarga nisbatan qator qarshi choralar qo’llaniladi.

5. *Yakuniy ishlanma:* tashkilot to’liq xavfsizlik siyosati hujjatlarini tasdiqlashi bilan ular tashkilotdagi barchaga tarqatiladi.

6. *Xodimlar tomonidan qabul qilinishi:* xavfsizlik siyosati tashkilot xodimlari tomonidan qabul qilinishi talab etilib, bunda xodimlar siyosatni batafsil ko’rib chiqadilar va imzolash asosida o’z roziliklarini bildiradilar.

7. *Siyosatini joriy qilish:* tashkilotda siyosatni amalga oshirish qo’shimcha joriy qilish vositalari yordamida bajariladi.

8. *Xodimlarni o’rgatish:* xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o’rgatilishi zarur va bu tashkilotdagi siyosatlar uzoq vaqt davomida foydalanilgan taqdirda ham yangi xodimlar uchun amalga oshirilishi shart. Bunda xodimlarni xavfsizlik siyosati bilan tanishtirib borishga muhim vazifa sifatida e’tibor berish talab etiladi.

9. *Ko’rish va yangilash:* tashkilot o’z faoliyatini uzoq vaqtdan beri amalga oshirayotgan bo’lsa ham, yangi texnologiyalarni kirib kelishi va yangi xavfsizlik muammolarini paydo bo’lishi xavfsizlik siyosatini yangilashni talab etadi. Xavfsizlik siyosatini yangilanmasligi himoya yaxshi amalga oshirilmasligiga sababchi bo’ladi va bu tashkilotga katta zarar yetkazishi mumkin.

Xavfsizlik siyosatini ishlab chiqish. Tashkilotlarda xavfsizlik siyosati maqsadini bilmasdan turib, uni amalga oshirish imkoniyati mavjud emas. Shuning uchun, xavfsizlik siyosatini loyihalashdan oldin, quyidagi savollarga javob berish talab etiladi:

- *Siyosatning maqsadi nima? Bu qo'shimcha xarajatmi yoki shunchaki rasmiyatchilikni?* Tashkilotlar yoki boshqaruvchi xavfsizlik siyosatini loyihalashda uning maqsadidan xabardor bo'lishi shart. Agar boshqaruvchi siyosatning maqsadini tushunsa, ularni xodimlarga yetkazishi oson bo'ladi.

- *Xavfsizlik biror o'quv dasturiga mos keladimi?* Odatda tashkilotlar xavfsizlik siyosatini xodimlarga o'rgatmasdan va amaliy seminarlarsiz joriy qiladi. Xodimlar xavfsizlik siyosatini o'rganmagan, ularni afzallik va kamchiliklari haqida ma'lumotga ega bo'lmagan taqdirda, xavfsizlik siyosati tashkilot uchun foydali bo'lmaydi. Shu sababli, xavfsizlik siyosati xodimlar tomonidan o'rganilishi shart.

- *Xavfsizlik siyosati tashkilot maqsadlari bilan mos keladimi?* Siyosatni hujjatlashtirish jarayonida uni tashkilot maqsadiga hamohang amalga oshirilganiga e'tibor berish shart. Agar xavfsizlik siyosati tashkilot maqadiga mos kelmasa, u muvaffaqqiyatga erisha olmaydi.

- *Siyosat yaxshiroq amaliyot uchun umumiy qoidalar bo'ladimi yoki u standartga asoslanishi kerakmi?* Taqdim qilinayotgan xavfsizlik siyosatining maqsadi turlicha bo'lishi mumkin. Shuning uchun, birinchi navbatda siyosat nima uchun joriy qilanayotganini bilish zarur. Odatda ma'lum siyosatlar hukumat tomonidan tartibga solinsa, ayrimlari tashkilot shaxsiy xavfsizligi uchun amalga oshiriladi.

- *Ushbu xavfsizlik siyosati nechta kishiga tegishli bo'ladi? Ular kimlar?* Xavfsizlik siyosatini loyihalashda ba'zida kam sonli xodimlar yoki ularning gruppasi talab etilishi mumkin. Bu turdagi xavfsizlik siyosatini tasniflash muhim bo'lib, ular tashkilotda soddalik bilan amalga oshiriladi.

- *Har bir xodim kamida nimani bilishi kerak?* Barcha xodim siyosatni hamma vaqt qanday amalga oshirish kerakligini bilishi kerak.

- *Haqiqatdan ham ushbu siyosatda yozilgan barcha tavsilotlar kerakmi yoki u AT xodimi uchun maxsus yozilganmi?* Siyosatni shakllantirishda maqsadni anglash muhim hisoblanib, bunda har bir siyosat bir hujjatni qismi bo'lishi shart emas.

- *Siyosatni qanday qilib semantik tashkil qilish mumkin?* Siyosat aniq va qisqa tarzda shakllantirilishi hamda unda tashkilotdagi bor bo'lgan va xodimlar amal qiladigan barcha joiz amallar mavjud bo'lishi shart.

- *Xodimlar siyosatdan nimani tushunishlari kerak?* Boshqaruvchi siyosatini xodimlar uchun tushunarli qilib shakllantirishida maqsadni aniqligini saqlab qolishi shart. Masalan, siyosat tashkilotdagi barchaga tegishli bo'lishi mumkin va bu holatda boshqaruvchi tomonidan turli seminarlarda xodimlar uchun tushuntirishlar berilishi shart. Bu esa tashkilotdagi har bir xodim o'zini xavfsizlik siyosatidagi bajarishi kerak bo'lgan vazifasini anglashiga katta yordam beradi.

Xavfsizlik siyosatini loyihalash. Xavfsizlik siyosatining tuzulmasi o'zida xavfsizlik vazifalarining umumiy ko'rinishini mujassamlashtiradi, xususan:

- foydalaniladigan siyosat tavsifi;
- siyosat holati haqidagi tavsilotlar va siyosat qo'llanilgan domenlar tavsifi;
- siyosatga jalb qilingan xodimlarning vazifalari va javobgarliklari;
- siyosat tashkilot standartlariga qaysi darajada mos kelishi;
- siyosatga tegishli va tegishli bo'lmagan vazifalar va muolajalar;
- agar siyosat tashkilot standartlariga mos kelmagan taqdirda olib keladigan oqibatlari.

Xavfsizlik siyosati tashkilot ish jarayonini muvaffaqiyatli amalga oshirishi uchun kerak bo'lgan barcha axborotdan iborat bo'lishi kerak. Xavfsizlik siyosatini loyihalash davomida quyidagi muhim jihatlarga e'tibor berish kerak:

- *tadbiq etish rejalashtirilgan siyosatlarni ishlab chiqish:* real vaqt rejimida xavfsizlik siyosatida keltirilgan barcha ko'rsatmalarni bajarish tarmoqdan foydalanishni cheklashda zarur hisoblanadi;

- *siyosatni maqsadini tushuntirish:* tashkilotning vazifalariga asoslangan holda, maxsus tarmoq maqsadlari uchun siyosatni ishlab chiqish;

- *qisqa vaqtda yangilanishni talab etmaydigan xavfsizlik siyosatini ishlab chiqish:* xavfsizlik siyosatini qisqa vaqtda qayta yangilanishni talab etmasligi uchun, umumiy tarmoq muammolarini oldindan hisobga olish talab etiladi;

- *siyosatlar, standartlar va tavsiyalarni ajratish:* xavfsizlik siyosatlari tushunarli, batafsil bo'lishi va shuning bilan birga juda ham qat'iy bo'lmasligi shart;
- *tashkilotni asosiy maqsadini taqdim qilish:* axborotga bog'liq holda, tashkilotning aktivlari tarmoq xavfsizligi ko'lamini ko'rsatadi;
- *siyosatni tushunarli ekanligiga ishonch hosil qilish:* tarmoq xavfsizligi sodda va shu bilan birga tushunarsiz bo'lmasligi kerak;
- *tashkilot siyosati xavfsizlikka oid treyninglarning bir qismi bo'lishi:* kamida bir xavfsizlik siyosati tashkilotdagi xavfsizlik treyningining bir qismi bo'lishi zarur;
- *kutilayotgan asosiy risklarni aniqlash:* tarmoqning asosiy risk faktorlari tarmoq administratori tomonidan oldindan hisobga olinishi shart.

Siyosatni amalga oshirilganligini tekshirish. Xavfsizlik siyosatini amalga oshirish uni shakllantirish, qayta ko'rib chiqish va yangilashdan so'ng bajariladi. Amalga oshirilgandan so'ng esa xavfsizlikning mos modeli va xulosasi yaratilishi shart. Xulosa manfaatdor tomonlarning takliflari tashkilot manfaatlari bilan bevosita bog'liqlikni ko'rsatishi shart. Xavfsizlik siyosati tugallangandan so'ng, uning oxirgi holati tashkilotdagi barcha xodimlarga tarqatilishi, zarur bo'lgan vaqtda xodimlar tomonidan foydalanish uchun joiz bo'lishi shart va shuning uchun takshilotning ichki tarmog'ida joylashtirilishi kerak.

Xavfsizlik siyosatini loyihalash va ishlab chiqish jarayonlaridan so'ng, uni foydalanishga tayyor holatga keltirish ham muhim hisoblanadi. Xavfsizlik siyosatini muvaffaqiyatli amalga oshirishdagi tavsiyalar:

- xavfsizlik siyosati tashkilotning tegishli rahbariyati tomonidan qo'llab-quvvatlanishi va rasmiy ravishda tashkilotning siyosati sifatida qabul qilinishini ta'minlash;
- har bir siyosatni ko'rib chiqish va tashkilot ichida qanday qo'llanilishi haqida o'ylash;
- siyosatga muvofiq bo'lgan mos vositalarning mavjudligiga ishonch hosil qilish;
- tarmoqni yoki siyosatni ixtiyoriy almashtirish kerakligi haqida rejani yaratish;

- siyosatni madadlashda muolajalarni o’rnatish uchun tashkilotdagi biror bo’lim (masalan, axborot texnologiyalari, axborot xavfsizligi va hak.) bilan ishlash;
- tashkilotni xavfsizlik bo’yicha asosiy o’quv seminar kurslari bilan ta’minlash;
- axborot aktivlaridan foydalanish huquqiga ega bo’lgan barcha xodimlar uchun xavfsizlik siyosatini taqdim etish;
- axborot xavfsizlik xodimi xavfsizlik siyosatini boshqarish va amalga oshirish uchun javobgar bo’lishi;
- xavfsizlik siyosatini mos boshqarish uchun tashkilotni zarur bo’lgan texnologiya va vositalar bilan ta’minlanganligiga ishonch hosil qilish;
- takshilotga tashrif buyuruvchilar uchun tarmoqdan foydalanish imkoniyati berilgan taqdirda, uni maqbul siyosat asosida amalga oshirish.

