cyber security

R.Y.MAMAJANOV, T.J.RAJABOV,
E.I.SAIDAXMEDOV, I.U.XUSHBOQOV.

KIBER XAVFSIZLIK

2024-yil

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

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

Taqrizchilar:

Yakumov.S.X – Qarshi DU “Texnologik ta’lim” kafedrasi professori.

dots.N. Ashurov – Denov tadbirkorlik va pedagogika institute “Boshlang’ich ta’lim metodikasi” kafedrasi mudiri.

MUNDARIJA

KIRISH

Bugungi kunda elektron xizmatlar bizning hayotimizda ajralmas o’rin egaladi. Dunyoda axborotkommunikatsiya texnologiyalariga tobora rivojlanib borib ko’p tarmoqli bo‘lib borayotganligi bois, ushbu texnologiyalarni himoya qilish va ulardan foydalanish davlat manfaatlar uchun hal qiluvchi ahamiyatga ega.

Shu sababli, har bir tashkilotga, kiberxavfsizlikni taminlash masalasiga olohida urg’u berib, mazkur soha bilan shug‘ullanuvchi xodimlar jalb qilinmoqda va xodimlarni kiberxavfsizlikka oid bilimlar bilan muntazam tanishtirib borish uchun qator seminar-treyning mashg‘ulotlari tashkil etilmoqda. Bugungi kunga kelib oliy ta’lim muassasalarida ham kiberxavfsizlikni fan sifatida o‘tilishi buning yaqqol misolidir.

O’zbekiston Respublikamiz axborot texnologiyalarining rivojlanishi bilan bir qatorda xo‘jalik va davlat boshqaruvi organlarida axborot xavfsizligini, xususan, kompyuter bilan bog‘liq bo‘lgan xavfsizlik muammolarini bartaraf etish yo‘nalishiga alohida e’tibor qaratilmoqda. 2017-2021 yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha harakatlar strategiyasida vazifalar belgilab qo’yildi, shular qatorida «...axborot xavfsizligini taminlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish» va kiberjinoyatchilikni oldini olish va fosh etish masalalariga alohida e’tibor qaratilgan. Bundan tashqari, “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yilida amalga oshirish bo’yicha 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.

Qo‘llanmaning birinchi bobida kiberxavfsizlik asoslari fani sohasining vazifalari va asosiy tushunchalari, uning qo‘llanilish sohasi hamda kiberxavfsizlikda inson omili masalalari ko‘rib chiqilgan. Kiberxavfsizlikning bilim sohalari, kiberxavfsizlik va axborot xavfsizligi tushunchalari o‘rtasidagi farq

misollar asosida keltirilgan. Shuningdek, kiberjinoyatchilik, kiberhuquq va kiberetika masalalariga to‘xtalib o‘tilib va talabalarga tushunarli tilda bayon qilindi.

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

Uchinchi bobda axborotning kriptografik himoyasi doirasidagi asosiy tushunchalar, simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, ma’lumotlar yaxlitligini taminlash usullari ko‘rib chiqilgan.

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

Beshinchi bob tarmoq xavfsizligini ta’minlashda amalga oshirilish kerak bo’lgan ishlar va tarmoq haqida boshlang’ich tushunchalar xavfsizlik muammolari va ularni bartaraf etishda tarmoqlararo ekrandan, virtual himoyalangan tarmoqdan va boshqa vositalardan foydalanish masalalari keltirilgan. Bundan tashqari, simsiz tarmoqlarda xavfsizlik muammolari va risklarni boshqarish masalalariga to‘xtalib o‘tilgan.

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

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

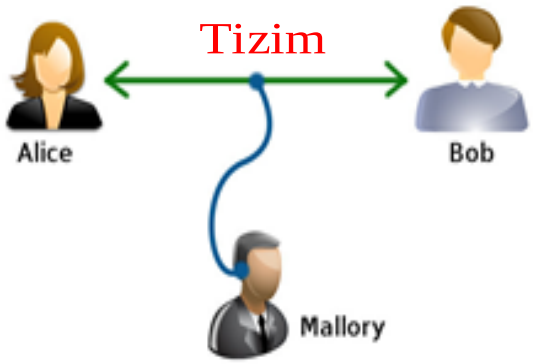
1 BOB.KIBERXAVFSIZLIK HAQIDA UMUMIY MA’LUMOT

1.1 Kiberxavfsizlikning asosiy tushunchalari

Axborotlarning himoyasini ta’minlash uzoq yillardan buyon dolzarb masalardan biri bo’lib kelmoqda. Shuning uchun ham axborotni himoyalash uchun turli xil usullar qo‘llanilib kelmoqda. Ulardan eng qadimgilarida biri – sirli yozuvdir. Undagi xabarni yuborilgan manzil egasidan boshqa shaxs o‘qiy olmagan.

Axborotni qayta ishlash sanoatining paydo bo‘lishi axborotni himoyalash sanoatining paydo bo‘lishiga olib keladi va axborotlani 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 taminlash axborot texnologiyalari rivojining yetakchi yo‘nalishlaridan biri hisoblanadi.

Axborot xavfsizligi hayotda mavjud timsollarga asoslanadi. Hayotda qonuniy faoliyat olib boruvchi shaxslar mavjud, ular 1.1-rasmda Alisa va Bob timsolida akslantirilgan. Biroq, hayotda qonuniy faoliyat yurituvchi insonlarning faoliyatiga qiziquvchi, ularning ishlariga xalaqit beruvchi insonlar ham mavjud va ular 1.1-tasvirda Mallory va Tridi timsolida tasvirlangan. Tridi timsoli barcha g‘arazli niyatlarni amalga oshiruvchi shaxslarni ifodalaydi. Bundan tashqari kiyingi yillarda passiv va itoatkor tinglovchi Momo Havo ham qo‘shildi.



1.1-rasm. Axborot xavfsizligining hayotdagi timsollari

O‘quv qo‘llanmaning keyingi bo‘limlarini yoritishda shu uchta obrizdan fodalanib senariy hosil qilamiz. Ushbu hayotiy senariy Alisaning onlayn banki

(AOB) deb ataladi. Bunga koʻra, Alisa onlayn bankning biznes faoliyatini amalga oshiradi. Mazkur senariyda Alisaning xavfsizlik muammosi nima? Alisaning mijozi boʻlgan Bobning xavfsizlik muammosichi? Alisa va Bobning xavfsizlik muammolari bir xilmi? Mallory nuqtai nazaridan qaraganda qanday xavfsizlik muammolari mavjud? Ushbu savollarga keyingi qismlarda javob berib oʻtiladi.

Tarmoq sohasida faoliyat yuritayotgan CISCO kompaniyasining fikriga koʻra, axborot xavfsizligi - bu maxfiy biznes maʼlumotlarini oʻzgartirish, buzish, yoʻq qilish va tekshirishdan himoya qilish uchun ishlab chiqilgan va foydalaniladigan jarayonlar va vositalar majmuasi hisobkanadi.

Kiberxavfsizlik - bu ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun xavfsizlik choralarini qo'llash jarayoni. Tizim ma'muri aktivlarni, shu jumladan kompyuterlar va serverlarning mahalliy tarmog'idagi ma'lumotlarni himoya qilishni ta'minlaydi.

Axborot xavfsizligi va kiberxavfsizlik koʻpincha chalkashib ketadi. CISCO maʼlumotlariga koʻra, axborot xavfsizligi kiberxavfsizlikning muhim qismidir, lekin faqat maʼlumotlar xavfsizligini taminlash uchun ishlatiladi.

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

1.2-rasm. Kiberxavfsizlik fani sohasining tuzilishi

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

Maxfiylik - bu ma'lumotlarning ruxsatsiz shaxslarga oshkor etilishining oldini olishdir. Bu shuningdek, ma'lumotlarni almashish va saqlashda ishtirok etuvchi vakolatli tomonlarning shaxsini maxfiy va anonim saqlashga harakat qilishni anglatadi. Ko'pincha maxfiylik yomon shifrlangan ma'lumotlarni buzish, Man-in-the-middle (MITM) hujumlari, nozik ma'lumotlarni oshkor qilish orqali buziladi. AOB senariysida Bob uchun maxfiylik juda muhim. Ya'ni, Bob o'z balansida qancha pul borligini Malloryning bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma'lumotlarning maxfiligini taminlash muhim hisoblanadi.

Maxfiylikni o'rnatish bo'yicha standart choralar quyidagilarni o'z ichiga oladi:

1. Ma'lumotlarni shifrlash
2. Ikki faktorli autentifikatsiya

3. Biometrik tekshirish
4. Xavfsizlik belgilari

Yaxlitlik- axborotni ruxsatsiz shaxslar tomonidan o‘zgartirishdan himoya qilishni anglatadi. Axborot va dasturlar faqat belgilangan va ruxsat etilgan tarzda o‘zgartirilishi talabidir. Yaxlitlikni xavf ostiga qo‘yishi mumkin bo‘lgan muammolar qatoriga mashinani “zombi kompyuter” ga aylantirish, zararli dasturlarni web-sahifalarga joylashtirish kiradi. AOB senariysida Alisaning banki qayd yozuvining yaxlitligini Mallorydan himoyalash shart. Masalan, Bob o‘zining akkauntida balansning o‘zgarishidan yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Yaxlitlikni kafolatlash uchun standart choralar quyidagilardan iborat:

1. Kriptografik nazorat summalari
2. Fayl ruxsatlaridan foydalanish
3. Uzluksiz quvvat manbalari
4. Ma’lumotlarning zaxira nusxalari

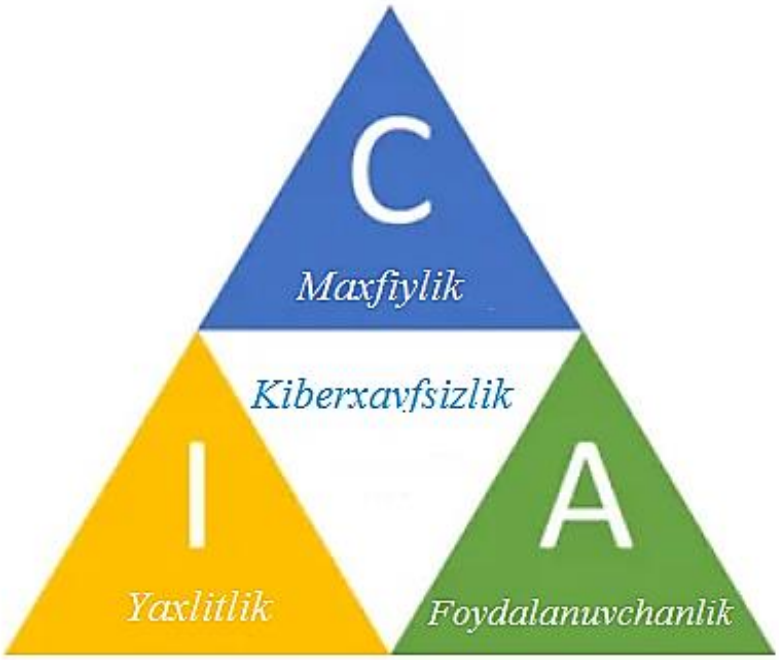
Shu o‘rinda maxfiylik va yaxlitlik bir xil tushuncha emasligiga e’tibor berish kerak. Masalan, Mallory biror ma’lumotni o‘qiy olmagan taqdirda ham uni sezilmaydigan darajada o‘zgartirishi mumkin.

Foydalanuvchanlik- bu vakolatli shaxslar kerak bo‘lganda ma’lumotlarga kirish imkoniyatiga ega ekanligiga ishonch hosil qilish. Ma’lumotlar faqat to‘g‘ri odamlar kerakli vaqtda kirish imkoniga ega bo‘lgan taqdirdagina qimmatga ega bo‘ladi. Axborotning mavjud emasligi DDoS hujumlari, apparatdagi nosozliklar, dasturlash xatolari, inson xatolari kabi xavfsizlik hodisalari tufayli yuzaga kelishi mumkin.

Foydalanuvchanlikni kafolatlash uchun standart choralar quyidagilarni o‘z ichiga oladi:

1. Ma’lumotlarni tashqi drayverlarga zaxiralash
2. Fayervollarni amalga oshirish
3. Zaxira quvvat manbalariga ega
4. Ma’lumotlarning ortiqchaligi

Barcha kiberhujumlar Markaziy razvedka boshqarmasi triadasining bir yoki bir nechta uch qismiga tahdid solishi mumkin. Maxfiylik, yaxlitlik va foydalanuvchanlik ma’lumotlaringizni xavfsiz saqlash uchun birgalikda ishlashi kerak. (1.3- rasm).



1.3- rasm Kiberxavfsizlikni saqlaninig asosiy uchligi.

Risk- bu tashkilot tarmog‘idagi kiberhujum yoki buzilish natijasida ta’sir qilish, muhim aktivlar va maxfiy ma’lumotlarning yo‘qolishi yoki obro‘siga putur yetkazish ehtimoli.

Masalan, Korxona xotimining tizimga kirish jarayonini ko‘raylik. Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina xodim login va parolni tizimga kiritganida, u tizimga kira olish yoki kira olmasiligi mumkin. Bu o‘z navbatida tizim qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga sabab bo‘ladi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda qaraladi.

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

Hujumchi kabi fikrlash- oq qalpoqli xakerlarning afzalliklaridan biridir. Ular zaifliklar va xatolarni ulardan foydalanish uchun emas, balki kompaniyalar va shaxslarni har qanday yo'qotishlardan himoya qilish uchun qidiradilar.

HackerOne ma'lumotlariga ko'ra, 450 000 dan ortiq oq qalpoqli xakerlar allaqachon platformada ro'yxatdan o'tgan va o'z xizmatlarini haq evaziga taqdim etadi.

Axborot xavfsizligi - bu axborotni, shuningdek, uning eng muhim elementlarini, shu jumladan ushbu ma'lumotlarni ishlatish, saqlash va uzatish uchun mo'ljallangan tizimlar va uskunalarni saqlash va himoya qilish. Boshqacha qilib aytganda, bu axborot xavfsizligini himoya qilish uchun zarur bo'lgan texnologiyalar, standartlar va boshqaruv amaliyotlari to'plamidir.

Axborot xavfsizligining maqsadi axborot ma'lumotlarini va qo'llab-quvvatlovchi infratuzilmani ma'lumotlarning yo'qolishiga yoki ruxsatsiz o'zgartirishga olib kelishi mumkin bo'lgan tasodifiy yoki qasddan buzishdan himoya qilishdir. Axborot xavfsizligi biznesning uzluksizligini ta'minlashga yordam beradi.

Axborotni himoyalash – axborot xavfsizligini taminlashga 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.

Risk nima ekanligi haqida keng tasavvurga ega bo‘ldik ammo, lekin uni hisoblashning o‘ziga xos usuli borligini bilmaymiz bu jarayonini shunday ko‘rinadi:

$$\boldsymbol{A + T + V = risk}$$

Ushbu tenglamada “***A***” “*aktiv*” ga, “**T**” “tahdid”ga va “**V**” zaiflikka ishora qiladi. Ushbu uchta elementni aniqlash va aniqlash orqali biz har bir xavf haqida aniq tasavvurga ega bo‘lamiz.

Aktiv-har qanday ma’lumot, qurilma yoki tashkilot tizimlarining boshqa komponenti bo‘lib, u ko‘pincha maxfiy ma’lumotlarni o‘z ichiga olganligi yoki bunday ma’lumotlarga kirish uchun ishlatilishi mumkinligi sababli qimmatlidir.

Masalan, xodimning ish stoli kompyuteri, noutbuki yoki kompaniya telefoni ushbu qurilmalardagi ilovalar kabi aktiv hisoblanadi. Xuddi shunday, muhim infratuzilma, masalan, serverlar va qo‘llab-quvvatlash tizimlari ham aktivlardir.

Tahdid - bu aktivga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan har qanday hodisa - masalan, agar u yo‘qolsa, oflayn rejimda bo‘lsa yoki ruxsat etilmagan shaxs tomonidan foydalanilsa.

Tahdidlar aktivning maxfiyligi, yaxlitligi yoki foydalanuvchanligini buzadigan holatlar sifatida tasniflanishi mumkin va ular qasddan yoki tasodifiy bo‘lishi mumkin.

Zaiflik - bu aktivni yo‘q qilish, zarar yetkazish yoki buzish tahdidi bilan foydalanish mumkin bo‘lgan tashkiliy nuqson.

Murakkabligi va yangilanish chastotasi tufayli dasturiy ta’minotingizda zaiflikka duch kelishingiz mumkin. Xatolar deb nomlanuvchi ushbu zaif tomonlardan jinoiy xakerlar maxfiy ma’lumotlarga kirish uchun foydalanishi mumkin.

Zaifliklar faqat texnologik kamchiliklarga taalluqli emas. Bular jismoniy zaifliklar bo‘lishi mumkin, masalan, ruxsatsiz shaxslarga sizning binolaringizning cheklangan qismiga kirishiga ruxsat beruvchi buzilgan qulf yoki xodimlarning ma’lumotlarni oshkor qilishiga olib kelishi mumkin bo‘lgan noto‘g‘ri yozilgan (yoki mavjud bo‘lmagan) jarayonlar.

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

Kiberxavfsizlik va axborot xavfsizligi o'rtasidagi farq

1) *Xavfsizlik*.Ikkala atama ham bir-biriga sinonimdir, ammo ular orasidagi farq juda nozik. Kiberxavfsizlik - bu sizning kibermakoningizni ruxsatsiz raqamli kirishdan himoya qilish. Shunday qilib, elektron shakldagi ma'lumotlarni himoya qilish haqida. Axborot xavfsizligi - bu sizning axborot aktivlaringizni ruxsatsiz kirishdan himoya qilishdir.

2) *Ma'lumotlar qiymati*. Ikkala holatda ham eng muhim komponent ma'lumotlarning qiymati hisoblanadi. Kiberxavfsizlik sohasida asosiy vazifa kompaniyangizning axborot va xavfsizlik texnologiyalarini (AKT) ruxsatsiz raqamli kirishdan himoya qilishdir. U kibermakon orqali kirish mumkin bo'lgan barcha narsalarni o'z ichiga oladi. Axborot xavfsizligi - bu sizning kompaniyangizning axborot aktivlarini har qanday tahdidlardan himoya qilishdir.

3) *Xavfsizlik bo'yicha mutaxassislar*.Xavfsizlik va kiberxavfsizlik bo'yicha mutaxassislar ilg'or doimiy tahdid bilan shug'ullanishadi. Bu degani, tahdid yaqin va sizning kibermakoningizga kirib borishi va ma'lumot olishi mumkin. Boshqa tomondan, axborot xavfsizligi ma'lumotlar xavfsizligining asosidir va xavfsizlik mutaxassislari tahdidlarga qarshi kurashishdan oldin AT resurslarining ustuvorliklari bilan shug'ullanishadi.

4) *Kiberxavfsizlik va axborot xavfsizligi funksiyasi*.Kiberxavfsizlik kiber sohada mavjud yoki bo'lmasligi mumkin bo'lgan tahdidlar bilan shug'ullanadi, masalan, sizning ijtimoiy media akkauntlaringizni, shaxsiy ma'lumotlaringizni va hokazolarni himoya qilish. Axborot xavfsizligi asosan axborot aktivlari va ularning yaxlitligi, maxfiyligi va mavjudligi bilan bog'liq. Bular axborot xavfsizligining uchta maqsadidir.

Kiberxavfsizlik va axborot xavfsizligi haqida qisqacha ma'lumot

Zo'ravon kiberhujumlar xakerlar hamjamiyatida keng tarqalgan amaliyotga aylanganligi sababli, tashkilotlar o'z infratuzilmasini ruxsatsiz kirishdan himoya qilishga mas'uldirlar. Bu xususiy sektor bilan cheklanmaydi; davlat muassasalari ham ushbu kiber hujumlarga nisbatan bir xil darajada zaifdir. Kundalik ravishda o'ta nozik ma'lumotlar bilan shug'ullanadigan kompaniyalar bilan ularning infratuzilmasini himoya qilish uchun ilg'or xavfsizlik tizimlarini o'rnatish kerak.

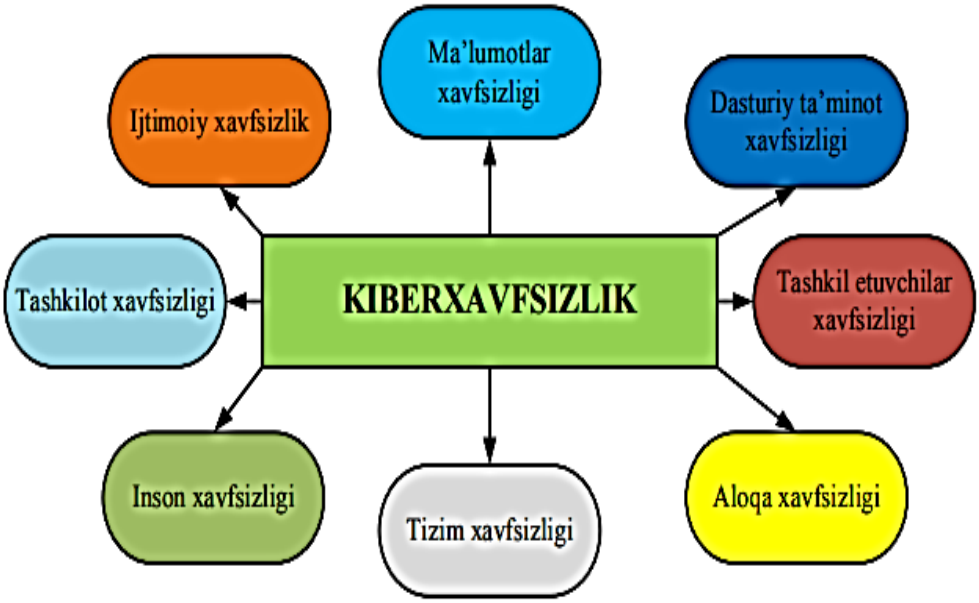
Bu kiberxavfsizlik va axborot xavfsizligini keltirib chiqaradi. Ikkala atama bir-biriga sinonim bo'lsa-da, ular orasidagi farq juda nozik. Kiberxavfsizlik tarmoqlar, kompyuterlar va ma'lumotlarni ruxsatsiz elektron kirishdan himoya qilish bilan shug'ullansa, axborot xavfsizligi axborot aktivlarini himoya qilish bilan shug'ullanadi. u jismoniy yoki raqamli formatdagi ma'lumot bo'ladimi. Xavfsizlik texnologiyalari va tahdidlarini tushunish kiberxavfsizlik va axborot xavfsizligi bo'yicha mutaxassislar uchun juda muhimdir.

Axborot xavfsizligi sohasi, axborotning ifodalanishidan qat'iy nazar (qog‘oz ko‘rinishidagi, elektron va insonlar fikrlashida, og‘zaki va vizual) intelektual huquqlarni himoyalash bilan shug‘ullanadi. Kiberxavfsizlik esa elektron shakldagi axborotni (barcha holatdagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug‘ullanadi.Bundan tashqari, hukumatlar tomonidan moliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced 12 persistent threats, APT) ham aynan kiberxavfsizlikka tegishli. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo‘nalishi deb tushunish uni to‘g‘ri anglashga yordam beradi.

Kiberxavfsizlikning bilim sohalari. CSEC2017 JTF manbasiga ko‘ra kiberxavfsizlik 8 ta bilim sohasiga bo‘lingan, o‘z o‘rnida ularning har biri qismsohalarga bo‘linadi (1.4-rasm).

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

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



1.4-rasm. Kiberxavfsizlikning bilim sohalari

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

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

"*Tizim xavfsizligi*" bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat tizim xavfsizligining jihatlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun, nafaqat uning tarkibiy qismlari va ularning bog‘lanishlarini tushunish, balki yaxlitlikni ham hisobga olish talab etiladi.

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

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

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

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

1.2. Kiberxavfsizlik inson omili

Kiberxavfsizlikdagi inson omillari inson xatosi muvaffaqiyatli ma’lumotlar yoki xavfsizlik buzilishiga olib keladigan vaziyatlarni nazarda tutadi; ular har qanday AKT infratuzilmasi xavfsizligi uchun eng zaif komponent bo‘lib, kompaniya yoki tashkilot uchun eng katta xavf va tahdidlarni nazarda tutadi.

Inson xatosi kiberxavfsizlik buzilishining asosiy sababidir. Masalan, 2021 yilda “IBM Cyber Security Intelligence Index Report” ma’lumotlariga ko‘ra, ushbu buzilishlarning 95 foizi uchun javobgar bo‘lgan. Bu shuni anglatadiki, agar inson omillari yumshatilsa, xavfsizlikning 20 ta buzilishidan faqat 1 tasi sodir bo‘ladi.

Eng muhim inson omillariga quyidagilar taalluqli:

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

— *Risklarni bartaraf etishni va ular haqida xabar berishning yetarli bo‘lmasligi* kiberxavfsizlikda takrorlanuvchi va kutilmagan buzilishlarga sababchi bo‘ladi. Insonlar odatda tashkilotlariga jiddiy xavf soluvchi risk mavjudligini bilishsada, uni oshkor qilishmaydi. Buning asosiy sababi sifatida risk bevosita

shaxsning o‘ziga, uni moliyaviy holatiga ta’sir etmasligini yoki oshkor qilinganida shaxsning obro‘si tushishini keltirishadi.

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

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

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

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

1.3. Kiberjinoyatchilik, kiberqonunlar va kiberetika

Kiberjinoyatchilik-har qanday noqonuniy harakatni sodir etish yoki unga yordam berish uchun har qanday aloqa moslamasidan noqonuniy foydalanish va

bitta tarmoq ostidagi kompyuter yoki kompyuterlar guruhiga zarar yetkazish maqsadida maqsadli yoki foydalaniladigan jinoyat turi tushuniladi hamda kompyuter tarmoqlari yordamida sodir etiladi. Ular jismoniy shaxslar, biznes guruhlari yoki hatto hukumatlarga qaratilgan bo‘lishi mumkin.

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

Ichki kiberjinoyatlar: tarmoqqa yoki kompyuter tizimiga, ular bilan tanish va ulardan qonuniy foydalanish huquqiga ega bo‘lgan shaxs tomonidan, amalga oshiriladi. Ba’zida xodim o‘z kompaniyasini ixtiyoriy ravishda sabotaj qilishiga ishonish qiyin bo‘lishi mumkin va ba’zida bu o‘z-o‘zidan sodir bo‘lsa-da, aksariyat hollarda bu tasodifiydir.

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

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

✓ *Elektron pochta va internetda firibgarlik*: qurbonlarni aldash yoki ulardan foydalanish uchun internetga kirish imkoniga ega onlayn xizmatlar va dasturlardan foydalanishni o‘z ichiga oladi. “Internet firibgarligi” atamasi odatda internet yoki elektron pochta orqali sodir bo‘ladigan kiberjinoyatchilik faoliyatini, jumladan, shaxsiy ma’lumotlarni o‘g‘irlash , fishing va odamlarni puldan olish uchun mo‘ljallangan boshqa xakerlik faoliyati kabi jinoyatlarni qamrab oladi.

Internetdagi firibgarlik hujumlarning bir nechta asosiy turlariga bo‘linishi mumkin, jumladan:

Fishing va firibgarlik: shaxsiy ma’lumotlar, login ma’lumotlari va moliyaviy ma’lumotlarni almashishda qurbonlarni aldash uchun elektron pochta va onlayn xabar almashish xizmatlaridan foydalanish.

Ma’lumotlarning buzilishi: maxfiy, himoyalangan yoki maxfiy ma’lumotlarni xavfsiz joydan o‘g‘irlash va ularni ishonchsiz muhitga ko‘chirish. Bunga foydalanuvchilar va tashkilotlardan o‘g‘irlangan ma’lumotlar kiradi.

Xizmatni rad etish (DoS): zararli niyatni keltirib chiqarish uchun onlayn xizmat, tizim yoki tarmoqqa trafikka kirishni to‘xtatish.

Zararli dastur: foydalanuvchilar qurilmalariga zarar yetkazish yoki o‘chirish yoki shaxsiy va maxfiy ma’lumotlarni o‘g‘irlash uchun zararli dasturlardan foydalanish.

Ransomware: foydalanuvchilarning muhim ma’lumotlarga kirishiga to‘sqinlik qiladigan, keyin esa kirishni tiklash vadasida to‘lov talab qiladigan zararli dastur turi. Ransomware odatda fishing hujumlari orqali yetkaziladi.

Biznes elektron pochta kelishuvi (BEC): tez-tez pul o‘tkazmalarini amalga oshiradigan korxonalarga qaratilgan hujumning murakkab shakli. Bu ruxsatsiz to‘lovlarni topshirish uchun ijtimoiy muhandislik texnikasi orqali qonuniy elektron pochta hisoblarini buzadi .

✓ *Identifikatsiya firibgarligi* (*shaxsiy ma’lumotlar o‘g‘irlangan va foydalanilganda*): o‘g‘irlangan shaxsni jinoiy faoliyatda aldash yo‘li bilan tovarlar yoki xizmatlar olish uchun foydalanish deb ta'riflash mumkin.

Firibgarlar sizning shaxsiy ma’lumotlaringizdan quyidagi maqsadlarda foydalanishi mumkin:

— Bank hisoblarini ochish.

— Kredit kartalari, kreditlar va davlat imtiyozlarini oling.

— O‘z nomingizdan tovarlarga buyurtma bering.

— Mavjud hisoblaringizni qabul qiling.

— Mobil telefon shartnomalarini olib tashlang.

— Pasport va haydovchilik guvohnomasi kabi haqiqiy hujjatlarni o‘z nomingizga oling.Shaxsning shaxsiy ma’lumotlarini o‘g‘irlash o‘z-o‘zidan shaxsiy firibgarlik hisoblanmaydi. Ammo bu identifikatordan yuqoridagi harakatlar uchun foydalanish.

✓ *Moliyaviy yoki karta to‘lovi ma’lumotlarini o‘g‘irlash*: u shaxsiy ma’lumotni o‘g‘irlashning bir turi bo‘lib, hisobdan xaridlarni to‘lash yoki undan pul mablag‘larini olib tashlash maqsadida birovning kredit karta ma’lumotlarini ruxsatsiz olib qo‘yishni o‘z ichiga oladi.

✓ *Korporativ ma’lumotlarni o‘g‘irlash va sotish*: shuningdek, ma’lumot o‘g‘irlash deb ham ataladi - shaxsiy, maxfiy yoki moliyaviy ma’lumotlarni noqonuniy uzatish yoki saqlash. Bunga parollar, dasturiy ta’minot kodi yoki algoritmlari hamda xususiy jarayonlar yoki texnologiyalar kiradi. Ma’lumotlarni o‘g‘irlash jiddiy xavfsizlik va maxfiylikning buzilishi hisoblanadi va jismoniy shaxslar va tashkilotlar uchun jiddiy oqibatlarga olib kelishi mumkin..

✓ Kiber tovlamachilik (tahdid qilingan hujumning oldini olish uchun pul talab qilish).

✓ Ransomware hujumlari (kiber tovlamachilikning bir turi).

✓ Cryptojacking (bu erda xakerlar o‘zlariga tegishli bo‘lmagan resurslardan foydalangan holda kriptovalyutani qazib olishadi).

✓ Kiberjosuslik (bu erda xakerlar hukumat yoki kompaniya ma’lumotlariga kirishadi).

✓ Tarmoqni buzadigan tarzda tizimlarga aralashish.

✓ Mualliflik huquqini buzish.

✓ Noqonuniy qimor o‘yinlari.

✓ Internetda noqonuniy narsalarni sotish.

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

kiberjinoatchilikni tartibga solishni maqsad qilgan qonunlar kiberqonunlar deb ataladi.

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

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

Xususan, Respublikamizda ham “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili ”da amalga oshirishga oid davlat dasturi 19 to‘g‘risida”gi O‘zbekiston Respublikasi Prezidenti Farmoni loyihasi va 2020 yil Davlat dasturi loyihasida 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqish rejalashtirilgan. Hujjatga asosan xavfsizlikni, millatlararo totuvlik va diniy bag‘rikenglikni taminlash, shuningdek, tashqi siyosat sohasida:

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

Loyihada:

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

− kiberxavfsizlikni taminlash sohasida davlat organlari, korxona va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish;

− ushbu sohadagi normativ-huquqiy hujjatlarni unifikatsiyalash nazarda tutiladi. Kiberqonunlar har bir davlatning milliy qonun me’yorlari asosida shakllantiriladi yoki ularning bir qismini tashkil qiladi. Quyida Respublikamizdagi qonun hujjatlarida kiberjinoyatni va kiberxavfsizlikni oldini olish va tartibga solishga aloqador bo‘lgan bandlar keltirilgan.

O‘zbekiston Respublikasining kiberxavfsizlik to’g’risidagi qonuni Qonunchilik palatasi tomonidan 2023-yil 25-fevralda qabul qilingan Senat tomonidan 2023-yil 17-martda ma’qullangan biz ushbu qonuni ba’zi moddalariga to’xtalib o’tamiz

9-modda. O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi prinsipi

O‘zbekiston Respublikasi kiberxavfsizlikni ta’minlash sohasida xalqaro shartnomalar doirasida xalqaro tashkilotlar, chet davlatlar va ularning vakolatli idoralari bilan xalqaro hamkorlikni amalga oshiradi.

10-modda. Kiberxavfsizlik sohasidagi yagona davlat siyosati

Kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi.

11-modda. Kiberxavfsizlik sohasidagi vakolatli davlat organi

O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organidir (bundan buyon matnda vakolatli davlat organi deb yuritiladi).

Vakolatli davlat organining kiberxavfsizlik sohasidagi vakolatlari jumlasiga quyidagilar kiradi:

kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqish;

kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirish;

kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish;

kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rish;

favqulodda vaziyatlarda axborot tizimlari va resurslarini kiberhimoya qilish hamda kiberxavfsizlik sohasidagi boshqa masalalar bo‘yicha chora-tadbirlarni o‘z ichiga olgan rejalarni ishlab chiqish;

kiberxavfsizlikni ta’minlashga doir ishlarni, shuningdek muhim axborot infratuzilmasi obyektlarida kiberhujumlarning oldini olishga, ularni aniqlashga va ularning oqibatlarini tugatishga doir ishlarni tashkil etish;

kiberxavfsizlik talablariga muvofiq axborot tizimlari va resurslaridagi apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirishga doir ishlarni tashkil etish;

kiberxavfsizlik sohasida tadqiqotlar o‘tkazilishini va monitoringni tashkil etish;

muhim axborot infratuzilmasi obyektlarining yagona reyestrini shakllantirish, shuningdek ushbu reyestrning yuritilishini tashkil etish va ta’minlash;

kiberxavfsizlik subyektlari tomonidan taqdim etilgan ma’lumotlar asosida obyektlarni muhim axborot infratuzilmasi obyektlarining yagona reyestriga kiritish to‘g‘risida qaror qabul qilish;

muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlashga doir talablarni belgilash;

axborotlashtirish obyektlarini va muhim axborot infratuzilmasi obyektlarini kiberxavfsizlik talablariga muvofiq attestatsiyadan o‘tkazish tartibini belgilash;

axborotni kriptografik himoya qilish vositalarini ishlab chiqishga, ishlab chiqarishga va realizatsiya qilishga doir faoliyatni litsenziyalash;

axborot tizimlaridan hamda resurslaridan foydalanuvchilarning huquqlari va qonuniy manfaatlarini himoya qilish choralarini ko‘rish;

kiberxavfsizlik subyektlarining axborot tizimlarini va resurslarini o‘rganish va tekshirishni, shuningdek muhim axborot infratuzilmasi obyektlarida o‘rganishlar va tekshirishlarni amalga oshirish;

muhim axborot infratuzilmasi obyektlariga bo‘lgan kiberhujumlarga urinishlarning oldini olishga doir rejalarni ishlab chiqish va ularni bevosita amalga oshirish;

kiberxavfsizlik bo‘linmalarining, mustaqil ekspertlar xizmatlari va guruhlarining faoliyatini tartibga solish, kibertahdidlarga qarshi kurashish sohasida huquqni muhofaza qiluvchi organlar bilan hamkorlik qilish;

davlat va xo‘jalik boshqaruvi organlarini, mahalliy davlat hokimiyati organlarini axborot tizimlari hamda resurslarida aniqlangan zaifliklar, kibertahdidlar, kiberhujumlar va boshqa buzg‘unchi xatti-harakatlar to‘g‘risida xabardor qilish;

huquqni muhofaza qiluvchi organlarni va muhim axborot infratuzilmasi subyektlarini muhim axborot infratuzilmasi obyektlarida kiberxavfsizlik hodisalarini birgalikda tekshirishga jalb etish;

kiberxavfsizlik sohasida xalqaro hamkorlikni amalga oshirish va kibertahdidlarga qarshi kurashish bo‘yicha umumiy yondashuvlarni ishlab chiqish, kiberjinoyatchilik bo‘yicha tergov harakatlarini olib borish hamda kiberjinoyatchilikning oldini olish borasidagi sa’y-harakatlarni birlashtirish, shuningdek O‘zbekiston Respublikasining kibermakonidan terrorchilik, ekstremistik va boshqa qonunga xilof faoliyatda foydalanilishiga yo‘l qo‘ymaslik choralarini ko‘rish;

muhim axborot infratuzilmasi obyektlarida kiberhujumlarni aniqlash, ularning oldini olish va oqibatlarini bartaraf etish vositalarini joriy etishga doir

ishlarni tashkil qilish, shuningdek kiberxavfsizlik hodisalariga nisbatan choralar ko‘rish;

muhim axborot infratuzilmasi obyektlaridagi mavjud zaifliklar va ehtimoldagi tahdidlar to‘g‘risidagi ma’lumotlarni aniqlashga, to‘plashga va tahlil qilishga doir ishlarni tashkil etish;

axborot tizimlari va resurslarida kiberxavfsizlikning ta’minlanganlik darajasi bo‘yicha tasniflagich yaratish;

kiberxavfsizlik obyektlarini kiberxavfsizlikni ta’minlash darajasiga ko‘ra tasniflash;

kiberxavfsizlik sohasida kadrlar tayyorlash bo‘yicha faoliyatni amalga oshirish;

kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertiza o‘tkazish mexanizmlarini belgilash;

kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini amalga oshirishni baholash usullarini belgilash va baholash;

muhim axborot infratuzilmasi obyektlarini toifalashtirish mezonlarini belgilash va toifalashtirish;

kiberxavfsizlik subyektlarining kiberxavfsizligini ta’minlashga jalb etilgan xodimlarni qonunchilikda belgilangan tartibda attestatsiyadan o‘tkazish.

Vakolatli davlat organining qonuniy talablarini (ko‘rsatmalarini) bajarish majburiydir.

12-modda. Vakolatli davlat organining huquqlari

Vakolatli davlat organi kiberxavfsizlik sohasidagi vakolatlarni amalga oshirish chog‘ida quyidagi huquqlarga ega:

kiberhujumlarni aniqlash, ularning oldini olish va oqibatlarini bartaraf etish, shuningdek kiberxavfsizlik hodisalariga nisbatan choralar ko‘rish uchun mo‘ljallangan texnik, dasturiy va apparat-dasturiy vositalarni ijaraga olish;

kiberhujumlarga barham berish bo‘yicha kechiktirib bo‘lmaydigan choralar ko‘rish uchun texnik qurilmalar va xizmatlardan tekin foydalanish;

davlat organlariga va boshqa tashkilotlarga kirish, zarur hujjatlar va materiallar bilan tanishish, shuningdek davlat organlaridan va boshqa tashkilotlardan, fuqarolardan ma’lumotlarni hamda boshqa zarur hujjatlarni va materiallarni so‘rash hamda olish, ularni identifikatsiyalashni amalga oshirish va ulardan kiberxavfsizlik hodisalari bo‘yicha tergov harakatlarida foydalanish;

kiberxavfsizlikni ta’minlash bo‘yicha ishchi organni tashkil etish, shuningdek o‘z vakolatlarining bir qismini unga o‘tkazish;

kiberxavfsizlik subyektlariga kiberxavfsizlikka tahdid soluvchi huquqbuzarliklar sodir etilishiga imkon bergan sabablar va shart-sharoitlarni bartaraf etish to‘g‘risida bajarilishi majburiy bo‘lgan taqdimnomalar hamda ko‘rsatmalar kiritish;

kiberxavfsizlik holati ta’minlanganligi yuzasidan davlat nazorati va tekshiruvi vazifasini amalga oshirish maqsadida davlat organlari hamda tashkilotlarining, muhim axborot infratuzilmasi obyektlarining axborot tizimlariga va resurslariga belgilangan tartibda to‘sqinliksiz kirish hamda ularga ulanish, shuningdek ushbu obyektlardagi axborot tizimlarining va resurslarning kiberxavfsizligini ta’minlash vositalarining joriy etilishiga hamda ulardan foydalanilishiga doir ma’lumotlarni o‘rganish;

kiberxavfsizlikni ta’minlash bo‘yicha monitoring ishlarini bajarish chog‘ida tashkiliy-texnik tadbirlarni amalga oshirish uchun monitoring tizimlariga yoki muhim axborot infratuzilmasi obyektlariga kirish;

jismoniy va yuridik shaxslarning turar joylariga va boshqa obyektlariga to‘sqinliksiz kirish, zarurat bo‘lganda qulflash moslamalarini va boshqa ashyolarni buzgan holda kirish, bu joylarni axborot texnologiyalari sohasida jinoyatlar sodir etganlikda gumon qilinayotgan shaxslarni ta’qib qilish chog‘ida yoxud u erda jinoyat sodir etilyapti yoki sodir etilgan yoxud huquqni muhofaza qiluvchi organlardan yashiringan shaxs bor deb hisoblash uchun yetarli asoslar mavjud bo‘lgan taqdirda yoxud agar kechiktirish fuqarolarning hayotini va sog‘lig‘ini tahdid ostida qoldiradigan bo‘lsa, yigirma to‘rt soat ichida prokurorga bu haqda

xabar bergan holda, shuningdek yetkazilgan zararning o‘rnini qonunchilikda belgilangan tartibda qoplagan holda ko‘zdan kechirish.

13-modda. Vakolatli davlat organining majburiyatlari

Vakolatli davlat organi kiberxavfsizlik sohasida zimmasiga yuklatilgan vakolatlarni amalga oshirish chog‘ida:

kiberjinoyatlarning oldini olish, aniqlash va bartaraf etish bo‘yicha barcha zarur choralarni ko‘rishi;

kiberxavfsizlik sohasidagi davlat dasturlarini ishlab chiqish va amalga oshirishda ishtirok etishi;

kiberxavfsizlik sohasidagi muammolar yuzasidan ilmiy-tadqiqot va tashkiliy-uslubiy faoliyatni amalga oshirishi;

kiberjinoyatlar hamda kiberxavfsizlikka tahdid soluvchi huquqbuzarliklar to‘g‘risidagi murojaatlar va ma’lumotlarni ro‘yxatdan o‘tkazishi, ular yuzasidan qonunchilikda belgilangan tartibda o‘z vaqtida choralar ko‘rishi;

kiberxavfsizlikka tahdid soluvchi huquqbuzarliklarning oldini olish, ularning sodir etilishiga imkon bergan sabablar va shart-sharoitlarni aniqlash hamda ularni bartaraf etish choralarini ko‘rishi;

vakolatli davlat organi xodimlari jismoniy va yuridik shaxslarning turar joylariga hamda boshqa obyektlariga mulkdorlar va ular vakillarining roziligisiz yoki ushbu shaxslar yo‘qligida kirganligi to‘g‘risidagi barcha holatlar yuzasidan prokurorni yigirma to‘rt soat ichida yozma shaklda xabardor qilishi shart.

Vakolatli davlat organining zimmasiga qonunchilikka muvofiq boshqa majburiyatlar ham yuklatilishi mumkin.

14-modda. Davlat organlari va tashkilotlarining kiberxavfsizlikni ta’minlash borasidagi huquq va majburiyatlari

Davlat organlari va tashkilotlari quyidagi huquqlarga ega:

kiberxavfsizlikni ta’minlash maqsadida vakolatli davlat organidan kibertahdidlar, dasturiy ta’minotdagi, uskunalar va texnologiyalardagi zaifliklar to‘g‘risidagi axborotni olish;

vakolatli davlat organidan kiberhujumlardan himoya qilish vositalari va usullari, ularni aniqlash hamda bartaraf etish yo‘llari to‘g‘risida axborot va maslahatlar olish;

kiberxavfsizlikni ta’minlashga doir chora-tadbirlarni ishlab chiqish va amalga oshirish.