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 jihozning vazifasini tavsiflaydi.

Axborot texnologiyalari sohasidagi korxonalarda quyidagi xavfsizlik siyosatlari qo’llaniladi:

- *Tashkilot axborot xavfsizligi siyosati (Enterprise Information Security Policies, EISP):* mazkur siyosat turi tashkilotlar xavfsiz muhitini unga g’oya, maqsad va usullarni taklif qilish orqali qo’llab – quvvatlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish uchun usullarni belgilaydi. Bundan tashqari, ushbu siyosatlar taklif etilgan va talab qilingan axborot xavfsizligi tuzilmasi talablarini kafolatlaydi.

- *Muammoga qaratilgan xavfsizlik siyosatlari (Issue-Specific Security Policies, ISSP):* bu siyosatlar tashkilotdagi aynan bir 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, foydalanuvchilarni kirish huquqini avtorizasiyalash uchun zarar 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 maqsad qiladi. Bunda tashkilotlar tizimni qo’llab-quuvatlash maqsadida muolajalar va standartlarni o’z ichiga olgan SSP 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 foydalanuvchilarni 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 cheklanishni 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 bo’lish mumkin:

1. *Tartibsiz siyosat (Promiscuous Policy):* ushbu siyosat tizim resurslaridan foydalanishda hyech qanday cheklovlarni amalga oshirmaydi. Masalan, bu siyosatga ko’ra foydalanuvchi istalgan saytga kirishi, istalgan dasturni yuklab olishi, masofadagi kompyuter yoki tarmoqdan foydalanishi mumkin bo’ladi. Bu siyosat korporativ tashkilotlarning ofislarida ishlovchi yoki tashkilotda 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 ciyosatga ko’ra faqat xavfli xizmatlar/ hujumlar yoki harakatlar bloklanadi. Masalan, ruxsat

berishga asoslangan Internet siyosatida qator keng tarqalgan zararli xizmatlar/ hujumlardan tashqari Internet trafigining asosiy qismi ochiq bo'ladi. Faqat ken tarqalgan hujumlar va zararli dasturlar bloklangani uchun, administrator 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 hamma narsa bloklanadi 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 qiladi.

4. *Ehtiyotkorlik siyosati (Prudent Policy):* Ehtiyotkorlik siyosati barcha xizmatlar bloklangandan so'ng amalga oshirilib, unda administator tomonidan xavfsiz va zarur xizmatlarga individual ravishda ruxsat beriladi. Bu maksimal xavfsizlikni ta'minlab, tizim/ tarmoq faoliyatiga oid barcha hodisalarni qayd qiladi.

Maqbul foydalanish siyosati. Maqbul foydalanish siyosati tarmoq va veb sayt egalari tomonidan qaror qilingan qoidalardan iborat bo'ladi 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, foydalanuvchi 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 uchun imzo olishadi. Maqbul foydalanish siyosati foydalanuvchilarni

axborot texnologiyalari infratuzilmasida 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 administrator 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.

7.3. Risklarni boshqarish

Risk kiberxavfsizlikka oid bo’lgan tushunchalardan biri bo’lib, u haqidagi dastlabki tushunchalar birinchi bobda keltirib o’tilgan edi. Ushbu bo’limda risk tushunchasi va uni boshqarish bo’yicha batafsil ma’lumotlar beriladi.

Risk bu – belgilangan sharoitlarda tahdidning manbalarga potensial zarar yetkazilishini kutish. Bundan tashqari, riskni quyidagicha tushunish mumkin:

- *Risk* bu – ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo’qotilishi yoki boshqa salbiy ta’sir ko’rsatishi mumkin bo’lgan voqyea.
- *Risk* bu – manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta’sirida tahdid bo’lishi ehtimoli.
- *Risk* bu – voqyea 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 tasvirlash mumkin:

$$\text{RISK} = \text{Tahdid} \times \text{Zaiflik} \times \text{Ta'sir}.$$

Boshqa tomondan, hodisaning axborot aktiviga ta’siri bu – aktivdagi yoki manfaatdor tomonlar uchun aktivning qiymatidagi zaiflikning natijasi ekanligini inobatga olgan holda, riskni quyidagicha ifodalash mumkin:

$$\text{RISK} = \text{Tahdid} \times \text{Zaiflik} \times \text{Aktiv qiymati}.$$

Risk o’zida quyidagi ikkita faktorni mujassamlashtiradi:

- zararli hodisani yuzaga kelish ehtimoli;
- va zararli hodisaning oqibatlari.

Riskning ta'siri. Risk normal amalga oshirish jarayoniga va loyiha narxiga yoki kutilgan qiymatga ta'sir yetadi. Risk ta'siri tashkilot, jarayon yoki tizimga zararli muhit sababli yuzaga keladi. Ta'sir riskni kuzatilish ehtimoli jiddiyligini ko'rsatadi.

Riskning chastotasi. Riskni aniqlash va baholashga bog'liq holda, risklarni tasniflashda ularning takrorlanish chastotatasiga va ko'p sonli ketma-ketliklarga asoslanadi. Chastota va ko'p sonlilik risklarni monitoring qilishda muhim hususiyat hisoblanib, shu nuqtai nazaridan risklar ikki guruhga: *minor risklar* – e'tibor talab qilmaydigan va *major risklar* – alohida e'tibor va kuzatuv talab qiluvchilarga ajratiladi. Risklar chastotasi va ko'p sonligiga asoslangan holda ularni ikki o'lchamli matrisa usuli yordamida guruhlarga ajratish mumkin.

Riskning darajalari. Risk darajasi tarmoqda (yoki tizimga) natijaviy ta'sirning bahosi bo'lib, risk chastotasi va uning ko'p sonligiga ko'ra risklarni darajaga ajratishning ko'plab usullari mavjud. Ulardan eng keng tarqalgan usullaridan biri bu – ikki o'lchamli matrisa usulidir.

Risklarni tahlil qilishda, chastota yoki mojaro kuzatilishi va natijasining ehtimoli bilan ishlash talab etiladi. Bu esa risk darajasini ifodalaydi. Risk quyidagi tenglik bilan ifodalanadi:

$$\text{Risk darajasi} = \text{natija} \times \text{ehtimollik}.$$

Risk darajalari 4 ta: ekstirmal yuqori, yuqori, o'rta va past, bo'lishi mumkin.

Ekstrimal yuqori yoki *yuqori* risk paydo bo'lishini va salbiy ta'sirini kamaytirish uchun 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 xavfni olib keladi va shuning uchun, zudlik bilan aniqlash hamda qarshi chora ko'rishni talab qiladi.

O'rta darajali risklar yuqori ehtimollikka ega past natijali hodisa yoki past ehtimollikka ega yuqori natijali hodisa bo'lishi mumkin. Alohida qaralganda 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 xarajatni keltirib chiqarmaydi.

Risk matrisasi 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 matrisasi riskning ortib boruvchi ko’rinishi uchun foydalaniluvchi sodda jarayon bo’lib, qarshi choralarni ko’rishda yordam beradi. Risk matrisasi risklarni turli darajalarda aniqlash va jiddiylik nuqtai nazaridan guruhlash imkonini beradi. Bundan tashqari, har bir tashkilot tomonidan amalga oshiriladigan risklarni o’lchash usullari ham mavjud (93-rasm).

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

93-rasm. Risk matrisasi

Yuqorida taqdim etilgan risk matrisasi risklarni vizual taqdim etish va o’zaro taqqoslash imkonini berib, undagi har bir yacheyka ehtimollik va oqibat kattaliklarining kombinasiyasidan iborat bo’ladi. Riskning jiddiyligi uning ehtimoli va ta’sir darajasiga bog’liq bo’ladi. Keltirilgan risk matrisasida 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 bu – risklarni aniqlash, baholash, javob berish va potensial ta’sirga tashkilot tomonidan qanday javob berilishini amalga oshirish jarayoni. Risklarni boshqarish xavfsizlikning hayotiy siklida o’zining muhim o’rniga ega bo’lib, u davomiy va hattoki murakkablashib boruvchi jarayon hisoblanadi. Risklar turli tashkilotlar uchun turlicha bo’lsada, risklarni boshqarishga tayyorgarlik ko’rish barcha tashkilotlar uchun umumiy bo’ladi. Risklarni boshqarishdan asosiy maqsad quyidagilar:

- potensial risklarni aniqlash;
- risk ta’sirini aniqlash va tashkilotlarga yaxshiroq risklarni 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, tahlil qilish va aniqlangan risk hodisalarini qayd etish;
- risklarni nazorat qilish va risk ta’siriga qarshi kurashish;
- xavfsizlik xodimlarini ogohlantirish va risklarni boshqarish strategiyasini ishlab chiqish.

Risklarni boshqarish risklarni aniqlashda tizimlashgan yondashuvni ta’minlaydi va quyidagi afzalliklarga ega:

- potensial 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 bajaruvchilar o’rtasida quyidagicha taqsimlangan:

– *Bosh boshqaruvchi.* Bosh boshqaruvchi tashkilotda risklarni boshqarish jarayonini olib borishga rahbar hisoblanib, u risk paydo bo’lganga ularni aniqlash

uchun talab qilinadigan siyosat va usullarni ishlab chiqadi. Bundan tashqari, kelajakda bo'lishi mumkin bo'lgan risklarni tutib olish uchun zarur bo'lgan 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 bo'lib, risklarni boshqarishdagi asosiy reja va siyosatlarda muhim rol o'ynaydi. Ushbu lavozim egasi uchun asosiy javobgarliklar bu – xodimlarni xavfsizlik bo'yicha o'qitish hamda axborot texnologiyalarida bo'lishi mumkin bo'lgan risklarni va ularni biznes jarayonlariga ta'sirini boshqarishdan iborat.

– *Tizim va axborot egalari.* Tizim va axborot egalarining vazifasi asosan axborot tizimlari uchun ishlab chiqilgan rejalar va siyosatlarni monitoring qilib 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 ularni ta'sirlarini tadqiq qilish;
- barcha tizimlar uchun xavfsizlik holati bo'yicha hisobotlarni tayyorlash;
- axborot tizimlarini himoyalash uchun zarur bo'lgan xavfsizlik nazoratlarini yangilab borish;
- doimiy ravishda xavfsizlikka oid hujjatlarni yangilab borish;
- mavjud xavfsizlik nazoratini o'zining samaradorligini ta'minlashi bo'yicha tekshirish va baholash.

– *Biznes va funksional menedjerlar*. Mazkur lavozim egalari tashkilotdagi barcha boshqaruv jarayonlarini madadlash uchun javobgar bo'lib, bu vazifani bajarishida tashkilot rahbariyati tomonidan qo'llab quvvatlanadi. Funksional menedjeri quyidagilarni anglatadi:

- rivojlantirish jamoasi menedjeri;
- savdo menedjeri;
- mijozlarga xizmat ko'rsatuvchi menedjer.

– *AT xavfsizlik dasturi menedjerlari va kompyuter xavfsizligi bo'limi direktori*. Ushbu lavozim egalari tizimni himoyalashda xavfsizlik nazoratlarini tanlash orqali axborot tizimi egalarini qo'llab quvvatlaydi. Ushbu lavozim egalari tashkilotda xavfsizlik nazoratini tanlashda va tuzatishda muhim ro'l o'ynaydi.

– *AT xavfsizlik amaliyotchilari*. AT xavfsizlik amaliyotchilari tashkilotda shaxsiy, fizik va axborot xavfsizligini amalga oshiradilar va ular quyidagilarga javobgar:

- tashkilotda yaxshiroq xavfsizlik 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 qayd qilish;
- tashkilotda xavfsizlik uchun rol va javobgarliklarni belgilash;
- tashkilotdagi barcha xavfsizlik o'lchovlarini nazorat qilish.

– *Xavfsizlik bo'yicha murabbiy*. Xavfsizlik bo'yicha murabbiy tashkilotdagi tayyorgarlik va o'quv kurslarini amalga oshiradi. Bu vazifani odatda soha mutaxassislari tomonidan bajarilishi tavsiya etiladi.

Muhim risk ko'rsatkichlari. Muhim risk ko'rsatkichlari risklarni samarali boshqarish jarayonida muhim 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 bo'lib, 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 muhim amalga oshirish ko'rsatkichlariga salbiy ta'sirlarni aks ettirishi kerak. Bu yerda, tashkilotning muhim amalga oshirish ko'rsatkichi tashkilotni o'zining maqsadalariga erishish jarayonini baholash ko'rsatkichi hisoblanadi.

Risklarni boshqarish bosqichlari. Risklarni boshqarish uzluksiz jarayon bo'lib, har bir bosqichda muvaffaqqiyatli amalga oshirilishni talab etadi. U aniqlangan va faol ishlaydigan xavfsizlik dasturidan foydalangan holda xavfni maqbul darajada oldini oladi. Risklarni boshqarish quyidagi asosiy to'rtta bosqichga bo'linadi:

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. Quyida ushbu bosqichlar bilan yaqindan tanishib chiqiladi.

Risklarni aniqlash. Risklarni boshqarishdagi dastlabki qadam bo'lib, uning asosiy maqsadi riskni tashkilotga zarar yetkazmasdan oldin aniqlash hisoblanadi. Risklarni aniqlash jarayoni mas'ul mutaxassislar qobiliyatiga bog'liq bo'lganligi sabab, ular turli tashkilotlar uchun farq qiladi. Risklarni aniqlash o'zida tashkilot xavfsizligiga ta'sir qiluvchi ichki va tashqi risklarning manbasini, sabablarini, natijasini va boshqalarni aniqlashni mujassamlashtirgan. Risklar odatda quyidagi 4 ta muhim sohalardan kelib chiqadi:

- *Muhit.* Muhitga aloqador bo'lgan risklar o'zida ish joyidagi kamchiliklar, turli xalaqitlar, issiq/ sovuq muhit, tutun, past yoritilganlik va elektr xavflari kabilarni birlashtiradi.
- *Jixoz.* Jixozga aloqador risklar sifatida jixozlarning past ta'mirlash muhiti, ishlamaslik, mavjud bo'lmaslik 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'ladi.

Risklarni aniqlash jarayoni ikki bosqichda amalga oshiriladi:

- *kontekstni belgilash:* xodim ichki va tashqi muhitni va tashkilot faoliyatidagi joriy holatni aniqlaydi;
- *risklarni sanash:* bo'lishi mumkin bo'lgan risklarni va ular sababli kutilayotgan natijalar aniqlanadi.

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 bo'lib, ular asosida turli dasturiy vositalar ishlab chiqilgan. Ko'plab risklarni aniqlash jarayonlari maxsus shakllantirilgan jamoa tomonidan amalga oshiriladi. Risklarni aniqlash jarayoni bir qancha faktorlarga, masalan, tarmoqning holati va jamoa a'zolarini risklarni boshqarishdagi qobiliyatlariga asoslanadi.

Riskni baholash. Risklarni baholash bosqichida tashkilotdagi risklarga baho beriladi va bu risklarning ta'siri yoki yuzaga kelish ehtimoli hisoblanadi. Risklarni baholash uzluksiz davom etuvchi jarayon bo'lib, riskka qarshi kurashish va rejalarni amalga oshirish uchun imtiyozlarni belgilaydi. Risklarni baholash ularning miqdor va sifat qiymatini aniqlaydi. Har bir tashkilot risklarni aniqlash, darajalarga ajratish va yo'q qilish uchun o'zida riskni baholash jarayonini qabul qilishi kerak.

Riskni baholash taqdim etilgan risk turini, riskning ehtimoli va miqdorini, uning darajasini hamda uni nazoratlash uchun rejani aniqlaydi. Tashkilotlar risklarni baholash jarayonini odatda xavf aniqlanganda va uni zudlik bilan nazoratlay olmaganlarida amalga oshiradilar. Riskni baholashdan so'ng ma'lum vaqt oralig'i bilan barcha axborot vositalarini yangilash talab etiladi.

Risklar baholangandan so'ng, ular miqdor va tashkilotga keltiradigan zarariga ko'ra darajalanadi. Darajalarga ajratish risklarga qarshi kurashishga va resurslarni joylashtirishga yordam beradi. Taqdim etilgan risklarning darajalari ularning miqdoriga bog'liq bo'ladi:

1-2: darajasi 1-2 ga teng bo'lgan risklarni zudlik bilan bartaraf etish talab etiladi yoki bartaraf etish imkoni bo'lmasa, nazorat harakatlari orqali uning xavflilik darajasini tushirish talab etiladi.

3-4: darajasi 3-4 ga teng bo’lgan risklarni o’ylangan biror vaqt oralig’ida bartaraf etish yoki xavfni nazoratga olish zarur hisoblanadi.

5-6: mazkur darajaga ega risklarni imkoni bor bo’lgan vaqtda bartaraf etish yoki imkoni bo’lsa xavfni nazoratga olish zarur.

Risklarni baholash quyidagi ikki bosqichdan iborat:

Riskni tahlil qilish: risk tabiatini aniqlash va uni paydo bo’lish darajasini hisoblash bosqichi bo’lib, u risklarni nazoratlashga yordam beradi.

Riskni darajalarga ajratish: risklarni tahlil qilish jarayonida ularning miqdoriy jixatdan reytingini aniqlash va qarshi choralarni loyihalash bosqichi hisoblanadi.

Risklarni bartaraf etish. Risklarni bartaraf etish jarayoni aniqlangan risklarni modifikasiyalash maqsadida mos nazoratni tanlash va amalga oshirishni ta’minlab, bunda 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, bunda risklarni individual ravishda yo’q qilish, monitoring qilish 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 usulini 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 usullaridan foydalanish riskdan qochish, ularni kamaytirish va ular uchun javobgarliklarni boshqaga o’tkazish kabi imkoniyatlar taqdim qiladi.

Xodimlar risklarni kamaytirish yoki minimallashtirish uchun quyidagilarni amalga oshirishi talab etiladi:

- riskni nazoratlash rejasini ishlab chiqish;
- ko’rsatilayotgan xizmatga riskni ta’sirini aniqlash;
- riskni nazoratlash rejasini tamomlash uchun qat’iy cheklovlarni qo’yish;
- risklarni nazoratlash strategiyasini amalga oshirish;
- risklarni nazoratlashda mijoz harakatini aniqlash;
- risklarni nazoratlash daravomida madadlovchi xodimlar/ ishchilar bilan aloqani o’rnatish;
- risklarni nazoratlash jarayonining bir qismi sifatida risklarni nazoratlash rejasini to’liq hujjatlashtirish.

Tashkilotda risklarni boshqarish freymvorki (Enterprise Risk Management Framework, ERM Framework). Risklarni boshqarish freymvorki tashkilotning risklarni boshqarish usuliga xos bo’lgan amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo’yicha faoliyatni birlashtiruvchi tarkibiy jarayonni ta’minlaydi. Tashkilotda risklarni boshqarish freymvorki quyidagi harakatlarni aniqlaydi, tahlil qiladi 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 freymvorkining 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 aniqlash;
- 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 boshqarishning doirasi va ilovalarini o’rnatish;
- tashkilotda risklarni boshqarishni takomillashtirish uchun vaqti-vaqti bilan tekshirishni amalga oshirish.

Amalda tashkilotda risklarni boshqarish freymvorklari sifatida NIST ERM, COSO ERM va COBIT ERM kabilardan keng qo'llaniladi.

Risklarni boshqarishning axborot tizimlari (Risk Management Information Systems, RMIS). RMIS bu – boshqaruv axborot tizimi bo'lib, axborotni saqlashni boshqarish, tahlil qilish 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 freymvorkini birlashtiradi. RMIS tizimlari quyidagi afzalliklarga ega:

- ma'lumot ortiqchaligi va xatoligini kamaytirish orqali ma'lumot ishonchligini yaxshilaydi;
- RMIS orqali xabarlar boshqaruvining yaxshilanishi natijasida tashkilotdagi xarajatlarni kamaytiradi;
- RMIS tashkilotning standartlariga muvofiq ravishda, ularga risklarni boshqarish siyosatidan samarali foydalanishda yordam beradi.

RMIS turli omillar bo'yicha hisobotlarni hosil qiladi 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 hosil qiladi:

- *Standart hisobotlar:* yuborilgan umumiy so'rovlarga javob sifatida RMIS standart hisobotlarni hosil qiladi. Ushbu hisobot guruhga ajratilgan ma'lumotlardan tashkil topmaydi.
- *Maxsus hisobotlar:* bundan tashqari RMIS tizimi maxsus so'rovlarga nisbatan maxsus javoblarni generasiya qiladi va ular turli guruhga tegishli ma'lumotlardan tashkil topgan bo'ladi.

Amalda RMIS tizimining turli ko'rishdagi 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. Arxitektura va tizim arxitekturasi tushunchalariga izoh bering?
2. Tizim arxitekturasi turlariga misollar keltiring?