Davlat organlari va tashkilotlari:

o‘z tasarrufidagi axborot tizimlari va resurslarining kiberxavfsizligini, tarmoqlar ishining barqarorligini ta’minlashi, shuningdek kiberxavfsizlik bo‘yicha o‘z majburiyatlarini bajarishi, vakolatli davlat organini kiberhujumlar to‘g‘risida ogohlantirishi;

o‘z axborot tizimlari va resurslarida saqlanayotgan ma’lumotlarning o‘g‘irlanishi hamda qalbakilashtirilishi holatlarining oldini olish choralarini ko‘rishi;

o‘z axborot tizimlari va resurslarini kiberhimoya qilish uchun sertifikatlashtirilgan apparat, apparat-dasturiy va dasturiy ta’minotdan foydalanishi;

kiberxavfsizlik sohasida ishlab chiqiladigan normativ-huquqiy hujjatlarni va texnik jihatdan tartibga solish sohasidagi normativ hujjatlarni vakolatli davlat organi bilan kelishishi shart.

15-modda. Ma’lumotlarning zaxira nusxalarini ko‘chirish

Davlat organlari va tashkilotlarining, shuningdek muhim axborot infratuzilmasi obyektlarining axborot tizimlari hamda resurslari ma’lumotlarining saqlanishini ta’minlash ichki axborot xavfsizligi siyosatiga muvofiq ma’lumotlarning zaxira nusxalarini yaratish yo‘li bilan amalga oshiriladi, ularning saqlanish muddati oxirgi uch oydan kam bo‘lmasligi kerak.

16-modda. Kiberxavfsizlik subyektlarining huquq va majburiyatlari

Kiberxavfsizlik subyektlari quyidagi huquqlarga ega:

o‘z kiberxavfsizligini ta’minlash maqsadida vakolatli davlat organidan kibertahdidlar, dasturiy ta’minotdagi, uskunalar va texnologiyalardagi zaifliklar to‘g‘risidagi ma’lumotlarni olish;

kiberhujumlardan himoya qilish vositalari va usullari, shuningdek ularni aniqlash hamda bartaraf etish usullari to‘g‘risida vakolatli davlat organidan ma’lumotlar va maslahatlar olish;

o‘z kiberxavfsizligini ta’minlash bo‘yicha chora-tadbirlarni ishlab chiqish va amalga oshirish.

Kiberxavfsizlik subyektlari:

axborot tizimlari va resurslaridagi ma’lumotlarning qonunga xilof ravishda tarqatilishi, o‘g‘irlanishi, yo‘qolishi, yaxlitligining buzilishi, bloklanishi va qalbakilashtirilishining, shuningdek axborot tizimlari va resurslariga ruxsatsiz kirishning boshqa ko‘rinishlarining oldini olishi, bunday hollar aniqlanganda o‘z vaqtida tegishli choralar ko‘rishi;

axborot tizimlari va resurslariga kirish tartibi buzilganda hamda ularga ruxsatsiz kirish natijasida ushbu tizimlar hamda resurslar o‘zgartirilgan yoki yo‘q qilingan taqdirda salbiy oqibatlarni kamaytirish maqsadida ularni tezkorlik bilan tiklash choralarini ko‘rishi;

sodir bo‘lgan kiberxavfsizlik hodisalari va kiberjinoyatlar to‘g‘risida vakolatli davlat organini xabardor qilishi, ushbu hodisalarni to‘liq fosh etish uchun tegishli raqamli izlarning yo‘qolishiga yo‘l qo‘ymaslik choralarini ko‘rishi, shuningdek kiberxavfsizlik hodisalarini tahlil qilish va kiberjinoyatlarni tekshirish uchun zarur bo‘lgan ma’lumotlarning doimiy saqlanishini ta’minlashi;

kiberxavfsizlik obyektlarini muhofaza qilish va ularning xavfsiz ishlashi monitoringini o‘tkazish sohasidagi ma’lumotlarni vakolatli davlat organi bilan o‘zaro almashishni amalga oshirishi;

axborot tizimlari va resurslarining kiberhimoyasini ta’minlashda vakolatli davlat organi tomonidan belgilangan kiberxavfsizlik talablariga rioya etishi;

kiberxavfsizlik hodisalariga nisbatan choralar ko‘rish mexanizmlarining ishlab turishini va kiberxavfsizlikni ta’minlash bo‘linmalarining ishlashini ta’minlashi, ular mavjud bo‘lmagan taqdirda esa vakolatli davlat organining ruxsati bilan autsorsing xizmatlaridan belgilangan tartibda foydalanishi;

vakolatli davlat organiga kiberxavfsizlikni ta’minlash monitoringining tashkiliy-texnik tadbirlarini amalga oshirish uchun monitoring tizimlariga va (yoki) kiberxavfsizlik obyektlariga kirish huquqini berishi shart.

17-modda. Kiberxavfsizlik obyektlarini tasniflash

Kiberxavfsizlik obyektlarini tasniflash kiberxavfsizlik obyektlari turining tashkiliy-texnik jihatdan murakkabligi darajasini aniqlashga qaratilgan tashkiliy tadbirlar majmuidan iboratdir.

Tasniflanishi lozim bo‘lgan kiberxavfsizlik obyektlarining toifalari qonunchilikka muvofiq belgilanadi.

20-modda. Axborotlashtirish obyektlarining va muhim axborot infratuzilmasi obyektlarining attestatsiyasi

Axborotlashtirish obyektlarining hamda muhim axborot infratuzilmasi obyektlarining attestatsiyasi axborotlashtirish obyektlarining haqiqiy himoyalanganlik holatining kiberxavfsizlik sohasidagi davlat standartlari va normativ-huquqiy hujjatlar talablariga muvofiqligini aniqlashga qaratilgan tashkiliy-texnik tadbirlar majmuidan iboratdir.

Attestatsiyadan o‘tkazilishi lozim bo‘lgan axborotlashtirish obyektlarining va muhim axborot infratuzilmasi obyektlarining toifalari qonunchilikka muvofiq belgilanadi.

Axborotlashtirish obyektlarining va muhim axborot infratuzilmasi obyektlarining kiberxavfsizlik talablariga muvofiqligini attestatsiyadan o‘tkazish tartibi vakolatli davlat organi tomonidan belgilanadi.

21-modda. Kiberxavfsizlikning ta’minlanganlik darajasini baholash

Kiberxavfsizlikning ta’minlanganlik darajasini baholash axborot tizimlari va resurslarining himoyalanganlik holatini, shuningdek ko‘rilayotgan tashkiliy choralarning samaradorligini aniqlashga qaratilgan tashkiliy-texnik tadbirlar majmuidan iboratdir.

Baholanishi shart bo‘lgan axborotlashtirish obyektlarining va muhim axborot infratuzilmasi obyektlarining toifalari qonunchilikka muvofiq belgilanadi.

Kiberxavfsizlikning ta’minlanganlik darajasini baholash tartibi vakolatli davlat organi tomonidan belgilanadi.

Vakolatli davlat organi baholash natijasida aniqlangan kamchiliklarni bartaraf etish to‘g‘risida bajarilishi shart bo‘lgan ko‘rsatmalar beradi.

22-modda. Kiberxavfsizlik hodisalarini tekshirish

Kiberxavfsizlik hodisalari vakolatli davlat organi yoki kiberxavfsizlikni ta’minlash bo‘yicha ishchi organning mansabdor shaxslari tomonidan tekshiriladi.

Kiberxavfsizlik hodisasi sodir bo‘lgan axborot resursining yoki axborot tizimining egasi, agar u tekshiruv o‘tkazish uchun zarur bo‘lgan resurslarga va texnik imkoniyatlarga ega bo‘lsa, kiberxavfsizlik hodisasining tekshiruvini o‘tkazishi mumkin. Bunda vakolatli davlat organi tekshiruv natijalari to‘g‘risida xabardor qilinishi kerak.

23-modda. Kiberxavfsizlik subyektlari tomonidan kiberxavfsizlik hodisalari bo‘yicha choralar ko‘rish

Kiberxavfsizlik subyektlari tomonidan kiberxavfsizlik hodisalariga nisbatan choralar ko‘rish quyidagi shakllarda amalga oshirilishi mumkin:

dasturiy ta’minotdagi va qurilmalardagi zaifliklarni hamda xatoliklarni bartaraf etish;

zararli dasturlarni yo‘q qilish, ularning tarqalishini cheklash, kiberhujumlar manbaini texnik jihatdan cheklash;

axborotlashtirish obyektlarini mavjud kibertahdidlardan ajratib qo‘yish;

huquqni muhofaza qiluvchi organlarga kiberxavfsizlik hodisalari to‘g‘risida ma’lumotlar taqdim etish.

25-modda. Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlari

Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlari quyidagilardan iborat:

muhim axborot infratuzilmasi obyektlarining normativ-huquqiy, tashkiliy va texnik jihatdan himoya qilinishini tartibga solish bo‘yicha yagona chora-tadbirlar majmuini yaratish;

davlat organlari va tashkilotlarining axborot tizimlarida hamda resurslarida, muhim axborot infratuzilmasi obyektlarida kiberxavfsizlikni ta’minlashga doir talablarni belgilash;

muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini samarali ta’minlash uchun shart-sharoitlar yaratishga ko‘maklashish.

26-modda. Muhim axborot infratuzilmasi obyektlarini toifalashtirish

Muhim axborot infratuzilmasi obyektlarini toifalashtirish muhim axborot infratuzilmasi obyektlarining ushbu moddaning ikkinchi qismida nazarda tutilgan toifalarga muvofiqligini aniqlash, shuningdek toifalashtirish natijalariga doir ma’lumotlarni tekshirish maqsadida amalga oshiriladi.

Muhim axborot infratuzilmasi obyektlari quyidagi toifalarga bo‘linadi:

yuqori darajadagi muhim axborot infratuzilmasi obyektlari;

o‘rta darajadagi muhim axborot infratuzilmasi obyektlari;

past darajadagi muhim axborot infratuzilmasi obyektlari.

Muhim axborot infratuzilmasi obyektlarini toifalashtirish mezonlari vakolatli davlat organi tomonidan belgilanadi.

27-modda. Muhim axborot infratuzilmasi obyektlarining yagona reyestri

Vakolatli davlat organi muhim axborot infratuzilmasi obyektlarining yagona reyestrini yuritadi.

Muhim axborot infratuzilmasi obyektlarining yagona reyestriga kiritilishi shart bo‘lgan kiberxavfsizlik obyektlarining toifalari qonunchilikka muvofiq belgilanadi.

Kiberxavfsizlik obyektlarini muhim axborot infratuzilmasi obyektlarining yagona reyestriga kiritish tartibi vakolatli davlat organi tomonidan belgilanadi.

29-modda. Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash bo‘yicha talablar

Muhim axborot infratuzilmasi subyektlari o‘ziga tegishli bo‘lgan muhim axborot infratuzilmasi obyektlarida kiberxavfsizlikni ta’minlash yuzasidan vakolatli davlat organi tomonidan belgilangan talablarni bajarishi shart.

Muhim axborot infratuzilmasi subyektlari vakolatli davlat organi bilan kelishgan holda, muhim axborot infratuzilmasi obyektlari ishining o‘ziga xos jihatlaridan kelib chiqib, kiberxavfsizlikni ta’minlash uchun qo‘shimcha talablarni belgilashi mumkin.

Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligi ta’minlanishi uchun mas’ul bo‘lgan xodimlar qonunchilikda belgilangan tartibda vakolatli davlat organi tomonidan o‘tkaziladigan attestatsiyadan o‘tadi.

Muhim axborot infratuzilmasi subyekti tomonidan yaratilgan muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tizimi vakolatli davlat organining muhim axborot infratuzilmasi obyektlaridagi monitoring va kiberxavfsizlik hodisalarini boshqarish tizimiga vakolatli davlat organining qaroriga asosan ulanadi.

30-modda. Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tizimi

Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tizimi quyidagilardan iborat:

vakolatli davlat organining muhim axborot infratuzilmasi obyektlarining kiberxavfsizlik hodisalarini monitoring qilish va boshqarish tizimi;

muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tizimlari.

Kiberxavfsizlikni ta’minlash tizimidagi kiberxavfsizlik hodisalari to‘g‘risidagi axborotning tarqatilishi cheklangan bo‘ladi. Mazkur axborot hodisalar to‘liq bartaraf etilganidan keyin oshkor etilishi mumkin.

31-modda. Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini baholash

Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini baholash kiberxavfsizlik sohasidagi davlat nazorati doirasida ushbu obyektlarning turli xil kibertahdidlardan himoyalanganlik holatini (darajasini) aniqlash maqsadida amalga oshiriladi.

Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini baholash ixtisoslashtirilgan tashkilotlar jalb etilgan holda, vakolatli davlat organining ruxsati bilan amalga oshiriladi.

32-modda. Kiberxavfsizlik subyektlarini davlat tomonidan qo‘llab-quvvatlash

Kiberxavfsizlik subyektlarini davlat tomonidan qo‘llab-quvvatlash quyidagilardan iborat:

kiberxavfsizlik sohasidagi normativ-huquqiy bazani takomillashtirish;

kiberxavfsizlik subyektlariga soliq, bojxona imtiyozlari va preferensiyalar berish;

xo‘jalik yurituvchi subyektlarning mablag‘larini kiberxavfsizlik sohasini moliyalashtirish uchun jalb etishga shart-sharoitlar yaratish;

kiberxavfsizlik sohasida ilmiy-texnika yutuqlariga asoslangan mahsulotlarning va ilg‘or texnologiyalarning kafolatlangan tarzda joriy etilishini ta’minlash maqsadiga qaratilgan davlat xaridlarini tashkil etish;

kiberxavfsizlik sohasida kadrlarni tayyorlashga, qayta tayyorlashga, shuningdek ularning malakasini oshirishga ko‘maklashish.

33-modda. Kiberxavfsizlik sohasida ilmiy-texnik va innovatsion faoliyatni qo‘llab-quvvatlash

Davlat boshqaruvi organlari, mahalliy davlat hokimiyati organlari va xo‘jalik yurituvchi subyektlar tomonidan kiberxavfsizlik sohasidagi ilmiy-texnik va innovatsion faoliyatni qo‘llab-quvvatlash quyidagilar vositasida amalga oshiriladi:

ilmiy-tadqiqot, tajriba-konstruktorlik va texnologik ishlarni davlat buyurtmasi doirasida bajarish uchun buyurtmalarni joylashtirish;

investitsiya loyihalarini amalga oshirish jarayonida amalga oshiriladigan ilmiy-tadqiqot, konstruktorlik va texnologik ishlarni moliyalashtirish uchun kiberxavfsizlik subyektlariga subsidiyalar ajratish;

innovatsion mahsulotlarga bo‘lgan talabni, shu jumladan davlat ehtiyojlari uchun sotib olinadigan tovarlarning (ishlarning, xizmatlarning) maqbullashtirilishini rag‘batlantirish;

kiberxavfsizlik darajasini yaxshilash bo‘yicha loyihalarni amalga oshiradigan, shu jumladan mavjud ilg‘or texnologiyalardan foydalangan holda xizmatlar ko‘rsatish borasidagi innovatsion faoliyat bilan shug‘ullanadigan tashkilotlarga moliyaviy yordam ko‘rsatish;

kiberxavfsizlik sohasida ilmiy, ilmiy-texnik va innovatsion faoliyatni amalga oshirish hamda muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash uchun shart-sharoitlar yaratish;

kiberxavfsizlikni ta’minlash bilan bog‘liq davlat xaridlarini amalga oshirishda mamlakatimizda ishlab chiqarilgan mahsulotga ustuvorlik berish.

34-modda. Kiberxavfsizlikni ta’minlash sohasidagi kadrlar salohiyatini rivojlantirish va qo‘llab-quvvatlash

Davlat boshqaruvi organlarining, mahalliy davlat hokimiyati organlarning va xo‘jalik yurituvchi subyektlarning kiberxavfsizlikni ta’minlash sohasidagi kadrlari salohiyatini rivojlantirish va qo‘llab-quvvatlash quyidagilar vositasida amalga oshirilishi mumkin:

kiberxavfsizlikni ta’minlash sohasidagi kadrlarni qayta tayyorlash va ularning malakasini oshirish bo‘yicha faoliyatni amalga oshiruvchi tashkilotlarga moliyaviy, axborot-maslahat yordami ko‘rsatish;

kiberxavfsizlikni ta’minlash sohasida o‘quv-uslubiy va ilmiy-pedagogik yordam ko‘rsatish.

Muhim axborot infratuzilmasi subyektlarining kiberxavfsizlikni ta’minlash uchun mas’ul bo‘lgan xodimlari xalqaro standartlarga hamda davlat standartlariga va talablariga muvofiq o‘z malakasini doimiy asosda oshirib borishi kerak.

35-modda. Muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash uchun mas’ul bo‘lgan xodimlarni rag‘batlantirish

Muhim axborot infratuzilmasi obyektlarining kiberxavfsizlikni ta’minlash uchun mas’ul bo‘lgan xodimlarini rag‘batlantirish qonunchilikda belgilangan tartibda amalga oshiriladi.

36-modda. Kiberxavfsizlik sohasidagi xalqaro hamkorlik

Vakolatli davlat organi kiberxavfsizlik sohasidagi xalqaro hamkorlikni o‘z vakolatlari doirasida amalga oshiradi.

Vakolatli davlat organi O‘zbekiston Respublikasining qonunchiligiga va xalqaro shartnomalariga muvofiq xalqaro kiberjinoyatchilikka qarshi kurashish masalalariga doir axborotni chet davlatlarga va xalqaro tashkilotlarga so‘rov bo‘yicha taqdim etadi.

Xalqaro kiberjinoyatlarga qarshi kurashish masalalariga doir axborot, agar bunday ma’lumotlar dastlabki tergov harakatlariga yoki sud jarayonlariga to‘sqinlik qilmasa hamda kiberhujumlarni to‘xtatishga, kibermakondan foydalanilgan holda sodir etiladigan jinoiy xatti-harakatlarni o‘z vaqtida aniqlashga va ularga barham berishga xizmat qilsa, chet davlatlarga va xalqaro tashkilotlarga oldindan so‘rovsiz berilishi mumkin.

37-modda. Kiberxavfsizlik to‘g‘risidagi qonunchilikni buzganlik uchun javobgarlik

Kiberxavfsizlik to‘g‘risidagi qonunchilikni buzganlikda aybdor bo‘lgan shaxslar belgilangan tartibda javobgarlikka tortiladi.

38-modda. Ushbu Qonunning ijrosini, yetkazilishini, mohiyati va ahamiyati tushuntirilishini ta’minlash

O‘zbekiston Respublikasi Davlat xavfsizlik xizmati va boshqa manfaatdor tashkilotlar ushbu Qonunning ijrosini, ijrochilarga yetkazilishini hamda mohiyati va ahamiyati aholi o‘rtasida tushuntirilishini ta’minlasin.

39-modda. Qonunchilikni ushbu Qonunga muvofiqlashtirish

O‘zbekiston Respublikasi Vazirlar Mahkamasi:

hukumat qarorlarini ushbu Qonunga muvofiqlashtirsin;

davlat boshqaruvi organlari ushbu Qonunga zid bo‘lgan o‘z normativ-huquqiy hujjatlarini qayta ko‘rib chiqishlari va bekor qilishlarini ta’minlasin.

40-modda. Ushbu Qonunning kuchga kirishi

Ushbu Qonun rasmiy e’lon qilingan kundan e’tiboran uch oy o‘tgach kuchga kiradi.

Kiberetika-kompyuter tizimidan foydalanganda foydalanuvchi tomonidan qabul qilinishi kerak bo‘lgan eng yaxshi amaliyotlarni belgilaydigan kompyuter texnologiyasi xatti-harakatlarining bir tarmog‘i. Oddiy qilib aytganda, kiberetika kompyuter tizimidan foydalanishda rioya qilinishi kerak bo‘lgan asosiy etika va odob-axloq qoidalarini anglatadi.

Kiberetika quyidagilarga yo‘nalishlarni o‘z ichiga oladi.

Maxfiylik: internetda mavjud bo‘lgan kontent shaxslarning axloqiy, hissiy yoki shaxsiy axloqiga zarar keltirmasligi, foydalanuvchilar ochiq baham ko‘rishni istamagan har qanday ma’lumotni himoya qilish, foydalanuvchining aloqa ma’lumotlari, manzili, bank rekvizitlari, kredit karta/debet karta ma’lumotlari kabi xavfsizlik bilan bog‘liq ma’lumotlarning barchasi foydalanuvchi maxfiyligining asosiy kiberetikasiga kiritilgan va hech qanday holatda buzilmasligi kerak. Maxfiylikning har qanday buzilishi foydalanuvchi identifikatori va foydalanuvchining shaxsiy ma’lumotlarini o‘g‘irlash/firibgarlikdir, bu qonun qoidalariga muvofiq jazolanadi.

Intellektual mulk huquqlar: internetda joylashtirilgan kontentga to‘liq huquqqa ega ekanligini belgilaydi, butun kontent faqat muallifga tegishli va hech kim asl ijodkor tomonidan nashr etilgan kontentni o‘ziniki deb da’vo qilishi, birovning ishini ruxsatsiz tarqatishi mumkin emas, chunki asar yaratuvchisiga ijod va pul foyda bermaslik axloqiy jihatdan noto‘g‘ri.

Xavfsizlik: internetdagi xavfsizlik har bir foydalanuvchi kirishi kerak bo‘lgan eng asosiy axloqiy huquqdir, internet foydalanuvchilari tarmoqni kezish paytida o‘zlarini xavfsiz his qilish, xavfsizlik, umuman olganda, faqat avtorizatsiya qilingan foydalanuvchilarning kompyuterdagi tarkibga kirishini anglatadi.

Ishonchlilik: internetda mavjud bo‘lgan tarkibga milliardlab foydalanuvchilar kirishadi, agar internetda joylashtirilgan ma’lumotlarning ishonchliligi bo‘lmasa, u ko‘pchilikni chalg‘itadi, kiberetika har tomonlama to‘g‘ri

bo‘lgan tarkibni internetda joylashtirish muhimligini takidlaydi, foydalanuvchilar internet mazmuniga ishonishadi va ko‘p faktlar uchun internetga tayanadilar, shuning uchun so‘ralgan ma’lumotlarning to‘g‘ri va ishonchli bo‘lishi juda zarur.

Axborot erkinligi - bu so'z erkinligi (so'z erkinligi), ommaviy axborot vositalarining erkin faoliyat ko'rsatishi (matbuot erkinligi), jamiyatning jamoatchilik manfaatlariga mos keladigan ma'lumotlarni olish huquqini o'z ichiga olgan huquq va erkinliklar guruhiga nisbatan qo'llaniladigan tushuncha. davlat xizmatlaridan, axborotni har qanday qonuniy yo'l bilan tarqatish erkinligi .

Axborot izlash, olish va tarqatish erkinligi insonning eng muhim siyosiy va shaxsiy huquqlaridan biri bo‘lib, Inson huquqlari umumjahon deklaratsiyasiga kiritilgan (19-modda). Axborot erkinligi kengaytmasi bo'lgan so'z erkinligi xalqaro huquqda tan olingan asosiy inson huquqidir.

Axborot erkinligi, o'z fikrini ifoda etish erkinligi sifatida, axborotni tashuvchisi va uzatish usuliga bog'liq emas: *og'zaki, yozma, bosma,* Internet orqali yoki badiiy ijod shaklida. Shunday qilib, bu erkinlikning huquqiy himoyasi axborot mazmuniga ham, uni ifodalash vositalariga ham taalluqlidir. Axborot erkinligi Internet va zamonaviy axborot texnologiyalari kontekstida shaxsiy daxlsizlik bilan bog'liq bo'lishi mumkin

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

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

Qimor o‘yinlari. Bu muammo ham etik masaladagi munozaralardan biri, uni kimlardir zarar deb hisoblasa, yana kimlardir ularga qonun aralashuvini yoqtirmaydilar. O‘z navbatida tomonlar orasida “Qaysi turdagi o‘yinlarga ruxsat

berish kerak? Ular qayerda o‘tkazilishi kerak? ” degan savollar keng munozaralarga sabab bo‘lmoqda. Hozirda aksariyat davlatlarda bu turdagi o‘yinlarga qonuniy ruxsat berilgan bo‘lsa, qolganlarida qat’iy cheklovlar mavjud.

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

- shaxsiy kompyuteringizdan boshqa odamlarga zarar yetkazish uchun foydalanmang;

- boshqa foydalanuvchilarning kompyuter ishlariga aralashmasligingiz kerak;

- boshqa foydalanuvchilarning kompyuter fayllarini aylanib o‘tmang; - o‘g‘irlik maqsadida kompyuterdan foydalanmang;

- yomonlik maqsadida kompyuterdan foydalanmang;

- soxta guvohlik berish kompyuterdan foydalanmang;

- siz to‘lamagan dasturiy ta’minotdan foydalanmang yoki nusxa ko‘chirmang;

- boshqa shaxslarning kompyuter resurslaridan ruxsatsiz foydalanmang;

- Siz boshqa odamlarning intellektual natijalariga mos kelmasligingiz kerak;

- siz yozgan dasturning ijtimoiy oqibatlari haqida o‘ylab ko‘ring;

- kompyuterdan e'tibor va hurmat ko‘rsatadigan usullardan foydalaning.

1.4. Inson faoliyati xavfsizligi

Ijtimoiy (sotsial) injineriya - bu kiberjinoyatchilar tomonidan kimnidir nozik ma’lumotlar va ma’lumotlarni berish uchun psixologik manipulyatsiya qilish uchun amalga oshiriladigan bir qator zararli harakatlar. Bu yerda jabrlanuvchining asosiy ma’lumotlari to‘planadi, unda ma’lumotlar potentsial zaif kirish nuqtalari va hujumni amalga oshirish uchun zarur bo‘lgan xavfsizlik protokollarini o‘z ichiga oladi.

Keyin tajovuzkor jabrlanuvchining ishonchini qozonish orqali uning xavfsizlik amaliyotiga xalaqit beradigan keyingi harakatlarni amalga oshirishga

harakat qiladi. Jabrlanuvchi tajovuzkorga ishonganidan so‘ng, ular maxfiy ma’lumotlarni oshkor qilishi yoki muhim va xavfsiz manbalarga kirish huquqini berishi mumkin.

Ijtimoiy muhandislik tarmoq tizimlari , dasturiy ta’minot va operatsion tizimlardagi zaifliklarga emas, balki inson xatolariga tayanadi. Qonuniy foydalanuvchilar tomonidan qilingan xatolarni oldindan aytib bo‘lmaydi, shuning uchun ularni aniqlash zararli dasturlarga asoslangan hujumni aniqlashdan ko‘ra qiyinroq.

Umuman olganda, ijtimoiy injineriya hujumlari birinchi navbatda ikkita asosiy maqsadga ega:

Sabotaj: biznesni buzish yoki ma’lumotlarni buzish orqali zarar yoki noqulaylik keltiring.

Kiber o‘g‘irlik: nozik va muhim ma’lumotlar yoki pul kabi qimmatbaho narsalarga kirish huquqiga ega bo‘ling.

Ijtimoiy injineriya hayotiy siklining bosqichlari quyidagilarni o‘z ichiga oladi(*1.5-rasm*).

Maqsadli tekshiruv: Hujumga tayyorgarlik jinoyatchidan oldindan rejalashtirishni talab qiladi. Tadqiqot vaqti maqsadning ismini, shaxsiy ma’lumotlarini va fon ma’lumotlarini aniqlashga sarflanadi. Ushbu ma’lumotlarga asoslanib, hujum usullari/kanallari tanlanadi:

Maqsad halqasi: bu bosqichda hujumchi birinchi bosqichda to‘plangan ma’lumotlarga asoslanib, ishonchli bo‘lishi mumkin bo‘lgan uydirma hikoya bilan nishon qurbonini jalb qiladi. Bu erda hujumchining maqsadi jabrlanuvchining ishonchini qozonishdir.

Hujum: maqsad kerakli ishonchni qo‘lga kiritgandan so‘ng, endi maqsad haqiqiy maqsad bo‘lgan ma’lumotni olishga o‘tadi. Niyatga asoslanib, tajovuzkor keyin ma’lumotdan foydalanadi yoki uni sotadi.

Chiqish: hujumning maqsadi tugallangandan so‘ng, hujumchi tomonidan ochilgan aloqa oynasi yopiladi. Keyin tajovuzkor ularning izlarini yopishga va imkoni boricha g‘oyib bo‘lishga harakat qiladi.

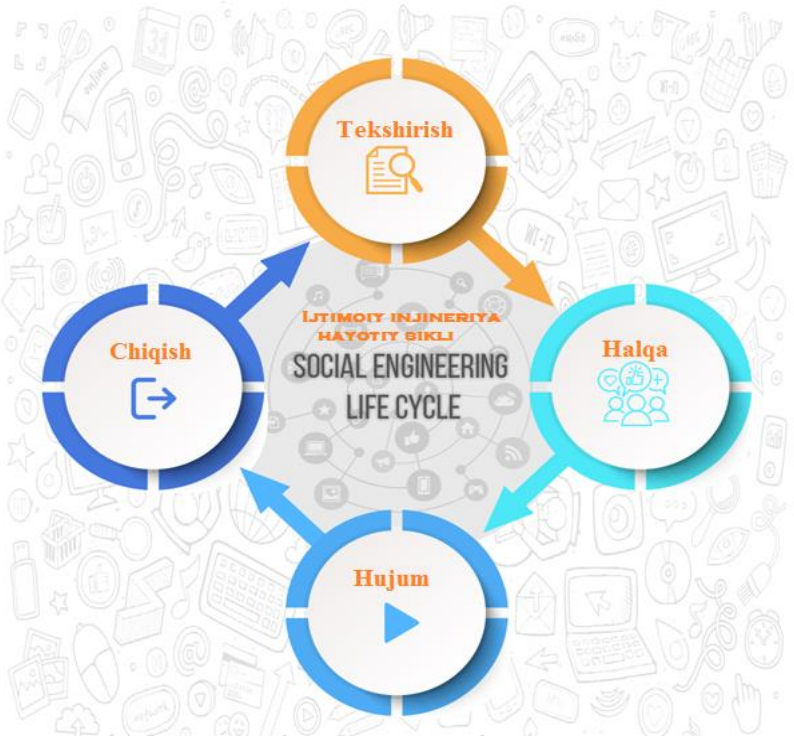
Ijtimoiy injineriya hujumlarini oldini olishda ko‘p hollarda kompaniyalar tomonidan murakkab, ko‘p darajali xavfsizlik tizimlari qo‘llaniladi. Bunday tizimlarning ba’zi xususiyatlari va majburiyatlari quyida keltirilgan:

- *Fizik xavfsizlik* -bu ob'ektning ishlashi xavfsizligini, uning moddiy boyliklarining saqlanishini, uning xodimlarining hayoti va sog'lig'ini himoya qilishga qaratilgan chora-tadbirlar majmui . Ob'ektlarni jismoniy himoya qilish, qoida tariqasida, ob'ektni yuzaga kelishi mumkin bo'lgan xavf va tahdidlar, ularni oldini olish usullari va eng samarali va oqilona xavfsizlik tizimi orqali o'ylash uchun tekshirishdan boshlanadi.

Ma’lumotlar. Biznes ma’lumotlari: qayd yozuvlari, pochta va boshqalar bo‘lib, tahdidlarni tahlillash va ma’lumotlarni himoya qilish choralarini rejalashtirishda qog‘oz, elektron ma’lumot taqdim eltuvchilari bilan ishlash prinsiplarini aniqlash kerak.

- *Ilovalar*. Foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofini himoya qilish uchun elektron pochta dasturlaridan, tezkor xabarlar xizmati va boshqa dasturlardan tajovuzkorlar qanday foydalanishlari mumkinligini ko‘rib chiqish kerak.

-*Kompyuterlar*. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini ko‘rsatadigan qat’iy prinsiplarni belgilash, foydalanuvchilar kompyuterlariga to‘g‘ridan-to‘g‘ri hujumlardan himoya qilish.



1.5-rasm. Ijtimoiy injineriya hayotiy siklining bosqichlari

- *Ichki tarmoq*. Korxona tizimlariga ta’sir qiladigan tarmoq, u mahalliy, global yoki simsiz bo‘lishi mumkin. So‘nggi yillarda masofadan ishlaydigan usullarning ommaviylashi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o‘zboshimchalik bilan kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari lozim.

-*Tarmoq perimetri*. Kompaniyaning ichki tarmoqlari va tashqi, masalan, internet yoki hamkor tashkilotlar tarmoqlari o‘rtasidagi chegara.

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

Fishing (texnikaviy hujum). Fishing (ing. Phishing – baliq ovlash) Internetdagi firibgarlikning eng mashhur ijtimoiy muhandislik hujumlarining bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan (*login/parol*) foydalanish imkoniyatiga ega bo‘lish bo‘lib u qurbonlarda shoshilinchlik, qiziqish yoki qo‘rquv hissini yaratish uchun elektron pochta va matnli xabarlarni jo‘natadi.

Fishing elektron pochta xabarida kiber jinoyatchilar odatda sizdan quydagilarni so‘rashdi:

Tug‘ilgan kuni

Ijtimoiy sug‘urta raqamlari

Telefon raqamlari

Kredit karta tafsilotlari

Uy manzili

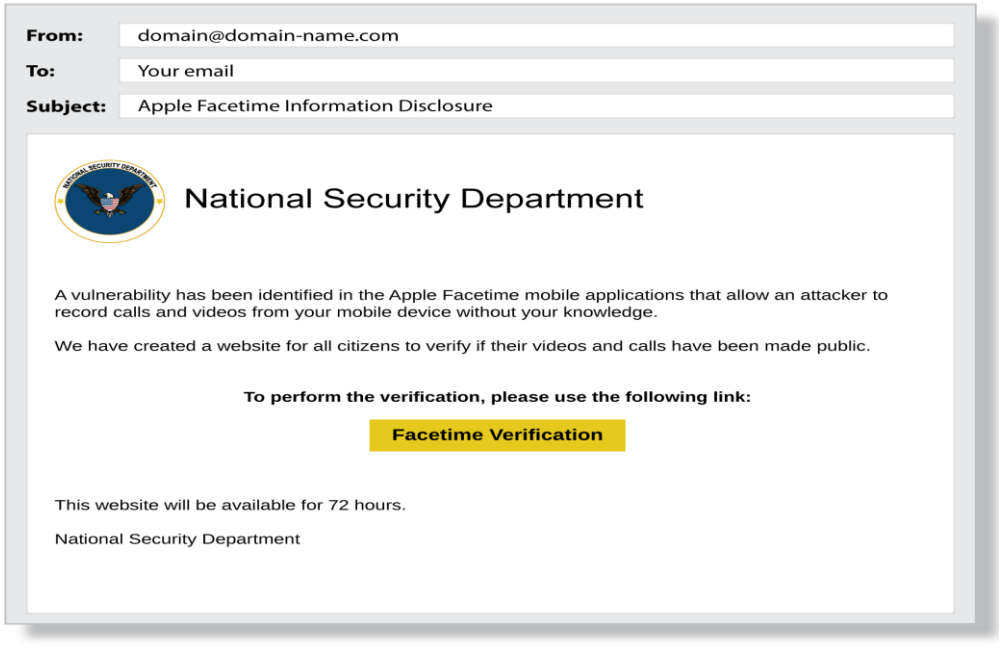
Parol ma’lumotlari (yoki parolingizni qayta o‘rnatish uchun nima kerak).

Keyinchalik kiber jinoyatchilar ushbu ma’lumotlardan jabrlanuvchining nomini o‘zgartirish va kredit kartalari yoki kreditlar, bank hisoblarini ochish va boshqa firibgarlik uchun ariza berish uchun foydalanadilar(*1.6-rasm*).

Fishing hujumlarining turlari quydagilar:

Ommaviy fishing - aldamchi fishing deb ham ataladi, bu eng keng tarqalgan fishing hujumidir.

Kiberjinoyatchilar yolg‘on vadalar beradigan soxta xabarlarni ommaviy ravishda yuborishadi: siz pul yutib oldingiz, to‘lovni qaytarish huquqiga egasiz yoki hisobingiz to‘lanmagan va chora ko‘rish talab etiladi. Ular hech bo‘lmaganda bir nechtasi shaxsiy ma’lumotlarni o‘g‘irlash nishoniga aylanishini bilib, ko‘p sonli odamlarga bir xil elektron pochta xabarini yuborishadi.



1.6-rasm. Fishing hujumiga misol

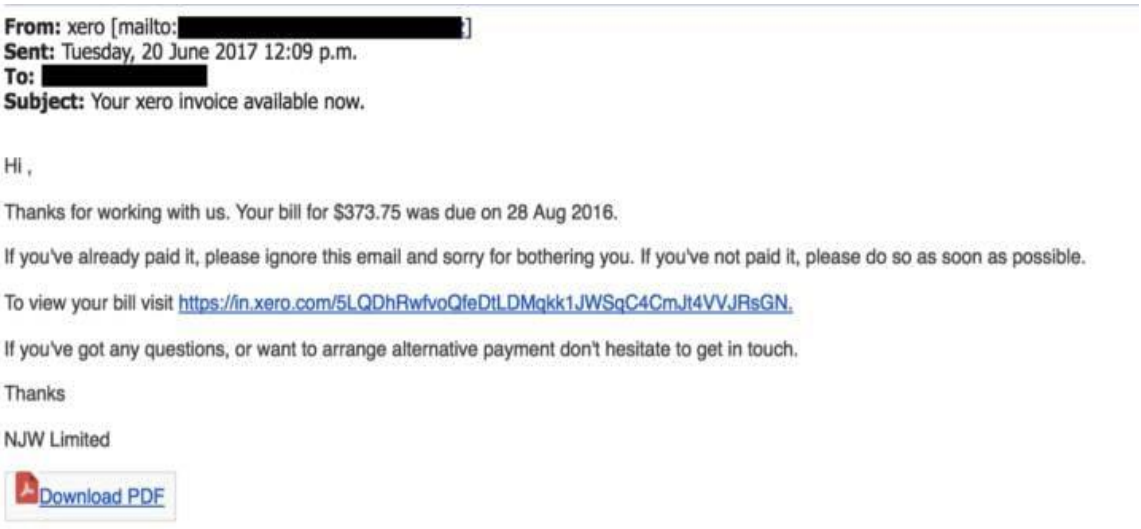
Spear Phishing - ushbu sxemaning ijrochilari uy vazifalarini bajarishdi. Kiberjinoyatchining kimnidir aldash ehtimolini oshirish uchun ular o‘zlarining potentsial qurboni haqida iloji boricha ko‘proq shaxsiy ma’lumotlarni topadilar. So‘ngra, ular nishonning qo‘riqchisini tushirish uchun ayniqsa qonuniy ko‘rinadigan xabarni tayyorlash uchun foydalanadilar.

Whaling Attack - bu nayzali fishingning bir turi bo‘lib, tajovuzkor kompaniya rahbarlarini nishonga oladi va ularning login ma’lumotlarini o‘g‘irlashga harakat qiladi. Muvaffaqiyatli bo‘lsa, jinoyatchilar ushbu nozik ma’lumotlardan kompaniyadan o‘g‘irlash yoki kompaniyaning boshqa xodimlarini aldash uchun rahbar sifatida foydalanishlari mumkin.

Fishingni klonlash - fishingning bu shakli ayniqsa aldamchi va uni aniqlash qiyinroq bo‘lishi mumkin. Buzg‘unchi maqsad allaqachon olgan qonuniy xabarning mazmunini ko‘chiradi va xabardagi asl havolalarni soxta web-saytga olib keladigan zararli havolalar bilan almashtiradi. Muvaffaqiyatli bo‘lishi uchun kiberjinoyatchi allaqachon jabrlanuvchining login ma’lumotlariga ega bo‘lishi kerak.

Fishing elektron pochta xabarlarining eng keng tarqalgan misollari:

Soxta hisob-faktura firibgarligi. Ko‘pgina fishing hujumlari singari, bu firibgarlik ham qo‘rquv va shoshilinchlikka tayanadi va oxirgi foydalanuvchini hech qachon buyurtma qilmagan yoki olmagan tovarlar yoki xizmatlar uchun to‘lovni topshirishga majbur qiladi. *(1.7-rasm).*


From: xero [mailto:[redacted]]
Sent: Tuesday, 20 June 2017 12:09 p.m.
To: [redacted]
Subject: Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2016.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit https://in.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

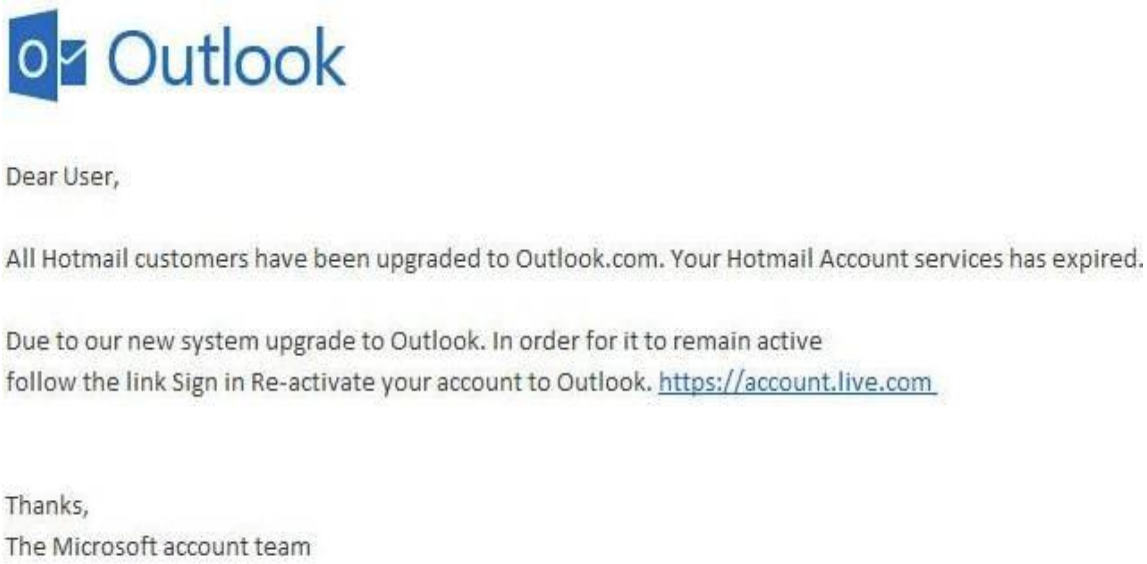
Thanks

NJW Limited

Download PDF

1.7-rasm. Soxta hisob-faktura firibgarligi

Elektron pochta hisobini yangilash firibgarligi. Agar zudlik bilan chora ko‘rilmasa, hisobingizning amal qilish muddati tugashiga duch kelganda, elektron pochta hisobini yangilash bo‘yicha firibgarlik Microsoft va Google kabi ishonchli elektron pochta provayderlaridan yoki oddiygina kompaniyangizning IT bo‘limidan kelgandek tuyulishi mumkin. *(1.8-rasm).*


Outlook

Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

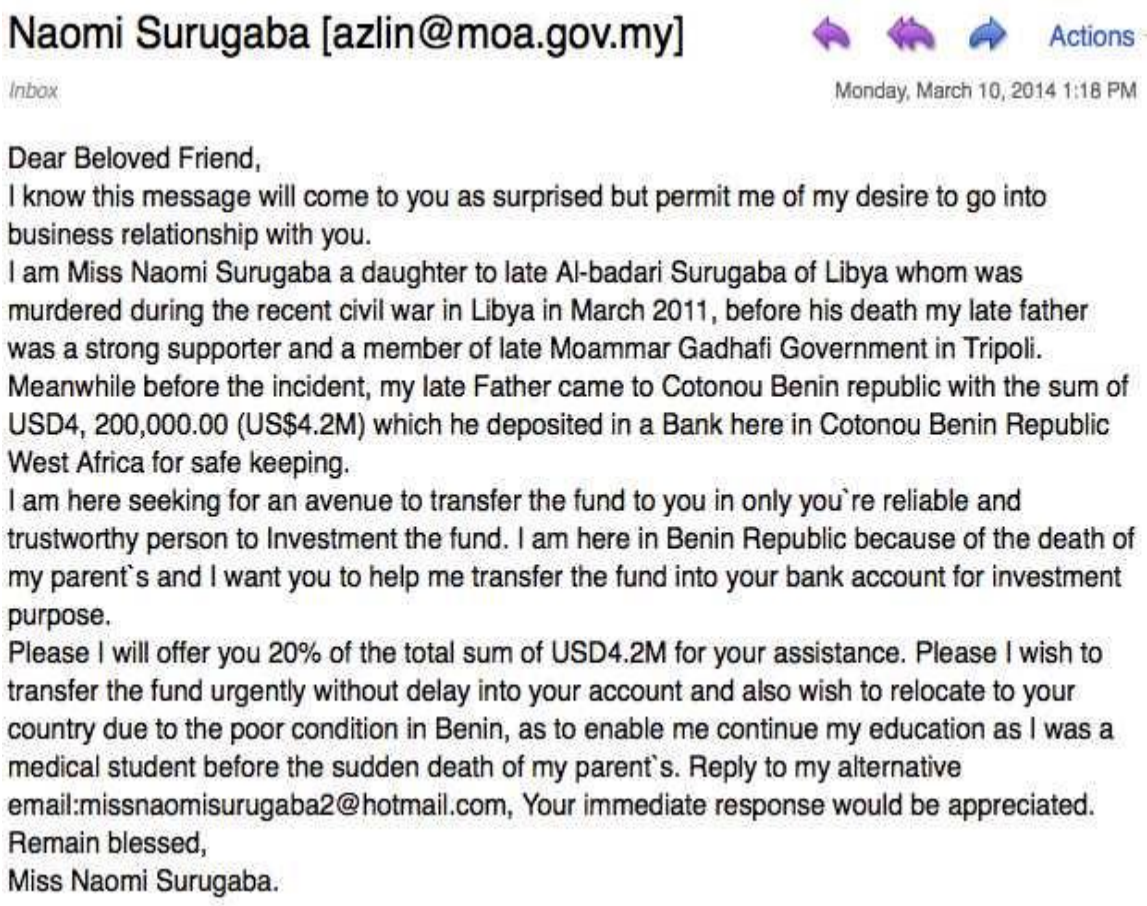
Thanks,
The Microsoft account team

1.8-rasm. Elektron pochta hisobini yangilash firibgarligi.