3. Tizimlar arxitekturasining asosiy fundamental prinsiplarini ayting va ularni tushuntiring?

4. Virtual mashinaga ta’rif bering va uning asosiy vazifalarini tushuntiring?

5. Virtual mashinalardan qaysi maqsadlarda foydalaniladi?

6. Narsalar Interneti tushunchasiga ta’rif bering va uning hozirgi kundagi ahamiyatini tushuntiring.

7. O’rnatilgan tizimlar nima va ularning asosiy vazifalari nimadan iborat?

8. Axborot xavfsizligi siyosati nima va uning asosiy vazifasi nimadan iborat?

9. Xavfsizlik siyosati nima uchun zarur?

10. Xavfsizlik siyosatining tarkibi va tuzulishi haqida ma’lumot bering?

11. Xavfsizlik siyosatining asosiy turlarini ayting?

12. Internetdan foydalanish siyosati haqida ma’lumot bering?

13. Risk tushunchasiga izoh bering?

14. Risk darajasi tushunchasiga izoh bering?

15. Risk matrisasi va uning asosiy vazifasini tushuntiring?

16. Risklarni boshqarish nima va uning asosiy bosqichlarini ayting?

17. Tashkilotda risklarni boshqarish freymvorki nima va uning asosiy vazifasini ayting?

18. Risklarni boshqarishning axborot tizimlari nima va ularga misollar keltiring.

8 BOB. KIBERJINOYATLARNING INSON XAVFSIZLIGIGA TA’SIRI

8.1. Kiberjinoyatchilik, kiberhuquq va kiberetika

8.1.1. Kiberjinoyatchilik

Kiberjinoyatchilik bu – kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat turi bo’lib, uning eng keng tarqalgan turlari - kompyuter qaroqchiligi, onlayn firibgarlik, kompyuter tizimlariga hujum qilish, shaxsiy ma’lumotlarni o’g’irlash va noqonuniy yoki taqiqlangan ma’lumotlarni tarqatish.

Kiberjinoyatni amalga oshirganda quyidagilar asosiy maqsad sifatida qaraladi:

- pul, qimmatli qog’ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko’chmas mulk, yoqilg’i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy olish;
- soliq va turli yig’imlarni to’lashdan bosh tortish;
- jinoiy daromadlarni legallashtirish;
- qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuqlar uchun kassa chiptalarini qalbakilashtirish yoki tayyorlash;
- shaxsiy yoki siyosiy maqsadlarda maxfiy ma’lumotlarni olish;
- ma’muriyat yoki ishdagi hamkasblardan shaxsiy dushmanlik munosabatlari uchun qasos olish;
- shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish;
- mamlakatdagi vaziyatni, hududiy ma’muriy tuzulishni beqarorlashtirish yoki siyosiy maqsadlar uchun tartibga solish;
- talonchilik, raqibni yo’q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ishining tartibini buzish;
- boshqa turdagi jinoyatlarni yashirish uchun;
- tadqiqot masalalarida;
- shaxsiy intelektual qobiliyat yoki ustunlikni namoyish qilish uchun.

Kiberjinoyatlar hajmini keskin oshishiga quyidagilar motiv bo’lib xizmat qilmoqda:

- moliyaviy qiyinchilikdan chiqish;
- jinoyatchidan bo’lgan qarzdorlikni kechikmasdan jamiyatdan olish;
- kompaniyadan va ish beruvchidan o’ch olish;
- o’zini tengsizligini ko’rsatish uchun.

Kiberjinoyatchilikning turlari. Kiberjinoyat turlarini qat’iy bir tasniflashning imkoni yo’q. Quyida kriminologiya sohasida aloqador holda 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 miliionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik bo’lib, u asosan bank hisobraqamlari 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 hisobvarag’i ma’lumotlarini olish va noqonuniy foydalanish bilan, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog’liq.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlari va erkinliklariga qarshi 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 huquqi) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo’qotishlarni olib keladi.

“Maykrosoft Armaniston” kompaniyasining direktori Grigor Barsegyanning takidlashicha, “kompyuter qaroqchiligi” ishlab chiqaruvchilarga yetkazgan zarari yiliga 66 milliard dollarni tashkil qiladi. Uning so’zlariga ko’ra Armanistonlik istemolchilar o’zlarining moliyaviy resurslarini tejash uchun viruslarni yuqtirish xavfi yuqori bo’lgan dasturlardan ongli ravishda foydalanadilar.

Kompyuter jinoyatchiligining oxirgi turi jamoat yoki davlat xavfsizligiga qarshi kompyuter jinoyatchiligi bo'lib, ularga davlat yoki jamoat xavfsizligiga qaratilgan jamoat uchun xavfli bo'lgan xatti - harakatlar kiradi. Ular ko'pincha ma'lumot uzatish qoidalarini buzilishi, mamlakat mudofaa tizimining yoki uning tarkibiy qismlarining buzilishi bilan bog'liq bo'ladi.

8.1.2. Kiberetika

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, veb-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 siqish 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 kinolar) intelektual mulk huquqlariga rioya qilinmasdan ommaga tarqalmoqda. Masalan, aksariyat katta mablag’ sarflangan kinolarning “peratiskiy” versiyasi chiqishi natijasida, o’z sarf xarajatini qoplay olmaslik holatlari kuzatilmoqda.

Bu holatni dasturiy ta’minotlar uchun ham ko’rish mumkin. Masalan, aksariyat dasturlar lisenziyaga ega hisoblansada, turli usullar yordamida ularning “crack” qilingan versiyalari amalda keng qo’llaniladi. Masalar, lisenziyaga 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, ko’plab insonlar lisenziyali CD diskni sotib olsam, undan ko’chirish imkoniyatiga ham ega bo’lishim kerak deb fikrlaydilar.

Xavfsizlik. Internet tarmog’idagi axborotdan foydalanganda xavfsizlik anchadan beri axloqiy munozaralar mavzusi bo’lib kelmoqda. Bu birinchi navbatda jamoat faravonligini himoya qilish yoki shaxs huquqini himoya qilish degan savolni o’rtaga qo’yadi. Internet tarmog’ida foydalanuvchilar sonini ortishi, shaxsiy ma’lumotlarni ko’payishi natijasida ularning o’g’irlanishi va kiberjinoyatlar soni ortmoqda.

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

Foydalanuvchanlik, senzura va filterlash. Foydalanuvchanlik, senzura va axborotni filterlash 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 filterlash asosida ushbu ma'lumotni tarqalishini oldini olish, foydalanuvchanligiga ta'sir qilish 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, ta'sirlangan mamlakat, jamiyat yoki madaniyatga ta'sir ko'rsatadigan cheklovlarga bog'liq. Cheklovlar turli ko'rinishlarda bo'lishi mumkin. Masalan, ayrim mamlakatlarda Internet ommaviy axborot vositalariga kirishning bir shakli hisoblanib, undan barcha davlat rezidentlari foydalanadi. Bundan tashqari, ayrim davlatlarda Internetdan foydalanish bo'yicha cheklovlar bir davlatning 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 doim axloqiy munozaralarga sabab bo'lgan. Ayrim davlatlarda bunday kontentlardan foydalanish qattiq taqiqlansa, ayrim davlatlarda bunga ruxsat berilgan.

Qimor o'yinlari. Bu muammo ham etik masaladagi munozaralardan biri bo'lib, uni kimlardir zarar deb hisoblasa, yana kimlardir ularga qonun aralashuvini yoqtirmaydigan. 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, qolganlariga qat'iy cheklovlar mavjud.

Kompyuterlan foydalanish etikalari. Kompyuter etikasi instituti notijoriy tashkilot bo'lib, vazifasi texnologiyani axloqiy nuqta nazardan 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 odamlarning kompyuter fayllariga qaramang;
- o'g'irlik uchun kompyuterdan foydalanmang;
- yomonlik uchun kompyuterdan foydalanmang;
- o'z pulingizga sotib olmagan dasturdan foydalanmang va nusxa ko'chirmang;
- birovni kompyuterini ruxsatsiz foydalanmang;
- birovlarni intellektual mehnati samarasiga zarar yetkazmang;
- siz yaratgan dasturni 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 besh tamoilga asoslanadi. Ushbu talablar AQSh sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligin 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 bitta 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 ular belgilangan maqsadlar uchun foydalanilishini ta'minlash va ulardan boshqa maqsadlarda foydalanilishiga qarshi choralar ko'rishi kerak.

8.1.3. Kiberqonunlar

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 Konstitusiyasiga 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, konstitusiyaviy 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 kommunikasiyalarning 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 voqyealar, 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 telekommunikasiyalar tizimlariga integrasiyalashuvi;

O’zbekiston Respublikasining konstitusiyaviy 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 kodeks:

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.

8.2. Inson xavfsizligi

8.2.1. Sotsial injineriya

Ijtimoiy (sosial) injineriya - turli psixologik usullar va firibgarlik amaliyotining to’plami bo’lib, uning maqsadi firibgarlik yo’li bilan shaxs to’g’risida maxfiy ma’lumotlarni olish hisoblanadi. 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 bo’lib, *xaker* - kompyuter tizimidagi zaifliklarni qidiradigan odam, boshqacha aytganda – “buzg’unchi”. Hozirgi vaqtda xakerlar har qanday tizimdagi asosiy zaiflik bu - mashina yemas, balki shaxs yekanligini 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” boshladilar. Gohida ular “aql xakerligi” deb ham ataladi.

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, akangizni 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 lichka ham bo’lishi mumkin) men akangman deb tanishtiradi va o’zini ko’chada bezorilarga duch kelganini, ular barcha narsalarini (telefon, pul, plastik kartochka va boshqalar) 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 20000 so’m pulni ko’chirib berishni talab qiladi. Mazkur holatlarning 8/10 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, sizning ovozni aniqlashangiz yanada qiyinlashadi.

Ushbu holatda xaker tomonidan foydalanilgan fikrlarni ko’rib chiqaylik:

1. Shaxsni 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 katta mexanizmidan foydalanilgan – achinishga ta’sir qilingan (hissiyotlarga murojaat qilish).

8.2.2. Sosial injineriya yo’nalishlari

Sosial 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 sosial injineriya uchun samarali vosita bo’lib qolmoqda. Telefonda gaplashayotganda, suhbatdoshning shaxsini tasdiqlashning imkoni yo’q. Bu hujumchilarga xodimga, xo’jayinga maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonish mumkin bo’lgan har qanday shaxsni o’rniga bo’lish imkonini beradi. Bunda, zo’ravonlik qurbonini “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, xatolar orqali pulni qaytarish to’g’risida 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 nomalum havolalarga e’tibor bermaslik.