Ko‘rib turganingizdek, ushbu elektron pochtadan hech qanday zararli narsa yo‘q. Hech qanday aniq grammatik xatolar yo‘q, batafsil so‘rovlar yo‘q va havolaning o‘zi shubhasiz foydalanuvchiga xavfsiz “*https*” web-sahifasiga yo‘naltirilgandek ko‘rinadi.

Foydali maslahat - shaxsiy ma’lumotlarni berish so‘ralganda kursorni havolaning o‘zi ustiga olib boring, chunki matnning o‘zi ko‘pincha havolaning haqiqiy manzilini bildirmaydi.

Avans to‘lovi bo‘yicha firibgarlik: chet ellikdan tuzoqqa tushib qolgan pulni qaytarib olishda yordam so‘rab elektron pochta xabarini olish, batafsil hikoya uchun kulgili bahonadir. Lekin aldanmang, bu firibgarlik bir muncha vaqtdan beri mavjud va buning yaxshi sababi bor *(1.9-rasm).*


Naomi Surugaba [azlin@moa.gov.my]

Actions

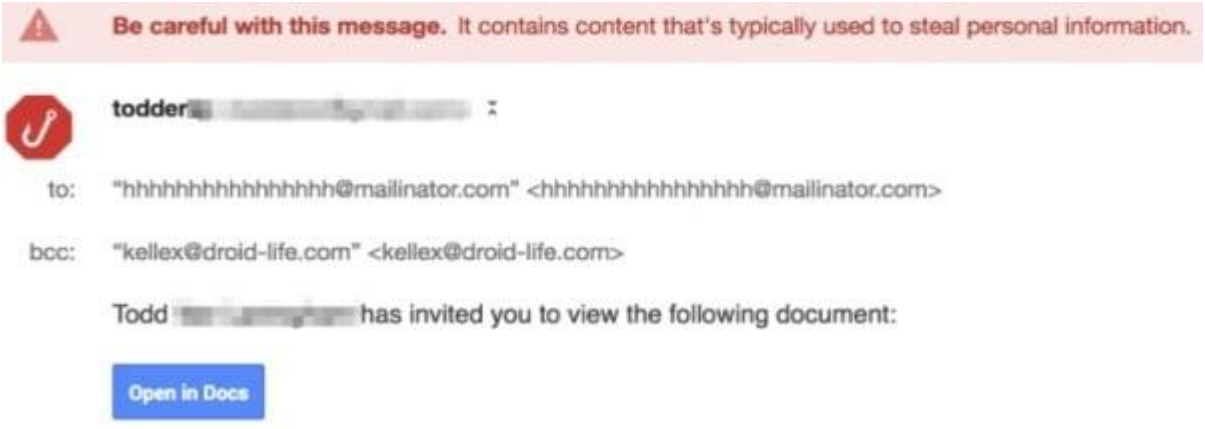
Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

1.9-rasm. Avans to‘lovi bo‘yicha firibgarlik.

Google Docs firibgarligi: eng so‘nggi mashhur fishing usullaridan biri bo‘lgan Google Docs firibgarligi qo‘shimcha daxshatli burilish taklif qiladi, chunki jo‘natuvchi ko‘pincha siz bilgan odam bo‘lib ko‘rinishi mumkin.*(1.20-rasm).*Ushbu o‘ta murakkab elektron pochta sizni “*hujjat*” ni ko‘rish uchun uning havolasini bosishga undaydi, bu esa sizni ***Gmail login*** sahifasining deyarli bir xil versiyasiga olib boradi. Hisob tanlangandan so‘ng, siz Google hisobingizga kirishga taklif qilinasiz, ya'ni buzg‘unchi erkin harakat qiladi.


Be careful with this message. It contains content that's typically used to steal personal information.

todder

to: "hhhhhhhhhhhhhhhh@mailinator.com" <hhhhhhhhhhhhhhhh@mailinator.com>

bcc: "kellex@droid-life.com" <kellex@droid-life.com>

Todd has invited you to view the following document:

Open in Docs

1.20-rasm. Google Docs firibgarligi

Taniqli korporativ brendidan foydalanishga asoslangan firibgarlik. Firibgarlikning mazkur ko‘rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchiga xabar yuboriladi va xabarda kompaniya tomonidan o‘tkazilgan biror tanlovda g‘alaba qozonilganligi haqidagi tabriklar bo’ladi hamda unda zudlik bilan qayd yozuvi ma’lumotlari va parolni o‘zgartirish kerakligi so‘raladi.

Soxta lotareyalar. Mazkur fishing sxemasiga ko‘ra foydalanuvchi har qanday taniqli kompaniya tomonidan o‘tkazilgan lotereyada g‘olib bo‘lgani to‘g‘risidagi xabarni olishi mumkin.

Soxta antivirus va *xavfsizlik dasturlari*. Mazkur dasturlar firibgar dasturiy ta’minoti yoki “*chaqqon dastur*” deb nomlanib, ular antivirus dasturlariga o‘xshasada, vazifasi boshqa. Bu dasturiy ta’minot turli tahdidlar to‘g‘risidagi yolg‘on xabarnomalar asosida foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ulardan foydalanganida elektron pochtada, onlayn e’lonlarda, ijtimoiy tarmoqlarda, qidiruv tizimlari natijalarida va hatto foydalanuvchi kompyuterida turli qalqib chiquvchi oynalarga duch kelishi mumkin.

IVR (Interactive Voice Response) yoki telefon orqali fishing. Fishing sxemasining mazkur usuli oldindan yozib olingan xabarlar tizimidan foydalanishga asoslangan, ular bank va boshqa TVR tizimlarining “rasmiy qo‘ng‘iroqlari”ni qayta tiklash uchun ishlatiladi. Bu hujumda jabrlanuvchi bank bilan bog‘lanib, qandaydir ma’lumotlarni tasdiqlash yoki yangilash kerakligi haqidagi so‘ovni qabul qiladi. Tizim PIN kodni 35 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.

Preteksting. Mazkur fishing sxemasida xaker o‘zini boshqa shaxs sifatida ko‘rsatadi va oldindan tayyorlangan senariy (skript) bo‘yicha maxfiy axborotni olishni maqsad qiladi. Ushbu fishing sxemasi odatda telefon yoki elektron pochta orqali amalga oshiriladi.

Kvid pro kvo (lotinchadan: Quid pro quo). Ushbu ibora ingliz tilida “*xizmat uchun* xizmat” degan ma’noni anglatib, sotsial injineriyaning mazkur turida xaker

korporativ tarmoq yoki elektron pochta orqali kompaniyaga murojaatni amalga oshiradi. Ko‘pincha xaker o‘zini texnik xizmat ko‘rsatuvchi sifatida tanitib, texnik xodimning ish joyidagi muammolarni bartaraf etishda “*yordam berishini*” aytadi. Texnik muammoni “*bartaraf*” etish vaqtida nishondagi shaxsni buyruqlarni bajarishga yoki jabrlanuvchining kompyuteriga turli xil dasturlarni o‘rnatishga undash amalga oshiriladi.

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

Ochiq ma’lumot to‘plash. Sotsial injineriya texnikasi nafaqat psixologik bilimlarni, balki, inson haqida kerakli ma’lumotlarni to‘plash qobilyatini ham talab etadi. Bunday ma’lumotlarni olishning nisbatan yangi usuli ochiq manbalardan, ijtimoiy tarmoqlardan to‘plash. Masalan, «*Одноклассники*», «*ВКонтакте*», «*Facebook*», «*Instagram*» kabi 36 saytlarda odamlar yashirishga harakat qilmaydigan juda ko‘p ma’lumotlar mavjud. Odatda, foydalanuvchilar xavfsizlik muammolariga yyetarlicha e’tibor bermasdan, xaker tomonidan foydalanilishi mumkin bo‘lgan ma’lumotlar va xabarlarni qarovsiz qoldiradilar.

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

Ijtimoiy injineriyadan himoyalanish choralari. Hujumlarni amalga oshirishda sotsial injineriya texnikasidan foydalangan tajovuzkorlar teztez muloyimlik, dangasalik, xushmuomilalik bilan foydalanuvchi va tashkilot

xodimlarining qiziqishlaridan foydalanadilar. Hujumlarni oldini olish esa, xodimlarning aldanayotganliklarini bilmasliklari sababli, murakkab hisoblanadi.

Sotsial injineriya hujumlarini quyidagicha aniqlash mumkin:

- o‘zini do‘stingiz yoki yordam so‘rab murojaat qilgan yangi xodim sifatida tanishtirish;

- o‘zini yetkazib beruvchi, hamkor kompaniyaning xodimi yoki qonun vakili sifatida tanishtirish;

- o‘zini biror rahbar sifatida tanishtirish;

- biror zaiflikni bartaraf etuvchi yoki jabrlanuvchiga biror nimani yangilash imkoniyatini taqdim qiluvchi sotuvchi yoki ishlab chiqaruvchi sifatida tanishtirish;

- muammo yuzaga kelganida yordam beruvchi sifatida tanishtirish;

- ishonchni hosil qilish uchun ichki xotirjamlik va terminologiyadan foydalanish;

Hayotda ko‘plab jabhalarda sotsial injineriyaga tegishli muammolarni ko‘rish mumkin.

Xususan, ommaviy madaniyatda (masalan, kinofilmlarda) sotsial injinerlikdan foydalanish holatlari tez-tez uchrab turadi. Masalan, quyidagi keltirilgan kinofilmlarda sotsial injineriyaga oid epizodlar mavjud:

− «Поймай меня, если сможешь»;

− «Поймай толстуху, если сможешь»;

− «Один дома»; − «Хакеры»;

− «Афера Томаса Крауна»;

− «Бриллианты навсегда»;

− «Кто я».

Nazorat savollari

1. Kiberxavfsizlikning hayotiy timsollari va ularning vazifalari.
2. Kiberxavfsizlik tushunchasiga ta’rif bering.
3. Kiberxavfsizlikning asosiy tushunchalari.
4. Axborotning konfidensialligini taminlash deganda nimani tushunasiz?
5. Axborotni yaxlitligini taminlash deganda nimani tushunasiz?

6. Axborot uchun foydalanuvchanlikning muhimligi.
7. Risk va uning kiberxavfsizlikdagi o‘rni.
8. Hujumchi kabi fikrlash nima uchun zarur?
9. Tizimli fikrlash nima va u nima uchun zarur?
10. Axborot xavfsizligi va axborotni himoyalash tushunchalarining bir-biridan farqi nimada?
11. Aktiv nima?
12. Tahdid va zaiflik tushunchalariga izoh bering.
13. Axborot xavfsizligi va kiberxavfsizlik tushunchalarining birbiridan farqi nimada?
14. Kiberxavfsizlikning bilim sohalari va ularning asosiy xususiyatlari nimalardan iborat?
15. Kiberxavfsizlikda inson omilini misollar yordamida tushuntiring.
16. Kiberjinoyatni amalga oshirishdan ko‘zlangan maqsadlar.
17. Kiberjinoyatchilikning asosiy turlari.
18. Kiberetika tushunchasiga izoh bering va ularga misollar keltiring.
19. Kompterdan foydalanish davomida qanday etika qoidalarga e’tibor berish talab qilinadi?
20. Kiberjinoyatchilikni oldini olish usullari va kiberqonunlar haqida ma’lumot bering.
21. “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonunda axborotdan foydalanish tartiblari haqida nimalar deyilgan?

2 BOB. KIBERXAVFSIZLIK ARXITEKTURASI, STRATEGIYASI VA SIYOSATI

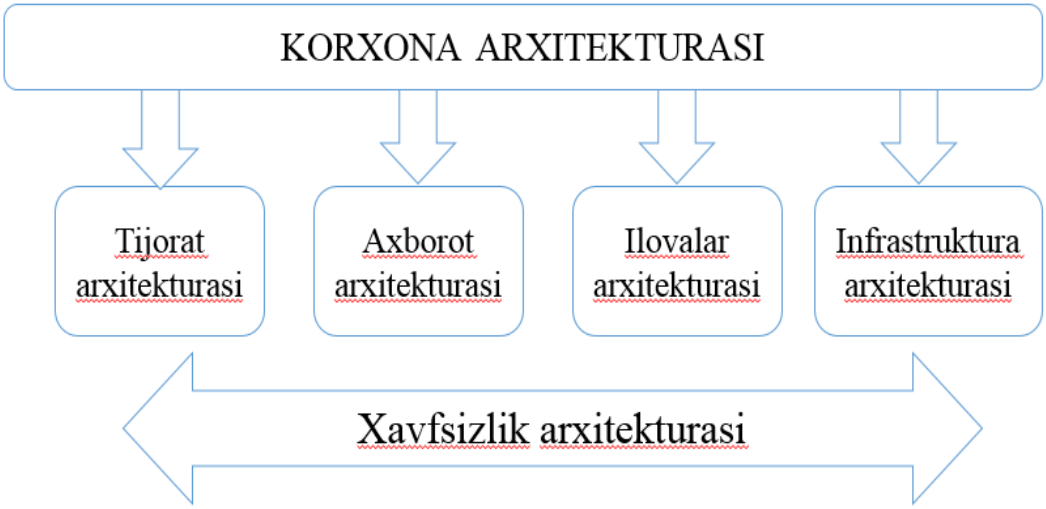
2.1 Kiberxavfsizlik arxitekturasi va strategiyasi

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

- daromadning oshishi;
- o‘zgaruvchi vaziyatlarga reaksiya tezligining oshishi;
- harajat va chiqimlarning pasayishi;
- raqobatlik qobiliyatining oshishi;
- me’yoriy talablarga moslikni taminlash.

Yuqorida keltirilgan barcha masalalarni yechishda korxona arxitekturasidan foydalaniladi *(2.1-rasm)*.

Korxona arxitekturasi prinsiplar, yondashishlar va texnologiyalar naborini shakllantirishga imkon beradiki, ular tashkilotning joriy holatini hisobga olgan holda uning kelgusi transformasiyasi, o‘sishi va rivojlanishi asosini belgilaydi.



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

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

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

Axborot va axborot tizimlari nafaqat tijoratdagi har qanday o‘zgarishlarni madadlaydi, balki ularni oldindan sezadi, ularga oldindan tayyorlanadi, ba’zi xollarda esa yangi tijorat-imkoniyatlarining paydo bo‘lishiga yordam beradi. Biroq tijorat doimo istalgancha rivojlanmaydi.

Bunda ma’lumotlarning sirqib chiqishi, axborot texnologiyalari *infrastrukturasi* elementlarining ishdan chiqishi va h. bilan bog‘liq axborot operatsion risklar anchagina rol o‘ynaydi. Hozirgi va kelajak risklarga tayyor bo‘lish uchun korxonaning boshqa arxitekturalari bilan uzviy bog‘langan axborot xavfsizligi arxitekturasi zarur.

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

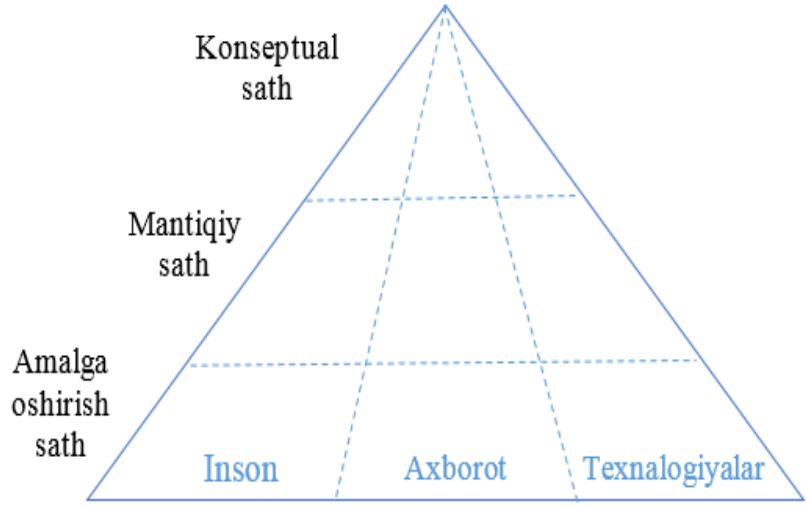
Odatda arxitekturaning 3 ta sathi ajratiladi – ***konseptual***, ***mantiqiy*** va ***amalga oshirish*** (texnologik). *2.2-rasm*da bunday arxitektura keltirilgan bo‘lib, odatda texnologiyalar jihatidagi qismi xavfsizlik xizmati nazoratidan chetda qoladi.

Joriy holatdan qanday qilib yangi, mukammalroq va quyilgan maqsadlarga mos holatga o‘tish mumkin?

Buning uchun strategiya, ya’ni quyilgan maqsadlarga erishish uchun harakat yo‘nalishi mavjud.

Kiberxavfsizlik strategiyasi tashkilot o‘z aktivlarini himoya qilish va kiberxavfni minimallashtirish bo‘yicha yuqori darajadagi rejalardan iborat. Kiberxavfsizlik siyosati singari, kiberxavfsizlik strategiyasi ham mavjud tahdidlar manzarasi va doimiy rivojlanayotgan biznes muhitiga moslasha oladigan

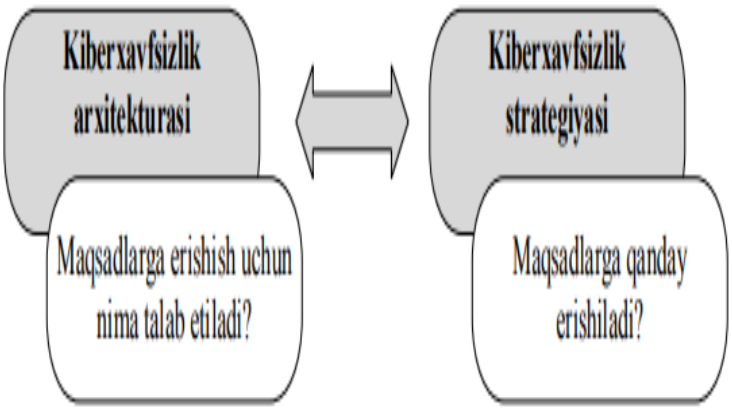
jonli, nafas oladigan hujjat bo‘lishi kerak. Odatda, kiberxavfsizlik strategiyalari uch yildan besh yilgacha bo‘lgan ko‘rinish bilan ishlab chiqiladi, ammo ularni imkon qadar tez-tez yangilab turish va qayta ko‘rib chiqish kerak.



2.2-rasm. Kiberxavfsizlik arxitekturasi

Kiberxavfsizlik siyosati batafsilroq va aniqroq bo‘lsada, kiberxavfsizlik strategiyalari kompaniya va biznes muhiti rivojlanishi davomida tashkilotingiz uchun asosiy manfaatdor tomonlarga yo‘l-yo‘riq ko‘rsatish uchun ko‘proq rejadir.

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



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

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

2.2. Kiberxavfsizlik siyosati va uni amalga oshirish

Axborot xavfsizligi siyosati (yoki xavfsizlik siyosati)- maxfiy biznes ma’lumotlari va ma’lumotlar aktivlarini ruxsatsiz kirishdan himoya qilish uchun ishlab chiqilgan va o‘rnatilgan siyosatlar, jarayonlar va vositalarni anglatadi.

Axborot xavfsizligining uchta asosiy jihati mavjud: ***maxfiylik***, ***yaxlitlik*** va ***mavjudlik***. Bu Markaziy razvedka boshqarmasi triadasi sifatida tanilgan.

Xavfsizlik siyosati (shuningdek, axborot xavfsizligi siyosati yoki AT xavfsizligi siyosati deb ham ataladi) tashkilot o‘z ma’lumotlarining maxfiyligi, yaxlitligi va mavjudligini taminlash uchun foydalanadigan qoidalar, taxminlar va umumiy yondashuvni tavsiflovchi hujjatdir . Xavfsizlik siyosatlari korxonaning umumiy xavfsizlik maqsadlari va tamoyillarini tavsiflovchi yuqori darajadagi tuzilmalardan tortib, masofaviy kirish yoki *Wi-Fi*-dan foydalanish kabi muayyan muammolarni hal qiluvchi hujjatlargacha bo‘lgan turli darajalarda mavjud.

Markaziy razvedka boshqarmasi triadasining tamoyillari uchta asosiy maqsadni himoya qiladi.

Maxfiylik: Ma’lumotlar aktivlariga kirish faqat vakolatli shaxslar uchun cheklangan bo‘lishi kerak.

Butunlik: AT tizimlarini saqlash, ularning ishonchli va maqsadga muvofiqligini taminlash.

Mavjudlik: kerak bo‘lganda vakolatli foydalanuvchilarning tegishli ma’lumotlar yoki siyosatlarga kirishini taminlash **Infosec** siyosatlari xodimlar va boshqa manfaatdor tomonlar (masalan, yetkazib beruvchilar) uchun kerak bo‘lganda amal qilishi kerak bo‘lgan qoidalar ro‘yxatini belgilaydi.

Xavfsizlik siyosati odatda standart operatsion protseduralar kabi boshqa turdagi hujjatlar bilan birgalikda qo‘llaniladi. Ushbu hujjatlar kompaniyaga xavfsizlik maqsadlariga erishishda yordam berish uchun birgalikda ishlaydi. Siyosat umumiy strategiya va xavfsizlik pozitsiyasini belgilaydi, boshqa hujjatlar ushbu amaliyot atrofida tuzilmani yaratishga yordam beradi. Xavfsizlik siyosati haqida "***nima***" va "***nima uchun***" degan savolga javob berish kerak, protseduralar, standartlar va ko‘rsatmalar esa "***qanday qilib***" degan savolga javob beradi.

Xavfsizlik siyosati muhim ahamiyatga ega bo‘lgan to‘rtta sabab-xavfsizlik siyosati byurokratiyaning navbatdagi qatlami kabi ko‘rinishi mumkin, lekin aslida ular har qanday axborot xavfsizligi dasturining hayotiy muhim tarkibiy qismidir. Yaxshi ishlab chiqilgan va amalga oshirilgan xavfsizlik siyosatining ba'zi afzalliklari quyidagilardan iborat:

Texnik nazoratni amalga oshirishga rahbarlik qiladi-xavfsizlik siyosati past darajadagi maxsus texnik ko‘rsatmalarni ta'minlamaydi, lekin u yuqori boshqaruvning xavfsizlikka oid niyatlari va umidlarini ifodalaydi. Keyinchalik bu niyatlarni aniq texnik harakatlarga aylantirish xavfsizlik yoki IT guruhlariga bog‘liq.

Misol uchun, siyosatda faqat avtorizatsiya qilingan foydalanuvchilarga kompaniyaning xususiy ma’lumotlariga kirish huquqi berilishi kerakligi ko‘rsatilishi mumkin. Ushbu siyosatni amalga oshirish uchun ishlatiladigan maxsus autentifikatsiya tizimlari va kirishni boshqarish qoidalari vaqt o‘tishi bilan o‘zgarishi mumkin, ammo umumiy maqsad bir xil bo‘lib qoladi. Boshlash uchun joy bo‘lmasa, xavfsizlik yoki IT guruhlari faqat yuqori rahbariyatning xohishlarini taxmin qilishlari mumkin. Bu turli guruhlar va xo‘jalik yurituvchi sub'ektlarda xavfsizlikni nazorat qilishning izchil qo‘llanilishiga olib kelishi mumkin.

Aniq taxminlarni belgilaydi-xavfsizlik siyosati bo‘lmasa, har bir xodim yoki foydalanuvchi nima to‘g‘ri va nima noto‘g‘riligini o‘zi hal qiladi. Turli xodimlar turli standartlarni qo‘llaganida, bu falokatga olib kelishi mumkin.

Shaxsiy foydalanish uchun kompaniya qurilmasidan foydalanish o‘rinlimi?

Menejer qulaylik uchun parollarni bevosita hisobotlari bilan bo‘lishishi mumkinmi?

Tasdiqlanmagan dasturlarni o‘rnatish haqida nima deyish mumkin?

Aniq siyosatlarsiz, turli xodimlar bu savollarga turli yo‘llar bilan javob berishlari mumkin. Xavfsizlik siyosatida muvofiqlik qanday nazorat qilinishi va amalga oshirilishi aniq ko‘rsatilishi kerak.

Normativ va muvofiqlik talablariga javob berishga yordam beradi-hujjatlashtirilgan xavfsizlik siyosati HIPAA va Sarbanes-Oxley kabi qonunchilik, shuningdek, PCI-DSS, ISO 27001 va SOC2 kabi qoidalar va standartlar talabidir. Hatto aniq talab qilinmasa ham, xavfsizlik siyosati ko‘pincha xavfsizlik va ma’lumotlar maxfiyligining tobora kuchayib borayotgan talablariga javob beradigan strategiyani ishlab chiqishda amaliy zarurat hisoblanadi.

Tashkiliy samaradorlikni oshiradi va biznes maqsadlariga erishishga yordam beradi-yaxshi xavfsizlik siyosati tashkilot samaradorligini oshirishi mumkin. Uning siyosati hammani bir sahifada to‘playdi, harakatlar takrorlanishiga yo‘l qo‘ymaydi va muvofiqlikni kuzatish va amalga oshirishda izchillikni ta’minlaydi. Xavfsizlik siyosati, shuningdek, siyosatdan istisnolar qachon va kim tomonidan berilishi haqida aniq ko‘rsatmalar berishi kerak.

Xavfsizlik siyosatining uch turi- Xavfsizlik siyosati turli tashkilotlarning ehtiyojlariga ko‘ra ko‘lami, qo‘llanilishi va murakkabligi jihatidan farq qilishi mumkin. Xavfsizlik siyosati uchun universal model mavjud bo‘lmasa-da, Milliy Standartlar va Texnologiyalar Instituti (NIST) maxsus nashrda (SP) 800-12 ning uchta turini ajratib ko‘rsatadi.

Dastur siyosati-dastur siyosati strategik, yuqori darajadagi rejalar bo‘lib, ular tashkilotning axborot xavfsizligi dasturini boshqaradi. Ular dasturning maqsadi va ko‘lamini ta’riflaydi, shuningdek, rol va mas’uliyat va muvofiqlik mexanizmlarini belgilaydi. Magistr yoki tashkiliy siyosat sifatida ham tanilgan ushbu hujjatlar yuqori darajadagi rahbariyatning yuqori darajadagi kiritishlari bilan ishlab chiqilgan va odatda texnologiya agnostik hisoblanadi. Ular eng kam

yangilanadigan siyosat turidir, chunki ular texnik va tashkiliy o‘zgarishlar orqali ham dolzarb bo‘lib qolishi uchun yetarlicha yuqori darajada yozilishi kerak.

Masalaga oid siyosat- muammolarga oid siyosatlar umumiy xavfsizlik siyosatiga asoslanadi va tashkilotning ishchi kuchi bilan bog‘liq bo‘lgan muayyan masalalar bo‘yicha aniqroq ko‘rsatmalar beradi. Umumiy misollar tarmoq xavfsizligi siyosati, o‘z qurilmangizni olib keling (BYOD) siyosati, ijtimoiy media siyosati yoki masofadan ishlash siyosatini o‘z ichiga olishi mumkin. Ular muayyan texnologiya sohalariga murojaat qilishi mumkin, lekin odatda umumiyroqdir. Masofaviy kirish siyosati saytdan tashqariga kirish faqat kompaniya tomonidan tasdiqlangan va qo‘llab-quvvatlanadigan VPN orqali mumkinligini ko‘rsatishi mumkin, ammo bu siyosatda ma'lum bir VPN mijozi nomlanmasligi mumkin. Shunday qilib, kompaniya yirik yangilanishlarsiz sotuvchilarni o‘zgartirishi mumkin.

Tizimga xos siyosat - bu xavfsizlik devori yoki web-server yoki hatto alohida kompyuter kabi tizimning ma'lum bir turiga qaratilgan AT xavfsizligi siyosatining eng nozik turi. Muammoga oid siyosatlardan farqli o‘laroq, tizimga xos siyosatlar ularni qo‘llab-quvvatlaydigan texnik xodimlarga eng mos kelishi mumkin. NIST ta'kidlashicha, tizimga xos siyosatlar ham xavfsizlik maqsadi, ham operatsion qoidalardan iborat bo‘lishi kerak. AT va xavfsizlik guruhlari tizimga xos siyosatlarni yaratish, amalga oshirish va amalga oshirishda jiddiy ishtirok etadilar, ammo asosiy qarorlar va qoidalar hali ham yuqori boshqaruv tomonidan qabul qilinadi.

Samarali xavfsizlik siyosatining etti elementi- xavfsizlik siyosati axborot xavfsizligi dasturining muhim tarkibiy qismi bo‘lib, ular to‘g‘ri ishlab chiqilishi, amalga oshirilishi va bajarilishi kerak. Samarali xavfsizlik siyosati quyidagi elementlarni o‘z ichiga olishi kerak:

Aniq maqsad va vazifalar- bu dastur siyosati uchun ayniqsa muhimdir. Esda tutingki, ko‘pchilik xodimlar xavfsizlik tahdidlari haqida kam ma’lumotga ega va har qanday xavfsizlik nazoratini yuk sifatida ko‘rishlari mumkin. Xavfsizlik siyosatining yuqori darajasida bayon etilgan aniq missiya bayonoti yoki maqsad

butun tashkilotga axborot xavfsizligi muhimligini tushunishga yordam berishi kerak.

Qo‘llash sohasi va qo‘llanilishi- har bir xavfsizlik siyosati, turidan qat'iy nazar, siyosat kimga nisbatan qo‘llanilishini aniq ko‘rsatuvchi qo‘llash doirasi yoki bayonotini o‘z ichiga olishi kerak. Bu to‘g‘ri belgilangan bo‘lsa, geografik mintaqa, biznes bo‘linmasi, ish o‘rni yoki boshqa har qanday tashkiliy kontseptsiyaga asoslangan bo‘lishi mumkin.

Yuqori rahbariyatdan majburiyat- xavfsizlik siyosati yuqori rahbariyatning niyatlarini bildirish uchun mo‘ljallangan, ideal holda C-suite yoki kengash darajasida. Etakchilikning ushbu darajasidan foydalanmasdan, har qanday xavfsizlik dasturi muvaffaqiyatsiz bo‘lishi mumkin. Muvaffaqiyatga erishish uchun sizning siyosatlaringiz xodimlarga yetkazilishi, muntazam yangilanishi va doimiy ravishda amalga oshirilishi kerak. Boshqaruv yordamining etishmasligi bularning barchasini qiyinlashtiradi, agar imkonsiz bo‘lmasa.

Haqiqiy va amalga oshirilishi mumkin bo‘lgan siyosat- xavfsizlik siyosatingizni mukammallik modeliga asoslash jozibador bo‘lishi mumkin bo‘lsa-da, sizning xodimlaringiz haqiqiy dunyoda yashashini yodda tutishingiz kerak. Haddan tashqari og‘ir siyosat keng qabul qilinishi mumkin emas. Xuddi shunday, ijro etish mexanizmi bo‘lmagan siyosat ko‘plab xodimlar tomonidan osongina e'tibordan chetda qolishi mumkin.

*Muhim atamalarning aniq ta'rifla*ri- xavfsizlik siyosatining auditoriyasi ko‘pincha texnik bo‘lmagan, qisqa va jargonsiz til muhim ahamiyatga ega va hujjatdagi har qanday texnik atamalar aniq belgilanishi kerak.

Tashkilotning tavakkalchilik ishtahasiga moslashtirilgan- xavfni hech qachon butunlay yo‘q qilib bo‘lmaydi, lekin har bir tashkilot rahbariyati xavf darajasining maqbulligini hal qilishi kerak. Xavfsizlik siyosati ushbu xavf ishtahasini hisobga olishi kerak, chunki u yoritilgan mavzular turlariga ta’sir qiladi.

Eng dolzarb ma’lumotlar- xavfsizlik siyosatini yangilash samaradorlikni saqlash uchun juda muhimdir.

*Dastur yoki asosiy siyosat tez-tez o‘zgarishi kerak bo‘lmasa*da, uni muntazam ravishda ko‘rib chiqish kerak. Texnologiya, ishchi kuchi tendentsiyalari va boshqa omillar o‘zgarganda muammoga oid siyosatlarni tez-tez yangilab turish kerak bo‘ladi. Vaqt o‘tishi bilan siz yangi siyosatlarga ehtiyoj sezishingiz mumkin: BYOD va masofaviy kirish siyosatlari so‘nggi o‘n yil ichida hamma joyda mavjud bo‘lgan siyosatlarning ajoyib namunasidir.

Xavfsizlik siyosatining afzalliklari:

-*Kuchaytirilgan ma’lumot va tarmoq xav*fsizligi: tashkilotlar o‘z ma’lumotlari xavfsizligini ta’minlovchi tarmoqqa asoslangan siyosatini amalga oshiradilar. Xavfsizlik siyosati tarmoqda boshqa tizimlardan ma’lumotlar uzatilishida himoyani ta’minlaydi.

- *Risklarni kamaytirish*: xavfsizlik siyosatini amalga oshirish orqali tashqi manbalardan bo‘lishi mumkin bo‘lgan risklar kamaytiriladi. Agar xodimlar xavfsizlik siyosati asosida harakat qilsalar, ma’lumot va resurslarning yo‘qolishi holatlari deyarli kuzatilmaydi.

-*Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlani*shi: xavfsizlik siyosati xodimlar tomonidan amalga oshirilgani bois, ma’murlar tashkilotdagi trafikni va foydalanilgan tashqi qurilmalarni doimiy tarzda monitoringlashi zarur. Kiruvchi va chiquvchi trafikning monitoringi va auditi doimiy ravishda amalga oshirilishi shart.

- *Tarmoqning yuqori unumdorligi*: xavfsizlik siyosati to‘g‘ri amalga oshirilganida va tarmoq doimiy monitoring qilinganida ortiqcha yuklamalar mavjud bo‘lmaydi. Tarmoqda ma’lumotni uzatish tezligi ortadi va bu umumiy samaradorlikni ortishiga olib keladi.

- *Muammolarga darhol javob berish va harakatsiz vaqtning kamligi*: xavfsizlik siyosatini amalga oshirilishi tarmoq muammolari kuzatilganida darhol javob berish imkoniyatini taqdim etadi.

- *Boshqaruvdagi hayajon darajasining kamayishi:* xavfsizlik siyosati amalga oshirilganida boshqaruvchi kam hayajonga ega bo‘ladi. Xavfsizlik siyosatidagi bir vazifa tashkilotning biror xodimiga biriktirilishi shart. Agar ushbu holat amalga

oshirilsa, tarmoqda biror nojo‘ya holat kuzatilsa ham, boshqaruvda hech qanday xavotir bo‘lmaydi.

- *Xarajatlarning kamayishi*: agar xodimlar siyosatga to‘g‘ri amal qilsalar, tashkilotga ta’sir qiluvchi turli xalaqitlar uchun ortiqcha harajat kamayadi.

Xavfsizlik siyosatining iyerarxiyasi:

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

- *Qonunlar*. Qonunlar iyerarxiyaning eng yuqori sathida joylashgan bo‘lib, ular tashkilotdagi har bir xodim amalga oshirishi kerak bo‘lgan vazifalarni o‘z ichiga oladi. Ushbu qonunlarga amal qilmagan har bir xodim uchun javobgarlik choralari ko‘rilishi shart bo‘ladi.

- *Normativ hujjatlar*. Normativ hujjatlar iyerarxiyadagi ikkinchi tashkil etuvchi bo‘lib, ular xodimlarning qonunlarga rioya qilishini kafolatlaydi. Normativ hujjatlar xavfsizlik siyosati qonuniga mos bo‘lgan yo‘l yo‘riq ko‘rsatuvchi hujjatlar to‘plami bo‘lib, ular hukumat yoki ijtimoiy normativ hujjatlardan tashkil topadi.

- *Siyosatlar*. Siyosatlar yordamida tashkilot shaxsiy tarmoq xavfsizligi uchun qonuniy ichki tarmoq talablarini yaratadi. Siyosat turli muolajalardan iborat bo‘lib, ular tashkilot uchun xavfsizlik arxitekturasini 45 ko‘rsatadi. Ushbu siyosatlarning amalga oshirilishi tashkilotga standartlarni o‘rnatish va risklarni boshqarish kabi vazifalarni bajarishiga imkon yaratadi.

- *Standartlar*. Standartlar siyosatni amalga oshirish usullarini tavsiflaydi va tashkilotlar tomonidan amalga oshiriladi. Standartlar korxona siyosatiga ixtiyoriy va mandatli aloqador 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, tashkilotning 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 shakl va hujjatlardan foydalanadilar?*

- *Umumiy qoidalar*. Umumiy qoidalar tanlovga ko‘ra maslahatlar bilan ta’minlovchi hujjat bo‘lib, ulardan biror maxsus standartlar bo‘lmagan holda foydalaniladi. Umumiy qoidalar tavsiyalar sifatida bo‘ladi va tashkilotlar ularni rad eta olmaydi. Umumiy qoidalarni amalga oshirish risklarni kamaytirsada, biznes talablari o‘zgarganida umumiy qoidalarni ham o‘zgartirish tavsiya etiladi.

Xavfsizlik siyosati quyidagi xususiyatlarga ega bo‘lishi shart:

- *Qisqa va aniq*: xavfsizlik siyosati infrastrukturada joriy qilishda 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 oshirishlari shart.

- *Amaliy bo‘lishi*: siyosatlar reallikka asoslangan amaliy bo‘lishi kerak. Real bo‘lmagan siyosatning amalga oshirilishi tashkilotga muammo tug‘diradi.

- *Barqaror bo‘lishi*: tashkilot o‘zining siyosatini amalga oshirishda barqarorlikga ega bo‘lishi kerak.

- *Mulojaviy bardoshli bo‘lishi*: siyosat muolajalari amalga oshirilganida, ular ish beruvchi va ishlovchiga mos bo‘lishi kerak.

- *Kiber va yuridik qonunlarga, standartlarga, qoidalarga va yo‘riqnomalarga mos bo‘lishi*: amalga oshiriluvchi ixtiyoriy siyosat kiber qonunlar asosida ishlab chiqilgan qoidalar va yo‘riqnomalarga mos bo‘lishi zarur.

Axborot xavfsizligi siyosatining turlari. Tashkilotda axborot xavfsizligini rejalashtirish, loyihalash va amalga oshirishda siyosat muhim hisoblanib, ular foydalanuvchilarga xavfsizlik maqsadlariga erishishda mavjud muammolarni bartaraf etish choralarini taqdim etadi.

Axborot texnologiyalari sohasidagi korxonalarda quyidagi xavfsizlik siyosatlari qo‘llaniladi:

- *Tashkilot axborot xavfsizligi siyosati* (Enterprise Information Security Policies, EISP): mazkur siyosat turi tashkilot xavfsiz muhitini, unga g‘oya, maqsad va usullarni taklif qilish orqali, madadlaydi. U xavfsizlik dasturlarini ishlab chiqish, amalga oshirish va boshqarish usullarini belgilaydi. Bundan tashqari, ushbu siyosat taklif etilgan va talab qilingan axborot xavfsizligi strukturasi talablarini kafolatlaydi.

- *Muammoga qaratilgan xavfsizlik siyosatlari* (Issue-Specific Security Policies, ISSP): bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi.

- *Tizimga qaratilgan xavfsizlik siyosatlari* (System-Specific Security Policies, SSSP): mazkur xavfsizlik siyosatini amalga oshirishda tashkilotdagi biror tizimning umumiy xavfsizligini taminlash ko‘zda tutiladi. Bunda tashkilotlar tizimni madadlash maqsadida muolajalar va standartlarni o‘z ichiga olgan SSSP siyosatini ishlab chiqadilar va boshqaradilar. Bundan tashqari, tashkilot tomonidan foydalanilgan texnologiyalar tizimga qaratilgan siyosatlarni o‘z ichiga oladi. Bu siyosat texnologiyani amalga oshirish, sozlash va foydalanuvchilar harakatlarini hisobga olishi mumkin.

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

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

va boshqa yo‘riqnomalarni qamrab oladi. Internetdan foydalanish siyosatini quyidagi to‘rtta kategoriyaga ajratish mumkin:

1. *Tartibsiz siyosat (Promiscuous Policy)*: ushbu siyosat tizim resurslaridan foydalanishda hech qanday cheklovlarni amalga oshirmaydi. Masalan, bu siyosatga ko‘ra foydalanuvchi istalgan saytga kirishi, istalgan dasturni yuklab olishi, masofadagi kompyuterdan yoki tarmoqdan foydalanishi mumkin. Bu siyosat korporativ tashkilotlarning ofislarida ishlovchi yoki tashkilotga kelgan mehmonlar uchun foydali hisoblansada, kompyuterni zararli dasturlar asosidagi tahdidlarga zaif qilib qo‘yishi mumkin.

2. *Ruxsat berishga asoslangan siyosat* (*Permissive Policy*): Bu siyosatga ko‘ra faqat xavfli xizmatlar/ hujumlar yoki harakatlar blokirovkalanadi. Masalan, ruxsat berishga asoslangan Internet siyosatida qator keng tarqalgan zararli xizmatlar/ hujumlardan tashqari Internet trafigining asosiy qismi ochiq bo‘ladi. Faqat keng tarqalgan hujumlar va zararli dasturlar blokirovkalanganligi tufayli, ma’mur joriy holatdagi zararli harakatlarga qarshi himoyani ta’minlay oladi. Bu siyosatda har doim yangi hujumlarni va zararli dasturiy ta’minotlarni tutish va bazaga kiritib borish talab etiladi.

3. *Paranoid siyosati* (*Paranoid Policy*): Paranoid siyosatga ko‘ra barcha narsa blokirovkalanadi va tizim yoki tarmoqdan foydalanuvchi tashkilot kompyuterlarida qat’iy cheklovlar mavjud bo‘ladi. Bu siyosatga ko‘ra foydalanuvchi Internetga umuman ulanmagan yoki qat’iy cheklovlar bilan ulangan bo‘lishi mumkin. Bunday hollarda, foydalanuvchilar odatda siyosatdagi qoidalarni aylanib o‘tishga harakat qiladilar.

4. *Ehtiyotkorlik siyosati* (*Prudent Policy*): Ehtiyotkorlik siyosati barcha xizmatlar blokirovkalanganidan so‘ng amalga oshirilib, unda xavfsiz va zarur xizmatlarga ma’mur tomonidan individual ravishda ruxsat beriladi. Bu maksimal xavfsizlikni ta’minlab, tizim/ tarmoq faoliyatiga oid barcha hodisalarni qaydlaydi.

Maqbul foydalanish siyosati. Maqbul foydalanish siyosati tarmoq va web sayt egalari tomonidan qaror qilingan qoidalardan iborat va u hisoblash resurslaridan to‘g‘ri foydalanishni belgilaydi. Ushbu siyosatda

foydalanuvchilarning o‘z akkauntlarida mavjud bo‘lgan ma’lumotlarni himoya qilish majburiyati ko‘rsatilgan bo‘lib, foydalanuvchidan tarmoqdan yoki Internetdagi kompyuterdan foydalanishida siyosat cheklovlarini qabul qilishi talab etiladi. Ehtiyotkorlik siyosati prinsiplar, taqiqlar, qayta ko‘rib chiqish va jazo choralarini o‘z ichiga olib, foydalanuvchini, shaxsiy sabablarga ko‘ra, korporativ resurslardan foydalanishini taqiqlaydi.

Maqbul foydalanish siyosati axborot xavfsizligi siyosatining ajralmas qismi hisoblanadi. Bunda, tashkilotlar, o‘zlarining yangi xodimlariga axborot resurlaridan foydalanishga ruxsat berishdan oldin, maqbul foydalanish siyosati bo‘yicha tanishganligi xususida kafolat imzosi olinadi.

Maqbul foydalanish siyosati to‘g‘ri amalga oshirilganiga ishonch hosil qilish uchun ma’mur doimiy ravishda xavfsizlik auditini olib borishi kerak. Maqbul foydalanish siyosatlarining aksariyatida siyosatni buzganlik uchun jazolar tayinlanadi. Bunday jazolar foydalanuvchi akkauntini vaqtincha yopib qo‘yishdan tortib qonuniy jazo choralarigacha bo‘lishi mumkin.

Nazorat savollari

1. Axborot xavfsizligi arxitekturasi va uning sathlari mohiyati.
2. Axborot xavfsizligi strategiyasi tushunchasi.
3. Korxona arxitekturasini tuzishda xavfsizlik strategiyasi va arxitekturasining o‘rni.
4. Axborot xavfsizligi siyosati maqsadi qanday?
5. Xavfsizlik siyosati zaruriylik sharti nimalarda ayon bo’ladi?
6. Xavfsizlik siyosatining tarkibiy tuzilmasi deganda nimani tushinasiz?
7. Xavfsizlik siyosatining asosiy turlari.
8. Internetdan foydalanish siyosati.

3 BOB. AXBOROTNING KRIPTOGRAFIK HIMOYASI

3.1. Kriptografiyaning asosiy tushunchalari

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

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

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

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

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

- axborotning konfidensialligini taminlash;
- axborotning yaxlitligini taminlash;
- autentifikatsiya usullarini amalga oshirish;
- harakatni rad qila olmaslikni taminlash.

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

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

- *simmetrik kriptotizimlar;*

- *ochiq kalitli kriptotizimlar;*

- *kriptografik xesh funksiyalar;*

- *raqamli imzolar;*

- *raqamli sertifikatlar*.

Quyida keyingi bayonlarda ishlatiluvchi asosiy atamalarga oydinlik kiritiladi.

Alfavit deganda axborotni ifodalashda ishlatiluvchi bilgilarning chekli to‘plami tushuniladi. Zamonaviy kriptotizimlarda ko‘pincha atigi ikkita simvoldan (0, 1) iborat ikkili alfavit ishlatiladi.

Matn yoki xabar – alfavit elementlaridan tartiblangan nabor.

Ochiq matn (plaintext) – shifrlashga atalgan dastlabki xabar.

Shifrmatn (cipher text) – ochiq matnni shifrlash natijasi.

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

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

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

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

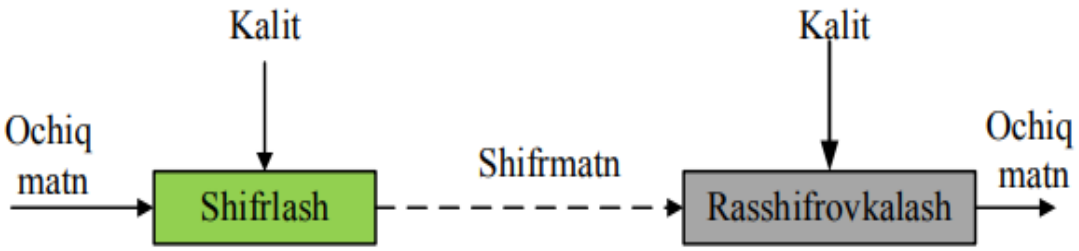
Kriptotizimlarni buzish usullari kriptotahlil (cryptanalysis)ni o‘rganish predmeti hisoblanadi.

Kriptografiya va *kriptotahlil* uzviy bog‘langanliklari sababli, ularni ko‘pincha birgalikda yagona fan – *kriptologiya* (cryptology) (*kryptos* - mahfiy, *logos*- ilm) sifatida qabul qilinadi.

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

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

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



3.1-rasm. Kriptotizimning «qaro quti» sifatidagi ko‘rinishi

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

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

Axborotni kodlash - signalni axborotdan bevosita foydalanish uchun qulay shakldan uzatish, saqlash yoki avtomatik qayta ishlash uchun qulay shaklga aylantirish jarayoni.

Tarmoq kodlash - bu oraliq tugunlarda ma'lumotlar paketlarini o'zgartirish usullaridan foydalangan holda tarmoq orqali ma'lumotlarni uzatishni optimallashtirish masalasini o'rganadigan axborot nazariyasi bo'limi.

Entropiyani kodlash - kodlangan ketma-ketlikdagi elementlarning paydo bo'lish ehtimolini o'rtacha hisoblash orqali ma'lumotlar hajmini (ketma-ketlik uzunligi) kamaytirish uchun bir ma'noda qayta tiklanish imkoniyati bilan qiymatlar ketma-ketligini kodlash.

Delta kodlash - bu ma'lumotlarni o'zi o'rniga ketma-ket ma'lumotlar orasidagi farq (delta) sifatida taqdim etish usuli.

Kodlash ma’lumotlardan foydalanish qulayligini taminlash uchun amalga oshiriladi va hamma uchun ochiq bo‘lgan sxemalardan foydalanadi.

Shifrlash jarayonida ham ma’lumot boshqa formatga o‘zgartiriladi, bunday o’zgartirishning asosiy maqasidi maxfiylikni taminlash hisoblanadi, bu shifrlangan matnni ochiq matnni ko’ra olish faqat muayyan shaxslar ruxsat etilgan.

Kriptografiya va *steganografiya* fan sohalari o‘xshashlikga ega bo‘lganligi sababli, aksariyat hollarda ularni chalkashtirish kuzatiladi.

Steganografiya (yunoncha "yashirin" + γrphō " yozaman"; lit. "kriptografik yozish") - ma'lumotlarni uzatish yoki saqlash usuli , bunday uzatish (saqlash) faktining maxfiyligini hisobga olgan holda. Bu atama 1499 yilda Sponheimdagi Benedikt monastiri Spongeymdagi Iogan Trithemius tomonidan joriy etilgan bo'lib , o'zining "Steganografiya" (lat. Steganographia) risolasida sehrli kitob sifatida shifrlangan.

Yashirin xabarning mazmunini yashiradigan kriptografiyadan farqli o'laroq , steganografiya uning mavjudligi faktini yashiradi. Odatda, xabar boshqa narsaga o'xshaydi, masalan, rasm, maqola, xaridlar ro'yxati, xat yoki sudoku . Steganografiya odatda kriptografik usullar bilan birgalikda qo'llaniladi, shuning uchun uni to'ldiradi.

Kriptografiyada jo‘natuvchi faqat ochiq matn ko‘rinishidagi xabar yuborishi mumkin. Bunda u xabarni ochiq tarmoq (masalan, Internet) orqali uzatishdan oldin shifrlangan matnga o‘zgartiradi. Ushbu shifrlangan xabar qabul qiluvchiga kelganida yana oddiy matn ko‘rinishiga qaytariladi. Umumiy holda ma’lumotni

shifrlashdan asosiy maqsad (simmetrik yoki ochiq kalitli kriptografik tizimlar asosida - farqi yo‘q) – ma’lumotni maxfiyligini qolganlardan sir tutish.

Kriptografiyaning tarixi: Ma’lumotlarni shifrlashning dastlabki ko‘rinishlaridan ming yillar avval foydalanib kelingan. Yaqin o‘n yilliklarga qadar foydalanilgan shifrlar *klassik shifrlar* deb atalgan. Kriptografiyani fan sifatida taraqqiy etishini turli qarashlarga asosan bir nechta darvrlarga bo’lib o’rganiladi, quyida biz ushbu davrlarni ko’rib chiqamiz.

1. *Qadimiy davr* (qadimiy davr klassik shifrlari). Ushbu davrda klassik shifrlar asosan bir alfavitli o‘rniga qo‘yish va o‘rin almashtirish akslantirishlariga asoslangan. Masalan, Sezar, Polibiya kvadrati usullari.

2. *O‘rta davr* (o‘rta davr klassik shifrlari). Ushbu davrda shifrlar asosan ko‘p alfavitli o‘rniga qo‘yishga asoslangan bo‘lib, ularga Vijiner, Atbash usullarini misol sifatida keltirish mumkin.

3. *1 va 2 – jaxon urushlari davri* (1 va 2- jaxon urushlari davridagi klassik shifrlar). Ushbu davr kriptotizimlari asosan elektromexanikaga asoslangan bo‘lib, radio to‘lqin orqali shifrmatnni uzatish (Morze alifbosi) amalga oshirilgan.

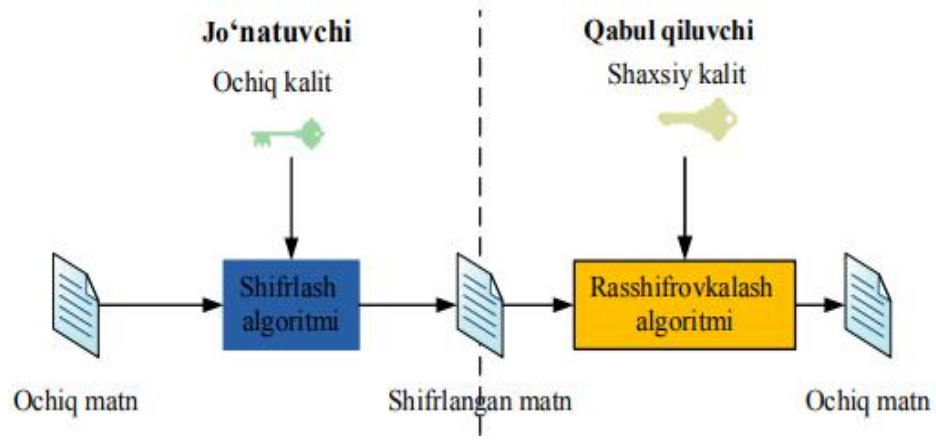
4. *Kompyuter davri* (zamonaviy shifrlar). Ushbu davr shifrlari hisoblash qurilmalariga mo‘ljallangan bo‘lib, yuqori xavfsizlik darajasiga ega. Zamonaviy shifrlarga misol sifatida DES, AES, ГОСТ Р 28147-89, IDEA, A5/1, RC4 (barchasi simmetrik) va RSA, El-Gamal (ochiq kalitli) larni keltirish mumkin.

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

1. *Simmetrik kalitli kriptografiya*. Simmetrik kalitli kriptografiyaning umumiy ko‘rinishi *3.1-rasm*dagi kabi bo‘lib, ma’lumotni shifrlash va rasshifrovkalashda yagona kalitdan (simmetrik kalitdan) foydalaniladi. Shuning uchun ***simmetrik kalitli kriptotizimlarni*** – bir kalitli kriptotizimlar deb ham yuritishadi. Demak, simmetrik kalitli shifrlash algoritmlaridan foydalanish uchun har ikkala tomonda bir xil kalit mavjud bo‘lishi zarur.

2. *Ochiq kalitli kriptografiya*. Ochiq kalitli kriptografiyada ma’lumotni shifrlash qabul qiluvchining ochiq kaliti bilan amalga oshirilsa, uni

rasshifrovkalash qabul qiluvchining shaxsiy kaliti bilan amalga oshiriladi. Shuning uchun ham ochiq kalitli kriptotizimlarni *ikki kalitli kriptotizimlar* deb ham yuritishadi. Ochiq kalitli kriptografiyaning umumiy ko‘rinishi 3.2-rasmda keltirilgan.



3.2-rasm. Ochiq kalitli shifrlashning umumiy ko‘rinishi

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

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

Odatda kriptografiyada ma’lumotlarni shifrlashda (rasshifrovkalashda) ikki turdagi akslantirishlardan foydalaniladi.

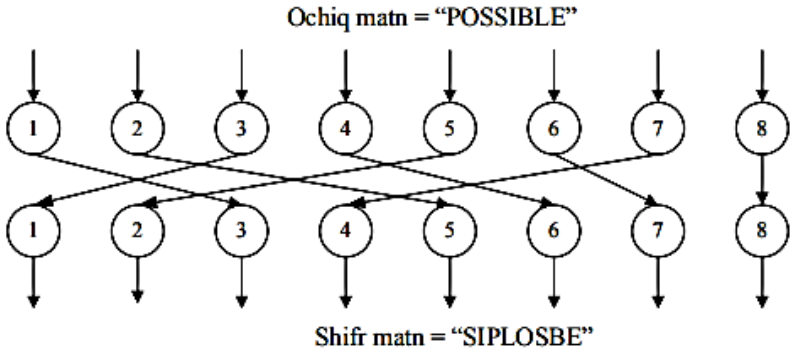
O‘rniga qo‘yish akslantirishi. Ushbu akslantirish sodda va zamonaviy simmetrik kriptografik algoritmlarning asosi hisoblanadi.

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

O‘rniga qo‘yish akslantirishiga misol (*3.1-jadval*)

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

O‘rin almashtirish akslantirishi.Ushbu akslantirishga ko‘ra, ochiq matn simvollarining o‘rni biror qoidaga ko‘ra o‘zaro almashtiriladi.



3.3-rasm. Sodda o‘rin almashtirish usuliga misol

Bir martali bloknot. Bir martali bloknot (one time pad) yoki “Vernam shifri” nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanib, tarixda keng foydalanilgan bo‘lsada, ko‘p hollarda amalga oshirishning imkoniyati mavjud bo‘lmagan. Uning bir martali deb atalishiga asosiy sabab, undagi kalitning (bloknotning) bir marta foydalanilishi bo‘lib, uni aksariyat hollarda amalga oshirishning imkoni bo‘lmaydi. Olingan alfavit simvollari va unga mos bo‘lgan

binar qiymatlar 3.2 - jadvalda keltirilgan. Alfavit simvollari va ularga mos bit qiymatlari barcha uchun ochiq va sir saqlanmaydi.

Ochiq matn uchun tanlangan alfavit 3.2-jadval

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

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

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

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

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

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

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

111 101 110 101 111 100 000 101

A tomon ushbu kalit asosida shifrmatnni quyidagicha hisoblaydi:

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

Shifrmatn:	010	001	000	011	101	100	011	100
	I	E	B	L	P	O	L	O

A tomonidan jo'natilgan shifrmatn B tomonda bir xir kalitdan foydalanib osongina rasshifrovkalanadi:

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

3.2. Simmetrik kriptografik algoritmlar

Simmetrik kriptotizimlar ikki turi mavjud: *oqimli* va *blokli* simmetrik shifrlash algoritmlari hisoblanadi va ulardan har bir tizim o’ziga kerakli turdagi algoritmni tanlab oladi.

Simmetrik kriptotizimlarning ishlashi bilan tanishishda quyidagi belgilashlar kiritiladi:

− ochiq matn P ni simmetrik kalit K bilan shifrlash:

$C = E(P,K)$;

.− shifrmatn C ni simmetrik kalit K bilan rasshifrovkalash:

$M = D(C,K)$.

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

Oqimli simmetrik shifrlash algoritmlari: bir martali bloknotga asoslangan, farqli jihati – bardoshligi yetarlicha pastligi va boshqariladigan kalitning mavjudligi.

Oqimli shifr n bitli kalit K ni qabul qiladi va uni ochiq matnni uzunligiga teng bo‘lgan ketma-ketlik S ga uzaytiradi. Shifrmatn C ketma- ketlik S ochiq matn P bilan X amali yordamida hosil qilinadi.

Oqimli shifrni quyidagicha sodda ko‘rinishda yozish mumkin:

StreamCipher(K)=S

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

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

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

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

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

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

A5/1 oqimli shifrlash algoritmi. A5/1 shifrlash GSM (Group Special Mobile) aloqalarini shifrlash uchun ishlatiladigan oqim shifridir. Bu mobil raqamli uyali telefonlar uchun Evropa standartidir. U telefon/tayanch stansiya kanalini shifrlash uchun ishlatiladi.

A5/1 shifrlash algoritmida dastlabki kalitning uzunligi 64 bitni tashkil etib, u quyidagi uchta registorga qiymat qilib beriladi:

X: 19 bit (x0,x1,x2,…,x18)

Y: 22 bit (y0,y1,y2,…,y21)

Z: 23 bit (z0,z1,z2,…,z22)

Har bir qadamda: m = maj(x8, y10, z10) hisoblanadi

masalan: maj(0,1,0) = 0 va maj(1,1,0) = 1

agarx8 = mga teng bo‘lsa, u holda X registor qiymatlari

t = x13⊕x16⊕x17⊕x18

$x_i = x_{i-1}$ for i = 18,17,…,1 va x_0 = t

agar y_{10} = m ga teng bo‘lsa, u holda y registor qiymatlari

t = y20⊕y21

$y_i = y_i{-}1$ for i = 21,20,…,1 and y_0 =t

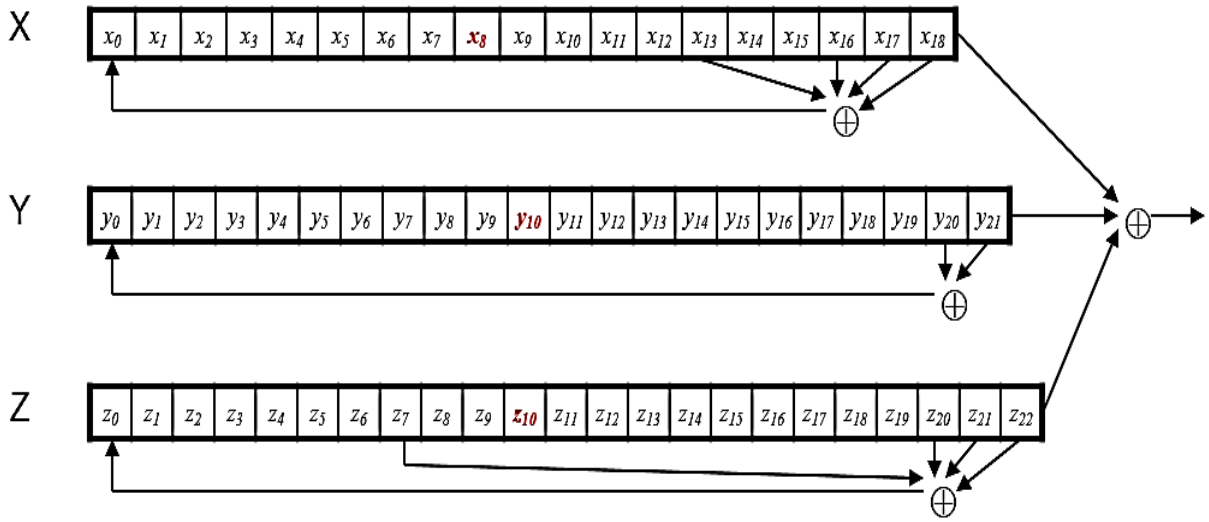
agar z10 = m ga teng bo‘lsa, u holda Z registor qiymatlari

t = z7⊕z20⊕z21⊕z22

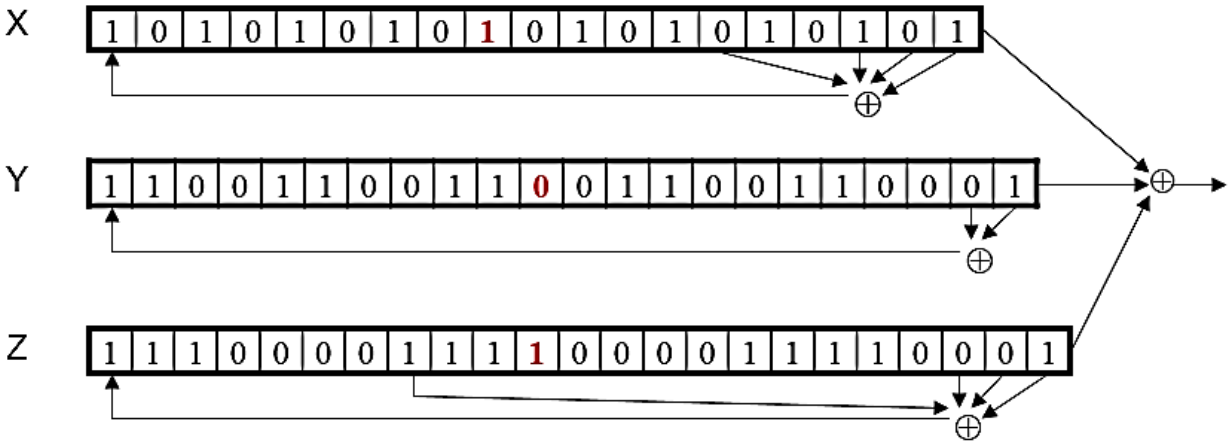
$z_i = z_{i-1}$ for i = 22,21,…,1 and z_0 = t

natijaviy kalit ketma-ketligi x18⊕y21⊕z22 ga teng bo‘ladi.

Bu amallar quyidagi rasmda ifodalangan:(3.4-rasm)



Masalan quyidagi ko‘rsatilgan hol uchun: (3.5-rasm)



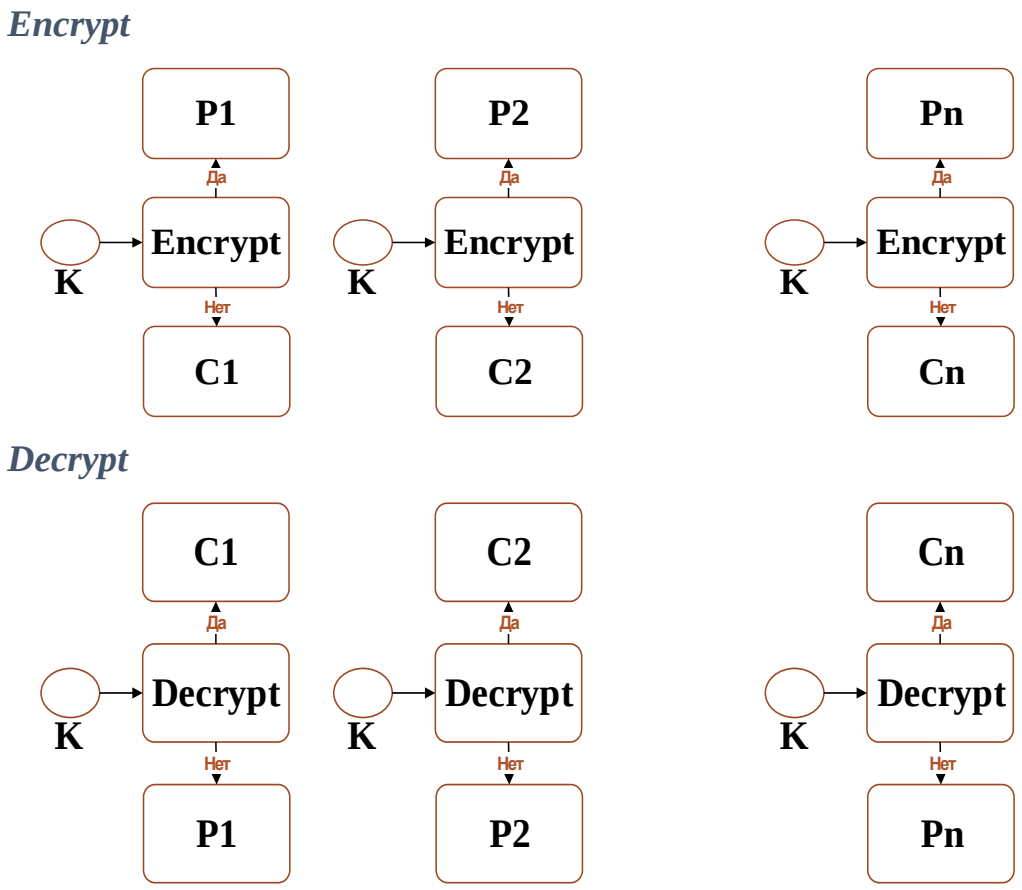
m = maj(x8, y10, z10) = maj(1,0,1) = 1 ga teng bo‘ladi. Natijada X registor siljiydi, Y registor siljimaydi va Z registor siljiydi. O‘ng tomondagi bitlar XOR amal bo‘yicha qo‘shiladi va 0 ⊕ 1 ⊕ 0 = 1 qiymat olinadi.

Blokli simmetrik shifrlash algoritmlari. Shifrlash algoritmlari kirish turiga ko‘ra blokli va oqimli shifr sifatida ikki toifaga bo‘linadi. Blok shifrlash - bu shifrlash algoritmi bo‘lib, u ma'lum hajmdagi kirish hajmini oladi va b bitli

shifrlangan matnni qayta ishlab chiqaradi . Agar kirish b bitdan katta bo‘lsa, uni yana bo‘lish mumkin. Turli xil ilovalar va foydalanish uchun blokli shifr uchun bir nechta ish rejimlari mavjud.

Elektron kod kitobi (ECB) - Elektron kod kitobi blokli shifrlashning eng oson ishlash rejmidir. Kirish ochiq matnning har bir blokini to‘g‘ridan-to‘g‘ri shifrlash tufayli osonroq bo‘ladi va chiqishi shifrlangan shifrlangan matn bloklari shaklida bo‘ladi. Odatda, agar xabar hajmi b bitdan katta bo‘lsa, uni bloklar to‘plamiga bo‘lish mumkin va protsedura takrorlanadi.

ECB protsedurasi quyida ko‘rsatilgan: (3.6-rasm)



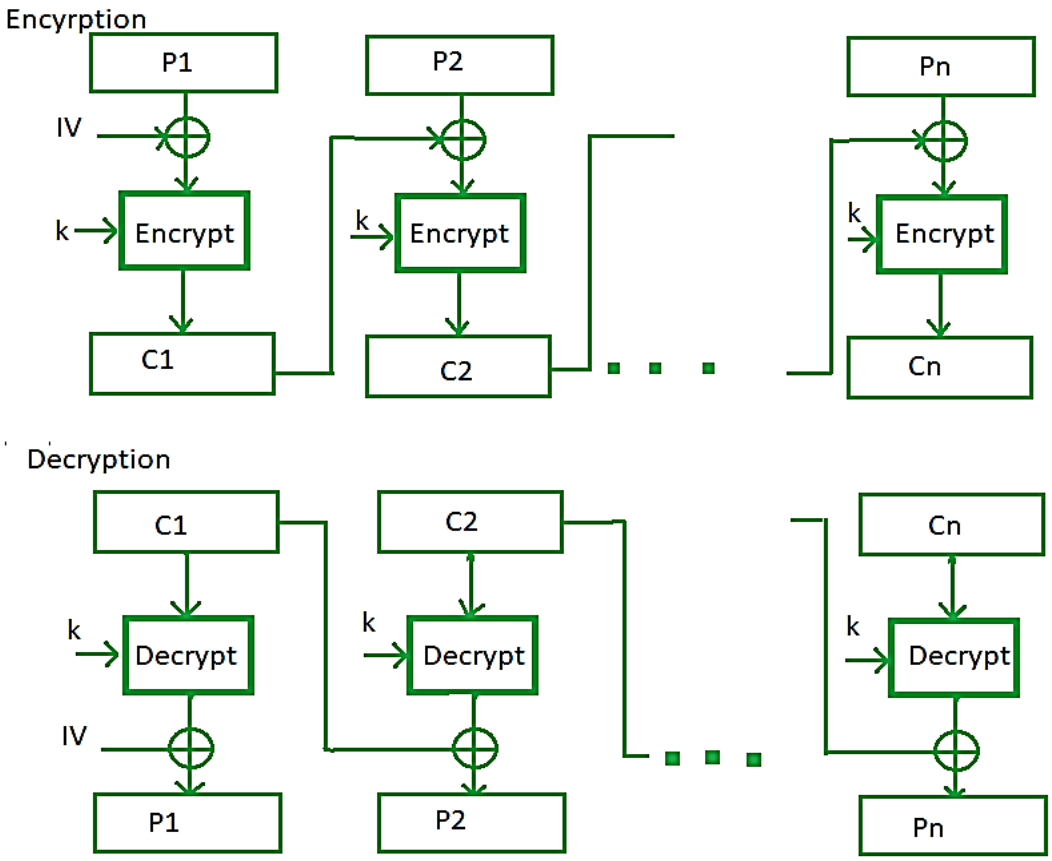
ECB dan foydalanishning afzalliklari - Bit bloklarini parallel shifrlash mumkin, shuning uchun bu shifrlashning tezroq usulidir.

Blok shifrlashning oddiy usuli.

ECB dan foydalanishning kamchiliklari -kriptanalizga moyil, chunki ochiq matn va shifrlangan matn o‘rtasida to‘g‘ridan-to‘g‘ri bog‘liqlik mavjud. Cipher blockchaining yoki CBC bu ECBda erishilgan yutuqlar, chunki ECB ba'zi xavfsizlik talablarini buzadi. CBC da oldingi shifrlash bloki XOR dan keyin asl

ochiq matn bloki bilan keyingi shifrlash algoritmiga kirish sifatida beriladi. Xulosa qilib aytganda, shifrlash bloki oldingi shifrlash blokining XOR chiqishini va hozirgi ochiq matn blokini shifrlash orqali ishlab chiqariladi.

Jarayon bu erda tasvirlangan: (3.7-rasm)



CBC afzalliklari - CBC b bitdan kattaroq kirish uchun yaxshi ishlaydi .

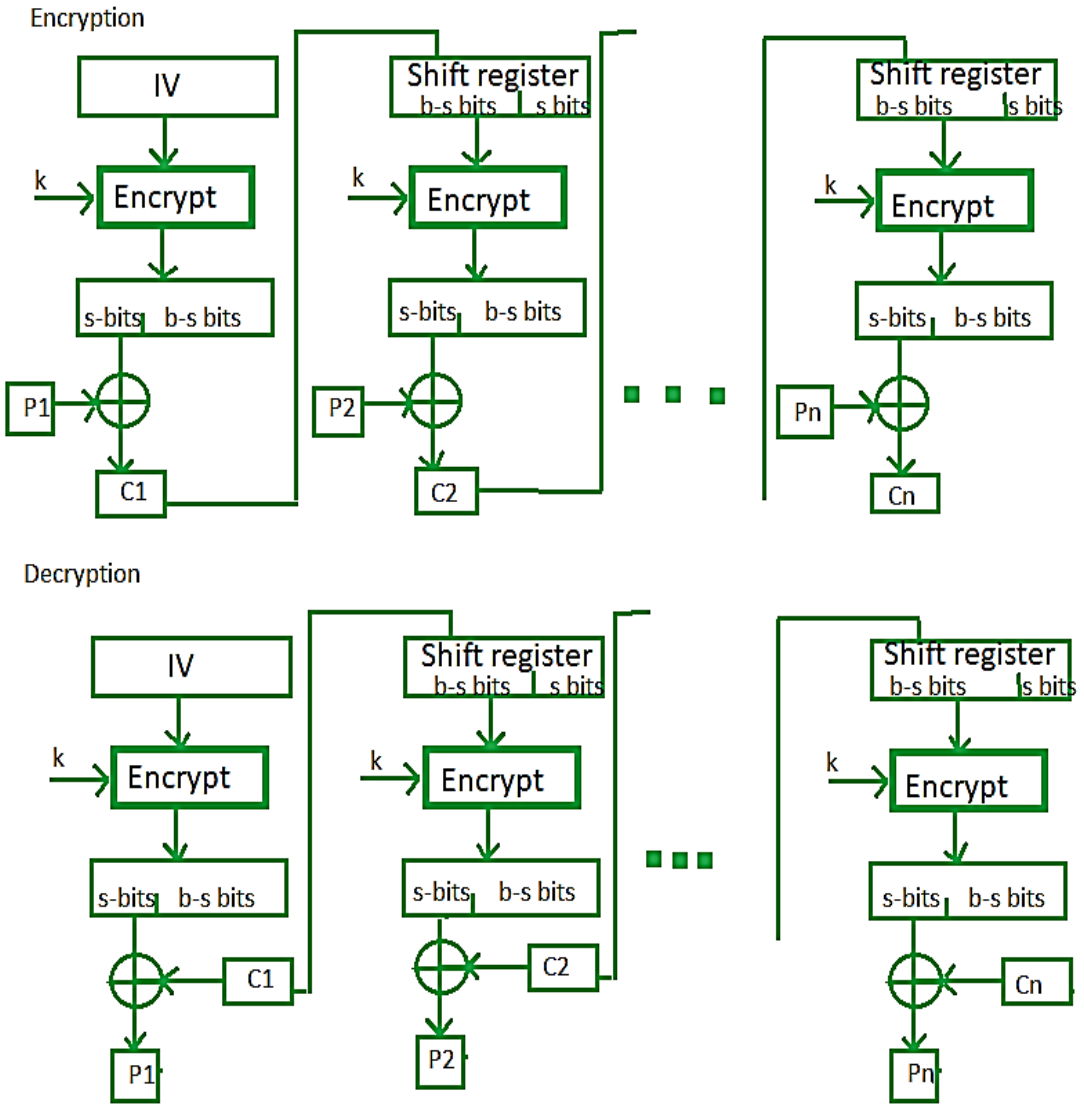
CBC yaxshi autentifikatsiya mexanizmi.

ECBga qaraganda kriptoanalizga nisbatan yaxshiroq qarshilik.

CBC ning kamchiliklari - parallel shifrlash mumkin emas, chunki har bir shifrlash oldingi shifrni talab qiladi.

Shifr bilan qayta aloqa rejimi (CFB) - bu rejimda shifr ba'zi yangi spetsifikatsiyalar bilan keyingi shifrlash blokiga fikr-mulohaza sifatida beriladi: birinchidan, birinchi shifrlash uchun boshlang‘ich vektor IV ishlatiladi va chiqish bitlari s va b_s to‘plamiga bo‘linadi. Chap tomondagi s bitlari XOR operatsiyasi qo‘llaniladigan ochiq matn bitlari bilan birga tanlanadi. Natija bs bitdan lhs ga, s bitdan rhs gacha bo‘lgan siljish registriga kirish sifatida beriladi va jarayon davom

etadi. Xuddi shu narsa uchun shifrlash va shifrni ochish jarayoni quyida ko‘rsatilgan, ikkalasi ham shifrlash algoritmlaridan foydalanadi. *(3.8-rasm)*

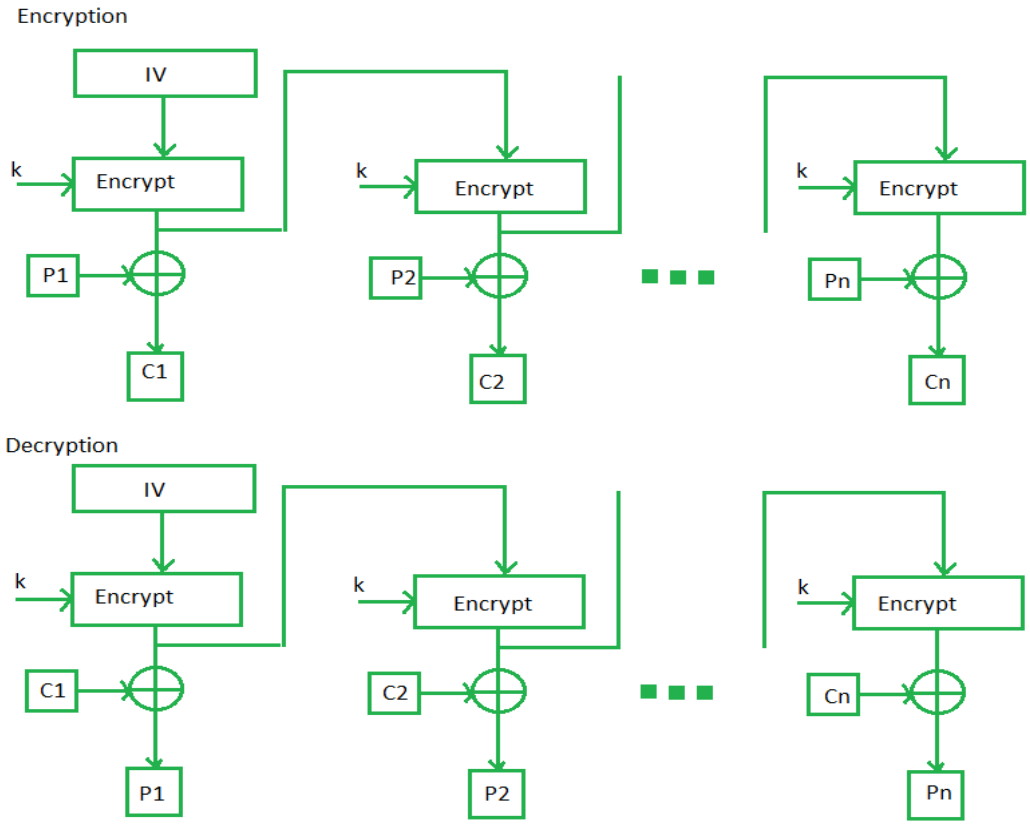


CFB afzalliklari - shift registridan foydalanish tufayli ma’lumotlarning bir oz yo‘qolishi borligi sababli, kriptoanalizni qo‘llash qiyin.

ECB dan foydalanishning kamchiliklari - CFB ning kamchiliklari CBC rejimining kamchiliklari bilan bir xil. Blokdagi yo‘qotishlar ham, bir nechta bloklarni bir vaqtda shifrlash ham shifrlash tomonidan qo‘llab-quvvatlanmaydi. Biroq, shifrni ochish parallelizatsiya qilinadi va yo‘qotishlarga chidamli.

Chiqish bilan bog‘liq fikr-mulohaza rejmi -chiqish teskari aloqa rejimi shifrlangan fikr-mulohaza rejimi bilan deyarli bir xil jarayonga amal qiladi, bundan tashqari u shifrlangan chiqishni XOR chiqishi bo‘lgan haqiqiy shifr o‘rniga qayta

aloqa sifatida yuboradi. Ushbu chiqish teskari aloqa rejimida tanlangan s bitlarini yuborish o‘rniga blokning barcha bitlari yuboriladi . Blok shifrining chiqish mulohazasi rejimi bit uzatish xatolariga katta qarshilik ko‘rsatadi. Bu shuningdek, shifrning ochiq matnga bog‘liqligini yoki aloqasini kamaytiradi. *(3.9-rasm)*

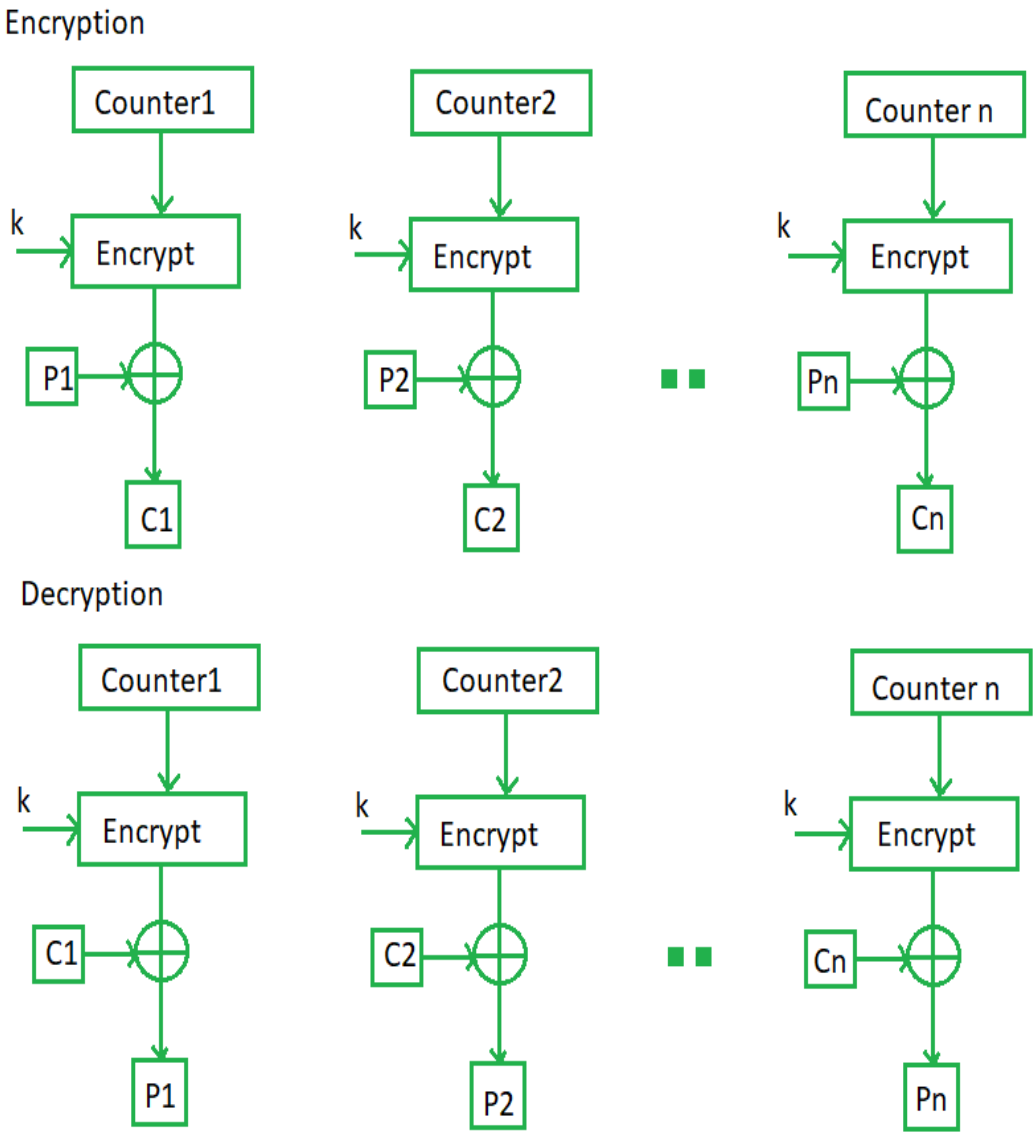


OFB afzalliklari -CFB holatida blokdagi bitta bit xatosi keyingi barcha bloklarga tarqaladi. Bu muammo OFB tomonidan hal qilinadi, chunki u ochiq matn blokida bit xatolaridan xoli.

OFB ning kamchiliklari shundaki, uning ish rejimlariga ko‘ra u CFBga qaraganda xabarlar oqimini o‘zgartirish hujumiga ko‘proq moyil bo‘ladi.

Hisoblagich rejimi yoki CTR oddiy hisoblagichga asoslangan blokli shifrni amalga oshirishdir. Har safar qarshi boshlangan qiymat shifrlanadi va XOR ga ochiq matn bilan kirish sifatida beriladi, bu esa shifrlangan matn blokiga olib keladi. CTR rejimi teskari aloqadan foydalanishdan mustaqil va shuning uchun parallel ravishda amalga oshirilishi mumkin.

Uning oddiy amalga oshirilishi quyida ko‘rsatilgan:*(3.1.1-rasm)*



Hisoblagichning afzalliklari - har bir blok uchun boshqa hisoblagich qiymati mavjud bo‘lgani uchun, to‘g‘ridan-to‘g‘ri ochiq matn va shifrlangan matn aloqasidan qoching. Bu shuni anglatadiki, bir xil oddiy matn turli xil shifrlangan matnga mos kelishi mumkin.

Shifrlashni parallel ravishda amalga oshirish mumkin, chunki oldingi bosqichlardagi chiqishlar CBC misolida bo‘lgani kabi zanjirlanmagan.

Blokli simmetrik shifrlash algoritmlari.Elektron ma'lumotlar bloklari bloklash algoritmlariga duchor bo'ladi. Maxfiy kalit bir vaqtning o'zida belgilangan bit uzunliklari to'plamini o'zgartirish uchun ishlatiladi

Shundan so'ng, kalit har bir blokga qo'llaniladi. Tarmoq oqimi ma'lumotlari shifrlanganda, shifrlash tizimi uni xotira komponentlarida saqlaydi va barcha

bloklar kelishini kutadi. Tizim kutayotgan vaqt jiddiy xavfsizlik teshigiga olib kelishi va ma'lumotlar xavfsizligini xavf ostiga qo'yishi mumkin. Yondashuv ma'lumotlar blokining hajmini kamaytirishni va qolgan bloklar kelguniga qadar uni oldingi shifrlangan ma'lumotlar bloklari tarkibi bilan birlashtirishni o'z ichiga oladi.

Bu fikr bildirish deb ataladi. Qabul qilingandan so'ng butun blok shifrlanadi. Boshqa tomondan, oqim algoritmlari shifrlash tizimining xotirasida saqlanmaydi, balki ma'lumotlar oqimi algoritmlarida keladi. Ushbu usul xavfsizroq, chunki ma'lumotlar xotira komponentlarida shifrlanmagan diskda yoki tizimda saqlanmaydi.