Elektron pochta bilan bog’liq tahdidlar. Ko’pgina xodimlar har kuni korporativ va shaxsiy pochta tizimlarida o’nlab, hatto yuzlab elektron pochta xabarlarini qabul qilishadi. Albatta, bunday yozishmalar oqimi bilan har bir harfga etarlicha 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 qiladi va xabarlarni qabul qilishda xotirjam bo’lishadi. Tajovuzkor pochta orqali oddiy so’rov yuborganda, uning qurboni ko’pincha uning xatti-harakatlari haqida o’ylamasdan ular so’ragan narsani 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. Agar buzg'unchi tomonidan yuborilgan giperhavolani bosish orqali foydalanuvchi zararli dasturni korporativ tarmoqqa yuklasa, bu 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 kiruvchi elektron pochta xabarlariga shubha bilan qarash. Ushbu yondashuvni butun tashkilotda tarqatish uchun quyidagi elementlarni o'z ichiga olgan xavfsizlik siyosatiga elektron pochtadan foydalanishning aniq prinsiplari kiritilishi kerak:

- hujjatlarga qo'shimchalar;
- hujjatdagi giperhavolalar;
- shaxsiy yoki korporativ ma'lumotlarni kompaniya ichiga 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 potensial 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 bo'lib, unda har qanday nomlarni moslashtirish qobiliyati bilan bir qatorda, bu omil tajovuzkorni boshqa odam bo'lib ko'rsatishga imkon beradi. Bu esa muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada oshiradi. Agar kompaniya tezkor xabarlar sababli keladigan xarajatlarni

kamaytirish va boshqa afzalliklardan foydalanmoqchi bo’lsa, korporativ xavfsizlik siyosatida tegishli tahdidlardan himoya qilish mexanizmlarini ta’minlash kerak. Korporativ muhitda tezkor xabar almashish ustidan ishonchli boshqaruvga ega bo’lish uchun bir nechta talablar bajarilishi shart:

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

Sosial injineriyaning mutaxassislari tomonidan tashkilotlar uchun quyidagi asosiy himoya usullarini qo’llash tavsiya etiladi:

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

Sosial 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 resurslarga kirishni cheklaydigan to’siqlar. Shuni 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 tahlil qilish va ma'lumotlarni himoya qilish choralarini rejalashtirishda qog'oz, elektron ma'lumotlar tashuvchilar bilan ishlash tamoyillarini aniqlash kerak.

- *Ilovalar* - foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofingizni himoya qilish uchun tajovuzkorlar elektron pochta dasturlari, tezkor xabarlar xizmati va boshqa dasturlardan qanday foydalanishlari mumkinligini ko'rib chiqishingiz kerak.

- *Kompyuterlar*. Tashkilotda ishlatiladigan serverlar va mijoz tizimlari. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini ko'rsatadigan qat'iy tamoyillarni belgilab, foydalanuvchilarni o'zlarining kompyuterlariga to'g'ridan-to'g'ri hujumlardan himoya qilish.

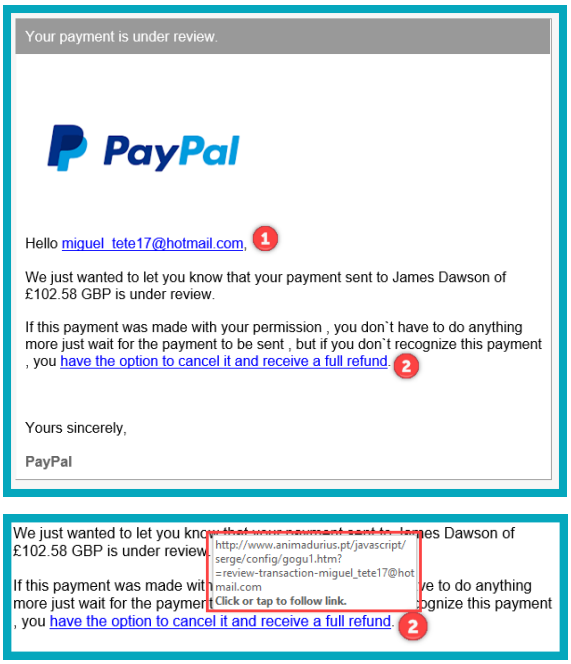
- *Ichki tarmoq*. Korxona tizimlariga o'zaro ta'sir qiladigan tarmoq bo'lib, u mahalliy, global yoki simsiz bo'lishi mumkin. So'nggi yillarda masofadan ishlaydigan usullarning ommalashishi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o'zboshimchalik asosida kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari kerak.

- *Tarmoq perimetri*. Kompaniyaning ichki tarmoqlari va tashqi, masalan, Internet yoki hamkor tashkilotlar tarmoqlari o'rtasidagi chegara.

Sosial injineriyaga tegishli ko'plab hujumlar mavjud bo'lib, quyida ularning ayrimlari bilan tanishib chiqiladi.

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 sosial injineriya sxemalaridan biri hisoblanadi. Katta hajmdagi shaxsiy ma'lumotlarni keng tarqalishi, fishing "shamolisiz" amalga oshmaydi. Fishingning eng keng tarqalgan na'munasi sifatida jabrlanuvchi elektron pochtasiga yuborilgan rasmiy ma'lumot ko'rinishidagi

bank yoki to’lov tizimidan yuborilgin soxta xabar hisoblanadi. Bunday elektron pochta xabarlari odatda rasmiy rasmiy veb-saytga o’xshash va shaxsiy ma’lumotlarni talab qiladigan shakldagi qalbaki veb sahifaga havolani o’z ichiga oladi [4] (94-rasm). Rasmda keltirilgan birinchi holatda mijozning yoki foydalanuvchining ismi va familiyasini yozish o’rniga pochta manzili yozilgan bo’lsa, ikkinchi holatda sichqoncha ko’rsatilgan havola ustiga olib borilganda, haqiqiy manzil (www.PayPal.com) emas, balki, boshqa manzilni ko’rish mumkin.



94-rasm. Fishing hujumiga misol

Quyida keng tarqalgan fishing sxemalariga misollar keltirilgan.

Mavjud bo’lmagan havola. Fishing hujumining mazkur turida biror veb saytga o’xshash bo’lgan veb saytga murojaat amalga oshirilishiga jalb qilinadi. Masalan, www.PayPai.com manzili www.PayPal.com manzili sifatida yuborish mumkin. Bu holda kamdan-kam holda foydalanuvchilar “l” harfini o’riniga “i” harfi borligiga e’tibor berishadi. Havolaga murojat qilinganda esa www.PayPal.com veb saytga o’xshash, biroq soxta veb 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 bloklangani va kredit karta ma’lumotlari blokdan chiqarilishi kerakligi keltirilgan

va unda rasmiy veb-saytga o’xshash soxta veb sahifaga olib boruvchi havola mavjud bo’lgan. Ushbu fishing hujumini keltirgan zarari bir necha yuz ming dollarga teng bo’lgan.

Taniqli korporativ brendidan foydalishga asoslangan firibgarlik. Firibgarlikning mazkur ko’rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchiga xabarlar yuboriladi. Bunda xabarlarda kompaniya tomonidan o’tkazilgan biror tanlovda g’alaba qozinilganligi 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 oshiririlishi mumkin.

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

Soxta antivirus va xavfsizlik dasturi. Mazkur dasturlar firibgar dasturiy ta’minot yoki “chaqqon dastur” deb nomlanib, ular antivirus dasturlariga o’xshasada, vazifasi boshqa bo’ladi. Bu dasturiy ta’minot turli tahdidlar to’g’risida yolg’on xabarnomalarni keltirib chiqaradi va foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ulardan foydalanganda elektron pochta, onlayn e’lonlar, ijtimoiy tarmoqlarda, qidiruv tizimlardagi natijalarida va hatto foydalanuvchi kompyuterida turli qalqib chiquvchi oynalarda duch kelishi mumkin. Quyida keltirilgan misolda, aslida Microsoft Security Essentials bo’lishi kerak bo’lgan biroq, o’ziga Security Essentials 2010 nomini bergan soxta antivirus dasturining ko’rinishi keltirilgan [5].

95-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 bo’lib, ular bank va boshqa IVR tizimlarining “rasmiy qo’nqiroqlari”ni qayta tiklash uchun ishlatiladi. Bu hujumda jabrlanuvchi bank bilan bog’lanishi va har qanday ma’lumotlarni tasdiqlash yoki yangilash kerakligi haqidagi so’rovni qabul qiladi. Tizim PIN 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.

Preteksting. Mazkur fishing sxemasida xaker o’zini boshqa shaxs sifatida ko’rsatadi va oldindan tayyorlangan skript bo’yicha maxfiy axborotni olishni maqsad qiladi. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko’riladi: tug’ulgan kun, INN, passport 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, sosial 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 ij 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’lshini ko’rsatdi.

“Yo’l-yo’lakay olma”. Sosial injineriyaning mazkur usulida xaker maxsus zararli dastur yozilgan ma’lumot eltuvchilardan foydalanadi va zararli dasturlar yozilgan eltuvchilar qurbon ish joyi yaqinida, jamoat joylarida va boshqa joylarda qoldiriladi. Bunda, ma’lumot eltuvchilar tashkilotga tegishli shaklda rasmiylashtiriladi. Masalan, xaker biror korporasiya logotipi va rasmiy veb-say manzili tushurilgan 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. Sosial injineriya texnikasi nafaqat psixologik bilimlarni, balki, inson haqida kerakli ma’lumotlarni to’plash qobilyatini ham talab qiladi. Bunday ma’lumotlarni olishning nisbatan yangi usuli uni ochiq manbalardan, ijtimoiy tarmoqlardan to’plashdir. Masalan, «Odnoklassniki», «VKontakte», «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’lumotlar foydalanishni cheklab qo’ygan taqdirda ham, foydalanuvchi firibgarlik qurboni bo’lmasligiga to’liq kafolat

yo’q. Masalan, Brazilyaning kompyuter xavfsizligi bo’yicha tadiqiqotchisi 24 soat ichida sosial injereniya 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’jayni uchun soxta qayd yozuvini yaratadi. Avval Neto jabrlanuvchining xo’jaynining do’stlariga va undan keyin to’g’ridan-to’g’ri jabrlanuvchining do’stiga do’stlik so’rovini yubordi. 7,5 soatdan so’ng esa tadqiqotchi jarblanuvchi bilan do’stlashdi. Shunday qilib, tadqiqotchi foydalanuvchining shaxsiy ma’lumotlarini olish ikoniyatiga ega bo’ldi.

“Yelka orqali qarash” hujumi. 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 hodimlar o’z ekranini ruxsatsiz odamlardan himoya qilishiga ishonishmagan.

Teskari sosial injineriya. Jabrlanuvchining o’zi tajovuzkorga ma’lumotlarini taqdim qilishi teskari sosial injineriyaga tegishli holat hisoblanadi. Bu bir qarashda ma’noga ega bo’lmagan qarash hisoblansada, aksariyat hollarda jarblanuvchilarning o’zi muammolarini hal qilish uchun tajovuzkorni yordamga jalb qiladi. Masalan, jabrlanuvchi bilan ishlovchi tajavuzkor 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 tajavuzkor tashkilot ichida

obro’ga ega bo’ladi va o’z qurbonlari sonini ortishiga erishadi. Bu holatni aniqlash esa ancha murakkab ish hisoblanadi.