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

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

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

$$\boldsymbol{P = (L_0, R_0)}$$

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

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

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

$$\boldsymbol{C = L_n, R_n}$$

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

$$\boldsymbol{R_{i-1} = L_i}$$

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

Oxirgi raund natijasi, rasshifrovkalangan matnni beradi:

$$P = (L_0, R_0)$$

Feystel tarmog‘ida har bir raundda foydalaniluvchi F funksiyasining teskari funksiyasi bo’lishi shart emas. Ammo, olingan har qanday F funksiya to‘liq xavfsiz bo‘la olmaydi. Simmetrik blokli shifrlarga AES, DES, GOST R 28147-89, O‘z Dst 1105:2009, IDEA, Blowfish va h. misol bo‘la oladi.

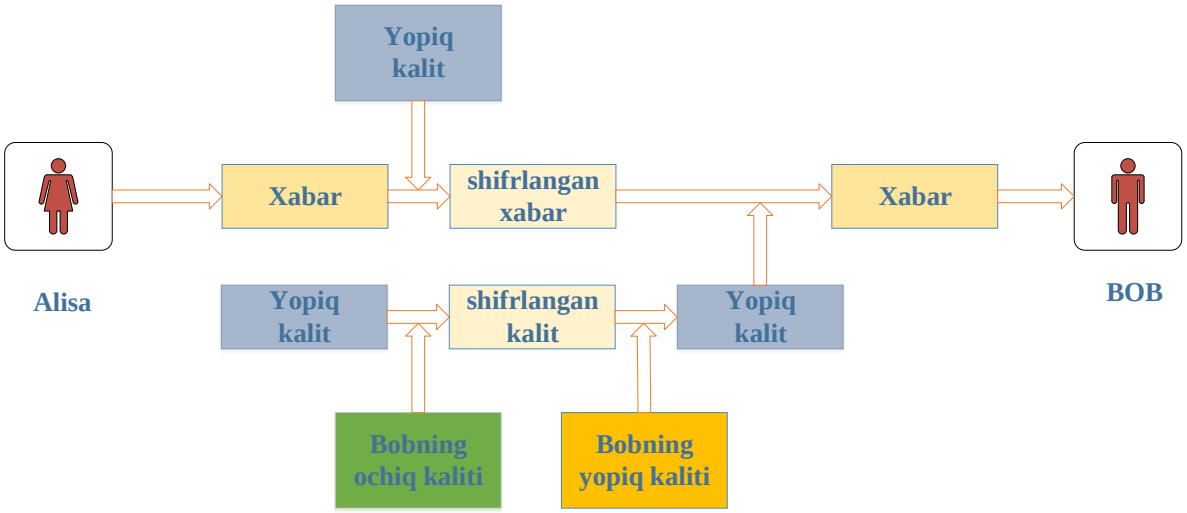
Simmetrik kriptotizimlardagi muammolar. Simmetrik shifrlash tizimlari eng katta muamolaridan biri shifrlash va qayta shifrlash jarayonlarida aynan bir kalitdan foydalanishidadir. Bu o’z navbatida ikki tamon o’rtasida ma’lumot almashishdan oldini kalit ikkinchi tamonga oldindan uzatilish zaruratini keltirib chiqaradi, kalitlarni tomonlar orasida xavfsiz uzatish simmetrik kriptotizimlar oldidagi asosiy muammo sanaladi. Bundan tashqari, bir foydalanuvchining, qolganlari bilan ma’lumot almashishida, ularning har biri bilan alohida kalitlarga ega bo‘lishi talab etiladi. Bu esa foydalanuvchiga ko‘p sonli kalitlarni xavfsiz saqlash zaruriyatini keltirib chiqaradi.

Simmetrik kriptotizimlar afzalliklar tezlik. Ochiq kalitli shifrlash usullarining kamchiliklaridan biri shundaki, ular ishlash uchun juda murakkab matematikani talab qiladi, bu esa hisoblashni intensiv qiladi. Simmetrik kalit ma'lumotlarini shifrlash va shifrini ochish juda oddiy, natijada o'qish va yozishning ajoyib ishlashi. Odatda juda tez ishlaydigan ko'plab qattiq disklar ma'lumotlarni ichida saqlash uchun simmetrik kalit shifrlashdan foydalanadi, ammo ular hali ham shifrlanmagan an'anaviy qattiq disklarga qaraganda tezroq.

Simmetrik kriptotizimlar kamchiliklari katta tarmoqdagi kalitlarni boshqarishning murakkabligi. Tarmoqda yaratilishi, uzatilishi, saqlanishi va yo‘q qilinishi kerak bo‘lgan kalit juftliklar sonining kvadratik o‘sishini anglatadi. 10 ta abonentli tarmoq uchun 45 ta kalit kerak, 100 tasi uchun allaqachon 4950, 1000 tasi uchun - 499500 va boshqalar, kalit almashinuvining murakkabligi. Qo‘llash uchun har bir abonentga kalitlarni ishonchli uzatish muammosini hal qilish kerak, chunki har bir kalitni ikkala tomonga uzatish uchun maxfiy kanal kerak.

Simmetrik shifrlashning kamchiliklarini qoplash uchun hozirda birlashgan (gibrid) kriptografik sxema keng qo‘llaniladi , bu erda sessiya kaliti nosimmetrik shifrlash yordamida ma’lumotlarni almashish uchun tomonlar tomonidan ishlatiladigan assimetrik shifrlash yordamida uzatiladi.

Simmetrik shifrlarning muhim xususiyati mualliflikni tasdiqlash uchun ulardan foydalanishning mumkin emasligidir, chunki kalit har bir tomon uchun ma'lum.



Gibrid kriptografik sxema (3.1.2-rasm)

Yuborish bosqichi:

Elisning xabari shaxsiy kalit bilan shifrlangan, keyin Elis shaxsiy kalitni Bobning ochiq kaliti bilan shifrlaydi (odatda u sessiya kaliti deb ataladi, chunki har safar xabar yuborilganda yangi kalit hosil bo‘ladi);

Elis Bobga shifrlangan xabar va shifrlangan shaxsiy kalitni yuboradi.

Qabul qilish bosqichi:

Bob Elisning shifrlangan xabarini va shifrlangan shaxsiy kalitini oladi,keyin Bob o‘zining shaxsiy kaliti bilan shaxsiy (sessiya) kalitining shifrini ochadi va bu shifrlangan kalitdan (Elis shifrlangan) foydalanib, Bob shifrlangan xabarni hal qiladi;

*Simmetrik kriptotizimlarda kalit uzunligi***.** Amalda kriptografik tizimlarning kalit uzunligiga qat’iy talablar qo‘yiladi. Ushbu talablar vaqt o‘tishi bilan hisoblash qurilmalari imkoniyatining o‘zgarishiga bog‘liq holda o‘zgarib boramoqda.

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.

3.1.3-jadval

Turli uzunlikdagi kalitlarning barcha variantlarini hisoblash vaqtlari

Kalit uzunligi / Qurilma narxi	**80 bit**	**112 bit**	**128 bit**
10 000 $	7 000 yil	10^{13} yil	10^{18} yil
100 000 $	700yil	10^{12} yil	10^{17} yil
1000000$	70yil	10^{11} yil	10^{16} yil
10000000$	7yil	10^{10} yil	10^{15} yil
100000000$	245 kun	10^{9} yil	10^{14} yil

3.3. Ochiq kalitli kriptotizimlar

Ochiq kalit kriptografik tizim (yoki assimetrik shifrlash, assimetrik shifr) - ochiq kalit ochiq (ya'ni himoyalanmagan, kuzatish uchun ochiq) kanal orqali uzatiladigan shifrlash va/yoki elektron raqamli imzo (ERI) tizimi . EDSni tekshirish va xabarni shifrlash uchun ishlatiladi. Maxfiy kalit EDS yaratish va xabarning shifrini ochish uchun ishlatiladi.

Ochiq kalitli kriptografik tizimlar hozirda turli tarmoq protokollarida, xususan, TLS protokollarida va uning oldingi SSL protokollarida (asosiy HTTP S), SSH da keng qo‘llaniladi. P G P , S /M I ME larda ham qo‘llaniladi.

Ochiq kalitli kriptotizimning tamoyillari va usullari: Ochiq kalitli kriptografiya printsipi bir tomonlama funktsiyalarning, ya'ni f (x) funktsiyalarining xossasi bilan juda chambarchas bog‘liq bo‘lib, x berilganda, x ni aniqlashda f (x) qiymatini topish juda oson bo‘ladi. f (x) dan nazariy ma'noda qiyin.

Ammo bir tomonlama funktsiyaning o‘zi dasturda foydasiz: u xabarni shifrlashi mumkin, lekin uni parolini hal qila olmaydi.

Shuning uchun ochiq kalit kriptografiyasi bo‘shliq bilan bir tomonlama funktsiyalardan foydalanadi.

Bo‘shliq - bu shifrni ochishga yordam beradigan bir xil sir (ko‘rsatma). Ya'ni, shunday y borki, f (x)ni bilan hisoblashingiz mumkin .

Misol uchun, agar siz soatni ko‘p qismlarga ajratsangiz, yana ishlaydigan soatni qayta yig‘ish juda qiyin. Ammo agar montaj bo‘yicha ko‘rsatma (bo‘shliq) mavjud bo‘lsa, unda bu muammoni osongina hal qilish mumkin.

Quyidagi misol, kompyuterda parollarni saqlash - ochiq kalit kriptografiya tamoyillari va usullarini tushunishga yordam beradi.

Quyidagi misol, kompyuterda parollarni saqlash - ochiq kalit kriptografiya tamoyillari va usullarini tushunishga yordam beradi.

Tarmoqdagi har bir foydalanuvchi har xil parolga ega. Kirish paytida u ismni belgilaydi va maxfiy parolni kiritadi. Ammo agar siz parolni kompyuter diskida saqlasangiz, kimdir uni o‘qiy oladi (ayniqsa, bu kompyuterning ma'muri uchun buni qilish juda oson) va maxfiy ma’lumotlarga kirish huquqiga ega bo‘ladi. Muammoni hal qilish uchun bir tomonlama funktsiyadan foydalaniladi. Yashirin parolni yaratishda kompyuter parolni o‘zi saqlamaydi, balki ushbu parol va foydalanuvchi nomidan funktsiyani hisoblash natijasidir.

Misol uchun, foydalanuvchi Elis " Gladiolus " parolini o‘ylab topdi. Ushbu ma’lumotlarni saqlashda f (ALISAGLADIOLUS) funksiyaning natijasi hisoblab chiqiladi, natijada tizimda saqlanadigan CAMOMILE satri bo‘lsin . Natijada, parol fayli quyidagi shaklni oladi:

Ism	f (parol nomi)

ALISA	ROMACHA
Elis	NARKISS

Endi tizimga kirish quyidagicha ko‘rinadi:

Nomi:	ALISA
Parol	GLADIOLUS

Elis " *maxfiy* " parolni kiritganda, kompyuter ALISAGLADIOLUS -ga qo‘llaniladigan funksiya kompyuterning diskida saqlangan CAMOMILE to‘g‘ri natija beradimi yoki yo‘qligini tekshiradi. Nom yoki parolda kamida bitta harfni o‘zgartirishga arziydi va funktsiyaning natijasi butunlay boshqacha bo‘ladi. "Yashirin" parol hech qanday shaklda kompyuterda saqlanmaydi. Parol fayli endi boshqa foydalanuvchilar tomonidan maxfiylikni yo‘qotmasdan ko‘rishlari mumkin, chunki funktsiyani qaytarib bo‘lmaydi.

Ushbu misol bo‘shliqsiz bir tomonlama funksiyadan foydalanadi, chunki shifrlangan xabardan asl xabarni olish shart emas.

Quyidagi misolda "orqa eshik", ya'ni topish qiyin bo‘lgan ma’lumotlardan foydalangan holda asl xabarni tiklash qobiliyatiga ega sxema ko‘rib chiqiladi.

Matnni shifrlash uchun siz bir nechta qalin jildlardan iborat katta obunachi katalogini olishingiz mumkin (uni ishlatadigan har qanday shahar aholisining raqamini topish juda oson, ammo ma'lum raqamdan foydalangan holda abonentni topish deyarli mumkin emas). . Shifrlangan xabarning har bir harfi uchun bir xil harf bilan boshlanadigan nom tanlanadi. Shunday qilib, xat abonentning telefon raqamiga tayinlanadi. Yuborilayotgan xabar, masalan, "BOX" quyidagi tarzda shifrlanadi:

Xabar	Tanlangan ism	Kriptomatn
Kimga	Korolev	5643452
O	Orexov	3572651
R	Ruzaeva	4673956
O	Osipov	3517289

B	Baturin	7755628
Kimga	Kirsanova	1235267
VA	Arseniyev	8492746

Kriptomatn: katalogdagi o‘zlari tanlagan tartibda yozilgan raqamlar zanjiri bo‘ladi. Shifrni ochishni qiyinlashtirish uchun siz kerakli harf bilan boshlangan tasodifiy nomlarni tanlashingiz kerak. Shunday qilib, asl xabar turli xil raqamlar ro‘yxati (kriptomatnlar) bilan shifrlanishi mumkin.

Matnni dekodlash uchun sizda ortib borayotgan raqamlar bo‘yicha tuzilgan ma’lumotnoma bo‘lishi kerak. Ushbu katalog faqat qonuniy foydalanuvchilarga ma'lum bo‘lgan bo‘shliq (boshlang‘ich matnni olishga yordam beradigan sir). Qo‘lda ma’lumotnoma nusxasi bo‘lmasa, kriptoanalitik shifrlash uchun ko‘p vaqt sarflaydi.

Ochiq kalit bilan kriptotizimlarni qurishning asosiy tamoyillari

Biz R muammosidan boshlaymiz. Nazariya ma'nosida hal qilish qiyin bo‘lishi kerak: muammoning o‘lchamiga nisbatan ko‘pnomli vaqt ichida P muammosini hal qilishning barcha variantlarini saralashning algoritmi yo‘q.

P dan oson kichik P1 kichik masalani ajratib ko‘rsatish mumkin. Uni chiziqli vaqtga qaraganda ko‘p nomli vaqtda yechish kerak.

P muammosini olish uchun " aralashtiring va silkiting" P1 " asl muammodan butunlay farq qiladi. P muammosi, hech bo‘lmaganda, P muammosi asl hal qilib bo‘lmaydigan P muammosiga o‘xshab ko‘rinishi kerak.

P" shifrlash kaliti sifatida qanday foydalanish mumkinligi tavsifi bilan ochiladi. P ni P dan qanday olish mumkin " maxfiy bo‘shliq sifatida sir saqlanadi.

Kriptotizim shunday tashkil etilganki, yuridik foydalanuvchi va kriptoanalitik uchun shifrni ochish algoritmlari sezilarli darajada farqlanadi. Birinchisi P muammosini hal qilsa, ikkinchisi maxfiy bo‘shliqdan foydalanadi va P muammosini hal qiladi.

Ochiq kalitli kriptotizim tushunchasi: Samarali kriptografik ma’lumotlarni himoya qilish tizimlari assimetrik kriptotizimlar bo‘lib, ular ochiq kalitli

kriptotizimlar deb ham ataladi. Bunday tizimlarda bitta kalit ma’lumotlarni shifrlash uchun, ikkinchi kalit esa ma’lumotlarni shifrlash uchun ishlatiladi (shuning uchun nomi - assimetrik). Birinchi kalit ommaviydir va ma’lumotlarni shifrlaydigan barcha tizim foydalanuvchilari tomonidan foydalanish uchun nashr etilishi mumkin. Ochiq kalit yordamida ma’lumotlarning shifrini ochish mumkin emas.

Ma’lumotlarning shifrini ochish uchun shifrlangan ma’lumotni oluvchi maxfiy bo‘lgan ikkinchi kalitdan foydalanadi. Albatta, shifrlash kalitini shifrlash kalitidan aniqlab bo‘lmaydi.

Modul arifmetikasi. Ochiq kalitli kriptotizimlar,asosini modul arifmetikasi tashkil qilganligi boyis, dastlab unga to‘xtalib o‘tiladi. Har qanday butun sonni $m \in z$ ga bo‘lsak, bu songa tayin bir qoldiq to‘g‘ri keladi. Masalan, $\frac{7}{2} = \mathbf{3} * \mathbf{2} + \mathbf{1}$ bo‘lib, unda qoldiq 1 ga va butun qism 3 ga teng bo‘ladi. Kriptografiyada a sonni b songa bo‘lgandagi qoldiq r ga teng bo‘lsa, u quyidagicha belgilanadi: a mod b ≡ r. Dasturlash tillarida esa $a\%b$ kabi belgilanadi. Quyida qoldiq arifmetikasiga oid bir qancha misollar keltirilgan:

$-7\ mod\ 2 \equiv (3 * 2)\ mod\ 3 + 1\ mod\ 3 \equiv 0 + 1 \equiv 1;$

$-14\ mod\ 3 \equiv (3 * 4)\ mod\ 3 + 2\ mod\ 3 \equiv 0 + 2 \equiv 2;$

$-2\ mod\ 3 \equiv (0 * 3)\ mod\ 3 + 2 mod\ 3 \equiv 2;$

$-5\ mod\ 7 \equiv 5;$

$-2\ mod\ 5 \equiv (-2 + 5)\ mod\ 5 \equiv 3\ mod\ 5 \equiv 3;$

$-7\ mod\ 3 \equiv (-7 + 3)\ mod\ 3 \equiv -4\ mod\ 3 \equiv (-4 + 3)\ mod\ 3 \equiv -1\ mod\ 3 \equiv (-1 + 3)\ mod\ 3 \equiv 2.$

RSA algoritmi. Asimmetrik ochiq/xususiy kalit kriptotizimi g‘oyasi kontseptsiyani 1976 yilda nashr etgan Uitfild Diffi va Martin Xelmanga tegishli. Shuningdek, ular raqamli imzolarni joriy qilishdi va raqamlar nazariyasini qo‘llashga harakat qilishdi. Ularni shakllantirishda ba'zi son modullarini tub songa eksponentlash orqali yaratilgan umumiy maxfiy kalit ishlatilgan. Biroq, ular bir tomonlama funktsiyani amalga oshirish muammosini ochiq qoldirdilar, ehtimol o‘sha paytda faktorizatsiyaning murakkabligi yaxshi tushunilmagan.

MITdagi Ron Rivest, Adi Shamir va Leonard Adleman bir yil davomida invertatsiya qilish qiyin bo‘lgan bir tomonlama funktsiyani yaratishga bir necha bor urinishdi. Rivest va Shamir kompyuter olimlari sifatida ko‘plab potentsial xususiyatlarni taklif qilishdi va Adleman matematik sifatida ularning zaif tomonlarini topishga mas'ul edi. Ular ko‘plab yondashuvlarni sinab ko‘rishdi, jumladan, "xalta" va "o‘zgartirish polinomlari". Bir muncha vaqt ular bir-biriga zid bo‘lgan talablar tufayli erishmoqchi bo‘lgan narsalarini imkonsiz deb o‘ylashdi. 1977 yil aprel oyida ular Pesachni bir talabaning uyida o‘tkazdilar va yarim tunda uylariga qaytishdan oldin juda ko‘p Manishevitz sharobini ichishdi. Rivest uxlay olmay, matematika darsligi bilan divanga yotib, o‘zining bir tomonlama funksiyasi haqida o‘ylay boshladi. U tunning qolgan qismini o‘tkazdi fikrini rasmiylashtirdi va tongga yaqin maqolaning katta qismi tayyor bo‘ldi. Algoritm endi RSA deb nomlanadi - familiyalarining bosh harflari qog‘ozdagi kabi tartibda.

Algoritmning tavsifi. Ochiq kalitli kriptografik tizimlar quyidagi xususiyatga ega bo‘lgan bir tomonlama funktsiyalardan foydalanadi:

ma'lum bo‘lsa $\boldsymbol{x}$, keyin $\boldsymbol{f}(\boldsymbol{x})$ hisoblash nisbatan oddiy;

ma'lum bo‘lsa $\boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x})$, keyin hisoblash uchun $\boldsymbol{x}$ oson (samarali) yo‘l yo‘q.

Bir tomonlamalik deganda matematik jihatdan isbotlangan bir yo‘nalishlilik tushunilmaydi, balki o‘zaro qiymatni oldindan taxmin qilinadigan vaqt oralig‘ida zamonaviy hisoblash vositalari yordamida hisoblashning amaliy imkonsizligi.

RSA ochiq kalitli kriptografik tizimi ikkita katta tub sonlar mahsulotini *faktorizatsiya qilish masalasining* murakkabligiga asoslanadi. Shifrlash uchun ko‘p sonli e*ksponentatsiya modulining* ishlashi qo‘llaniladi. *O‘rtacha vaqt ichida shifrni ochish (teskari operatsiya) uchun siz berilgan katta sonning Eyler funktsiyasini* hisoblashingiz kerak, buning uchun siz sonning tub omillarga bo‘linishini bilishingiz kerak.

Ochiq kalitli kriptografik tizimda har bir ishtirokchi ochiq kalitga *(ingliz tilidagi* ochiq kalit) va shaxsiy kalitga (*inglizcha* xususiy kalit) ega. RSA kriptografik tizimida har bir kalit bir juft butun sondan iborat. Har bir ishtirokchi

o‘zining ochiq va shaxsiy kalitini mustaqil ravishda yaratadi. Ularning har biri shaxsiy kalitni sir saqlaydi va ochiq kalitlar har kimga berilishi yoki hatto nashr etilishi mumkin. RSA kriptotizimidagi har bir xabar almashish ishtirokchisining ochiq va shaxsiy kalitlari o‘zaro teskari ma'noda "*mos juftlik*" hosil qiladi, ya'ni: yaroqli ochiq va shaxsiy kalit juftliklari $(\boldsymbol{p}, \boldsymbol{s})$ tegishli shifrlash funktsiyalari $\boldsymbol{E_p(x)}$ va shifrni ochish $\boldsymbol{D_s(x)}$ shu kabi xabarlar $\boldsymbol{m \in M}$, qayerda M ruxsat etilgan xabarlar to‘plami, $\boldsymbol{m = D_s\left(E_p(m)\right) = E_p\left(D_s(m)\right)}$

Ochiq va shaxsiy kalitlarni yaratish algoritmi.

RSA kalitlari quyidagicha ishlab chiqariladi.

1) ikki xil *tasodifiy tub sonlar tanlanadi* p va q berilgan o‘lcham (masalan, har biri 1024 bit);

2) ularning mahsuloti hisoblanadi $\boldsymbol{n = p \cdot q}$, *bu modul deb ataladi* **;**

3) *sondan Eyler funksiyasining qiymati* hisoblanadi $\boldsymbol{n}$:

$\boldsymbol{\varphi(n) = (p-1) \cdot (q-1)}$;

4)*butun son tanlanga*n $\boldsymbol{e(1 < e < \varphi(n))}$ funksiyaning qiymati bilan taqqoslang $\boldsymbol{\varphi(n)}$ raqam e umumiy ko‘rsatkich deyiladi, odatda e ikkilik yozuvda kichik sonli bitlarni o‘z ichiga olgan tub sonlarni oling , masalan, *Fermat raqamlaridan* tub sonlarni oling: 17, 257 yoki 65537, chunki bu holda *tez eksponentsiya* yordamida shifrlash uchun talab qilinadigan vaqt kamroq bo‘ladi;

5) raqam hisoblanadi $\boldsymbol{d}$, songa ko‘paytma teskari $\boldsymbol{e \bmod \varphi(n)}$, ya'ni taqqoslashni qanoatlantiradigan raqam:$\boldsymbol{d \cdot e = 1 \ (mod \ \varphi(n))}$(raqam d maxfiy ko‘rsatkich deb ataladi ; *odatda kengaytirilgan Evklid algoritmi* yordamida hisoblab chiqiladi);

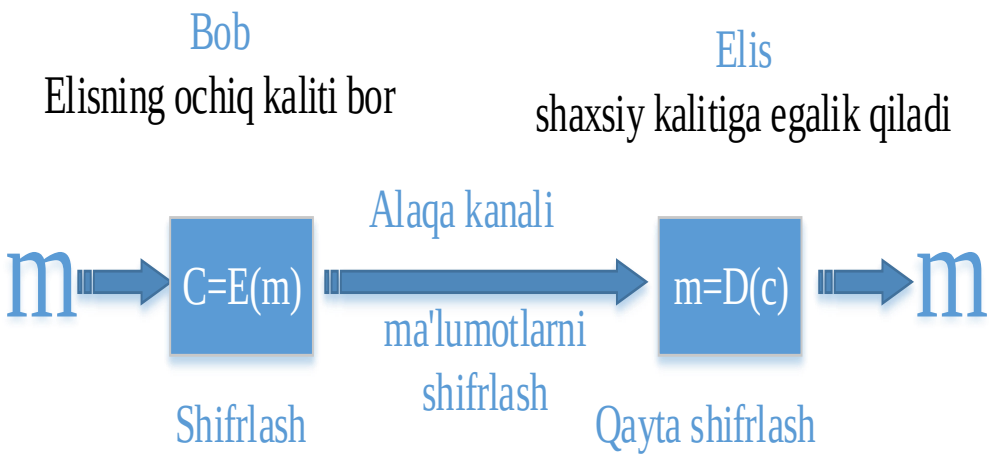
6) juftlik $(\boldsymbol{e, n})$ RSA ochiq kaliti (RSA ochiq kaliti) sifatida nashr etilgan ;

7) juftlik $(\boldsymbol{d, n})$ RSA shaxsiy kaliti rolini o‘ynaydi va sir saqlanadi.

Shifrlash va dekodlash:

Faraz qilaylik, Bob Elisga xabar yubormoqchi $\boldsymbol{m}$.

Xabarlar butun sonlardir 0 oldin $\boldsymbol{n-1}$



Shifrlash algoritmi:

RSA ochiq kaliti yordamida M ochiq matnni shifrlash uchun biz oddiy matnni 0 va N-1 orasidagi raqam sifatida ko'rsatamiz va keyin C shifrlangan matnni quyidagicha hisoblaymiz:

$$C = M^e \bmod N$$

Shifrni ochish algoritmi:

RSA ochiq kaliti yordamida C shifrlangan matnning shifrini ochish uchun biz oddiy M matnini quyidagicha hisoblaymiz:

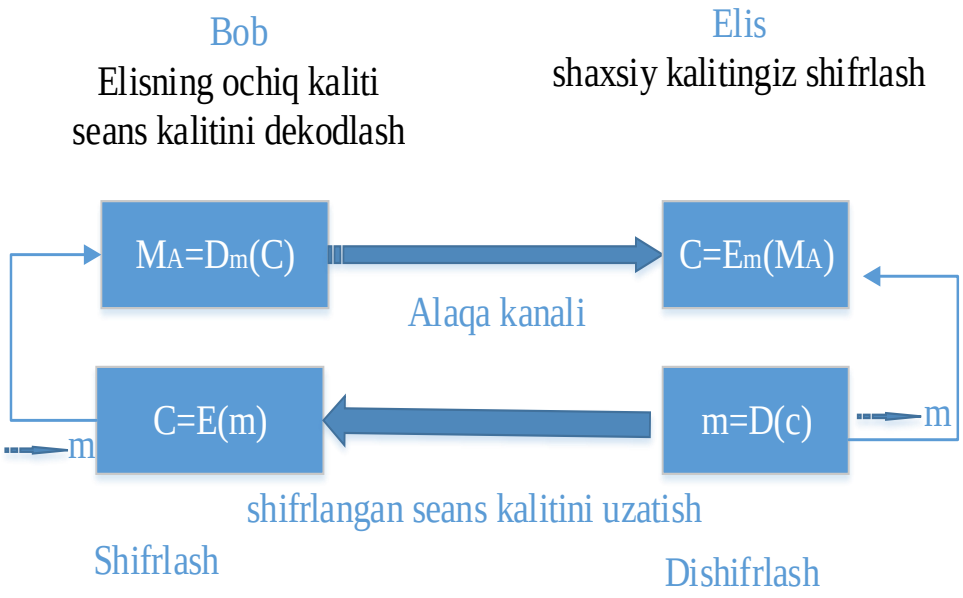
$$M = C^d \bmod N$$

Shuni yodda tutingki, RSA shifrlash ham, RSA shifrini hal qilish ham modulli eksponentsiyani o'z ichiga oladi va shuning uchun biz ushbu jarayonlarni oqilona samarali qilishni xohlasak, takrorlanuvchi kvadratlar algoritmidan foydalanishni tavsiya qilamiz.

Seans kalitini shifrlash algoritmi

Ishonchliroq aralash shifrlash algoritmi bo‘lib, unda seans kaliti avval shifrlanadi, so‘ngra uning yordami bilan ishtirokchilar o‘z xabarlarini simmetrik tizimlar bilan shifrlashadi. Seans tugagandan so‘ng, seans kaliti odatda yo‘q qilinadi.

Seans kalitini shifrlash algoritmi quyidagicha



Algoritm:	Algoritm :
Umumiy kalitni oling $(\boldsymbol{e}, \boldsymbol{n})$ Elis Tasodifiy seans kalitini yarating m Alice ochiq kaliti yordamida sessiya kalitini shifrlang: c=E(m)=me mod n Xabarni shifrlash M simmetrik algoritm yordamida sessiya kalitidan foydalanish: C = Em (MA)	Bobning shifrlangan seans kalitini qabul qiling $\boldsymbol{c}$ Shaxsiy kalitingizni oling (d, n) Seans kalitining shifrini ochish uchun shaxsiy kalitdan foydalaning: m = D (c) = cd mod n Xabarning shifrini ochish C simmetrik algoritm yordamida sessiya kalitidan foydalanish: M_A=Dm(C)

Seans kaliti moduldan kattaroq bo‘lsa $\boldsymbol{n}$, sessiya kaliti kerakli uzunlikdagi bloklarga bo‘linadi (agar kerak bo‘lsa, nol bilan to‘ldirilgan) va har bir blok shifrlangan.

Ochiq kalitli kriptotizimlardan foydalanish

Ochiq kalit kriptografik tizim (assimetrik shifrlashning bir turi, assimetrik shifr) - shifrlash va / yoki elektron imzo (ES) tizimi bo‘lib, unda ochiq kalit ochiq (ya'ni himoyalanmagan, kuzatilishi mumkin) kanal orqali uzatiladi va uni tekshirish uchun ishlatiladi. ES va shifrlash xabarlari uchun. ES yaratish va

xabarning shifrini ochish uchun shaxsiy kalitdan foydalaniladi. Ochiq kalitli kriptografik tizimlar hozirda turli tarmoq protokollarida ,xususan, TLS protokollarida va undan oldingi SSL protokollarida keng qo‘llaniladi. HTTPS), SSH ga PGP , S/MIME da ham foydalaniladi.

Ochiq kalitli kriptotizim g‘oyasi

Assimetrik ochiq kalitlarni shifrlash quyidagi printsiplarga asoslanadi:

Juda katta raqamlar juftligini (ochiq kalit va shaxsiy kalit) yaratish mumkin, shuning uchun ochiq kalitni bilish bilan shaxsiy kalitni oqilona vaqt ichida hisoblash mumkin emas. Bunday holda, ishlab chiqarish mexanizmi yaxshi ma'lum.

Xabarni ochiq kalit bilan shifrlash uchun kuchli shifrlash usullari mavjud bo‘lib, u faqat shaxsiy kalit bilan shifrlanishi mumkin. Shifrlash mexanizmi yaxshi ma'lum.

Ikki kalit egasi shaxsiy kalitni hech kimga oshkor qilmaydi, lekin ochiq kalitni kontragentlar bilan baham ko‘radi yoki uni hammaga ma'lum qiladi.

Agar kalitlar egasiga shifrlangan xabarni uzatish zarur bo‘lsa, jo‘natuvchi ochiq kalitni olishi kerak. Yuboruvchi o‘z xabarini qabul qiluvchining ochiq kaliti bilan shifrlaydi va uni ochiq kanallar orqali qabul qiluvchiga (kalitlar egasiga) uzatadi. Shu bilan birga, shaxsiy kalit egasidan boshqa hech kim xabarni parolini hal qila olmaydi.

Natijada, xabarlar xavfsiz shifrlanishi mumkin, shu bilan birga shifrni ochish kaliti hamma uchun, hatto xabar jo‘natuvchilar uchun ham sir saqlanadi.

Ushbu tamoyilni posilka jo‘natish uchun "qulflash - qulf kaliti" kundalik analogiyasi orqali tushuntirish mumkin. Ishtirokchi A shaxsiy qulf va uning kalitiga ega. Agar A ishtirokchisi B ishtirokchisidan maxfiy paketni olishni istasa, u unga o‘z qal'asini ochiqchasiga beradi. Ishtirokchi B maxfiy paketdagi qulfni qulflaydi va uni A ishtirokchisiga yuboradi. Paketni olgan A ishtirokchisi kalit bilan qulfni ochadi va paketni oladi.

Qulfni uzatish va paketni ushlab qolish haqida bilish potentsial tajovuzkorga hech narsa bermaydi: faqat A ishtirokchisida qulfning kaliti bor, shuning uchun paketni ochib bo‘lmaydi.

Bir tomonlama funksiya orqali amalga oshirish: Ochiq kalitli kriptografiya g‘oyasi bir tomonlama funktsiyalar , ya'ni bunday funktsiyalar g‘oyasi bilan chambarchas bog‘liq $\boldsymbol{f}(\boldsymbol{x})$,bu ma'lum $\boldsymbol{x}$ qiymatini topish juda oson $\boldsymbol{f}(\boldsymbol{x})$, ta'rifi esa $\boldsymbol{x}$ dan $\boldsymbol{f}(\boldsymbol{x})$oqilona vaqt ichida topish mumkin emas.

Ammo bir tomonlama funktsiyaning o‘zi dasturda foydasiz: u xabarni shifrlashi mumkin, lekin uni parolini hal qila olmaydi. Shuning uchun ochiq kalit kriptografiyasi bo‘shliq bilan bir tomonlama funktsiyalardan foydalanadi. Bo‘shliq - bu parolni ochishga yordam beradigan sir. Ya'ni, shunday bor $\boldsymbol{y}$ shuni bilish $\boldsymbol{f}(\boldsymbol{x})$ va $\boldsymbol{y}$, hisoblashingiz mumkin $\boldsymbol{x}$. Misol uchun, agar siz soatni ko‘p qismlarga ajratsangiz, yana ishlaydigan soatni qayta yig‘ish juda qiyin. Ammo agar montaj bo‘yicha ko‘rsatma (bo‘shliq) mavjud bo‘lsa, unda bu muammoni osongina hal qilish mumkin.

Axborotni qabul qiluvchi ochiq kalit va “trapdoor” (boshqacha aytganda, kalitning ochiq va yopiq qismini) hosil qiladi, so‘ngra ochiq kalitni jo‘natuvchiga o‘tkazadi va “trapdoor”ni o‘zi uchun saqlab qoladi. Yuboruvchi ma’lumotni ochiq kalit asosida shifrlaydi: agar sizda bir vaqtning o‘zida ochiq kalit va "orqa eshik" mavjud bo‘lsa, bunday shifrlangan ma’lumotni parolini ochish oson. Funktsiya nuqtai nazaridan qabul qiluvchi shakllanadi $\boldsymbol{f}()$ bo‘shliq bilan $\boldsymbol{y}$, keyin funksiya parametrlari haqidagi ma’lumotlarni uzatadi $\boldsymbol{f}()$ jo‘natuvchi (bir vaqtning o‘zida, hatto funktsiya parametrlarini bilish $\boldsymbol{f}()$, oqilona vaqt ichida "bo‘shliq" topish mumkin emas). Shundan so‘ng, jo‘natuvchi shifrlangan xabarni yaratadi $\boldsymbol{f}(\boldsymbol{x})$, va qabul qiluvchi uni oladi $\boldsymbol{x}$ dan $\boldsymbol{f}(\boldsymbol{x})$,bilish $\boldsymbol{y}$ (qayerda x - shifrlanmagan asl xabar).

Misollar

Quyidagi misol ochiq kalit kriptografiyasining g‘oyalari va usullarini tushunishga yordam beradi - parollarni foydalanuvchilar ulanishi kerak bo‘lgan masofaviy kompyuterda saqlash. Tarmoqdagi har bir foydalanuvchi har xil parolga ega. Kirishda u ismni ko‘rsatadi va maxfiy parolni kiritadi. Ammo agar siz parolni

masofaviy kompyuterning diskida saqlasangiz, kimdir uni o‘qiy oladi (ayniqsa, bu kompyuterning ma'muri uchun buni qilish juda oson) va maxfiy ma’lumotlarga kirish huquqiga ega bo‘ladi. Muammoni hal qilish uchun bir tomonlama funktsiyadan foydalaniladi. Yashirin parolni yaratishda kompyuter parolni o‘zi saqlamaydi, balki ushbu parol va foydalanuvchi nomidan funktsiyani hisoblash natijasidir. Misol uchun, foydalanuvchi Elis "Gladiolus" parolini o‘ylab topdi. Ushbu ma’lumotlarni saqlashda funktsiyaning natijasi hisoblanadi f (ALICE GLADIOLUS), natijada tizimda saqlanadigan CAMOMILE qatori bo‘lsin. Natijada, parol fayli quyidagi shaklni oladi:

Ism	f(Ism: parol)
ALISA	ROMACHA
loviya	NARKISS

Endi tizimga kirish quyidagicha ko‘rinadi:

Nomi:	ALISA
Parol:	GLADIOLUS

Elis "*maxfiy*" parolni kiritganda, kompyuter ALICE_GLADIOLUS-ga qo‘llaniladigan funksiya kompyuter diskida saqlangan CAMOMILE to‘g‘ri natijani beradimi yoki yo‘qligini tekshiradi. Nom yoki parolda kamida bitta harfni o‘zgartirishga arziydi va funktsiyaning natijasi butunlay boshqacha bo‘ladi. "*Yashirin*" parol hech qanday shaklda kompyuterda saqlanmaydi. Parol faylini endi boshqa foydalanuvchilar maxfiylikni yo‘qotmasdan ko‘rishlari mumkin, chunki funktsiya deyarli qaytarib bo‘lmaydi.

Oldingi misolda bo‘shliqsiz bir tomonlama funksiya qo‘llaniladi, chunki shifrlangan xabardan asl xabarni olish shart emas. Quyidagi misolda "orqa eshik", ya'ni topish qiyin bo‘lgan ma’lumotlardan foydalangan holda asl xabarni tiklash qobiliyatiga ega sxema ko‘rib chiqiladi. Matnni shifrlash uchun siz bir nechta qalin jildlardan iborat katta obunachi katalogini olishingiz mumkin (uni ishlatadigan har qanday shahar aholisining raqamini topish juda oson, ammo ma'lum raqamdan

foydalangan holda abonentni topish deyarli mumkin emas). Shifrlangan xabarning har bir harfi uchun bir xil harf bilan boshlanadigan nom tanlanadi. Shunday qilib, xat abonentning telefon raqamiga tayinlanadi. Yuborilayotgan xabar, masalan, " BOX " quyidagi tarzda shifrlanadi:

Xabar	Tanlangan ism	Kriptomatn
Kimga	Korolev	5643452
O	Orexov	3572651
R	Ruzaeva	4673956
O	Osipov	3517289
B	Baturin	7755628
Kimga	Kirsanova	1235267
VA	Arseniyev	8492746

Kriptomatn katalogdagi o‘zlari tanlagan tartibda yozilgan raqamlar zanjiri bo‘ladi. Shifrni ochishni qiyinlashtirish uchun siz kerakli harf bilan boshlangan tasodifiy nomlarni tanlashingiz kerak. Shunday qilib, asl xabar turli xil raqamlar ro‘yxati (kriptomatnlar) bilan shifrlanishi mumkin.

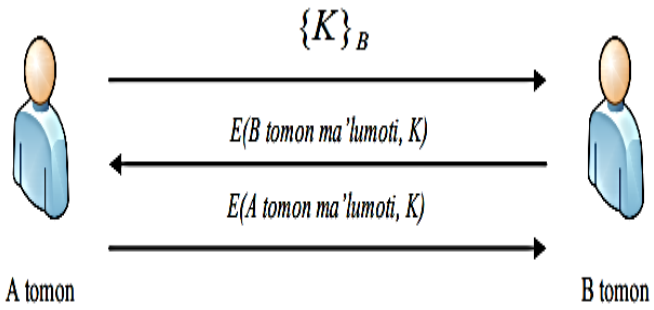
Ochiq kalitli kriptografik tizimlardan foydalanishda quyidagi belgilashlar kiritiladi:

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

Simmetrik shifrlar bilan bajarilgan ixtiyoriy amalni, ochiq kalitli shifrlash algoritmlari bilan ham amalga oshirish mumkin. Masalan, tarmoqda ma’lumotlarni uzatishda va xavfsiz bo‘lmagan muhitda axborot konfidensialligini taminlashda simmetrik shifrlash algoritmlarining o‘rniga ochiq kalitli kriptografik tizimlardan foydalanish mumkin.

Har ikkala kriptotizimning afzalliklarini birlashtirish imkoniyati mavjudmi? Ya’ni, ma’lumotni shifrlashda yuqori samaradorlikka ega va kalitlarni taqsimlash muammosi bo‘lmagan kriptotizimni yaratish mumkinmi?

Albatta, buning imkoniyati mavjud va bunday tizimlar gibrid kriptotizimlar deb ataladi. Kriptografiyada gibrid kriptotizim - bu ochiq kalitli kriptotizimning qulayligini simmetrik kalitli kriptotizimning samaradorligi bilan birlashtiradigan tizimdir. Gibrid kriptotizim sxemasi 3.7-rasmda aks ettirilgan.



3.7-rasm. Gibrid kriptotizim

Ochiq kalitli kriptotizimlarda kalit uzunligi.Simmetrik kalitli kriptotizimlarda bo‘lgani kabi ochiq kalitli kriptotizimlarda ham real hayotda foydalanish uchun kalit uzunligiga talablar qo‘yiladi. Simmetrik va ochiq kalitli kriptotizimlarning matematik asosi turlicha bo‘lgani bois, ular bir xil bardoshlik darajasida bo‘lganida turli kalit uzunliklariga ega bo‘ladilar (*3.8-jadval*).

Bir xil bardoshlikka ega simmetrik va ochiq kalitli kriptotizimlar kalitlarining uzunligi

Simmetrik shifrlash algoritmi	RSA algoritmi ($\boldsymbol{p}$ va $\boldsymbol{q}$ 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.

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

N ning bitdagi uzunligi	Talab etiluvchi yillar
512	**30000**
768	$\mathbf{2 \cdot 10^8}$
1024	$\mathbf{3 \cdot 10^{11}}$
1280	$\mathbf{10^{14}}$
1536	$\mathbf{3 \cdot 10^{16}}$
2048	$\mathbf{3 \cdot 10^{20}}$

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

3.4. Ma’lumotlar yaxlitligini taminlash usullari

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

Xesh funksiya. Xesh funksiyasi (ing. hash function from hash - “turn into qiyma”, “hash”) yoki konvolyutsiya funksiyasi ixtiyoriy uzunlikdagi kirish ma’lumotlari massivini chiqish bit qatoriga aylantiruvchi funksiyadir ,belgilangan uzunlik, ma'lum bir algoritm tomonidan amalga oshiriladi. Xesh funktsiyasi tomonidan amalga oshirilgan transformatsiyaga *xashing* deyiladi. Kirish ma'lumotlari kirish massivi, “*kalit* “ yoki “*xabar* “ deb ataladi. Konvertatsiya

natijasi “*xesh* “, “*xesh kodi* “, “*xesh summasi* “, “*hash*” deb nomlanadi. Xesh funksiya quyidagi xususiyatlarga ega:

1. Ixtiyoriy uzunlikdagi matnga qo‘llash mumkin.

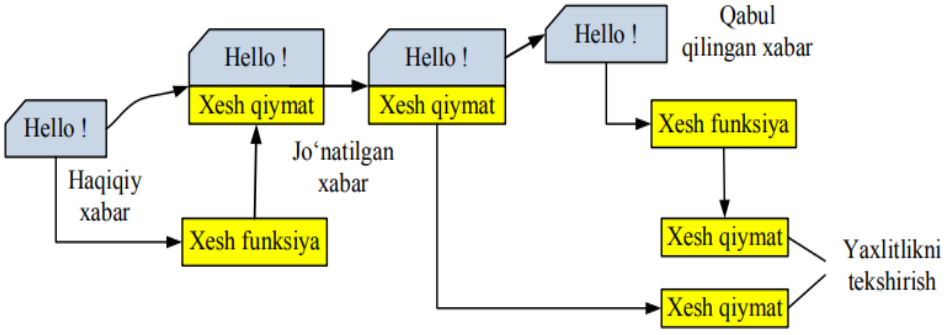
2. Chiqishda tayinlangan uzunlikdagi qiymat shakllanadi.

3. Berilgan ixtiyoriy x bo‘yicha $h(x)$ oson hisoblanadi.

4. Berilgan ixtiyoriy H bo‘yicha $h\ (x) = N$ tenglikdan x ni hisoblab topib bo‘lmaydi (bir tomonlilik xossasi).

5. Olingan x va $y \neq x$ matnlar uchun $h(x) \neq h(y)$ bo‘ladi (kolliziyaga bardoshlilik xossasi).

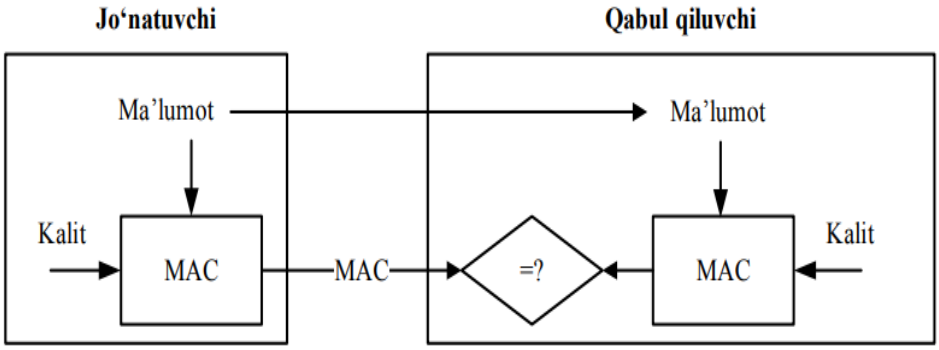
Xesh funksiya yordamida uzatilayotgan ma’lumotlar yaxlitligini tekshirishning sodda ko‘rinishi 3.9-rasmda keltirilgan. Jo‘natuvchi xabarning xesh qiymatini hisoblaydi va uni qabul qiluvchiga xabar bilan birgalikda yuboradi. Qabul qiluvchi dastlab xabarning xesh qiymatini hisoblaydi va qabul qilingan xesh qiymat bilan taqqoslaydi. Agar har ikkala xesh qiymat teng bo‘lsa, ma’lumotning yaxlitligi o‘zgarmagan, aks holda o‘zgargan deb topiladi. Odatda xesh funksiya kirishda ma’lumotdan tashqari xech qanday qiymatni talab etmagani bois, kalitsiz kriptografik funksiyalar deb ham ataladi (kalit talab qiluvchi ma’lumotlarning yaxlitligini taminlash usullari ham mavjud).



3.9-rasm. Xesh funksiya asosida ma'lumotlar yaxlitligini tekshirish

Yuqorida keltirilgan usulda xavfsizlik muammosi jiddiy bo‘lgani bois, undan amalda foydalanilmaydi. Ya’ni, hujumchi tomonidan faqat ma’lumot o‘zgartirilgan holda yaxlitlikni tekshirish imkoniyati mavjud. Biroq, hujumchi ma’lumotning xesh qiymatini almashtirish orqali foydalanuvchini osonlik bilan ma’lumot yaxlitligiga ishontirishi mumkin. Ushbu muammoni bartaraf etuvchi –

xabarlarni autentifikatsiyalash kodi (message authentication code, MAC) tizimlari mavjud bo‘lib, unga ko‘ra biror maxfiy kalit asosida ma’lumotning xesh qiymati hisoblanadi (3.10-rasm).



3.10-rasm. MAC tizimi

MAC tizimini ishlab chiqishda blokli shifrlardan ham foydalanish mumkin. Buning uchun blokli shifrni CBC (Cipher Block Chaining – shifr bloklar zanjiri) rejimida foydalanish va eng oxirgi shifrmatn blokini olishning o‘zi yetarli (qolganlari tashlab yuboriladi). Albatta, mazkur usul MAC tizimini yaratishning yagona usuli emas. Quyida xesh funsiyalar asosida MAC tizimini yaratish bilan tanishib chiqiladi.

Xesh – funksiyalar asosida ma’lumot yaxlitligini tekshirish.

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

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

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

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

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

$$\mathbf{H}(\mathbf{M},\mathbf{K}) = \mathbf{H}(\mathbf{K} \oplus \mathbf{opad}, \mathbf{H}(\mathbf{K} \oplus \mathbf{ipad}, \mathbf{M})).$$

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

$i$pad = $0x36$ ni B marta $t$akrorlash $n$atijasida

opad=$0x5c$ ni B $m$arta $t$akrorlash $n$atijasida

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

Ochiq kalitli shifrlash algoritmlari asosida ma’lumot yaxlitligini tekshirish va rad-etishdan himoyalash. Quyida ochiq kalitli kriptotizimlar va xesh funksiyalar asosida ishlovchi – elektron raqamli imzo tizimi bilan tanishib o‘tiladi.

O‘zbekiston Respublikasining Elektron raqamli imzo to‘g‘risidagi qonunida elektron raqamli imzoga quyidagicha ta’rif berilgan:

Elektron raqamli imzo (ERI) -elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda, maxsus o‘zgartirish natijasida hosil qilingan, hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradi va bu shaxsiy imzo kaliti yordamida ma'lumotlarni kriptografik o'zgartirish natijasida olingan elektron hujjatning atributi bo'lib , imzo tuzilgan paytdan boshlab elektron hujjatda ma'lumotlarning buzilishi (yaxlitligi) yo'qligini tekshirish imkonini beradi. Imzo imzo kaliti sertifikati (mualliflik) egasiga tegishli bo'lib, muvaffaqiyatli tekshirilgan taqdirda elektron hujjat imzolanganlik faktini tasdiqlaydi (rad etmaslik).

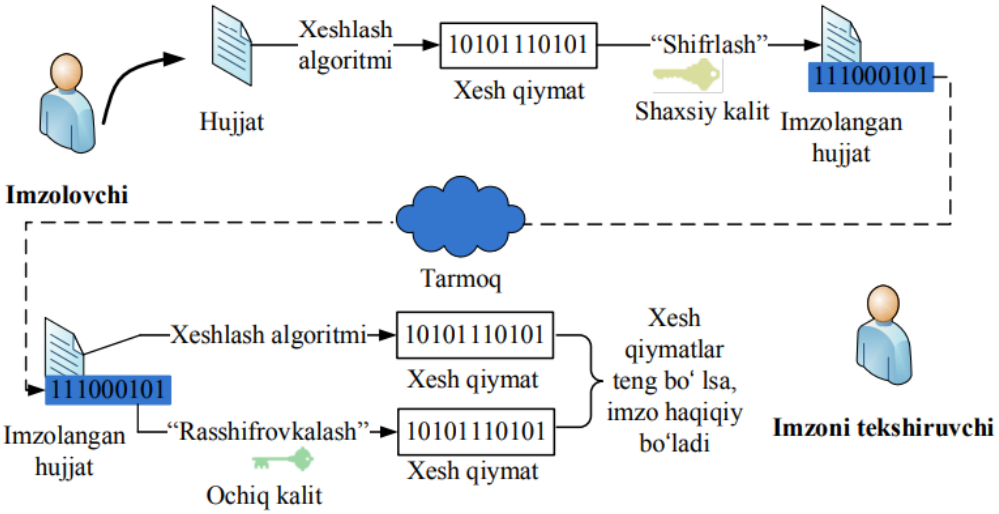
Axborot xavfsizligida rad etish muammosi mavjud, unga ko‘ra foydalanuvchi hujjatni imzolaganini rad etadi (ya’ni, men imzolamadim deb turib oladi). Mazkur muammoni oldini olishda aynan elektron raqamli imzo tizimlaridan foydalaniladi.

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

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

shaxsiy kalit egasi xabarni imzolaydi, qolganlar esa, uning ochiq kalitidan foydalanib, imzoni haqiqiyligini tekshiradi.

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



3.11-rasm. Elektron raqamli imzo sxemasi

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

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

Rad etishdan himoyalashni tushunishdan oldin, MAC asosida yaxlitlikni taminlashga biror sodda misol keltiraylik. Faraz qilaylik, A tomon o‘zining

dilleriga B tomondan 100 ta aksiyani olishga buyurtma berdi. Berilgan buyurtmani yaxlitligini taminlash uchun A tomon B tomon bilan taqsimlangan kalit $\boldsymbol{K_{AB}}$ yordamida MAC ni hisoblaydi. Ma'lum vaqt o'tganidan so'ng, buyurtmalar tayyor bo'ladi. Biroq, A tomon to'lovni amalga oshirishdan oldin aksiyalarning narxi tushib ketadi. Bu vaqtda, AA tomon buyurtmani men bermadim deb turib oladi va uni rad etadi. Bunga yaxlitlikni taminlash uchun hisoblangan MAC ni har ikkala tomon ham hosil qilishi sabab bo'ladi.

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

Ochiq kalitlar infrastrukturasi (Public key infrastructure, PKI). Ochiq kalitli kriptografiya bilan bog'liq bo'lgan muammolardan yana biri - ochiq kalitning kimga tegishli ekanligini aniqlash. Faraz qilaylik, AA 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 infrastrukturasidan foydalaniladi.

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

Raqamli sertifikat (yoki ochiq kalit sertifikati yoki qisqacha sertifikat) foydalanuvchining ismi va uning ochiq kalitidan iborat (amalda foydalanuvchiga va sertifikatga tegishli ma'lumotlar ham bo'ladi) va u sertifikat markazi (certificate

authority yoki CA) tomonidan imzolanadi. Masalan, A tomonning sertifikati quyidagidan iborat bo‘ladi:

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

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

$\boldsymbol{C_A}$ tomoniga, odatda, ishonchli uchinchi tomon (trusted third party yoki TTP) sifatida qaraladi. Ya’ni, odatda A tomon foydalanuvchi uchun shaxsiy va ochiq kalitlar juftini generatsiyalaydi. Shaxsiy kalit A tomonga taqdim etilganidan so‘ng, C_{A} 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 C_{A} ning ochiq kalitini (ya’ni, unga teng bo‘lgan sertifikatni) bilishi talab etadi. Demak, C_{A} tomonning ochiq kaliti (yoki sertifikati) oldindan foydalanilayotgan tizimda mavjud va bu haqida barcha ma’lumotga ega bo‘ladi.

Nazorat savollari

1. Kriptografiyaning asosiy tushunchalarig.
2. Rasshifrovkalashning deshifrlashdan farqi nimada?
3. Axborotni simmetrik va ochiq kalitli shifrlash algoritmlari yordamida shifrlashdagi afzallik va kamchiliklari.
4. Kerkgoff prinsipining mohiyatini tushuntiring.
5. Kodlash va shifrlash tushunchalarining bir – biridan farqi nimada?
6. Kriptologiya va steganografiya fan sohalari va ularning o‘zaro farqi.
7. Simmetrik kriptografiyaning axborotni himoyalashdagi o‘rni.
8. Ochiq kalitli kriptografiyaning axborotni himoyalashdagi o‘rni.
9. Xesh funksiya, unga qo‘yilgan talablar va uning axborot himoyalashdagi o‘rni.
10. Kriptografik akslantirishlar: o‘rniga qo‘yish va o‘rin almashtirish nima?
11. Bir martali bloknot yordamida ma’lumotlarni shifrlash va uning xavfsizligi.

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

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

14. Modul arifmetrikasidagi asosiy amallar.

15. RSA algoritmi va u asoslangan matematik muammo.

16. Ma’lumotlarning yaxlitligini taminlash usullari.

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

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

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

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

4 BOB. FOYDALANISHNI NAZORATLASH

4.1. Identifikatsiya va autentifikatsiya vositalari

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

Axborot tizimlarida identifikatsiya - bu sub'ektlar va ob'ektlarga identifikatorni belgilash va/yoki identifikatorni tayinlangan identifikatorlar ro'yxati bilan solishtirish. Masalan, shtrix kodini identifikatsiya qilish.

Axborot xavfsizligi sohasida foydalanuvchilarning identifikatoriga nisbatan "identifikatsiya"atamasi autentifikatsiya va avtorizatsiya tushunchalari o'rniga noto'g'ri ishlatiladi.

Identifikatsiya - ob'ektlarning ma'lum belgilarga ko'ra o'xshashligini tekshirish (shaxsni kim ekanligini tanishtirish jarayoni). Elektron pochta tizimida pochta manzilini identifikator, manzilini taqdim etish jarayonini esa identifikatsiyalash deb ataladi.

Autentifikatsiya – bu autentifikatsiya jarayoni. Bu atama ko'pincha axborot texnologiyalari muhitida qo'llaniladi. Foydalanuvchi tomonidan kiritilgan parolni server ma'lumotlar bazasida saqlangan parol bilan solishtirish autentifikatsiyaning bir misolidir.

Foydalanuvchi autentifikatsiyadan o‘tganidan so‘ng, tizim resurslaridan foydalanish imkoniyatiga ega bo‘ladi. Biroq, autentifikatsiyadan o‘tgan foydalanuvchi tizimda faqatgina ruxsat berilgan amallarni bajarishi mumkin.

Avtorizatsiya –sizning shaxsingiz tizim tomonidan muvaffaqiyatli tasdiqlanganidan so'ng amalga oshiriladi. Shuning uchun sizga ma'lumot, fayllar, ma'lumotlar bazalari, fondlar va boshqa manbalarga to'liq kirish huquqini beradi.

Ammo avtorizatsiya sizning kirish huquqingizni aniqlagandan keyingina manbalarga kirish huquqini tasdiqlaydi. Boshqacha qilib aytganda, avtorizatsiya - bu autentifikatsiya qilingan foydalanuvchining muayyan manbalardan foydalana olishini aniqlatuvchi jarayon hisoblanadi.

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

Identifikatsiya – siz kimsiz?

Autentifikatsiya – siz haqiqatan ham sizmisiz?

Avtorizatsiya – sizga buni bajarishga ruxsat bormi?

Bir tomonlama autentifikatsiya (Single-Factor Authentication***)***-bu autentifikatsiya jarayonining eng oddiy shakli bo'lib, foydalanuvchiga veb-sayt yoki tarmoqda muayyan tizimga kirish huquqini berish uchun parolni talab qiladi.

Masalan, foydalanuvchi nomiga tegishli parolnigina talab qilish orqali faqat bitta faktorli autentifikatsiya yordamida login ma'lumotlarini tekshirishi mumkin.

Ikki tomonlama autentifikatsiya (Two-Factor Authentication***)***-ushbu autentifikatsiya ikki bosqichli tekshirish jarayonini talab qiladi, bu nafaqat foydalanuvchi nomi va parolni, balki faqat foydalanuvchi biladigan ma'lumotni ham talab qiladi.

Ko‘p omilli autentifikatsiya (Multi- Factor Authentication***)***-bu autentifikatsiyaning eng ilg'or usuli bo'lib, foydalanuvchilarga tizimga kirish huquqini berish uchun mustaqil autentifikatsiya kategoriyalaridan ikki yoki undan ko'p darajadagi xavfsizlikni talab qiladi. Autentifikatsiya qilishning ushbu shakli har qanday ma'lumotlarga ta'sir qilishni bartaraf etish uchun bir-biridan mustaqil bo'lgan omillardan foydalanadi. Masalan, elektron pochtaga kirishda faqat parolni bilishning o‘zi yetarli bo‘lsa, binoga kirishda barmoq izini to‘g‘ri kiritishning o‘zi eshikning ochilishi uchun yetarli bo‘ladi. Ya’ni, server faqat foydalanuvchidan parolni yoki barmoq izi tasvirini to‘g‘ri bo‘lishini talab qiladi.

Bir omilli autentifikatsiyada tekshirish faqat bitta omil bo‘yicha (masalan, parol) amalga oshirilsa, bunday autentifikatsiya *bir omilli autentifikatsiya* deb yuritiladi.

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

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

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

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

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

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

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

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

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

protokoli yordamida). Parol axborotini shifrlash protokollari va vositalari esa yyetarlicha kriptobardoshlikka ega emas.

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

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

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

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

− parol va qayd yozuvlari himoyasi siyosatini kuchaytirish.

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

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

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

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

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

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

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

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

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

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

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

$$\boldsymbol{H = n \cdot log_2 |A|},$$

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

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

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

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

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

Elektron qurilmalarni quyidagicha tasniflash mumkin:

- amalga oshirilishi bo‘yicha passiv (faqat xotirali) va aktiv (mikroprosessorli) elektron qurilmalar farqlanadi;

- o‘qish qurilmalarining mavjudligi bo‘yicha alohida o‘qish qurilmasili (reader), kalit bilan integrallangan o‘qish qurilmasili (*masalan USB- portga ulanadi*) va kompyuterning kiritish qurilmasidan va asosiy xotirasidan foydalanuvchi elektron qurilmalar farqlanadi;

- funksional belgilanishi bo‘yicha *statik*, *sinxron dinamik* va *asinxron dinamik* elektron qurilmalar farqlanadi.

Statik qurilmalar doimiy noyob axborotni saqlashni ta’minlaydi va subyektni autentifikatsiyalash yoki identifikatsiyalash uchun ishlatiladi. Oddiygina

statik qurilmalarga disketa, xotira kartasi, magnit tasmali, qog‘oz karta, tarkibida identifikator, parol, sertifikat va h. bo‘lgan ATM karta misol bo‘la oladi.

Zamonaviy statik qurilmalarga quyidagilar taalluqli:

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

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

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

− kontaktsiz radiochastota identifikatorlari – RFID– radiometkalar.

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

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

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

Elektron qurilmalar qator kamchiliklarga ega:

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

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

− oddiy qurilmalar klonlashtirilishi mumkin;

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

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

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

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

− autentifikatsiya axborotini yashirish uchun simmetrik algoritmdan foydalaniladi;

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

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

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

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

- mijoz Kerberos serveriga, tarkibida mijoz identifikatori va so‘raluvchi server servisi bo‘lgan so‘rovni jo‘natadi;

- Kerberos, serverning maxfiy kaliti bilan shifrlangan shakllantirilgan biletni va mijozning maxfiy kaliti bilan shifrlangan biletdagi axborot qismi nusxasini mijozga qaytarib jo‘natadi;

- mijoz biletdagi axborotning ikkinchi qismini rasshifrovkalab, uni bilet bilan birga serverga jo‘natadi;

- server biletni rasshifrovkalab, uning tarkibini mijoz jo‘natgan axborot bilan taqqoslaydi. Mos kelishi mijoz va serverning o‘zaro muloqotning vakolatli abonentlari ekanligini tasdiqlaydi.

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

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

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

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

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

- *barmoq izlari bo‘yicha*. Barmoq izlarini skanerlash usuli har bir inson barmoqlarining kapilyar shakllarining noyobligiga asoslangan. Barmoq izi skanerlarining o‘lchami kichik, ular universal, arzon va keng qo‘llaniladi;

- *qo‘l kaftining biometrik shakli bo‘yicha*. Ushbu usul qo‘l panjasining shakliga asoslangan. Kaftni skanerlash vositalarining samaradorligi barmoq skanerlari samaradorligi bilan taqqoslana oladi;

- *ko‘z to‘rpardasi bo‘yicha*. Bunda ko‘z qorachig‘i orqali uning orqa devori qon tomirlariga yorug‘likning infraqizil nuri yo‘naltiriladi. Shu tariqa yoritilgan ko‘z tubi maxsus kamera yordamida skanerlanadi;

- *ko‘zning rangdor pardasi bo‘yicha*. Rangdor pardadagi dog‘ insonning eng noyob xarakteristikasi hisoblanadi. Usulning afzalligi shundaki, masofadan

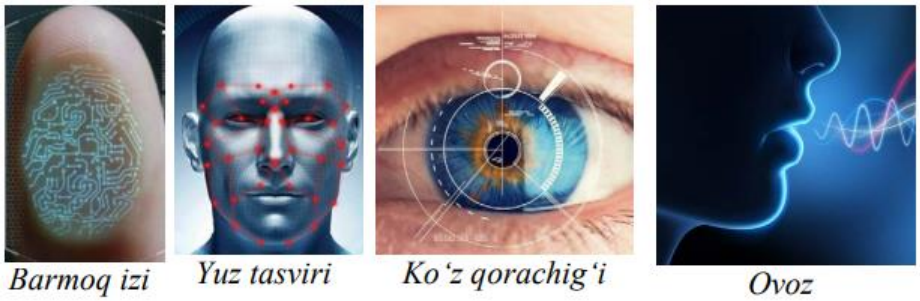
skanerlash mumkin. Bu skanerlarni kuzatuv kameralari bilan integrallashga imkon beradi;

- *yuzning shakli bo‘yicha*. Usul inson yuzining ko‘p o‘lchamli qiyofasini qurishga asoslangan;

- *qo‘lyozma dastxat bo‘yicha*. Usul imzoning yoki maxsus iboraning grafik identifikatsiyasiga asoslangan;

- *klaviatura dastxati bo‘yicha*. Usul, odatda, oldindan belgilangan matnni klaviuaturada terishning o‘ziga xos xususiyatlariga asoslangan;

- *ovoz bo‘yicha*. Usul inson nutqining chastotasi yoki statistik xarakteristikalari profiliga asoslangan. Afsuski, usul inson holatiga bog‘liq.



4.2-rasm. Biometrik namunalarga misol.

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

- *universal bo‘lishi* – biometrik parametrlar barcha foydalanuvchilarda bo‘lishi;

- *farqli bo‘lish*i – barcha insonlarning tanlangan biometrik parametri bir-biridan farqlanishi;

- *o‘zgarmaslik* – tanlangan biometrik parametr vaqt o‘tishi bilan o‘zgarmay qolishi;

- *to‘planuvchanlik* – fizik xususiyat osonlik bilan to‘planuvchan bo‘lishi. Amalda fizik xususiyatni to‘planuvchanligi, insonning autentifikatsiya jarayonga e’tibor berishiga ham bog‘liq bo‘ladi.

Biometrik tizimlarning eng ishonchligi – ko‘zning rangdor pardasi yoki ko‘z to‘rpardasi bo‘yicha skanerlash. Hozirda beshta barmoq skaneri va bir vaqtda

barmoq izi va ko‘zning rangdor pardasidan foydalanuvchi kombinatsiyalangan qurilmalar eng yuqori aniqlikni ta’minlaydi.

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

- biometrika faqat tirik organizmga mo‘ljallangan;

- ehtimollik xarakterga ega bo‘lganligi sababli, asboblarning ta’sirchanligini hisobga olish lozim;

- aksariyat vositalar atrof-muhitga hamda insonning yoshi va sog‘lig‘iga bog‘liq;

- hozirda barmoq izlari skanerlaridan tashqari barcha vositalar yetarlicha qimmat;

- davlat tomonidan total nazorat tahdidi xususida foydalanuvchilarda ishonchsizlikning mavjudligi.

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

- FAR (False Acceptance Rate) – foydalanishga yolg‘on ruxsatlar chastotasi;

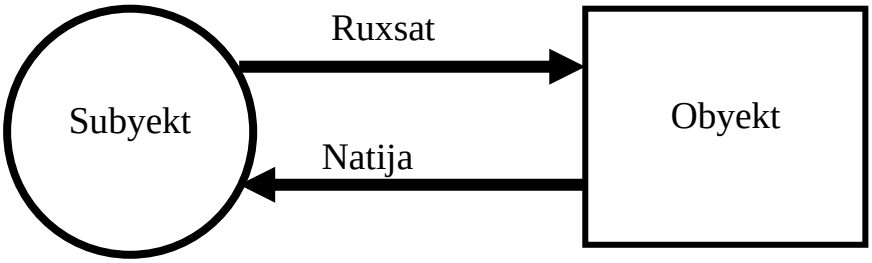
- FRR (False Rejection Rate) – foydalanishga yolg‘on inkorlar chastotasi.

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

4.2. Ma’lumotlardan foydalanishni mantiqiy boshqarish

Mantiqiy boshqaruv. Avtorizatsiya (inglizcha avtorizatsiya “ruxsat; avtorizatsiya”)foydalanishlarni nazoratlashning autentifikatsiyadan o‘tgan foydalanuvchilar harakatlarini cheklash qismi bo‘lib, aksariyat hollarda foydalanishni boshqarish modellari yordamida amalga oshiriladi.

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



4.3-rasm.Foydalanishni boshqarish sxemasi

Hozirda tizimlarda obyektlardan foydalanishni boshqarishning quyidagi usullari keng tarqalgan:

- foydalanishni diskretsion boshqarish usuli (*Discretionary access control, DAC*);

- foydalanishni mandatli boshqarish usuli (*Mandatory access control, MAC*);

- foydalanishni rollarga asoslangan boshqarish usuli (*Rolebased access control, RBAC*);

- foydalanishni atributlarga asoslangan boshqarish usuli (*Attribute-based access control, ABAC*).

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

Foydalanishni boshqarishning DAC usuli. Ixtiyoriy kirishni boshqarish (DAC) - ob'ekt egalari guruhi va/yoki sub'ektlar tomonidan aniqlangan kirish siyosati orqali ob'ektga kirishni ta'minlaydigan yoki cheklaydigan xavfsizlikka kirishni boshqarishning bir turi. DAC mexanizmi boshqaruvlari foydalanuvchi nomi va parol kabi autentifikatsiya paytida taqdim etilgan hisobga olish ma'lumotlari bilan foydalanuvchi identifikatsiyasi orqali aniqlanadi. DAClar ixtiyoriydir, chunki sub'ekt (egasi) autentifikatsiya qilingan ob'ektlarni yoki ma'lumotlarga kirishni boshqa foydalanuvchilarga o'tkazishi mumkin. Boshqacha qilib aytganda, egasi ob'ektga kirish huquqini belgilaydi.

DAC atributlariga quyidagilar kiradi:foydalanuvchi ob'ektga egalik huquqini boshqa foydalanuvchilarga o'tkazishi mumkin.

Foydalanuvchi boshqa foydalanuvchilarning kirish turini aniqlashi mumkin.

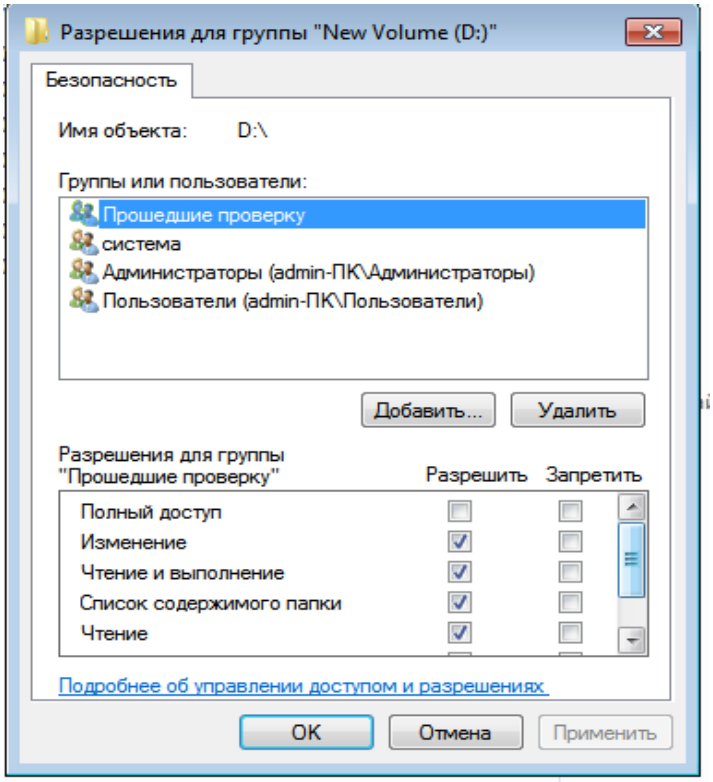
Bir nechta urinishlardan so'ng, avtorizatsiya xatosi foydalanuvchi kirishini cheklaydi.

Ruxsatsiz foydalanuvchilar fayl hajmi, fayl nomi va katalog yo'li kabi ob'ekt xususiyatlaridan ko'r.

Ob'ektga kirish kirishni boshqarish ro'yxati (ACL) avtorizatsiyasi paytida va foydalanuvchi identifikatsiyasi va/yoki guruh a'zoligiga asoslangan holda aniqlanadi.

DAC da subyektlar tomonidan obyektlarni boshqarish subyektlarning identifikatsiya axborotiga asoslanadi. Umumiy holda DAC usuli aksariyat operatsion tizimlarda foydalanishlarni boshqarishda foydalaniladi.

Masalan, 4.4-rasmda DAC usulini Windows 7 OTlarida foydalanish holati keltirilgan.



4.4-rasm. Windows 7 da DACdan foydalanish

Biroq, DACning jiddiy xavfsizlik muammosi - ma’lumotlardan foydalanish huquqiga ega bo‘lmagan subyektlar tomonidan foydalanilmasligi to‘liq kafolatlanmaganligi. Bu holat ma’lumotlardan foydalanish huquqiga ega bo‘lgan biror bir foydalanuvchining ma’lumot egasining ruxsatisiz foydalanish huquqiga ega bo‘lmagan foydalanuvchilarga yuborish imkoniyati mavjudligida namoyon bo‘ladi. Bundan tashqari, DACning yana bir kamchiligi tizimdagi barcha obyektlar ulardan foydalanishni belgilaydigan suyektlarga tegishli ekanligi.

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

Foydalanishni boshqarishning MAC usuli. MAC usuli bo‘yicha foydalanishni boshqarish xavfsizlik siyosati ma’muriga markazlashgan holda boshqarishni amalga oshirish imkoniyatini beradi.

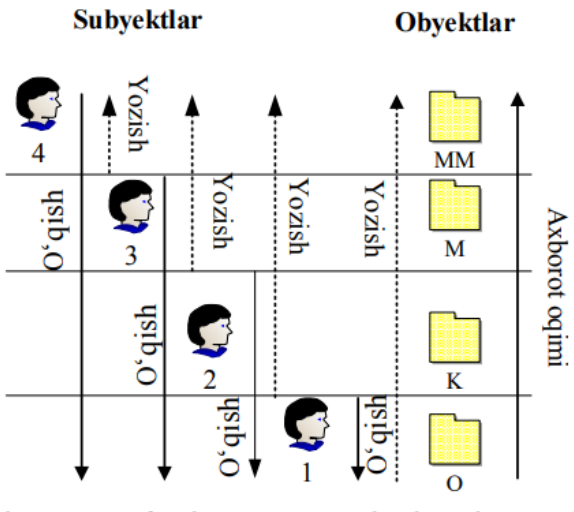
Foydalanishni boshqarishning MAC usuli xavfsizlik siyosati ma’muriga tashkilot bo‘ylab xavfsizlik siyosatini amalga oshirish imkoniyatini beradi. MAC usulida foydalanuvchilar tasodifan yoki atayin ushbu siyosatni bekor qilaolmaydilar.

MAC usulida foydalanishni boshqarish subyektlar va obyektlarni tasniflashga asoslanadi. Tizimning har bir subyekti va obyekti bir nechta xavfsizlik darajasiga ega bo‘ladi. Oddiy holda xavfsizlik darajasi uchun: “*mutlaqo maxfiy*” (MM), “maxfiy” (M), “*konfidensial*” (K) va “*ochiq*” (O) belgilar tayinlanadi. Bu yerda, MM>M>K>O.

MAC asosida axborot maxfiyligini taminlash. Agar obyekt va subyektning xavfsizlik darajalari orasidagi bir qancha bog‘liqlik shartlari bajarilsa, u holda subyekt obyektdan foydalanish huquqiga ega bo‘ladi. (4.5-rasm):

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

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



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

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

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

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

- agar subyektning xavfsizlik darajasi obyektning xavfsizlik darajasiga teng bo‘lsa, yozishga ruxsat beriladi;

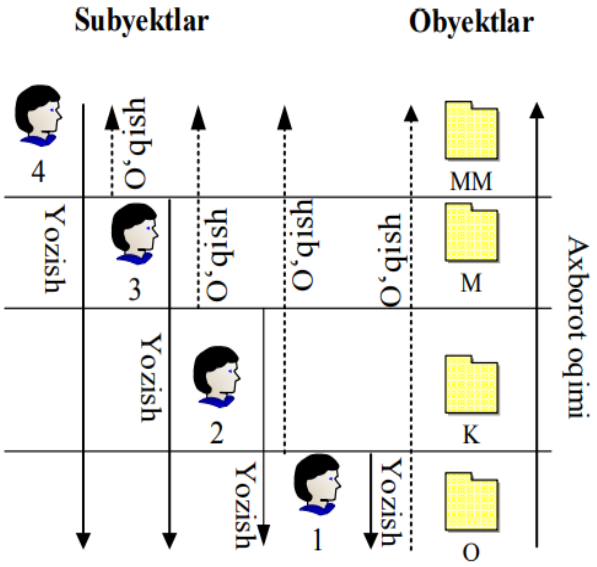
2. Sxemadan ko‘rinib turibdiki, yuqori darajali ishonchga ega foydalanuvchilar xavfsizlik darajasi past bo‘lgan obyektlarni o‘zgartira olmaydi. Ushbu muammoni bartaraf etishda foydalanuvchi turli hujjatlardan foydalanish uchun turli darajadagi ishonchga ega bo‘lgan subyektlar nomidan ish ko‘rishi mumkin.

Axborot ishonchligini taminlash. Axborot konfidensialligini taminlashdan tashqari, ba’zida axborot ishonchligini taminlash ham talab etiladi. Ya’ni, obyektning ishonchlik darajasi qanchalik yuqori bo‘lsa, subyektning ishonchligi ham shunchalik yuqori va subyektning xavfsizlik darajasi qanchalik yuqori bo‘lsa, u tizimga shuncha ishonchli ma’lumotlarni kiritishi mumkin.(4.6-rasm)

Foydalanishni boshqarishning RBAC usuli. Rolga asoslangan kirishni boshqarish (RBAC) tashkilot ichidagi shaxsning roliga qarab tarmoqqa kirishni cheklaydi va kirishni ilg'or boshqarishning asosiy usullaridan biriga aylandi. RBACdagi rollar xodimlarning tarmoqqa kirish darajasiga ishora qiladi.

Xodimlarga faqat o'z mehnat vazifalarini samarali bajarish uchun zarur bo'lgan ma'lumotlardan foydalanishga ruxsat beriladi. Kirish vakolat, mas'uliyat va ish malakasi kabi bir qancha omillarga asoslanishi mumkin. Bundan tashqari, kompyuter resurslariga kirish faylni ko'rish, yaratish yoki o'zgartirish kabi muayyan vazifalar bilan cheklanishi mumkin.

Natijada, quyi darajadagi xodimlar, agar ular o'z majburiyatlarini bajarish uchun kerak bo'lmasa, odatda maxfiy ma'lumotlarga kirish imkoniga ega emaslar. Bu, ayniqsa, agar sizda ko'plab xodimlar bo'lsa va tarmoqqa kirishni diqqat bilan kuzatishni qiyinlashtiradigan uchinchi tomonlar va pudratchilardan foydalansangiz foydali bo'ladi. RBAC-dan foydalanish kompaniyangizning maxfiy ma'lumotlari va muhim ilovalarini himoya qilishga yordam beradi.



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

Umuman olganda, foydalanuvchi turli vaziyatlarda turli rollarni bajarishi mumkin. Xuddi shu rolni ba’zida bir nechta foydalanuvchilar bir vaqtning o‘zida ishlatishlari mumkin.

RBAC usulining asosiy afzalliklari quyidagilar:

1. *Ma’murlashning osonligi*. RBAC yordamida siz xodim ishga qabul qilinganda yoki uning rolini o'zgartirganda qog'oz va parolni o'zgartirishga bo'lgan ehtiyojni kamaytirishingiz mumkin. Buning o'rniga, siz rollarni tezda qo'shish va almashtirish uchun RBAC dan foydalanishingiz mumkin va ularni operatsion tizimlar, platformalar va ilovalarda global miqyosda amalga oshirishingiz mumkin. Bundan tashqari, foydalanuvchi ruxsatlarini tayinlashda xatolik ehtimolini kamaytiradi. Ma'muriy vazifalarga sarflangan vaqtni qisqartirish RBACning bir nechta iqtisodiy afzalliklaridan biridir. RBAC shuningdek,

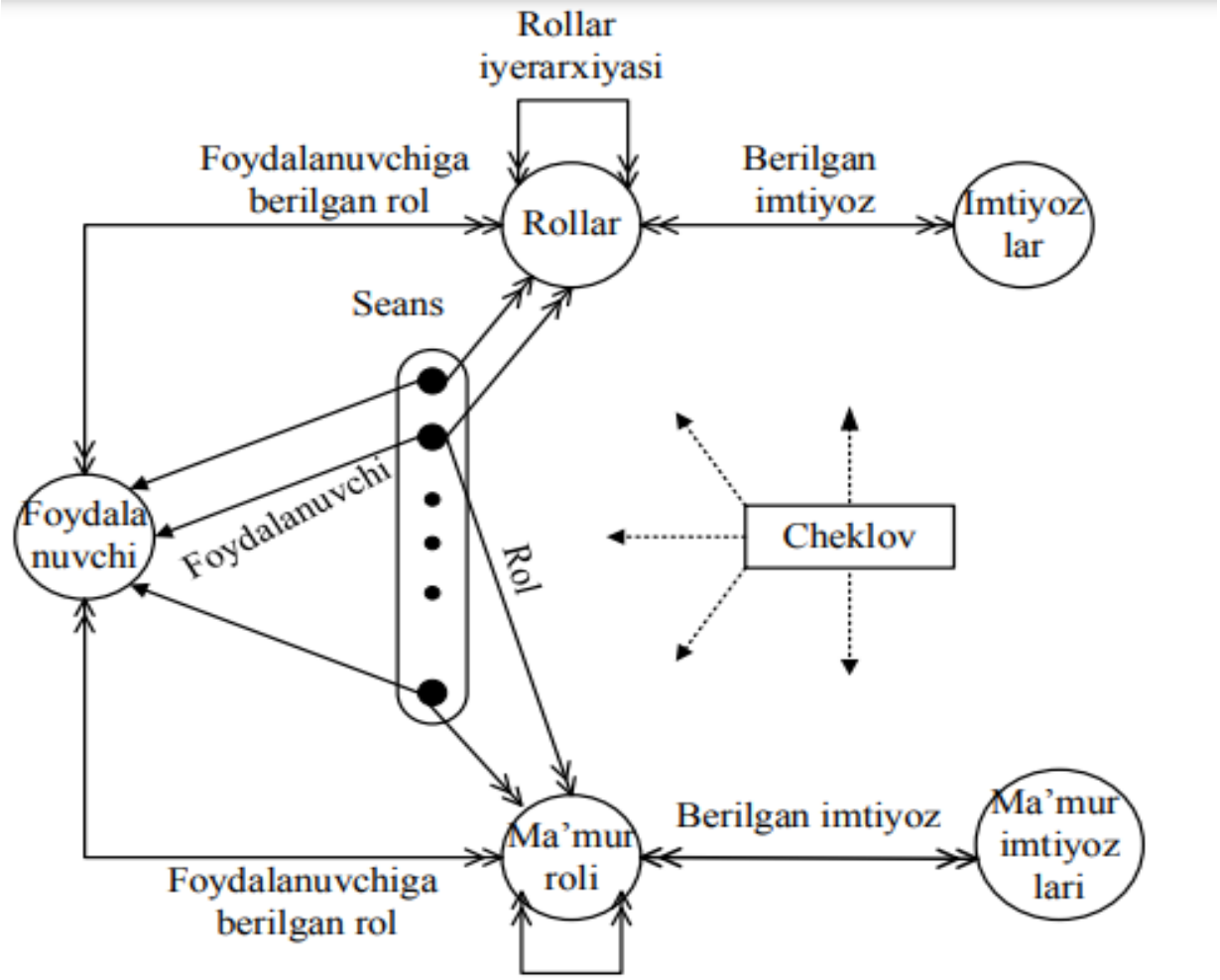
uchinchi tomon foydalanuvchilariga oldindan belgilangan rollarni berib, ularni tarmog'ingizga osonroq integratsiyalashga yordam beradi

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.

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.

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

Rasman RBAC modelini quyidagicha tasvirlash mumkin (4.7-rasm)



Foydalanishni boshqarishning ABAC usuli. ABAC (Atributga asoslangan kirishni boshqarish) an'anaviy RBAC (rolga asoslangan kirishni boshqarish) metodologiyasining evolyutsiyasidir. Bu batafsilroq yondashuv uchun qo'shimcha atributlardan foydalanishga imkon beradi. Foydalanuvchi, atrof-muhit va manba atributlaridan foydalanish imkoniyati endi SaaS korxonalariga yanada murakkab foydalanish holatlarini hal qilish imkonini beradi. Ushbu model so‘rovni, resursni va harakatni kim bajarayotgani to‘g‘risidagi holatlar “AGAR (*IF*), U HOLDA (*THEN*)” dan tashkil topgan qoidalarga asoslanadi. Masalan, AGAR talabgor boshqaruvchi bo‘lsa, U HOLDA (THEN) 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.

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

XACML standartida quyidagi asosiy tushunchalar mavjud: qoidalar (*rules*), siyosat (*policy*), qoidalar va siyosatni mujassamlashtirgan algoritmlar (*rule-combing algorithms*), atributlar (*attributes*) (*subyekt, obyekt, harakat va muhit shartlari*), majburiyatlar (*obligations*) va maslahatlar (*advices*). Qoida markaziy element bo‘lib, maqsad, ta’sir, shart, majburiyat va maslahatlarni o‘z ichiga oladi. Maqsad – subyektning obyekt ustida qanday harakatlarni amalga oshirishi (o‘qish, yozish, o‘chirish va h.). Ta’sir mantiqiy ifodalarga asoslangan va tizimdan foydalanish uchun ruxsat, taqiq, mumkin emas, aniqlanmagan holatlaridan biriga asoslangan ruxsatni berishi mumkin. Mumkin emas buyrug‘ining mantiqiy shart noto‘g‘ri bo‘lganida qaytarilishi, ifodani hisoblash vaqtida yuzaga kelgan xatoliklar uchun aniqlanmagan ta’sirning mavjudligini ko‘rsatadi. Quyida ABAC usuliga misol keltirilgan.

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

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

Foydalanishni boshqarish matritsasi. Avtorizatsiyaning klassik ko‘rinishi Lampsonning foydalanishni boshqarish matritsasidan boshlanadi. Ushbu matrisa operatsion tizimni barcha foydalanuvchilar uchun turli ma’lumotlarni boshqarishi xususidagi qarorni qabul qilishida zarur bo‘lgan barcha axborotni o‘z ichiga oladi. Bunda, operatsion tizimdagi foydalanuvchilar subyekt sifatida va tizim resurslari obyekt sifatida qaraladi. 4.1-jadvalda foydalanishni boshqarish matrisasi keltirilgan, unda imtiyozlar UNIX operatsion tizimidagi imtiyozlar shaklida, ya’ni, x, r va w lar mos ravishda bajarish, o‘qish va yozish amalini anglatadi.

Keltirilgan jadvalda buxgalteriyaga oid dastur ham subyekt ham obyekt sifatida olingan. Bu foydali tanlov bo‘lib, buxgalteriyaga oid ma’lumotlarni faqat buxgalteriyaga oid dastur tomonidan foydalanish imkonini beradi. Ya’ni, turli buxgalteriya tekshiruvlari va balans haqidagi ma’lumotlar faqat buxgalteriyaga oid dasturiy ta’minot tomonidan foydalanilishi shart va yuqoridagi matrisada eltirilgan shakl buni ta’minlaydi.