Mashhur sosial injinerlar. *Kevin Mitnik* tarixdagi eng mashhur sosial injnerlardan biri bo’lib, u dunyodagi mashhur kompyuter xakeri, xavfsizlik bo’yicha mutaxassisi va sosial injineriyaga asoslangan kompyuter xavfsizligiga asoslangan 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’lishiga qaramasdan aka-uka Mushid va Shadi Badirlar 1990 yillarda Isroilda sosial injineriya va ovozni soxtalashtirish usullaridan foydalangan holda bir nechta yirik firibgarlik sxemalarini amalga oshirishgagan. Televideniyaga bergan intervyusida ular: “faqat telefon, elektr va noutbuklardan foydalanmaydiganlar tarmoq xavfsizdir” deb aytishgan.

Sosial injineriyadan himoyalanish choralari. Hujumlarni amalga oshirishda sosial injineriya texnikasidan foydalangan tajovuzkorlar tez-tez muloyimlik, dangasalik, xushmomilalik bilan foydalanuvchi va tashkilotlar xodimlarining qiziqishlaridan foydalanadilar. Hujumlarni oldini olish ular aldanayotganliklarini bilmasliklari sababli murakkab hisoblanadi.

Sosial 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 sifatidan tanishtirish;
- muammo yuzaga kelganda yordam beruvchi sifatida tanishtirish;
- ishonchli hosil qilish uchun ichki jarangdorlik 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 eltuvchilarni foydalanuvchi stoliga tashlash;
- turli ovozli qo’ng’iroqlardagi ovozli xabarlar va h.

Hayotda ko’plab jabhalarda sosial injineriyaga tegishli muammolarni ko’rish mumkin. Xususan, ommaviy madaniyatda (masalan, kinolarda) sosial injinerlikdan foydalanish holatlari tez-tez uchrab turadi. Masalan, quyidagi keltirilgan kinolarda sosial 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. Kiberjinoyatchilik tushunchasiga izoh bering?
2. Kiberjinoyatni amalga oshirishdan ko’zlangan maqsadlarni ayting?
3. Kiberjinoyatchilikning asosiy turlarini ayting va ularga misollar keltiring?
4. Kiberetika tushunchasiga izoh bering va ularga misollar keltiring?
5. Kompterdan foydalanish davomida qanday etika qoidalarga e’tibor berish talab qilinadi?

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

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

8. O’zbekiston Respublikasining Ma’muriy javobgarlik to’g’risidagi kodeksda kiberjinoyatchilikka oid qanday bandlar mavjud?

9. O’zbekiston Respublikasi jinoyat kodeksida kiberjinoyatchilikka oid qanday bandlar mavjud?

ADABIYOTLAR RO‘YXATI

1. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria (1991) Luxembourg: Office for Official Publications of the European Communities, 1991 ISBN 92-826-3004-8, Catalogue Number: CD-71- 91-502-EN-C © ECSC-EEC-EAEC, Brussels • Luxembourg.
2. National Information Systems Security (InfoSec) Glossary (2000) National Security Telecommunications and Information Systems Security Committee. National Security Agency US.
3. Pfleeger, C.P. (1997) Security in Computing. Second Edition, Prentice Hall, Upper Saddle River.
4. Guttman, B. and Roback, E. (1995) An Introduction to Computer security: The NIST Handbook. DIANE Publishing. http://dx.doi.org/10.6028/NIST.SP.800-12
5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
6. Purdy G. ISO 31000: 2009—setting a new standard for risk management //Risk Analysis: An International Journal. – 2010. – Т. 30. – №. 6. – С. 881-886.
7. ISACA C. S. X. Cybersecurity Fundamentals //Study Guide. – 2014.
8. Curricula C. Curriculum guidelines for post-secondary degree programs in cybersecurity. – 2017.
9. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши // Тошкент, 2008, -Б. - 394.
10. Ганиев С.К., Каримов М.М., Худойқулов З.Т., Кадиров М.М. Ахборот хавфсизлиги бўйича атама ва тушунчаларнинг рус, ўзбек ва инлиз тилларидаги изоҳли луғати // Тошкент 2017, -Б. - 480.
11. Ferguson N., Schneier B. Practical cryptography // New York: Wiley, 2003. – P. - 432.
12. Bruce S. Applied cryptography: protocols, algorithms, and source code in C //New York: Wiley. – 1996, - P. - 1027.
13. Smart N. P. et al. Cryptography: an introduction. – New York : McGraw-Hill, 2003. – Т. 3.
14. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
15. Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П., Давлатов А.Б. “Криптотаҳлил ва унинг махсус усуллари” электрон ўқув қўлланма. 2010 й.
16. Акбаров Д.Е., Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П. “Криптографиянинг математик асослари” электрон ўқув қўлланма. 2010 й.

17. Zlatanov, Nikola. (2015). Hard Disk Drive and Disk Encryption. 10.13140/RG.2.1.1228.9681.
18. Healy, Michael & Newe, Thomas & Lewis, Elfed. (2008). Analysis of Hardware Encryption Versus Software Encryption on Wireless Sensor Network Motes. 10.1007/978-3-540-79590-2_1.
19. Scarfone K. et al. Guide to storage encryption technologies for end user devices //NIST Special Publication. – 2007. – Т. 800. – С. 111.
20. Chuvakin A., Williams B. R. PCI Compliance. – Syngress, 2011.
21. Shinder D. L., Cross M. Scene of the Cybercrime. – Elsevier, 2008.
22. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250, с.
23. Regulations O., Guidance R. Code of Federal Regulations //Respiratory Protection. – 1910.
24. Frields J. National Industrial Security Program. Operating Manual Supplement. – DEPARTMENT OF DEFENSE WASHINGTON DC, 1995. – №. DOD-5220.22-M-SUP-1.
25. 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.
26. Rathgeb C., Uhl A. A survey on biometric cryptosystems and cancelable biometrics //EURASIP Journal on Information Security, 2011, №1, – P. 1-25.
27. 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
28. http://smartkardtechnologies.com/productdetails/acr39u-smart-card-rader
29. https://www.turbosquid.com/3d-models/3d-airport-x-ray-machine-security-1405223
30. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/
31. https://www.nuigalway.ie/itsecurity/howtospotphishingemails/
32. https://techjaws.com/beware-of-fake-microsoft-security-essentials/
33. https://www.pcmag.com/roundup/256703/the-best-antivirus-protection
34. https://www.us-cert.gov/ncas/tips/ST05-003
35. https://blog.layershift.com/why-high-availability-for-your-business/
36. https://en.wikipedia.org/wiki/Zimmermann_Telegram

37. https://www.rutoken.ru/
38. https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
39. https://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit
40. https://ciser.cornell.edu/wp-content/uploads/2017/01/CRADC_Destruction_and_Return_of_Restricted_Data.pdf
41. https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis
42. https://www.pctattletale.com/blog/1505/best-keylogger-software-windows-10

BELGILAR VA QISQARTMALAR

ABAC - Attribute-based access control

ACL - Access control list

AES - Advanced Encryption Standard

APT - Advanced persistent threats

ARP - Address Resolution Protocol

ASCII – American Standard Code for Information Interchange

BLP - Bell–LaPadula Model

CA - Certificate authority

CBC - Cipher block chaining

CCTV - Closed-circuit television

C-list - Capability list

CSEC2017 – Cybersecurity Curricular 2017

DAC - Discretionary access control

DES – Data Encryption Standard

DNS - Domain name system

DoD – Department of Defence

DOS – Denial of Service

ECB - Electronic codebook mode

EEPROM – Electrically erasable programmable read-only memory

FBI - Federal Bureau of Investigation

FDE - Full disk encryption

FTP - File Transfer Protocol

GNFS - General number field sieve

HMAC – Hashed Message authentication code

HTTP - HyperText Transfer Protocol

ICMP - Internet Control Message Protocol

IDEA - International Data Encryption Algorithm

IDS - Instrusion Detection System

IEEE - Institute of Electrical and Electronics Engineers

IO - Input/output

IP - Internet Protocol

ISO – International Organization for Standardization

MAC - Mandatory access control

MAC - Message authentication code

MAC - Media Access Control

MBR - Master boot record

MD5 - Message-digest algorithm

MIPS - One-million-instruction-per-second

MITM - Man in the middle attack

OSI - Open System Interconnection

OTP - One time password

OWASP - Open Web Application Security Project

PIN – Personal identification number

PKI - Public key infrastructure

RAID - Redundant Array of Independent Disks

RBAC - Role-based access control

RC4 - Rivest Cipher 4

RSA – Rivest, Shamir and Adleman

SHA1 – Secure Hash Algorithm 1

SMS - Short message service

SMTP – Simple Mail Transfer Protocol

SSD - Solid-State Drive

SSID - Service Set Identifier

SSL - Secure Sockets Layer

TCG – Trusted Computing Group

TCP - Transmission Control Protocol

TEA - Tiny Encryption Algorithm

UDP - User Datagram Protocol

USB – Universal Serial Bus

VPN - Virtual Private Network

WEP - Wired Equivalent Privacy

WPA - Wi-Fi Protected Access

XOR – Exclusive OR

AOB - Alisaning onlayn banki

EKUB – Eng kichik umumiy bo’luvchi

ERI – Elektron raqamli imzo

OT – Operatsion tizim

TE - Tapmoqlararo ekran

TERMINLAR LUG'ATI

Ajratilgan xonaning akustik himoyasi – ovozning to’siq konstruktsiya orqali to’g’ridan – to’g’ri o’tishi yo’li bilan nutqiy maxfiy yoki konfidentsial axborotni ajratilgan xona tashqarisiga sirqib chiqishini oldini olish bo’yicha rejalashtirilgan tashkiliy-texnik tadbirlarni amalga oshirish jarayoni.

Akkreditatsiya (sertifikatsiya organining akkreditatsiyasi) - tashkilotning ma’lum (so’ralgan) sohada sertifikatsiya buyicha muayyan ishlarni bajarishga kompetentligini (qodirligini) vakolatli (nufuzli) organ tomonidan rasman tan olinishi.

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.

Akustik axborot – eltuvchisi akustik signallar bo’lgan axborot.

Anonimlik - ishtirokchiga (protokol ishtirokchisiga) qandaydir harakatni anonim tarzda, ya’ni o’zini identifikatsiyalamasdan, bajarilishini ifodalaydi. Bunda, lekin, ishtirokchi ushbu harakatni bajarishga haqli ekanligini isbotlashi lozim. Anonimlik absolyut va chaqiriluvchi bo’lishi mumkin.

Antibot – robot-dasturlarni, ayg’oqchi dasturlarni (Spyware), ruxsatsiz o’rnatilgan reklama dasturiy ta’minotni (Adware) va boshqa zarar keltiruvchi dasturiy ta’minot turlarini avtomatik tarzda aniqlovchi va yo’q qiluvchi dasturiy ta’minot.

Anti–spufing - qonuniy identifikatsiya va autentifikatsiya ma’lumotlaridan ruxsat etilmagan foydalanishga qarshi qabul qilinuvchi choralar.

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.

AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.

Audit jurnali – tizim harakatlarining xronologik yozuvi. Berilgan muddatda bajariluvchi tizimli foydalanishlar va amallar yozuvlarini o’z ichiga oladi.

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.

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.

Avariya vaziyati – masalalar yechilishining to’xtalishiga sabab bo’luvchi hisoblash tizimining buzilishi.

Avtomatlashtirilgan axborot tizimi – ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo’ljallangan dasturiy va apparat vositalar majmui.

Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.

Axborot egasi - axborot resurslariga, axborot mulkdori bilan shartnoma asosida egalik qilish, ulardan foydalanish va ularni idora qilish huquqiga ega axborot munosabatlarining subyekti.

Axborot kafolati - axborot va axborot tizimlarining foydalanuvchanligini, yaxlitligini, autentifikatsiyalanishini, konfidensialligini va rad etmasligini ta’minlash orqali himoyalash va qo’riqlash choralari.

Axborot urushi - dushmanning axborotiga, axborotga asoslangan jarayonlariga va axborot tizimlariga zarar yetkazish, bir vaqtning o’zida tegishli axborotni, axborotga va axborot tizimlariga asoslangan jarayonlarni himoyalash yo’li bilan axborot ustunligiga erishish uchun zarur choralarni ko’rish harakatlari.

Axborot xavfsizligi – axborot egasiga yoki foydalanuvchiga va madadlovchi infrastrukturaga ziyon keltiruvchi tabiiy yoki sun’iy xarakterli, tasodifiy yoki atayin

qilingan ta’sirlardan axborotning va madadlovchi infrastrukturaning himoyalanganligi.

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.

Axborot xavfsizligi arxitektori - tashkilotning asosiy missiyasini himoyalash uchun kerakli axborot xavfsizligi talablari va etalon modelni, segment va yechimlar arxitekturasini o’z ichiga olgan barcha tashkilot arxitektura jixatlarida adekvat adreslangan biznes - jarayonlar va bu missiya va biznes jarayonlarni madadlovchi axborot tizimlarini ta’minlashga javobgar bo’lgan jismoniy shaxs, guruh yoki tashkilot.

Axborot xavfsizligi doktrinasi - axborot xavfsizligini ta’minlash maqsadlariga, masalalariga, prinsiplariga va asosiy yo’nalishlariga rasmiy qarashlar majmui.

Axborotdan foydalanish – shtatga oid texnik vositalardan foydalanib axborot bilan tanishish, uni xujjatlash, nusxalash, modifikatsiyalash yoki axborotni yo’q qilish jarayoni.

Axborotni texnik himoyalash - himoyalashga loyiq axborotning (ma’lumotlarning) xavfsizligini xarakatdagi qonunlarga muvofiq, texnik, dasturiy va dasturiy - texnik vositalarni ishlatib, nokriptografik usullar yordamida ta’minlashdan iborat axborot himoyasi.

Axborotni fizik (bevosita) himoyalash - himoya obyektiga vakolatsiz shaxslarning suqilib kirishlariga yoki undan foydalanishlariga to’siqlar yaratuvchi tashkiliy tadbirlar yoki vositalar majmuini ishlatish yo’li bilan axborotni himoyalash.

Axborotni himoyalash konsepsiyasi – axborotni himoyalash bo’yicha qarashlar va umumiy texnik talablar tizimi.

Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.

Axborotni huquqiy himoyalash – axborotni himoyalash bo'yicha subyektlar munosabatini rostlovchi qonuniy va me'yoriy xujjatlarni (aktlarni) ishlab chiqishni, hamda ularning bajarilishini nazorat qilishni o'z ichiga oluvchi axborotni xuquqiy usullar yordamida himoyalash.

Axborotni ishlovchi himoyalangan texnik vosita – himoyalash vositalari va usullari ishlab chiqish va tayyorlash bosqichida amalga oshirilgan axborotni ishlovchi texnik vosita.

Axborotning buzilishi – tashqi ta'sirlar (halallar), apparatura ishlashidagi buzilishlar, yoki xizmatchi xodimning bilimsizligi natijasida texnik vositalarida ishlanuvchi axborotning tasodifiy ruxsatsiz modifikatsiyalanishi.

Bot - oddiy foydalanuvchi interfeysi orqali avtomatik tarzda va/yoki berilgan jadval bo'yicha qandaydir harakatlarni bajaruvchi maxsus dastur. Kompyuter dasturlari muhokama qilinganida bot atamasi asosan Internetga qo'llash bilan ishlatiladi.

Botnet - ishga tushirilgan botlarga ega bir qancha sonli xostlardan tashkil topgan kompyuter tarmog'i. Odatda kompyuterlarga bo'ladigan tarmoq xujumlarini (spamni tarqatish, foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash, masofadagi tizimda parollarni saralash, xizmat qilishdan voz kechishga undash hujumlari va x.) koordinatsiyalash uchun ishlatiladi (inglizcha robot va network so'zlaridan olingan.).

Buferning to'lib – toshishi hujumi – buferdagi oldindan aniqlangan hajmdagi makonni qaytadan yuklash usuli bo'lib, xotiradagi ma'lumotlarni qayta yozishi va shikastlashi mumkin.

Buzilmaslik – tizimning unga yuklatilgan vazifalarni berilgan sharoitda, istalgan vaqt onida bajarish qobiliyati.

Davlat sirlaridan foydalanish - fuqarolarning davlat siridan iborat ma'lumotlardan foydalanish huquqini, korxonalar, idoralar va tashkilotlarni esa bunday ma'lumotlardan foydalanib ish yuritish huquqini rasmiylashtirish muolajasi.

Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Dezinformatsiya – foydalanuvchi shaxslarga yolg'on tasavvurni shakllantirish maqsadida ularga uzatiluvchi xabarni atayin buzib ko'rsatish; yolg'on axborotni uzatish.

Faol hujum - dushman va/yoki buzg'unchi qonuniy foydalanuvchi harakatiga ta'sir etishi, masalan, qonuniy foydalanuvchi xabarini almashtirishi yoki yo'q qilishi va xabarni yaratib uning nomidan uzatishi va h. mumkin bo'lgan kriptotizimga yoki kriptografik protokolga hujum.

Faol tahdid – tizim holatini atayin ruxsatsiz o'zgartirish tahdidi.

Firibgarlik hujumi - foydalanuvchilarning yoki dasturlarning ma'lumotlarni soxtalashtirish va noqonuniy afzallikka ega bo'lish yo'li bilan boshqa subyektlar sifatida muvaffaqiyatli niqoblanish vaziyati.

Foydalanish nazorati – foydalanuvchilarning, dasturlarning yoki jarayonlarning hisoblash tizimlari qurilmalaridan, dasturlaridan va ma'lumotlaridan foydalanishlarini aniqlash va cheklash.

Foydalanishni diskretsion boshqarish – mavzu alomati bo'yicha obyektdan foydalanish konsepsiyasi (modeli). Unga binoan vakolatlarning ma'lum darajasiga ega foydalanish subyekti o'z xuquqini ixtiyoriy boshqa subyektga berishi mumkin.

Foydaluvchanlik - avtorizatsiyalangan mantiqiy obyekt so'rovi bo'yicha mantiqiy obyektning tayyorlik va foydalanuvchanlik holatida bo'lishi xususiyati.

Himoya ma'muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Himoyaning faol texnik vositasi – texnik razvedka vositalariga yoki ushbu vositalarning me'yorida ishlashini, buzuvchi, niqoblovchi yoki imitatsiyalovchi faol halallar yaratilishini ta'minlovchi himoyaning texnik vositasi.

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

Hujumni aniqlash va ogohlantirish – qaror qabul qiluvchiga maqbul javobni amalga oshirish uchun bildirish orqali ataylab qilingan ruxsat etilmagan harakatlarning aniqlanishi, korrelyatsiyasi, identifikatsiyalanishi va tavsiflanishi.

Identifikator – subyekt yoki obyektning farqlanuvchi alomatidan iborat foydalanishning identifikatsiya vositasi. Foydalanuvchilar uchun asosiy identifikatsiya vositasi parol hisoblanadi.

Identifikatsiya ma'lumotlari - tizimda muayyan qatnashchini bir ma'noli identifikatsiyalashga imkon beruvchi, unga tegishli noyob identifikatsiya ma'lumotlari majmui.

Ijtimoiy injeneriya – xizmatchi xodimlar va foydalanuvchilar bilan, turli nayrang, aldash va h. orqali chalg'itish asosidagi muloqotdan olinadigan axborot yordamida axborot tizimining xavfsizlik tizimini chetlab o'tish.

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Imzo verifikatsiyasi - ma'lumotlardagi raqamli imzoni tekshirish uchun raqamli imzo algoritmi va ochiq kalitdan foydalanish.

Insayder – guruxga tegishli yashirin axborotdan foydalanish xuquqiga ega guruh a'zosi. Odatda, axborot sirqib chiqishi bilan bog'liq insidentda muhim shaxs hisoblanadi. Shu nuqtai nazaridan, insayderlarning quyidagi xillari farqlanadi: beparvolar, manipulyatsiyalanuvchilar, ranjiganlar, noxolislar, qo'shimcha pul ishlovchilar va h.

Insident – ruxsatsiz foydalanish xuquqiga ega bo'lishga yoki kompyuter tizimiga hujum o'tkazishga urinishning qayd etilgan holi.

Internet–firibgarlik – kredit – moliya sohasidagi "yuqori-texnologiyali'' jinoyatchilik xili bo'lib, uyushgan va, odatda, xalqaro xarakterga ega. Jinoiy strukturalar tomonidan noqonuniy daromadlar olish maqsadida foydalanishni blokirovka qilish hujumi yoki bot-tarmoqlarni yaratish kabi zamonaviy texnologiyalar ishlatiladi.

Jamiyat axborot xavfsizligi – “shaxs axborot xavfsizligi” kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo’llaniladi.

Kalit – fayldagi yozuvlarni identifikatsiyalash va undan tezda foydalanish uchun ishlatiladigan belgilar majmui; yana - qandaydir axborotdan foydalanish vakolatini tasdiqlash uchun ishlatiladigan kod; yana - asosida shifrlash amalga oshiriluvchi qiymat; yana - ma’lumotlar elementlari naboridagi identifikator.