4.1-jadval

Foydalanishni boshqarish matrisasi

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

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

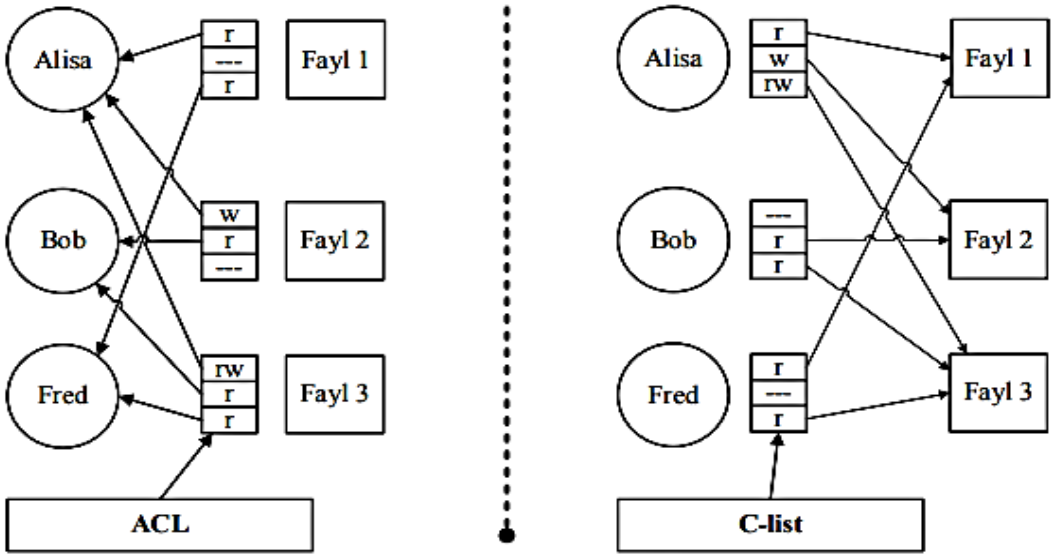
Avtorizatsiya amallarini maqbul amalga oshirish uchun, foydalanishni boshqarish matritsasi boshqariluvchi qismlarga bo'linishi shart. Foydalanishni boshqarish matritsasini qismlarga ajratishning ikkita usuli mavjud. Birinchi usulga binoan matritsa ustunlar bo'yicha bo'linadi va har bir ustun mos obyekt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

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

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

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

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



4.8-rasm. ACL va C-list

4.8-rasmdagi ko‘rsatkichlar qarama-qarshi yo‘nalishlardaligini, ya’ni, ACL uchun ko‘rsatkichlar resurslardan foydalanuvchilarga qarab yo‘nalgan bo‘lsa, C-list uchun esa ko‘rsatkichlar foydalanuvchilardan resurslarga qarab yo‘nalganligini ko‘rish mumkin. Bu ahamiyatsiz ko‘ringan farq imtiyozlar ro‘yxati (C-list) bilan foydalanuvchilar va fayllar orasidagi aloqadorlik tizim ichida qurilishini anglatadi. ACLga 108 asoslangan tizimda esa, foydalanuvchilarni fayllarga aloqadorligi uchun alohida usullar talab etilgani bois, C-list ACL ga nisbatan xavfsizlik nuqtai nazaridan, bir qancha afzalliklarga ega va shuning uchun C-list ustida kam sonli ilmiy tadqiqot ishlari olib borilgan.

4.3. Ko‘p sathli xavfsizlik modellari

Ko‘p sathli xavfsizlik modellari. Xavfsiz tizimning asosiy talabi sub'ektlarning muayyan ob'ektlarga kirish huquqini belgilaydigan ko'rsatmalar to'plamining mavjudligidir. “Kirish” asosiy tushunchadir; u sub'ektdan ob'ektga yoki ob'ektdan sub'ektga axborot oqimini nazarda tutadi. Masalan, foydalanuvchi

(sub'ekt) ma'lumotlar to'plamini (ob'ektni) yangilaganda, axborot sub'ektdan ob'ektga oqib chiqadi. Foydalanuvchi ma'lumotlar to'plamidan yozuvni o'qiganda, ma'lumot ob'ektdan sub'ektga oqadi.

Ushbu o'zaro ta'sirlarda sub'ekt faoldir; sub'ekt ob'ektga (yoki ob'ekt tarkibidagi ma'lumotlarga) kirishga harakat qilmoqda. Ob'ekt esa passivdir; unda sub'ekt kirishni istagan ma'lumotlar mavjud yoki u sub'ektdan ma'lumot oluvchi hisoblanadi. Har safar sub'ekt ob'ektga kirishga harakat qilganda, tizim kirishga ruxsat berish yoki yo'qligini hal qilishi kerak.

Xavfsizlikning ikkita markaziy tushunchasi xavfsizlik siyosati va javobgarlikdir. Xavfsizlik siyosati - bu tashkilot o'zining maxfiy ma'lumotlarini qanday boshqarishi, himoya qilishi va tarqatilishini tartibga soluvchi qonunlar, qoidalar va amaliyotlar to'plami. Bu tizim ma'lum bir sub'ektning ma'lum bir ob'ektga kira olishini hal qilish uchun foydalanadigan qoidalar to'plamidir. Hisobdorlik xavfsizlik bilan bog'liq har bir hodisa mavzu bilan bog'lanishini talab qiladi. Javobgarlik har bir harakatni harakatga sababchi bo'lgan foydalanuvchiga kuzatish mumkinligini ta'minlaydi.

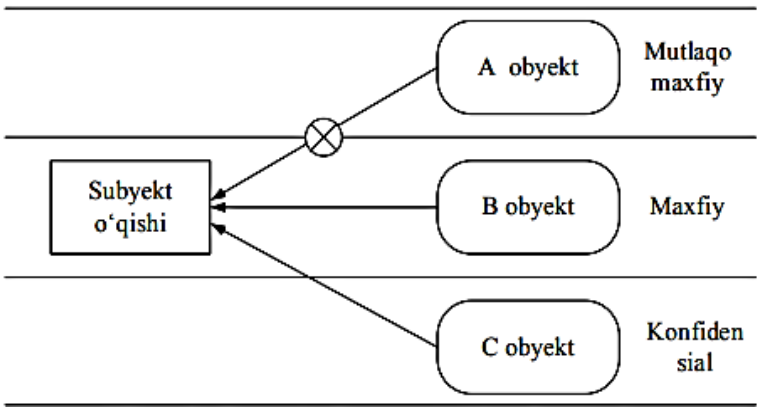
Ko'p darajali xavfsizlik - ierarxik bo'lmagan xavfsizlik toifalari tizimi bilan birlashtirilgan ierarxik xavfsizlik darajalari tizimi asosida ma'lumotlar va foydalanuvchilarni tasniflash imkonini beruvchi xavfsizlik siyosati. Ko'p darajali xavfsiz xavfsizlik siyosati ikkita asosiy maqsadga ega. Birinchidan, nazorat vositalari ruxsatsiz shaxslarning ruxsat etilganidan yuqoriroq tasnifdagi ma'lumotlarga kirishiga yo'l qo'ymasliklari kerak. Ikkinchidan, nazorat vositalari shaxslarning ma'lumotlarning maxfiyligini ochishga yo'l qo'ymasliklari kerak.

Bell-LaPadul modeli. Bell-Lapadula modeli axborot resurslariga kirishni boshqarish va nazorat qilish algoritmi bo‘lib, u mandat usuliga asoslangan. 1975 yilda MITER xodimlari Devid Bell va Leonard Lapadula tomonidan yaratilgan. Bell-Lapadula huquqlarni taqsimlash paradigmasi bir qator aniqlangan holatlarga ega. Ular foydalanuvchilarning harakatlariga qarab avtomatlashtirilgan ISga tayinlanadi.

Axborot tizimi barcha komponentlarni ob'ektlar va sub'ektlarga ajratadi. Har qanday AIS mavzusiga ma'lum bir kirish darajasi beriladi. Unda saqlanadigan ma'lumotlarning maxfiyligi toifasiga mos keladi. Tizimning har bir axborot resursi (obyekti) kompaniyaning axborot xavfsizligi siyosatiga mos keladigan maxfiylik darajasini oladi.

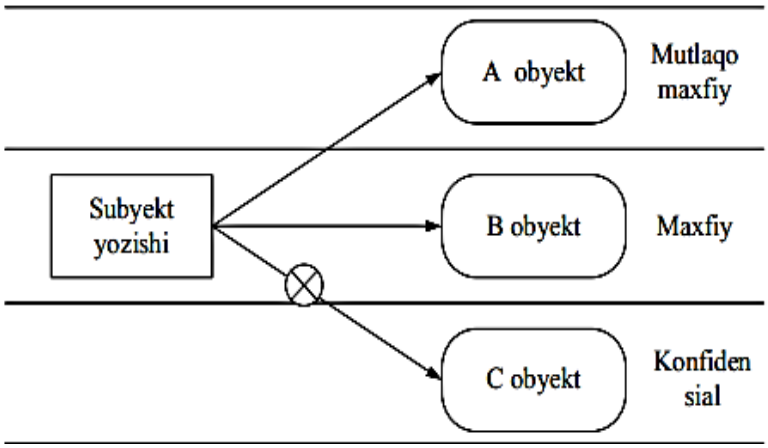
Bell-LaPadul modelida tizimdagi subyektlar va obyektlar maxfiylik grifi bo‘yicha taqsimlanadi va quyidagi mualliflik qoidalari bajariladi:

1. “Xavfsizlikning oddiy qoidasi” (Simple Security). Ushbu qoidaga binoan subyekt faqat xavfsizlik sathi o‘zining xavfsizlik sathidan yuqori bo‘lmagan hujjatlardan axborotni o‘qishga haqli. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.9–rasmda keltirilgan.



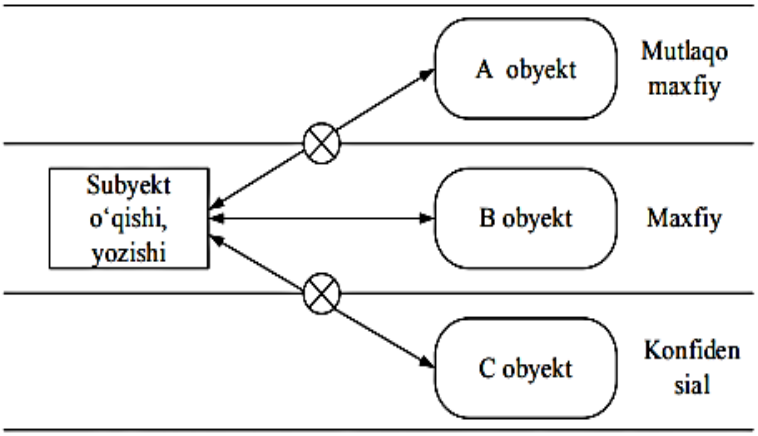
4.10-rasm. “Simple Security” xususiyati uchun axborot oqimlari sxemasi

2. “-Xususiyat” (-Property). Ushbu qoidaga binoan subyekt xavfsizlik sathi o‘zining xavfsizlik sathidan past bo‘lmagan hujjatlarga axborot kiritishi mumkin. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.10–rasmda keltirilgan.



4.10-rasm. "Property" xususiyati uchun axborot oqimlari sxemasi

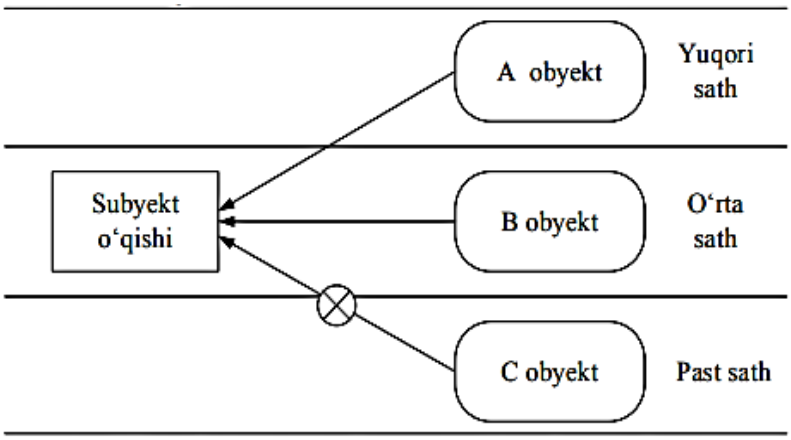
3. "-Qat'iy xususiyat" (-Strong Property). Ushbu qoidaga binoan o'qish va yozish xuquqiga ega subyekt faqat o'zining sathidagi 111 obyektlar bilan amallar bajarishi mumkin. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.12–rasmda keltirilgan.



4.11-rasm. "Strong-property" xususiyati uchun axborot oqimlari sxemasi

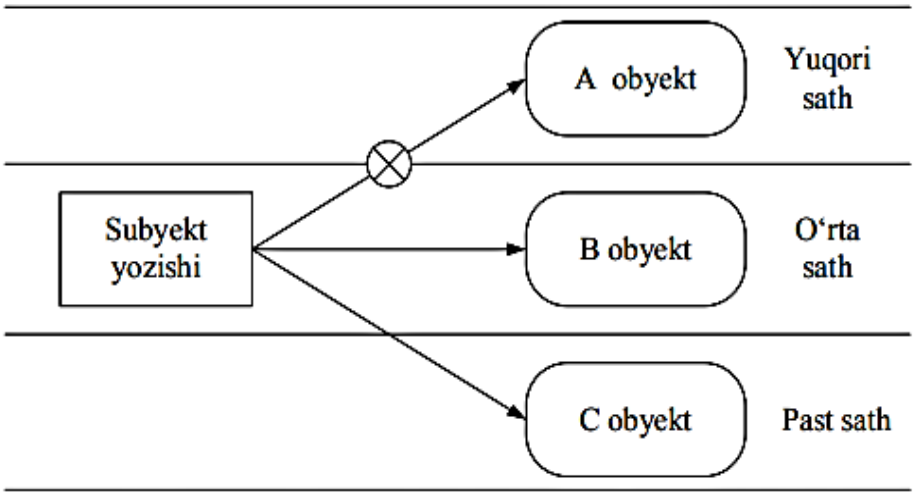
Biba modeli. Ushbu model Bell-LaPadul modelining modifikatsiyasi bo'lib, ma'lumotlar yaxlitligini taminlashga yo'naltirilgan. Biba modelining bazaviy qoidalari quyidagicha ifodalanadi:

1. "Yaxlitlikning oddiy qoidasi" (Simple Integrity, SI). Ushbu qoidaga binoan subyekt o'zining sathidan past yaxlitlik sathidan axborotni o'qiy olmaydi. Yaxlitlikning uchta sathiga ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 4.12–rasmda keltirilgan.



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

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



4.13-rasm.”Property” xususiyati uchun axborot oqimlari sxemasi

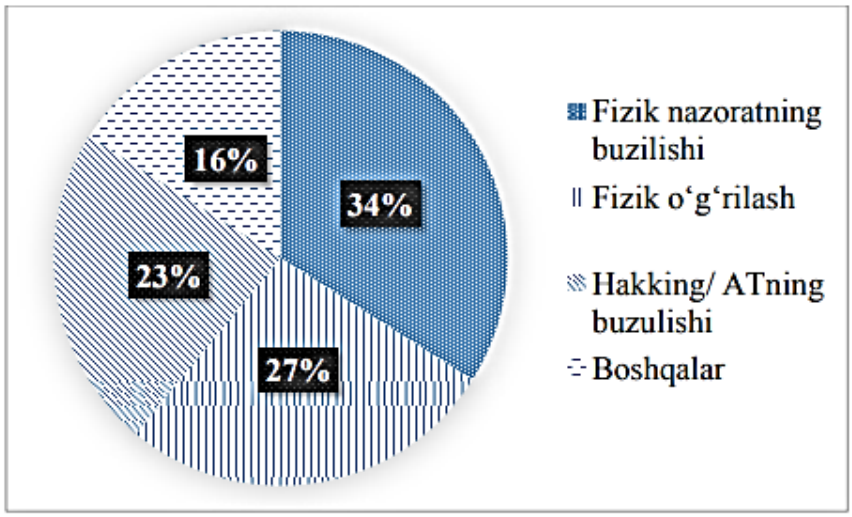
3. “Chaqiruv xususiyati” (Invocation Property). Ushbu qoidaga binoan subyekt yaxlitlikning yuqori sathidagi subyektdan servisni so‘ray olmaydi.

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

4.3. **Ma’lumotlarni fizik himoyalash**

*Ma’lumotlarni fizik himoyalash: a*xborot xavfsizligini taminlashda amalga oshiriladigan dastlabki choralardan biri – fizik xavfsizlik. Ruxsatsiz fizik boshqaruvni, shaxslar amalga oshiradigan va muhitga bog‘liq tahdidlarni oldini olish uchun tashkilotlar mos fizik xavfsizlik boshqaruvi sharoitida bo‘lishi shart.

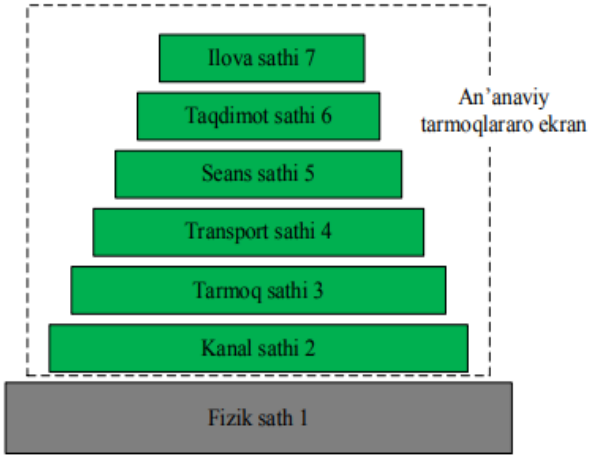
Fizik xavfsizlikning zaruriyati. Kiberxujumlarning murakkablashuvi hujumchilarning tashkilot fizik xavfsizligini buzishda turli usullardan foydalanishlariga sabab bo‘lmoqda. AQShning Department of Health and Human Services Breach Portal tashkiloti tadqiqotlari 2015 yilda tashkilotlarda eng ko‘p uchraydigan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



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

Fizik xavfsizlikning buzilishi boshqa xavfsizliklarni buzilishlaridan keskin farq qilib, juda ham kam hollarda texnik ma’lumotisiz amalga oshirilishi mumkin.

Masalan, tarmoqlararo ekran OSI modelining turli sathlarida himoyani tashkil etadi. Biroq, tashkilotning fizik xavfsizligiga ta’sir eta olmaydi (4.16-rasm).



4.15-rasm. Tarmoq sathlarida tarmoqlararo ekranlardan foydalanish

Fizik xavfsizlik OSI modelining fizik sathida himoyani ta'minlaydi. Fizik sath texnik vositalariga quyidagilar kiradi:

- ✓ Kabel (koaksiyal , o'ralgan juftlik , optik tolali , simsiz media)
- ✓ Ulagich (masalan: 8P8C)
- ✓ Yamoq paneli
- ✓ Plintus
- ✓ Signal takrorlagichi
- ✓ Ko'p portli takrorlagichlar yoki markazlar
- ✓ Media konvertorlari yoki media konvertorlari (transceiver)
- ✓ MAU (Media kirish birligi)
- ✓ Tarmoq adapteri (NIC) - u ma'lumotlar uzatish qatlamida ham ishtirok etadi
- ✓ PHY

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.

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.

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

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

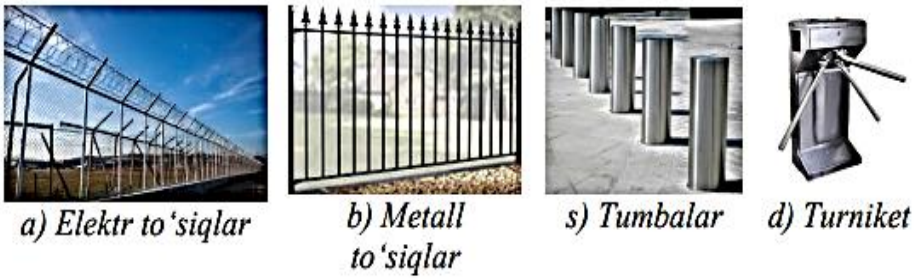
Terrorizm. Tashkilot yaqinidagi yoki uning ichidagi terrorchilik harakatlari, masalan, mashinaga qo‘yilgan, shaxslarda mavjud bo‘lgan yoki masofadan turib boshqariluvchi bomba portlashi natijasida tashkilot fizik xavfsizligiga turlicha zarar yetkazilishi mumkin.

Ijtimoiy injineriya. Ijtimoiy injineriyaga shaxsiy axborotni boshqa shaxslar tomonidan noqonuniy qo‘lga kiritish maqsadida qilgan harakatlari sifatida qaraladi.

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

Fizik xavfsizlikni nazoratlash. Biror fizik xavfsizlikni mos xavfsizlik nazoratisiz, amalga oshirish qiyin.

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



4.17-rasm. To’siqlarga misollar

Fizik to‘siqlarni amalga oshirishdan asosiy maqsad:

— hujumchini blokirovkalash va ushlab qolish;

— tashkilot chegarasini belgilash;

— xavfsiz hududni tashqi hujumlardan himoyalash;

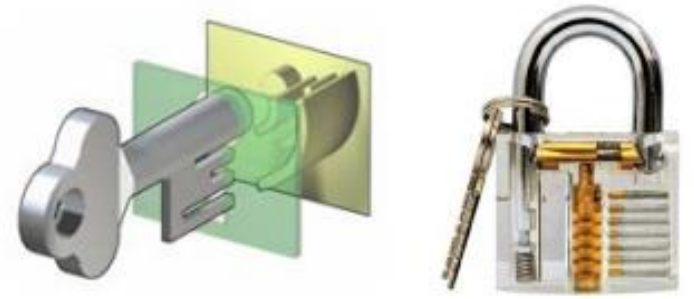
— transportlarni kirishidan himoyalash;

— qo‘poruvchilik hujumlaridan himoyalash.

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

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

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



4.18-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.

Fizik xavfsizlikni nazoratlash: Yashirin qurol/kontrabanda qurilmalarini aniqlash moslamasi. Tashkilotlarda odatda shaxslar tomonidan olib kiriladigan jixozlar yoki vositalar maxsus skanerlar yordamida turli qurollar yoki kontrabanda vositalarini, bombalar, yoki o‘q otar qurilmalari aniqlanadi. Mazkur skanerlarga misol tariqasida, metallni aniqlovchilar, X-ray aniqlash tizimlari va harakat bo‘ylab metallni aniqlash tizimlarini keltirish mumkin. *4.19-rasm. X-Ray metall detektori*

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

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

4.21-rasm. Ogohlantiruvchi belgilar

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

4.22-rasm. Kuzatuv kameralari

Har bir tashkilot samarali fizik xavfsizlikni amalga oshirish uchun talab qilingan fizik xavfsizlik siyosatini va muolajalarini amalga oshirishi zarur. Xususan, tashkilot fizik xavfsizligining siyosati o‘zida quyidagilarni mujassamlashtiradi:

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

Fizik xavfsizlik muolajalari o‘z ichiga quyidagilarni oladi:

- qulflash tizimini boshqarish;

- suqilib kirish insidentlarini qaydlash;

- tashrif buyuruvchilarni boshqarish;

- konfidensial materiallarni yo‘q qilish;

- qog‘ozdagi axborot uchun toza stol siyosatini va axborotni ishlashda toza ekran siyosatini amalga oshirish.

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

- server va zaxira nusxalash qurilmalarini alohida xonada saqlash. Bu chora ushbu qurilmalarning noma’lum shaxslar yoki xodimlar tomonidan ruxsatsiz boshqarilishini cheklaydi;

- server va zaxira nusxalash vositalari joylashgan xonaga yoki muhitga kuzatuv kameralarini va smart karta yoki biometrik parametrlarga asoslangan autentifikatsiyani joriy etish;

- serverlarni, o‘g‘irlinishidan va zararlanishidan himoyalash uchun, maxsus tagliklarga o‘rnatish;

- turli energiya o‘zgarishidan himoyalash uchun serverlarni zaxira UPS vositasiga ulash;

- qurilmalarni qulflanuvchi xonalarda saqlash;

- xodimlar tomonidan ruxsatsiz zaxira nusxalamasligini va server vositalarini olib chiqib ketilmasligini taminlash.

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

harakatlanganligi sababli, tashkilot tarmoq kabellarining joylashuvi va ularning xavfsizligiga ham jiddiy e’tibor berish lozim.

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

- hujumlarni kamaytiruvchi usullarni taminlashni;

- maxfiy axborotni olib yurishdagi risklarni;

- xavfsizlik xodimlarining muhimligini;

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

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

- sinf mashg‘ulotlari–ma’ruzaga asoslangan interaktiv sinf mashg‘ulotlarining afzalligi:

barcha noravshan va noaniq masalalar shu joyning o‘zida aniqlanadi;

webga asoslangan yoki uchrashuvga asoslangan o‘qitish sessiyalarini amalga oshiradi;

rol o‘ynash yoki simulyatsiya o‘yinlari orqali yanada interaktiv bo‘lishi mumkin.

- Aylana stol mashg‘ulotlari - mazkur kurslar odatda oylik yoki xaftalik bo‘lib, fizik xavfsizlik zarur bo‘lganda tashkilot xodimlarini o‘qitish uchun amalga oshiriladi.

- Xavfsizlik haqida xabardor qiluvchi web sayt – xavfsizlik haqida xabardor qiluvchi web saytni yaratish orqali xodimlar o‘zlariga biriktirilgan vazifalarni chuqurroq o‘rganadilar. Bunda turli rasm, video va misollar asosida mavjud holat tushuntiriladi.

- Master klass darslari – parolni almashtirish yoki parolni bilmasdan uni olib tashlash master klass darslarida amalga oshiriladi.

Nazorat savollari

1. Ruxsatlarni nazoratlashning asosiy tushunchalari.

2. Foydalanuvchilarni autentifikatsiyalash usullari va ularning o‘ziga xos xususiyatlari nimadan iborat?

3. Parolga asoslangan autentifikatsiya usuli, uning afzallik va kamchiliklari.

4. Parollar ma’lumotlar bazasida qanday saqlanadi va ularni taqqoslash usullari.

5. Axborotning fizik himoyasi va uning muhimligini tushuntiring.

6. Axborotni fizik xavfsizligiga ta’sir qiluvchi tabiiy va sun’iy omillar.

7. Yong‘inga qarshi himoyalash usullari.

8. Tashkilotda qo‘riqlash xodimlari va kuzutuv kameralarining o‘rni.

9. Foydalanishni mantiqiy boshqarish deganda nimani tushunasiz?

10. Foydalanishni boshqarishning DAC usuli va uning xususiyatlari.

11. Foydalanishni boshqarishning MAC usuli va uning asosiy xususiyatlari.

12. Foydalanishni boshqarishning RBAC usuli va uning asosiy xususiyatlari.

13. Foydalanishni boshqarishning ABAC usuli va uning asosiy xususiyatlari.

14. Foydalanishni boshqarish matritsasi, ACL va C-list tushunchalarini tushuntiring.

15. Bell-LaPadul modeli va uning asosiy maqsadi.

16. Biba modeli va uning asosiy maqsadi.

5 BOB. TARMOQ XAVFSIZLIGI

5.1. Kompyuter tarmoqlarining asosiy tushunchalari

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

Mos tarmoq servislaridan foydalanish orqali turli xil tarmoq resurslarini taqdim etish vazifasi yuklatilgan tarmoq kompyuteri server deb ataladi. Tarmoq resurslaridan va turli tarmoq servislaridan foydalanish maqsadida serverga so‘rov yuboruvchi tarmoq qurilmalari mijozlar deb ataladi.

Avtonom ishlovchi yoki mijoz sifatida tarmoqqa ulangan kompyuterni, odatda, ishchi stansiyasi deb atashadi. Kompyuter tarmoqlarini quyidagicha tasniflash mumkin:

− xududiy alomat bo‘yicha;

− ma’murlash usuli bo‘yicha;

− topologiya bo‘yicha.

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

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

Global hisoblash tarmog‘i katta geografik muhitni qamrab olgan va tarkibida aloqaning magistral liniyalari yordamida birlashtirilgan ko‘plab hisoblash tarmoqlari va masofadagi kompyuterlar bo‘lgan hududiy taqsimlangan tizimdan iborat. Megapolis va region doirasida tashkil etilgan tarmoqlar mos holda shahar tarmog‘i (MAN, Metropolitan Area Network) va regional tarmoq (PAN, Personal Area Network) deb yuritiladi. Eng mashhur global tarmoq Internet TCP/IP

protokollari steki bazasiga asoslangan megatarmoq hisoblanadi. Ba’zi adabiyotlarda “korporativ tarmoq” iborasi ishlatiladi. Bu ibora orqali turli texnik, dasturiy va informatsion prinsiplarda qurilgan bir necha tarmoqlarning birlashmasi tushuniladi.

Megatarmoq Internet foydalanuvchilarini birlashtirish uchun ishlatiluvchi global tarmoq Ekstranet (extranet) deb yuritiladi. TCP/IP protokoli bazasida amalga oshirilgan, ammo megatarmoq Internetdan ajratilgan tarmoq Intranet (Intranet) deb ataladi.

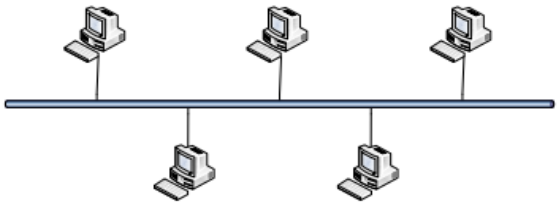
Ma’murlash usuli bo‘yicha tarmoqlar “bir rutbali (одноранговый)” va “mijoz serverli” turlariga bo‘linadi. Bir rutbali tarmoqlarda barcha kompyuterlar ham mijoz, ham server bo‘lishi mumkin. UNIX tarmoqlari bunga misol bo‘ladi.

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

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

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

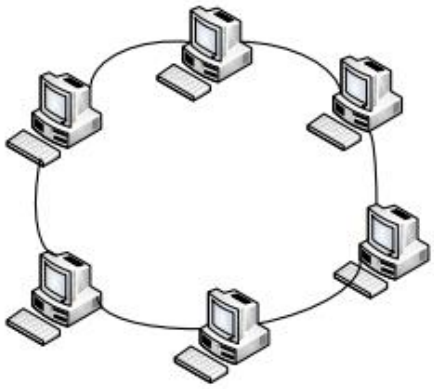
Tarmoq topologiyasi bo‘yicha umumiy shinali (bus), xalqasimon (ring), yulduzsimon (star), uyali (mesh) va aralash topologiyali tarmoqlar farqlarnadi. “Umumiy shina” topologiyasi bitta chiziq bo‘yicha yotqizilgan tarmoqdan iborat. Kabel bitta kompyuterdan keyingi kompyuterga, so‘ngra undan keyingisiga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



5.1rasm. ”Umumiy shina” topologiyasi

Shinaning har bir uchida terminator (signalning akslanishini istisno qiluvchi) bo‘lishi lozim. Shinaning bir uchi yerga ulanishi kerak. Shinali topologiya “passiv” hisoblanadi, chunki kompyuterlar signallarni regenerasiyalamaydi. Signal so‘nishi muammosini hal etishda tarkorlagichlardan foydalaniladi. Shinaning uzilishi butun tarmoq ishlashining buzilishiga sabab bo‘ladi (signalning akslanishi hisobiga). Tizimning fizik sathida axborotning sust himoyalanganligini aytish lozim. Chunki, bir kompyuterning ikkinchi kompyuterga yuborgan xabari boshqa ixtiyoriy kompyuterda qabul qilinishi mumkin.

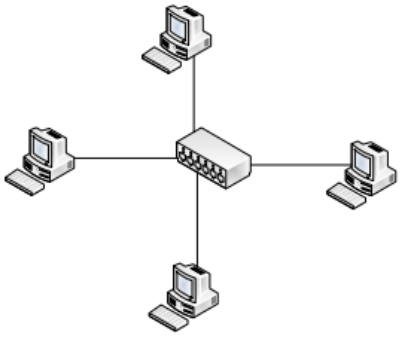
“Xalqasimon” topologiyada har bir kompyuter boshqa ikkita kompyuter bilan ulangan va signal aylana bo‘yicha o‘tadi (5.2-rasm).



5.2-rasm. “Xalqasimon” topologiya

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

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



5.3-rasm. “Yulduzsimon” topologiya

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

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

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

Tarmoqqa qo‘yiladigan talablar:

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

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

− *samaradorlik* – kam sarf-xarajat evaziga foydalanuvchilarga xizmat qilishning talab etiladigan sifatini taminlash.

Tarmoq – turli uskunalarning birlashmasi, demak ularni birgalikda ishlatish muammosi jiddiy muammolardan hisoblanadi. Ishlab chiqaruvchilarning uskuna qurilishidagi umumiy qoidalarga rioya qilmaslaridan turli tarmoqlarni qurishda

taraqqiyotga erishish mumkin emas. Shu sababli kompyuter sohasidagi yuksalishlar standartlarda akslanadi. Boshqacha aytganda, har qanday texnologiya, uning mazmuni standartlarda o‘z aksini topganidagina “qonuniy” himoyaga ega bo‘ladi.

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

Jo’natuvchi	**Qabul qiluvchi**
7.Tatbiqiy sath	7. Tatbiqiy sath
6.Taqdimiy sath	6.Taqdimiy sath
5.Seans sathi	5.Seans sathi
4.Transport sathi	4.Transport sathi
3.Tarmoq sathi	3.Tarmoq sathi
2.Kanal sathi	2.Kanal sathi
1. Fizik sathi	1. Fizik sathi

5.4-rasm. Axborotning OSI modeli bo’yicha abonentdan abonentga o’tish yo’li

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

Faraz qilaylik, ilova so‘rov bilan tatbiqiy sathga, masalan, fayl xizmatiga murojaat etsin. Ushbu so‘rovga binoan tatbiqiy sathning dasturiy ta’minoti

axborotning standart formatini shakllantiradi. Oddiy axborot sarlavxa va ma’lumotlar hoshiyasidan iborat bo‘ladi. Axborot shakllanganidan so‘ng tatbiqiy sath uni pastga-taqdimiy sathga uzatadi. Taqdimiy sathning protokoli tatbiqiy sathning sarlavhasidan olingan axborotga asosan talab qilingan harakatlarni bajaradi va ma’lumotga o‘zining xususiy xizmat axborotini-taqdimiy sathning sarlavhasini qo‘shadi. Natijada olingan axborot pastga-seans sathiga uzatiladi. Seans sathning protokoli taqdimiy sathning sarlavhasidan olingan axborotga asosan talab qilingan xarakatlarni bajaradi va ma’lumotga o‘zining xizmat axborotini – seans sathning sarlavhasini qo‘shadi. Bu sarlavhada mashina adresatining seans sathi protokoli uchun ko‘rsatmalar bo‘ladi. Natijada olingan axborot pastga, transport sathiga uzatiladi. Transport sathi o‘z navbatida o‘zining sarlavhasini qo‘shadi. Nihoyat, axborot pastki – fizik sathga yetib boradi. Fiziq sath o‘zining sarlavhasini qo‘shib, axborotni mashina adresatiga aloqa liniyalari orqali uzatadi. Bu paytga kelib, axborot barcha sath ilovalariga “o‘sadi”. Axborot mashina-adresatiga yetib kelganidan so‘ng yuqoriga qarab sathlar bo‘yicha ko‘chiriladi. Har bir sath, ushbu sathga mos vazifalarni bajargani holda, o‘z sathi sarlavhasini tahlillaydi va ishlatadi. So‘ngra bu sarlavhani chiqarib tashlab, axborotni yuqori sathga uzatadi.

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

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

5.2. Tarmoq xavfsizligi muammolari

Korxonalar o'z tizimlari va kompyuterlarini ulashganda, bitta foydalanuvchining muammolari tarmoqdagi barchaga ta'sir qilishi mumkin. Tarmoqlardan foydalanishning ko'plab afzalliklariga qaramay, tarmoq quyidagi kabi xavfsizlik muammolari uchun katta imkoniyatlar yaratadi:

- ma'lumotlar yo'qolishi
- xavfsizlik buzilishi
- xakerlik va viruslar kabi zararli hujumlar

Tarmog'ingizning ruxsatsiz kirish yoki shikastlanishga qarshi zaifligini kamaytirish choralarini ko'rishingiz mumkin. Barcha zaifliklarni bartaraf etishning iloji bo'lmasligi yoki iqtisodiy jihatdan amaliy bo'lmasligi mumkin, shuning uchun AT risklarini baholash qanday choralarni amalga oshirishni hal qilishda muhim ahamiyatga ega.

Zaiflik – “portlaganida” tizim xavfsizligini ta’minlash yetarlicha tashkil qilinmaganligi bilan bog’liq kamchilik, loyihani amalga oshirishdagi xatolik.

Taxdid – (axborot xavfsizligiga taxdid) - axborot xavfsizligini buzilish mumkin bo’lgan yoki haqiqiy mavjud xavfni tug‘diruvchi sharoitlar va omillar majmui.

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

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

Qurilma yoki dasturiy vositaning sozlash jarayonin noto’g’ri amalga oshirish. Xavfsizlikni ta’minlashdagi bo’shliqlar sozlash jarayonlarni noto’g’ri amalga oshirish yoki tarmoq qurtlarining tarmoqda paydo bo’lish natijasida vujudga keladi. Masalan, noto‘g‘ri sozlangan yoki shifrlash mavjud bo‘lmagan protokoldan foydalanish tarmoq orqali yuboriluvchi maxfiy ma’lumotlarning oshkor bo‘lishiga sababchi bo‘lishi mumkin.

Tarmoqni xavfsiz bo‘lmagan tarzda va zaif loyihalash. Ilovalarni loyihalashda ishlab chiquvchilarga xavfsiz qurulmalari, sinchkovlik bilan

rejalashtirilgan tahdidlarni modellashtirish va ilovani xavfsizlik bo'shliqlarisiz saqlaydigan mos yozuvlar arxitekturalaridan foydalanish tavsiya etiladi. 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.

Texnalogiyani yaratishdagi texnologik zaiflik. Agar yaratilgan texnik va dasturiy vosita hujymlarga bardosh bera olmasa ushbu taxnalogiya va dasturiy vositalar hujumlarga zaif hisoblanadi. Masalan, agar tizimlarda foydalanilgan web brauzer yangilanmagan bo‘lsa, u taqsimlangan hujumlarga ko‘proq bardoshsiz bo‘ladi.

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

Tarmoq xavfsizligiga tahdid turlari. Kompyuter tarmoqlariga qaratilgan tahdidlar odatda ikki turga bo’linadi. (5.5-rasm):

- *ichki tahdidlar;*
- *tashqi tahdidlar.*

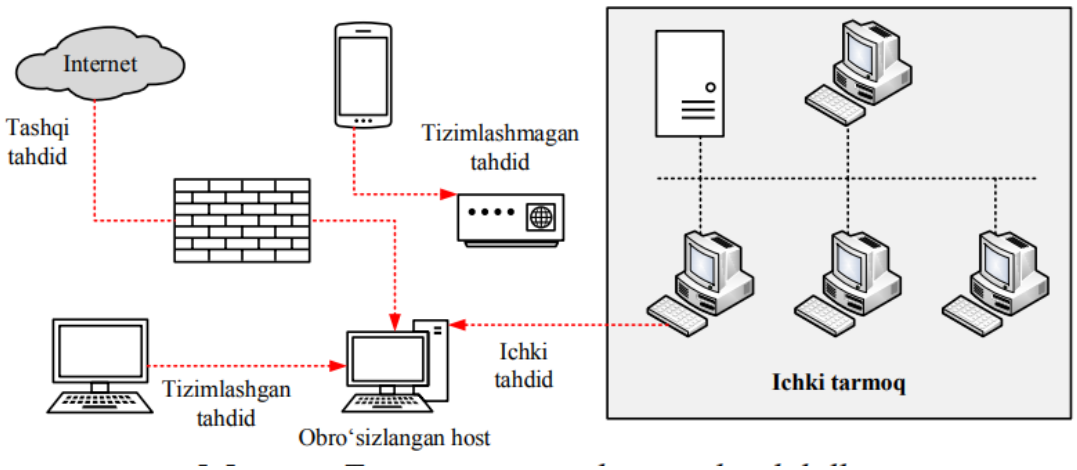
Ichki tahdidlar. Ichki tahdid deganda kompaniya ichidan tizimdan ma'lumotlarga zarar yetkazish yoki o'g'irlash yo'li bilan foydalanishi mumkin bo'lgan shaxsning xavfi tushuniladi. Bunday tahdidlar ayniqsa tashvishlidir, chunki xodimlar osonlikcha suiste'mol qilinishi mumkin bo'lgan kengaytirilgan imtiyozlarga ega ishonchli shaxslar bo'lishi kutiladi.

Tashqi tahdidlar. Tashqi tahdid zararli dasturiy ta'minot, buzg'unchilik, sabotaj yoki ijtimoiy muhandislik orqali tizim zaifliklaridan foydalanishga urinayotgan kompaniya tashqarisidan kimningdir xavfini anglatadi.

Ular bilan kurashish ichki tahdidlarga qaraganda ancha qiyin bo'lishi mumkin, chunki siz xodimlar kabi odamlarni tashqaridan kuzata olmaysiz va ular keyin nima qilishini oldindan aytib bera olmaysiz.

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

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



5.5-rasm. Tarmoqqa qaratilgan turli tahdidlar

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

Razvedka hujumlari. Razvedka hujumi - bu tajovuzkor haqiqiy hujumni boshlashdan oldin nishon haqida barcha mumkin bo'lgan ma'lumotlarni to'plash uchun foydalanadigan xavfsizlik hujumining bir turi. Hujumchi razvedka hujumidan haqiqiy hujumga tayyorgarlik vositasi sifatida foydalanadi.

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

- *tarmoq haqidagi;*
- *tizim haqidagi;*

- tashkilot haqidagi.

Razvedka hujumlarining turlari.

*Ijtimoiy razvedka hujumlari***.** Ushbu turdagi hujumda xaker maqsad haqida ma'lumot to'plash uchun ijtimoiy muhandislikdan foydalanadi. Foydalanuvchilar ijtimoiy tarmoq saytlarida ko'plab shaxsiy va biznes ma'lumotlarini almashadilar. Xaker maqsad haqida ma'lumot to'plash uchun ijtimoiy tarmoq saytlaridan foydalanishi mumkin. Misol uchun, agar maqsad kompaniya bo'lsa, xaker ijtimoiy tarmoq saytlaridan kompaniya xodimlari haqidagi ma'lumotlarni oshkor qilishi mumkin.

Xaker xodimni o'ziga jalb qilish uchun asal tuzog' usullaridan foydalanishi mumkin. Xodim xakerning do'stlik so'rovini qabul qilgandan so'ng, xaker keyingi bosqichni boshlaydi. Keyingi bosqichda xaker xodimni o'z biznesi haqidagi ma'lumotlarni oshkor qilishga ishontiradi. Masalan, xaker o'z loyihasi bo'yicha xodimga texnik yordam ko'rsatishi mumkin. Yoki xaker kompaniya haqidagi ma'lumotlarni oshkor qilgani uchun qandaydir pul mukofotini taklif qilishi mumkin.

Ijtimoiy razvedka hujumlarini kamaytirish uchun kompaniya o'z xodimlarini kompaniya ichida va tashqarisida qanday ma'lumotlarni boshqalar bilan baham ko'rmasliklari haqida o'rgatishi kerak. Xodimlar hech qachon biron bir ijtimoiy platformada nozik ma'lumotlarni baham ko'rmasliklari kerak. Agar xodim biron bir maxfiy ma'lumotni noma'lum shaxslar yoki tashqi foydalanuvchilar bilan baham ko'rsa, kompaniya xodimga nisbatan tegishli choralar ko'rishi kerak.

Ommaviy razvedka hujumlari. Ushbu turdagi hujumda xaker ommaviy domenlardan maqsad haqida ma'lumot to'playdi. Kompaniyalar o'z veb-saytlarida joylashuvi va biznes modeli ma'lumotlarini almashadilar. Xaker ushbu ma'lumotdan maqsadning joylashishini aniqlash uchun foydalanishi mumkin. Ushbu ma'lumotlarga asoslanib, xaker maqsad qanday infratuzilmadan foydalanishini ham aniqlashi mumkin. Masalan, ko'pgina veb-xosting kompaniyalari o'z serverlari va xavfsizlik uskunalari haqida ma'lumot almashadilar. Kompaniyalar yangi mijozlarni jalb qilish va mavjud mijozlarning

ishonchini qozonish uchun ushbu ma'lumotlarni almashadilar. Xakerlar ushbu ma'lumotlardan kompaniya tarmog'idagi zaifliklarni topish uchun foydalanishlari mumkin.

Ommaviy razvedka hujumlarini yumshatish uchun kompaniyalar maxfiy ma'lumotlarni ommaviy platformalarda baham ko'rmasliklari kerak. Biznes talablari uchun, agar kompaniya o'z infratuzilmasi haqida ma'lumot almashishni istasa, aniq apparat ma'lumotlarini almashish o'rniga, u umumiy ma'lumotlarni almashishi kerak. Umumiy ma'lumot biznes talabiga javob beradi. Umumiy ma'lumotlardan xaker mahsulot ma'lumotlarini taxmin qila olmaydi. Misol uchun, agar kompaniya Cisco Firepower 4100 xavfsizlik devoridan foydalansa, u biz Cisco Firewalldan foydalanayotganimizni e'lon qilishi mumkin.