Kalit uzunligi (o’lchovi) - kalitni ifodalovchi ma’lum alfavitdagi so’z uzunligi. Ikkili kalit uzunligi bitlarda o’lchanadi.

Keylogger - klaviaturali kiritishni ushlab qolishga mo’ljallangan dastur yoki apparat vosita. Bosilgan klavishlar skan-kodlarini aniqlashni va ularni yashirincha saqlashni va/yoki yashirincha qandaydir kanal orqali uzatishni amalga oshiradi.

Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o’z ichiga oladi.

Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo’luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.

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.

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.

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

Kiberterrorizm - insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug’diruvchi kompyuter tizimlarini izdan chiqarish bo’yicha harakatlar.

Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo’riqlash yoki himoyalash imkoniyati.

Koder (dasturchi) - internet-firibgarlik texnologiyalari bilan shug’ullanuvchi uyushgan jinoiy guruh ichidagi ixtisosliklardan biri; troyan va boshqa zarar yetkazuvchi dasturlarni yozuvchi va ularni yopiq anjumanlarda “o’ziga o’xshashlarga” sotuvchi ishtirokchini belgilaydi.

Kodlar kitobi – tarkibida tartibga solingan ochiq matn va kodlar ekvivalenti yoki so’zlarni almashtirish texnologiyasidan foydalanuvchi mashina shifrlash usuli bo’lgan hujjat.

Kodlar lug’ati – kod tizimida kod ekvivalenti berilgan ochiq matn so’zlari, raqamlari, iboralari yoki gaplar nabori.

Kompyuter xavfsizligi – axborot tizimlari aktivlarining, jumladan apparat vositalarining, dasturiy ta’minotning, o’rnatilgan mikrodasturiy vositaning va ishlanuvchi, saqlanuvchi va uzatiluvchi axborotning konfidensialligini, yaxlitligini va foydalanuvchanligini kafolatlovchi choralar va nazoratlash vositalari.

Konfidensial axborot – egasi tomonidan himoyalashni talab etuvchi tijoriy yoki shaxsiy sirdan iborat axborot.

Kriptografik algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.

Lug’atga asoslangan hujum – ochiq matn elementlari lug’atidan foydalanishga asoslangan kriptotizimga hujum.

Ma’lumotlar – odam ishtiroki bilan yoki avtomatik tarzda uzatishga, izohlashga yoki ishlashga yaroqli, formallashgan ko’rinishda ifodalangan axborot.

Ma’lumotlarni tiklash – eltuvchining asl nusxasida ma’lumotlar yaxlitligi buzilganida unga ma’lumotlarning himoya nusxasi bo’lgan eltuvchidan nusxalash jarayoni.

Ma’muriy xavfsizlik choralari – tanlashni, ishlab chiqishni, tatbiq etishni, sog’liqni saqlashga oid elektron axborotni himoyalash bo’yicha xavfsizlik choralarini madadlash va ushbu axborotni himoyalashga nisbatan tashkilot xodimlarini boshqarish bo’yicha ma’muriy harakatlar, siyosatlar va muolajalar.

Mantiqiy bomba – “qurbon” kompyuterida rezident joylashgan va ma’lum mantiqiy shart bo’yicha, masalan, ma’lum sanada yoki tizimning ma’lum xolatlari naborida, faollashuvchi destruktiv dasturiy komplekslarni umumlashtiruvchi atama.

Mualliflik huquqi – fan, adabiyot va san’at asarlarini yaratish va foydalanish bilan bog’liq vujudga keladigan munosabatlarni tartibga soluvchi huquqiy normalar majmui.

Nuqson - axborot tizimidagi topshiriq, adashish yoki etiborsizlik asosidagi xato bo’lib, himoya mexanizmlarini aylanib o’tishga imkon beradi.

Ochiq axborot – barcha manfaatdor shaxslarning foydalanishlari bo’yicha cheklash bo’lmagan axborot: umumfoydalanuvchi axborot.

Ochiq kalit - odatda imzoni tekshirish yoki ma’lumotni shifrlashda foydalaniluvchi asimetrik kalit juftining ochiq qismi.

Parol yordamida himoyalash – foydalanish uchun parol kiritilishi zarur bo’lgan ma’lumotlarni himoyalash usuli.

Parollarni fosh qiluvchi - parollarni saralash yoki o’g’rilashni amalga oshiruvchi kompyuter dasturi.

Parolni buzib ochish - axborot tizimidan (tarmog’idan) yashirincha foydalanish texnikasi (usuli) bo’lib, unda hujum qiluvchi taraf parollarni fosh qiluvchi yordamida parollarni aniqlashga (tanlashga) yoki o’g’irlashga urinib ko’radi.

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.

Raqamli axborot – kompyuter tizimlarida ishlashga, saqlashga va almashishga mo’ljallangan ma’lumotlar ko’rinishida ifodalangan axborot.

Raqamli imzo algoritmi - ma’lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

Raqamli imzoni shakllantirish algoritmi – raqamli imzo sxemasining tarkibiy qismi. Kirish yo’liga imzolanuvchi xabar, maxfiy kalit, hamda raqamli imzo sxemasining ochiq parametrlari beriluvchi algoritm (umuman randomizatsiyalangan

algoritm). Algoritm ishining natijasi raqamli imzo hisoblanadi. Raqamli imzo sxemasining ba’zi turlarida imzoni shakllantirishda protokol ishlatiladi.

Risk matritsasi - rutbalash va oqibatlariga va imkoniyatlariga rutbalar berish yo’li bilan riskni ifodalash instrumenti.

Risk menejmenti — axborot-telekommunikatsiya texnologiya resurslariga ta’sir etishi mumkin bo’lgan xavfli xodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to’liq jarayoni.

Riskni nazoratlash - riskni modifikatsiyalovchi (o’zgartiruvchi) chora. *1-izoh.* Riskni nazoratlash o’z ichiga har qanday jarayonni, siyosatni, usulni, amaliyotni va riskni modifikasiyalovchi boshqa harakatlarni olishi mumkin. *2-izoh.* Riskni nazoratlash doimo istalgan va kutilgan effektni bermasligi mumkin.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo’ljallangan shifrlash algoritmi.

Shaxsiy axborot – tarqalishi faqat mos shaxslar yoki tashkilotlar ruxsati bilan mumkin bo’lgan mamlakat fuqarolari yoki tashkilotlari manfaatlariga daxldor axborot.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

Tahdid turlari - tahdidlarni tasodifiy va atayinlariga, aktiv va passivlariga tasniflash mumkin.

Tarmoq xavfsizligi - axborot tarmog’ini ruxsatsiz foydalanishdan, me’yoriy ishlashiga tasodifiy yoki atayin aralashishdan yoki tarmoq komponentlarini buzishga urinishdan ehtiyot qiluvchi choralar. Asbob-uskunalarni, dasturiy ta’minotni, ma’lumotlarni himoyalashni o’z ichiga oladi.

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.

Tizim ma’muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta’minlashga javobgar shaxs.

Tizim xavfsizligi - tizim resurslaridan va funksional imkoniyatlaridan ruxsatsiz foydalanishdan hamda ishlashida turli bashorat qilinadigan yoki qilinmaydigan holatlar sabab bo’luvchi, bo’lishi mumkin bo’lgan buzilishlardan tizimning himoyalanishi.

Virus – boshqa dasturlar bajarilayotganida o’zini ularga kirituvchi unchalik katta bo’lmagan dastur; yana - nusxalarini beixtiyor yaratish va keyinchalik yangi nusxasini nazoratlash va qayta yaratishga erishish maqsadida fayllardagi va tizimli sohalardagi boshqa dasturlarni modifikatsiyalash imkoniyatiga ega dastur.

Virusga qarshi himoya - hisoblash texnikasi va avtomatlashtirilgan tizim vositalarini dasturiy virus ta’siridan himoyalashni ta’minlashda ishlatiluvchi tashkiliy, xuquqiy, texnik va texnologik choralar kompleksi.

Xabar haqiqiyligi kodi - bir-biriga ishonuvchi ishtirokchilar tomonidan xabarlarni autentifikatsiyalash protokollarida xabarga qo’shiladigan va uning yaxlitligini va ma’lumotlar manbaining autentifikatsiyasini ta’minlashga mo’ljallangan simvollarning maxsus nabori.

Xatoliklar jurnali – tizim tomonidan adashishlar xususidagi axborot yoziladigan fayl.

Xavfsiz o’chirish - qattiq diskni qayta yozish uchun dasturiy - aparat vositalari asosidagi jarayonlardan foydalanib qayta yozish texnologiyasi.

Xavfsiz operatsion tizim – ma’lumotlar va resurslar mazmuniga mos himoyalash darajasini ta’minlash maqsadida apparat va dasturiy vositalarni samarali boshqaruvchi operatsion tizim.

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.

Xavfsizlik atributi – baholanish obyektining xavfsizlik siyosatini amalga oshirishda ishlatiluvchi subyektlar, foydalanuvchilar va/yoki obyektlar bilan bog’lik axborot.

Xavfsizlik auditi – kompyuter tizimi xavfsizligiga ta’sir etuvchi bo’lishi mumkin bo’lgan xavfli harakatlarni xarakterlovchi, oldindan aniqlangan hodisalar to’plamini ro’yxatga olish (audit faylida qaydlash) yo’li bilan himoyalanishni nazoratlash.

Xavfsizlik xizmati ma’muri – xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to’liq tasavvurga ega shaxs (yoki shaxslar guruhi).

Xavfsizlikni aktiv testlash – nishon bilan to’g’ridan – to’g’ri o’zaro aloqaga mo’ljallangan xavfsizlikni testlash, masalan, talab qilingan nishongacha paketni yuborish.

Xavfsizlikning avtomatlashtirilgan domeni - asboblar, texnologiyalar guruhini hamda ma’lumotlarni o’z ichiga olgan axborot xavfsizligi sohasi.

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.

Xodim xavfsizligi – qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizatsiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.

Yolg’on axborot – xarakteristikalari va alomatlari noto’g’ri akslantiriluvchi hamda real mavjud bo’lmagan obyekt xususidagi axborot.

Zombi - tizimda o’rnatilgan, boshqa tizimlarga hujum qilishga majbur qiluvchi dastur.

MUNDARIJA

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, 2020

“Kiberxavfsizlik asoslari”

5330300 – Axborot xavfsizligi, 5330500 – Kompyuter njiniringi (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.Ganiyev
A.A.Ganiyev
Z.T.Xudoyqulov

Taqrizchilar: K.A.Tashev
O.P.Axmedova

Mas’ul muharrir:

Musahhih: S.X.Abdullaeva