Dasturiy ta'minot razvedka hujumlari. Ushbu turdagi hujumda xaker maqsad haqida ma'lumot to'plash uchun dasturiy vositalardan foydalanadi. Operatsion tizimlar va dasturiy paketlar disk raskadrovka va nosozliklarni bartaraf etish uchun ko'plab vositalar va yordamchi dasturlarni o'z ichiga oladi. Hacker ulardan tarmoq va uning resurslari haqida ma'lumot to'plash uchun foydalanishi mumkin. Masalan, xaker DNS qidiruvini amalga oshirish uchun nslookup buyrug'idan foydalanishi mumkin. Nslookup buyrug'i to'liq malakali domen nomidan IP-manzilni hal qiladi. Xaker biznesning domen nomini bilganidan so'ng, xaker whois ma'lumotlar bazasidan domen egalari, pochta serverlari, aloqa ma'lumotlari, nufuzli DNS serverlari va boshqalar haqida batafsil ma'lumotni ochish uchun foydalanishi mumkin.

-*Aktiv razvedka hujumlari*. Aktiv razvedka hujumlari asosan portlarni va operaesion tizimni skanerlashni maqsad qiladi. Buning uchun, hujumchi maxsus dasturiy vositalardan foydalangan holda, turli paketlarni yuboradi. Masalan, maxsus dasturiy vosita router va tarmoqlararo ekranga boruvchi barcha IP manzillarni to‘plashga yordam beradi.

- *Passiv razvedka hujumlari*. Passiv razvedka hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Buning uchun hujumchi sniffer deb

nomlanuvchi dasturiy vositadan foydalanadi. Bundan tashqari, hujumchi ko‘plab vositalardan foydalanishi mumkin.

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

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

- lug‘atga asoslangan hujum;

- qo‘pol kuch hujumi yoki barcha variantlarni to‘liq tanlash hujumi;

- gibrid hujum (lug‘atga va qo‘pol kuch hujumlariga asoslangan);

-rainbow jadvali hujumlari (oldindan hisoblangan keng tarqalgan parollarning xesh qiymatlari saqlanuvchi jadvallar).

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

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

saytning ishlashiga ham ta’sir qiladi. Ushbu hujum bilan web-sayt faoliyatini to‘xtatib qo‘yish mumkin.

Taqsimlangan DOS hujumlar: (Distributed DOS, DDOS). Taqsimlangan xizmatni rad etish (DDoS) hujumi maqsadli yoki uning atrofidagi infratuzilmani Internet-trafik oqimi bilan to'ldirish orqali maqsadli server, xizmat yoki tarmoqning normal trafigini buzishga qaratilgan zararli urinishdir.

DDoS hujumlari hujumlar trafigining manbalari sifatida bir nechta buzilgan kompyuter tizimlaridan foydalanish orqali samaradorlikka erishadi. Ekspluatatsiya qilingan mashinalar kompyuterlar va IoT qurilmalari kabi boshqa tarmoq resurslarini o'z ichiga olishi mumkin.

Yuqori darajadan qaraganda, DDoS hujumi kutilmagan tirbandlikka o'xshab, avtomagistralni to'sib qo'yadi va muntazam transportning belgilangan joyga etib borishiga to'sqinlik qiladi.

Zararli hujumlar. Zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta’sir qiladi.

Zararli dastur – fayl bo‘lib, kompyuter tizimiga tahdid qilish imkoniyatiga ega va troyanlar, viruslar, “qurtlar” ko‘rinishida bo‘lishi mumkin.

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

- *viruslar*: Kompyuter virusi kompyuter dasturining bir turi bo‘lib , u bajarilganda boshqa kompyuter dasturlarini o‘zgartirish va shu dasturlarga o‘z kodini kiritish orqali o‘zini takrorlaydi;

- *troyan otlari*: bir qarashda yaxshi va foydali kabi ko‘rinuvchi dasturiy vosita sifatida o‘zini ko‘rsatsada, yashiringan zararli koddan iborat;

- adware: Reklama dasturi bu sizning kompyuteringizda reklamalarni ko'rsatish, qidiruv so'rovlarini reklama veb-saytlariga yo'naltirish va reklamalarni qiziqishlaringizga ko'proq moslashtirish uchun siz haqingizda marketing ma'lumotlarini to'plash (masalan, qanday veb-saytlar kabi) uchun mo'ljallangan dasturiy ta'minot;

- *spyware*: (josuslik dasturi) - bu shaxs yoki tashkilot haqida ma'lumot to'plash va uni foydalanuvchiga zarar etkazadigan, masalan, shaxsiy hayotini buzish yoki qurilma xavfsizligini xavf ostiga qo'yish orqali boshqa shaxsga yuborishga qaratilgan zararli xatti-harakatlarga ega dasturiy ta'minot . Bunday xatti-harakatlar zararli dasturlarda ham, qonuniy dasturlarda ham bo'lishi mumkin;

- *rootkits*: - bu odatda zararli, kompyuterga yoki uning dasturiy ta'minotining boshqa yo'l bilan ruxsat etilmagan qismiga (masalan, ruxsatsiz foydalanuvchiga) kirishni ta'minlash uchun mo'ljallangan va ko'pincha uning mavjudligini yoki mavjudligini maskalash uchun mo'ljallangan kompyuter dasturlari to'plami;

-*backdoors*: zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan, aylanib o‘tib tizimga kirish imkonini beradi, masalan, ma’mur parolisiz imtiyozga ega bo‘lish;

- *mantiqiy bombalar*: zararli dasturiy vosita bo‘lib, biror mantiqiy shart qanoatlantirilgan vaqtda o‘z harakatini amalga oshiradi;

- *botnet*: Internet tarmog‘idagi obro‘sizlantirilgan kompyuterlar bo‘lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi;

- *ransomware*: mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki blokirovkalab, to‘lov amalga oshirilishini talab qiladi.

5.3. Tarmoq xavfsizligini ta’minlovchi vositalar

Hozirda tarmoq xavfsizligini ta’minlovchi vositalarga tarmoqdan foydalanishni cheklashning bazaviy vositalari (tarmoqlararo ekran) va

ma’lumotlarni himoyalangan holda uzatish vositalari (kriptoshlyuzlar va VPN yechimlar), hamda himoyalanganlikni ta’minlovchi qo‘shimcha tarmoq vositalari, trafikni monitoringlash vositalari, yolg‘on tarmoq nishonlari va h. taalluqli.

Tarmoqlararo ekranlash. Tarmoqlararo ekran (firewall, brandmaver) – trafikni filtrlash mexanizmiga asoslangan tarmoqdan foydalanishni cheklashning bazaviy vositasi. Filtratsiya mexanizmi o‘tuvchi trafikni ma’lum qoidalar (filtrlar) bilan taqqoslashni va tarmoq paketlarini o‘tkazish yoki o‘tkazmaslik xususida qaror qabul qilishni ko‘zda tutadi.

Tarmoqlararo ekranlarni, odatda, ishlatiladigan filtrlash texnologiyasiga va OSI modelining bazaviy sathiga nisbatan tasniflashadi (5.1-jadval).

5.1-jadval Tarmoqlararo ekran turlari

OSI modeli sathlari	Filtratsiya texnologiyalari	Tarmoqlararo ekran turlari
Tatbiqiy sath	Proksi	Tatbiqiy vositachi
Seans sathi	Proksi	Seans vositachisi
	Paketlar inspektori	Holat inspektori
	Paketlar filtrasiyasi	Dinamik filtr
Tarmoq sathi	Paketlar filtrasiyasi	Ekranlovchi marshrutizator, paket filtri
Kanal sathi	Trafikni segmentlash	Boshqariluvchi (ekranlovchi) kommutator

Kanal sathida ishlatiluvchi boshqariluvchi kommutatorlar, masalan, MAC-adreslar, portlar va kadrlar sarlavhalaridan olingan boshqa parametrlar asosida, trafikni filtrlash vazifasining bajarilishiga imkon beradi. Boshqariluvchi kommutatorlarning afzalligi sifatida tarmoq qurilmalari guruhini ma’murlashning qulayligini, lokal tarmoq unumdorligining oshishini ko‘rsatish mumkin. Funksionallikning cheklanganligi, fizik rekonfiguratsiyalashning noqulayligi va MACadresni almashtirish hujumiga zaifligi boshqariluvchi kommutatorlarning kamchiligi hisoblanadi.

Tarmoq sathining paket filtrlari va marshrutizatorlar IP-adres, portlar, protokol turi va h. bo‘yicha filtrlash vazifasining bajarilishiga imkon beradi.

Tarmoq va transport sathlari funksionalliklarining cheklanganligi va IP-adresni almashtirish hujumiga zaifligi paket filtrlarining kamchiligi hisoblanadi.

Seans sathining paket filtrlari, seansga mos filtrlash parametrlarining katta sonini hisobga olgan holda, filtrlashni bajarishga imkon beradi.

Vositachilar - oraliq tarmoq vositalari o‘ziga tegishli ulanishni amalga oshirib, trafikni qo‘shimcha qurilmada ishlaydi. Bu o‘z navbatida quyidagi vazifalarni bajarishga imkon beradi:

− autentifikatsiyani;

− mijozlar va serverlarning asinxron muloqotini;

− adreslarning translyatsiyasini va yashirishni;

−tarmoq yukini qayta taqsimlash maqsadida adresni o‘zgartirishni; − almashish unumdorligini oshirish maqsadida xeshlashni;

− trafikni qaydlashni.

Ayni paytda, vositachilardan foydalanilganda, trafik qo‘shimcha qurilmada takroriy ishlangani sababli, tarmoq perimetri bo‘yicha istalgan unumdorlikni taminlash masalasini yechish talab etiladi.

Vositachi tomonidan amalga oshiriluvchi marshrutlash texnologiyasiga alohida e’tibor berish lozim. Unga binoan tarmoq adreslarining translyatsiyasi (Network Address Translation, NAT) amalga oshiriladi, ya’ni hostning ichki adresi vositachining shaxsiy adresiga almashtiriladi. Boshqacha aytganda, NAT ichki tarmoq adreslarini tashqi tomondan yashirish siyosatini amalga oshiradi va ichki tarmoq uchun vositachiga bitta IP-adresni belgilash imkoniyatini yaratadi. Adreslarni translyatsiyalash statik va dinamik tarzda belgilanishi mumkin.

Seans sathidagi vositachilarga, yuqori unumdorlikka, adreslarni yashiruvchi samaradorli apparatga va TCP/UDP – trafikni ajratish imkoniyatiga ega SOCKet Secure (SOCKS5) vositachisi taalluqli. Tatbiqiy vositachi sifatida HTTP/HTTPS vositachilari va FTP vositachi keng tarqalgan. Ushbu vositachilar tatbiqiy protokol kontenti bo‘yicha filtrlashga imkon tug‘diradi.

Holat inspektorlari (seans sathining imkoniyati kengaytirilgan filtrlari), seans sathidagi protokollar sarlavhalaridan olinuvchi ma’lumotlar asosida,

intelektual filtrlashni bajaradi. Bu yuqori sathlarda filtrlash effektini olishga imkon beradi. Bunday tarmoqlararo ekranlar vositachini o‘rnatishni talab qilmaydi. Shu sababli, tarmoq unumdorligi pasaymaydi, ammo xavfsizlikning kerakli darajasi ta’minlanadi. Holat inspektorining afzalligiga masshtablashning qulayligini ham qo‘shish mumkin.

Amaliyotda axborot resurslarining tarmoqlararo himoyasini taminlashda UTM (Unifield Threat Management) qurilma tushunchasini va keyingi avlod tarmoqlararo ekranlarini (Next Generation, NG firewall) uchratish mumkin.

UTM – qurilma perimetrli himoyalash masalasining kompleks yechimi hisoblanadi. Uning tarkibida tarmoqlararo ekranlash modullaridan tashqari, suqilib kirishlarni aniqlash tizimlari, oqimli antivirus, spamga qarshi yechim, kriptoshlyuz va h. mavjud bo‘lishi mumkin.

NG firewall UTMga o‘xshash va portlar bo‘yicha filtrlash texnikasini, suqilib kirishlardan ogohlantirish tizimlarini va ilovalar sathida trafikni filtrlashni birlashtirish maqsadida yaratilgan.

Virtual xususiy tarmoqlar. Virtual xususiy tarmoq (Virtual Private Network, VPN) deganda ma’lumotlarni inkapsulyatsiyalash mexanizmlari, hamda qo‘shimcha autentifikatsiya, shifrlash, yaxlitlikni nazoratlash bazasida vaqtinchalik himoyalangan aloqa kanalini yaratish yo‘li bilan uzatiluvchi ma’lumotlarni himoyalash vositasi tushuniladi. Nomidan ko‘rinib turibdiki, VPNning asosiy g‘oyasi vaqtinchalik (seans davrida) ma’lumotlarni uzatish uchun inkapsulyatsiyalash, ya’ni bir sathning tarmoq paketini yuqori sathning yagona paketiga birlashtirish yo‘li bilan himoyalangan tunnelni yaratishdan iborat. Aynan, doimiy himoyalangan kanalni yoki ajratilgan liniyani ijaraga olishni tashkil etish oldida, vaqtinchalik tunnelni tashkil etish imkoniyatining afzalligi namoyon.

Ma’lumotlar paketining yuqori sath paketiga inkapsulyatsiyasi esa ma’lumotlarni shifrlash va ularning yaxlitligini nazoratlash talablarini osongina qondirishga imkon beradi.

Virtual xususiy tarmoqlarni, asosan OSI-modeli sathlari va ulanish usullari bo‘yicha tasniflash qabul qilingan. Ulanish bo‘yicha “nuqtanuqta” (“uzel-uzel”),

“nuqta-tarmoq” va “tarmoq-nuqta” usullari farqlanadi. *5.2-jadvalda virtual xususiy tarmoqning eng ommaviy protokollari keltirilgan.*

OSI modeli sathlari	**Tunnellashning bazaviy protokoli**	**Shifrlash vositalari**
Seans sathi	SOCKS	Quyidagi protokollardan foydalanadi.
Transport sathi	SSH	AES, 3DES, Blowish
	SSL/TLS	AES,3DES,IDEA, RC4 va h.
Tarmoq sathi	IPSec(ESP)	AES,3DES va h.
Kanal sathi	L2TP	Yuqoridagi protokollardan foydalanadi.
	PPTP	MPPE(RC4)

PPTP (Point-to-Point Tunneling Protocol) – “nuqta-nuqta” xilidagi kanal sathining tunnel protokoli. Ushbu protokol, tunnelga xizmat qilish uchun, qo‘shimcha TCP-ulanish yordamida PPP-kadrlarni IP-paketlarga inkapsulyatsiyalaydi. Mijozlarni autentifikatsiyalash uchun masofaviy foydalanishning turli protokollarini, jumladan MSCHAPv2 protokolini, madadlaydi. Shifrlashda RC4 algoritmni amalga oshiruvchi MPPE protokol madadlanadi.

L2TP (Layer 2 Tunneling Protocol) – PPP-kadrlarni tarmoq sathi paketlariga inkapsulyatsiyalovchi kanal sathining tunnel protokoli. Protokolning afzalligi sifatida foydalanish ustuvorliklarini va multiprotokollikni (nazariy jixatdan IPga bog‘liq emaslikni) madadlashini ko‘rsatish mumkin. Shifrlash mexanizmi o‘zidan yuqori sathga ishonib topshiriladi, masalan IPSec apparat yordamida amalga oshirilishi mumkin. PPTPdan farqli holda, TCP/IP tarmoqlarida ushbu protokol transport protokoli UDPga moslangan.

IPSec (IP Security) protokoli ikkita rejimda – transport va tunnel rejimida ishlaydi. Transport rejimida (ushbu rejim hostlar orasidagi ulanishlarni o‘rnatishda ishlatiladi) IPSecdan, qandaydir boshqa usul, xususan, shifrlash funksiyasi bo‘lmagan L2TP tomonidan tashkil etilgan “nuqta-nuqta” xilidagi tunnellarni himoyalashda foydalanish mumkin. Tunnel rejimi shunday tunnelarni yaratishga imkon beradiki, shifrlangan butun paket (transport rejimidan farqli holda, butun

paket sarlavhasi bilan shifrlangan) adresatga yetkazish uchun yuqori sathga inkapsulyatsiyalanadi.

Tarmoq xavfsizligini ta'minlovchi qo'shimcha vositalar. Suqilib kirishlarni aniqlash tizimlari (Intrusion Detection System, IDS). IDSning asosini tarkibida mosshablonlar, signaturalar yoki profillar bo'lgan hujumlarning ma'lumotlar bazasi tashkil etadi va aynan ushbu baza bilan sensorlardan olingan ma'lumotlar taqqoslanadi. Shu sababli, IDSning samaradorligi hujumlarning ma'lumotlar bazasining nufuziga bog'liq. Suqilib kirishlarni aniqlashda quyidagi usullardan foydalanish mumkin:

− signatura usuli – qandaydir hujumga xarakterli ma'lumotlar nabori bo'yicha suqilib kirishlarni aniqlash;

− anomallarni aniqlash usuli –normal holatiga harakterli bo'lmagan alomatlarni aniqlash;

− xavfsizlik siyosatiga asoslangan usul – xavfsizlik siyosatida belgilangan parametrlarning buzilganligini aniqlash.

Monitoring darajasi bo'yicha IDS – tizimlar quyidagilarga bo'linadi:

− tarmoq sathi IDSi (Network based IDS, NIDS);

− uzel sathi IDSi (Host based IDS, HIDS).

NIDS tarmoq segmentiga ulangan bir necha xostlardan keluvchi tarmoq trafigini monitoringlash orqali ushbu xostlarni himoyalashi mumkin. HIDS yagona kompyuterda yig'ilgan, asosan operatsion tizimning va axborotni himoyalash tizimining jurnallaridan, foydalanuvchi profilidan va h. yig'ilgan, axborot bilan ish ko'radi. Shu sababli NIDSdan kompyuter hujumlarini oldinroq aniqlashda foydalanish qulay hisoblansa, HIDSdan ruxsatsiz foydalanishning ishonchli faktini qaydlashda foydalaniladi.

IDSning aktiv (in-line) xili suqilib kirishlarni ogohlantirish tizimi (Intrusion Prevention System, IPS) deb ataladi.

Himoyalanganlikni tahlillash vositalari. Texnik audit bo'yicha mutaxassislar bo'lishi mumkin bo'lgan va real zaifliklarni aniqlashda turli himoyalanganlikni

tahlillash vositalaridan foydalanishadi. Himoyalanganlikni tahlillash vositalarining quyidagi sinflari mavjud:

− zaifliklarning tarmoq skanerlari;

− web-ilovalar xavfsizligining skanerlari;

− tizim konfiguratsiyasini tahlillash vositalari;

− testlashning maxsus vositalari.

Zaifliklarning tarmoq skanerlari maxsus dasturiy vositalar bo‘lib, undagi kirish axboroti sifatida skanerlanuvchi IP-adreslarning ro‘yxati, chiqish axboroti sifatida esa aniqlangan zaifliklar xususidagi hisobot ishtirok etadi. Asosiy ishlash prinsipi – masofadagi uzelda o‘rnatilgan dasturiy ta’minotning aniq versiyasini aniqlash va zaifliklarning yangilanuvchi lokal bazasiga dasturiy ta’minotning ushbu versiyasi uchun xarakterli zaifliklar xususidagi axborotni qidirish.

Web-ilovalar xavfsizligining skanerlari maxsus dasturiy vositalar bo‘lib, web-tizimlar strukturasini tahlillaydi. Natijada axborotni kiritishning bo‘lishi mumkin bo‘lgan variantlari aniqlanadi va zaiflikdan foydalanish maqsadida so‘rov shakllantiriladi.

Tizim konfiguratsiyasini tahlillash vositalari – tizim himoyalanganligini uning sozlanishi bo‘yicha baholovchi dastur. Bu xil yechim kompleks mahsulot yoki lokal skript (senariy) sifatida ifodalanishi mumkin.

Testlashning maxsus vositalari:

− parollarni online va offline saralash dasturlari;

− zaifliklardan foydalanish freymworklari;

− ma’lum tarmoq hujumlarini amalga oshiruvchi dasturlar (masalan, ARP-spoofing);

− web-serverga uzatiluvchi HTTP so‘rovlarni o‘zgartirish uchun loakl HTTP proksilar va h.

Zaifliklarning turli onlayn – bazalari mavjud. CVE (Common Vulnerabilities and Exposures, cve.mitre.org) zaifliklar bazasi mashhur.

Ma’lumotlarning sirqib chiqishini oldini olish tizimlari (Data Leakage Prevention, DLP). Ushbu tizimlardan, tarkibida tijoriy, kasbiy yoki boshqa turdagi

sir bo‘lgan ma’lumotlarning noqonuniy tarzda tashqi tarmoqqa jo‘natilishini aniqlashda va blokirovkalashda foydalaniladi.

DLP tizimlar ulanish sxemasi bo‘yicha IDS – yechimlarga o‘xshash – tahlillanuvchi axborot tarmoq sathida yoki hostsathida yig‘ilishi mumkin.

Axborot oqimlarini, ularda konfidensial axborotning mavjudligini aniqlash maqsadida, nazoratlashning ikkita usuli qo‘llaniladi:

− hujjatda berilgan belgilar bo‘yicha aniqlash;

− ma’lumotlar nabori kontenti bo‘yicha aniqlash.

Birinchi usul bo‘yicha axborotni dastlabki kategoriyalash va markirovkalash amalga oshiriladi. Bunda konfidensial hujjatga (masalan, faylga, ma’lumotlar bazasi yozuviga va h.) qandaydir ajralmaydigan formal alomat (masalan, nazorat yig‘indisi, inventar nomeri, konfidensiallik grifi) moslashtiriladi. So‘ngra, uzatiluvchi axborot oqimida ushbu alomat aniqlansa, mos hujjat blokirovkalanadi. Bunday yondashish hujjatni faqat butunligicha himoyalashga qodir. Yondashishning afzalligi sifatida huquqiy risklarning pasayishini va turli xil yolg‘on nishonlar ishlashi darajasining yuqori emasligini ko‘rsatish mumkin.

Yolg‘on nishonlar yoki tuzoqlar (honeypot). Tarmoq xavfsizligini ta’minlovchi ushbu vositadan niyati buzuq tomonidan yolg‘on nishonlarni aniqlash, hamda buzib ochish usullarini tadqiqlash maqsadida hujumni yuzaga keltirishga urinishda foydalaniladi.

Yolg‘on nishonlarni tasniflashda alomat sifatida ularning interaktivligi ishlatiladi, ya’ni quyidagi tuzoqlar farqlanadi:

− interaktiv tuzoqlar;

− interaktivlik darajasi past tuzoqlar;

− interaktivlik darajasi yuqori tuzoqlar.

Interaktivlik darajasi past tuzoqlar bitta tarmoq servisining, masalan, FTP-servisning emulyatsiyasi bo‘lishi mumkin. Joylashtirilishining va nazoratlanishining osonligi bunday tuzoqlarning afzalligi hisoblansa, kamchiligi sifatida ular yordamida ko‘pincha faqat hujum faktining aniqlanishini ko‘rsatish mumkin.

Interaktivlik darajasi yuqori tuzoqlarni to‘laqonli operatsion tizimga va servislar naboriga ega virtual mashina sifatida tasavvur etish mumkin. Bunday tuzoqlar niyati buzuq xususida ancha ko‘p axborotni yig‘ishga imkon beradi (ayniqsa, u bilan intellektual teskari bog‘lanish tashkil etilgan bo‘lsa).

“Bo‘sh” tarmoqlar (DarkNet) tuzoqlarning alohida sinfi hisoblanadi. Ularga muvofiq korporativ tarmoqda, biznes-masalalarni yechishda real ishlatilmaydigan, tashqi adreslar diapazoni ajratiladi. “Bo‘sh” tarmoqqa har qanday murojaat konfiguratsiyadagi xatolikni yoki noqonuniy faoliyatni anglatadi.

Ta’kidlash lozimki, IDS va DLP – yechimlar hujumlarning ma’lum sinfiga mo‘ljallangan. Amaliyotda axborot tizimi ishlashidagi har qanday xavfsizlik va ishonchlik hodisalarni yig‘ish masalasi paydo bo‘ladi. Bunday tizimlarga quyidagilar taaluqli:

− jurnallarni boshqarish tizimlari (log management). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishni tashkil etish uchun mo‘ljallangan;

− xavfsizlik xususidagi axborotni boshqarish tizimlari (Security Information Management, SIM). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishga, hamda turli hisobotlarni shakllantirishga va tahlillashga mo‘ljallangan;

− xavfsizlik hodisalari hususidagi axborotni boshqarish tizimlari (Security Event Manager, SEM). Ushbu tizimlar vaqtning real rejimida monitoringlashga, axborot xavfsizligi hodisalarini korrelyatsiyalashga mo‘ljallangan;

− xavfsizlik va xavfsizlik hodisalari xususidagi axborotni boshqarish tizimlari (Security Information and Event Management, SIEM). Ushbu tizimlar monitoring tizimlari rivojining keyingi qadami hisoblanadi, chunki SEM va SIM funksionalliklarini kombinasiyalaydi.

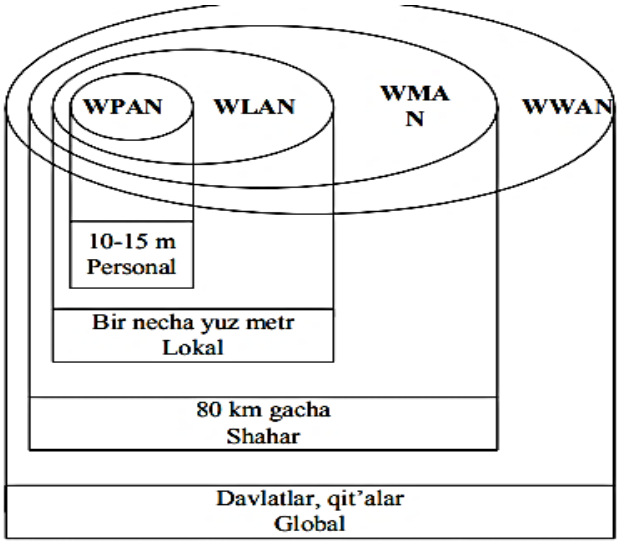
Qo‘shimcha sifatida aytish mumkinki, tarmoqlararo ekranlar uchun belgilangan mexanizm – filtratsiya, VPN uchun – inkapsulyatsiya, SIEM uchun esa korrelyatsiya.

5.4. Simsiz tarmoq xavfsizligi

Simsiz tarmoq turlari. Ma’lumki, radio ixtiro etilganidan so‘ng, ko‘p o‘tmay telegraf aloqani simsiz amalga oshirish imkoniyati paydo bo‘ldi. Aslida, hozirgi raqamli kodni radiokanal bo‘yicha uzatishda o‘sha prinsipdan foydalanishadi, ammo ma’lumotlarni uzatish imkoniyati bir necha bor oshdi.

Zamonaviy simsiz tarmoqlarni ta’sir doirasi va vazifasi bo‘yicha quyidagilarga ajratish mumkin (5.6-rasm):

- shaxsiy (Wireless Personal Area Network, WPAN);
- lokal (Wireless Local Area Network, WLAN);
- shaxar (Wireless Metropolitan Area Network, WMAN);
- global (Wireless Wide Area Network, WWAN).



5.3-rasm. Simsiz tarmoqlar tasnifi

Simsiz tarmoqlarning asosiy xarakteristikalari

Simsiz tarmoqlar / Xarakte-ristikalar	WPAN (shaxsiy simsiz tarmoqlar)	WLAN (lokal simsiz tarmoqlar)	WMAN (shaxar simsiz tarmoqlar)	WWAN (global simsiz tarmoqlar)
Ko‘llanish sohasi	Tashqi qurilma simlarini almashtirish	Simli tarmoqlarning mobil kengaytirishlari	Keng polosali simsiz foydalanish	Bino tashqarisida Internetdan mobil foydalanish
Taxnologi-yalar	Bluetooth, UMB, ZigBee	Wi-Fi (802.11)	WiMax (802.16), MBWA-m (802.20)	GSM, GPRS, WCDMA, EDGE, HSPA+, WiMax, LTE

5.4-jadvalda yuqorida keltirilgan simsiz tarmoqlarning xarakteristikalari keltirilgan

Simsiz tarmoqlarda axborot xavfsizligiga asosiy tahdidlar. Simsiz mahalliy tarmoqlar (WLAN) simlar emas, balki radio to'lqinlar yordamida ma'lumotlarni uzatadi va qabul qiladi. Jismoniy to'siqning yo'qligi WLAN-larni noqonuniy ushlash, tinglash, buzish va boshqa bir qator kiberxavfsizlik muammolariga qarshi himoyasiz qiladi.

Simli va simsiz tarmoqlar orasidagi asosiy farq – simsiz tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan hududning mavjudligi. Uyali tarmoqlarning yetarlicha keng makonida simsiz muhit aslo nazoratlanmaydi.

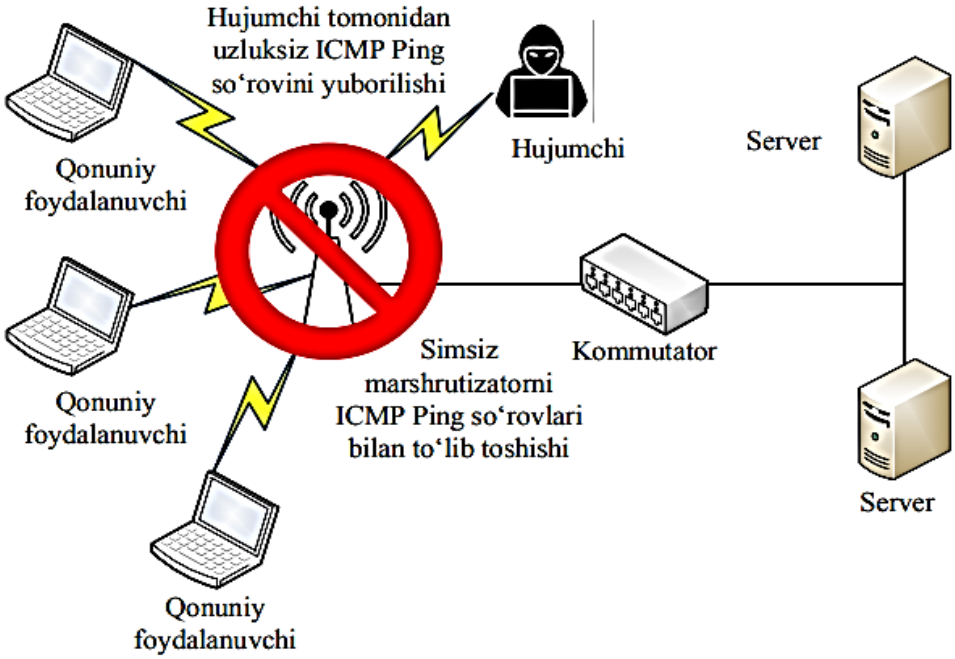
Ruxsatsiz suqilib kirish. Agar simsiz tarmoq himoyasi amalga oshirilmasa, ixtiyoriy simsiz ulanish imkoniyatiga ega qurilma undan foydalanishi mumkin. Mazkur holda, odatda, kirish joyining yopiq eshittirish diapazoni 50-100 metrni tashkil qilsa, tashqi maydonda 300 metrgacha bo‘lishi mumkin.

Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda keng tarqalgan muammo - anonim hujumlarning mavjudligi bo‘lib, uzatishni ushlab qolish uchun niyati buzuq uzatgich (передатчик) oldida bo‘lishi lozim.

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

lokal tarmoqlarda WEP protokolidan foydalanilgan bo‘lsa, katta ehtimollik bilan tarmoqni eshitish imkoniyati tug‘iladi.

Xizmat ko‘rsatishdan voz kechishga undash. Butun tarmoqda, jumladan, bazaviy stansiyalarda va mijoz terminallarida, shunday kuchli interferensiya paydo bo‘ladiki, stansiyalar bir-birlari bilan bog‘lana olmasligi sababli, DoS xilidagi xujum tarmoqni butunlay ishdan chiqarishi mumkin. Bu xujum ma’lum doiradagi barcha kommunikatsiyani o‘chiradi (5.7-rasm).



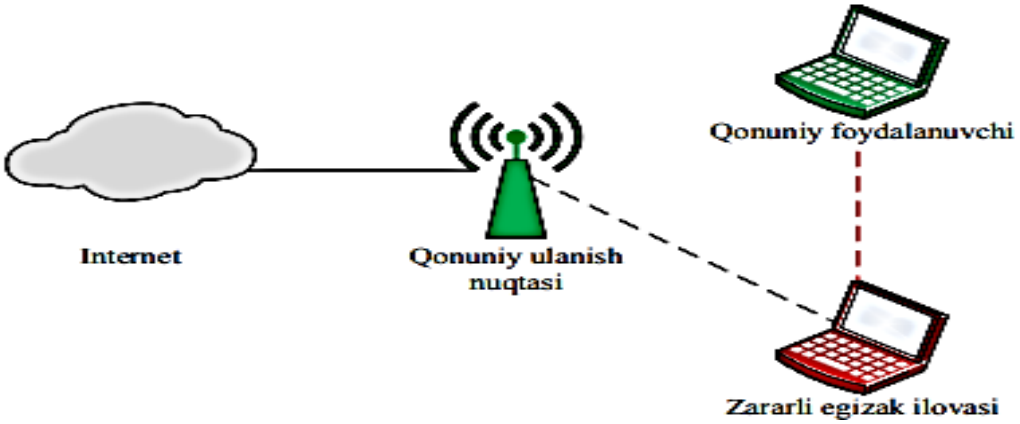
5.7-rasm. Simsiz tarmoqda DoS hujumining oshirilishi

O‘rtada turgan odam hujumi. MITM xujumi yuqorida tavsiflangan suqilib kirish hujumlariga o‘xshash, ular turli shakllarda bo‘lishi mumkin va aloqa seansining konfidensialligini va yaxlitligini buzish uchun ishlatiladi. Hujum qurboni ulanishni boshlaganida, firibgar uni ushlab qoladi va istalgan resurs bilan ulanishni tugallaydi va so‘ngra ushbu resurs bilan barcha ulanishlarni o‘zining stansiyasi orqali o‘tkazadi (5.8-rasm).

Tarmoqdan foydalanishning yolg‘on nuqtalari (zararli egizak hujumi). Tajribali hujumchi tarmoq resurslarini imitatsiya qilish bilan foydalanishning yolg‘on nuqtalarini tashkil etishi mumkin. Abonentlar, hech shubhalanmasdan foydalanishning ushbu yolg‘on nuqtasiga murojaat etadilar va uni o‘zining muhim rekvizitlaridan, masalan, autentifikatsiya axborotidan xabardor qiladilar.

Hujumning bu xili tarmoqdan foydalanishning xaqiqiy nuqtasini “bo‘g‘ish” maqsadida ba’zida to‘g‘ridan-to‘g‘ri bo‘g‘ish bilan birgalikda amalga oshiriladi (5.6-rasm).

5.8-rasm. MITM hujumining amalga oshirilishi



5.6-rasm. Zararli egizak hujumi

Rouming muammosi. Simsiz tarmoqning simli tarmoqdan yana bir muxim farqi foydalanuvchining tarmoq bilan aloqani uzmasdan joyini o‘zgartirish qobiliyatidir. Rouming konsepsiyasi turli simsiz aloqa standartlari CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) va simsiz Ethernet uchun bir xil bo‘lib, TCP/IPning ko‘pgina tarmoq ilovalari server va mijoz IPadreslarining o‘zgarmasligini talab etadi. Simsiz tarmoqlarda mobil IP-adreslarning va boshqa rouming mexanizmlarining ishlatilishi ushbu talabga asoslangan.

Foydalanishni cheklash. Tarmoqdan foydalanishni faqat ruxsatga egalar uchun joiz bo‘lishini taminlash muhim ahamiyatga ega. Har bir qurilma ajralmas MAC (Media access control) manziliga ega, ushbu manzillarni tekshirish orqali ularga foydalanishni taqdim etish mumkin.

Tarmoq orqali uzatiluvchi ma’lumotlarni shifrlash. Agar simsiz tarmoq orqali uzatilayotgan har bir ma’lumot shifrlangan taqdirda, ularni ruxsatsiz o‘qishdan himoyalash mumkin bo‘ladi. Simsiz lokal tarmoqlarda tarmoq nuqtasi va foydalanuvchi qurilmalari orasidagi ma’lumotlar odatda Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 va WPA3 protokollari asosida shifrlangan holda uzatiladi.

Simsiz tarmoq qurilmasini (SSID, Service Set Identifier) himoyalash. Tarmoq tashqarisidan simsiz tarmoqni osonlik bilan boshqarilishini oldini olish uchun, SSIDni oshkor etmaslik talab etiladi. Barcha Wi-Fi qurilmalar SSID ni himoyalash imkoniyatiga ega, bu hujumchining simsiz tarmoqni topishini qiyinlashtiradi.

Tarmoqlararo ekran vositasini o‘rnatish. Simsiz qurilmalarda bevosita hostga asoslangan tarmoqlararo ekranni o‘rnatish yoki uy tarmog‘i uchun modemga asoslangan tarmoqlararo ekranni o‘rnatish tavsiya etiladi.

Fayl almashishini ehtiyotkorlik bilan amalga oshirish. Tomonlar orasida faylni almashtirishga zaruriyat bo‘lmagan taqdirda, ushbu imkoniyat o‘chirilgan holatda bo‘lishi kerak. Fayl almashishini har doim shaxsiy yoki uy tarmog‘ida amalga oshirish zarur. Ochiq bo‘lgan tarmoqda fayllarni almashtirish tavsiya etilmaydi. Bundan tashqari, uzatilayotgan har bir fayllarni parol asosida himoyasini taminlash zarur (faylni blokirovkalash).

5.5. Risklar va risklarni boshqarish

Kiberxavfsizlik risklar- bu tashkilotingizga kiberhujum yoki ma'lumotlarning buzilishi natijasida ta'sir qilish yoki yo'qotish ehtimoli. Yaxshiroq va kengroq ta'rif - bu texnik infratuzilma, texnologiyadan foydalanish yoki tashkilotning obro'si bilan bog'liq bo'lishi mumkin bo'lgan yo'qotish yoki zarar. Quyida risk tushunchasi va uni boshqarish bo‘yicha batafsil ma’lumotlar keltirilgan.

Riskni ikki xil bo’lishi mumkin ichki va tashqi:

Risk – ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo‘qotilishi yoki boshqa salbiy ta’sir ko‘rsatishi mumkin bo‘lgan hodisa.

- *Risk* – manbaga zarar keltiradigan ichki yoki tashqi zaiflik tahdidi bo‘lishi ehtimoli.

- *Risk* – hodisa sodir bo‘lishi ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta’siri.

Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish mavjud bo‘lib, ularni quyidagicha ifodalash mumkin:

RISK = Tahdid × Zaiflik × Ta’sir.

Boshqa tomondan, hodisaning axborot texnologiyalari aktiviga ta’siri – aktivdagi yoki manfaatdor tomonlar uchun aktivning qiymatidagi zaiflikning natijasi, ya’ni:

RISK = Tahdid × Zaiflik × Aktiv qiymat.

Risk o‘zida quyidagi ikkita omilni mujassamlashtiradi:

- zararli hodisaning yuzaga kelishi ehtimoli;

- va zararli hodisa oqibatlarining ehtimoli.

Risk ta’siri. Risk normal amalga oshirish jarayoniga va loyiha narxiga yoki kutilgan qiymatga ta’sir etadi. Ta’sir riskning kuzatilishi ehtimoli jiddiyligini ko‘rsatadi.

Risk chastotasi. Riskni aniqlash va baholash nuqtai nazaridan risklarni tasniflashda ularning takrorlanish chastotasiga va ko‘p sonliligiga asoslanadi. Chastota va ko‘p sonlilik risklarni monitoringlashda muhim hususiyat hisoblanib, risklar ikki guruhga: minor risklar – e’tibor talab qilmaydigan va major risklar – alohida e’tibor va kuzatuv talab qiluvchilarga ajratiladi.

Risk darajasi. Risk darajasi tarmoqga (yoki tizimga) natijaviy ta’sirning bahosi bo‘lib, quyidagi tenglik bilan ifodalanadi:

RISK darajasi= natija × ehtimollik

Risk darajalari 4 ta: ekstremal yuqori, yuqori, o‘rta va past.

Ekstremal yuqori yoki yuqori risk paydo bo‘lishini va salbiy ta’sirini kamaytirish maxsus yo‘naltirilgan qarshi choralarni talab etadi. Bu darajadagi risklar yuqori yoki o‘rtacha ta’sirning yuqori ehtimolligiga ega bo‘ladi. Mazkur

darajadagi risklar jiddiy xavfga sabab bo‘ladi va shuning uchun, zudlik bilan aniqlash hamda qarshi chora ko‘rish talab etiladi.

O‘rta darajali risklar yuqori ehtimollikka ega past natijali hodisa yoki past ehtimollikka ega yuqori natijali hodisa bo‘lishi mumkin. O‘rta darajali risklarga zudlik bilan chora ko‘rish talab etilmasada, himoyani dastlabki vaqtda o‘rnatish talab etiladi.

Past darajali risklar odatda e’tibor bermasa bo‘ladigan yoki keyingi baholashlarda e’tibor bersa bo‘ladigan risklar toifasi bo‘lib, ularni bartaraf etish qisqa muddatda amalga oshirilishni talab qilmaydi yoki ortiqcha sarf xarajatga sabab bo‘lmaydi.

Risk matritsasi risklarni paydo bo‘lish ehtimolini ularning natijasi va ta’siri orqali aniqlaydi hamda risk jiddiyligini va unga qarshi himoya chorasi sathini grafik taqdim etadi. Risk matritsasi riskning ortib boruvchi ko‘rinishi uchun foydalaniluvchi sodda jarayon bo‘lib, qarshi choralarni ko‘rishda yordam beradi. Risk matritsasi risklarni turli darajalarda aniqlash va jiddiylik nuqtai nazaridan guruhlash imkonini beradi. (5.4-jadval).

Yuqorida taqdim etilgan risk matritsasi risklarni vizual taqdim etish va o‘zaro taqqoslash imkonini beradi va undagi har bir yacheyka ehtimollik va oqibat kattaliklarining kombinasiyasidan iborat. Riskning jiddiyligi uning ehtimoli va ta’sir darajasiga bog‘liq. Keltirilgan risk matritsasida paydo bo‘lish ehtimoli bo‘yicha ular 5 ta guruhga ajratilgan. Shunga mos ravishda, risk oqibati ham 5 ta darajaga ajratilgan.

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

Risklarni boshqarish – risklarni aniqlash, baholash, javob berish va bo‘lishi mumkin bo‘lgan ta’sirga tashkilot tomonidan javob berilishini amalga oshirish jarayoni. Risklarni boshqarish xavfsizlikning hayotiy siklida o‘zining muhim o‘rniga ega, u davomiy va hattoki murakkablashib boruvchi jarayon hisoblanadi. Risklarni boshqarishdan asosiy maqsad quyidagilar:

- bo‘lishi mumkin bo‘lgan risklarni aniqlash;

- risk ta’sirini aniqlash va tashkilotlarga risklarni yaxshiroq boshqarish strategiyasi va rejasini ishlab chiqishga yordam berish;

- jiddiylik darajasiga asoslangan holda risklarni tasniflash va yordam berish uchun risklarni boshqarish usullari, vositalari va texnologiyalaridan foydalanish;

- risklarni tushunish, tahlillash va aniqlangan risk hodisalarini qaydlash;

- risklarni nazorat qilish va risk ta’siriga qarshi kurashish;

- xavfsizlik xodimlarini ogohlantirish va risklarni boshqarish strategiyasini ishlab chiqish.

Risklarni boshqarish ularni aniqlashda tizimlashgan yondashuvni ta’minlaydi va quyidagi afzalliklarga ega:

- bo‘lishi mumkin bo‘lgan risk ta’siri sohasiga e’tibor qaratadi;

- risklarni darajalari bo‘yicha manzillaydi;

- risklarni tutish jarayonini yaxshilaydi;

- kutilmagan holatlarda xavfsizlik xodimini samarali harakat qilishiga ko‘mak beradi;

- resurslardan samarali foydalanish imkonini beradi.

Risklarni boshqarishda muhim rollar va javobgarliklar. Risklarni boshqarishda rollar va javobgarliklar xodimlar o‘rtasida quyidagicha taqsimlangan:

Bosh boshqaruvchi. Bosh boshqaruvchi tashkilotda risklarni boshqarish jarayonini olib borishga rahbar hisoblanib, risklar paydo bo‘lganiga qadar ularni aniqlash uchun talab qilinadigan siyosat va usullarni ishlab chiqadi.

Tizim va axborot egalari. Tizim va axborot egalarining vazifasi, asosan, axborot tizimlari uchun ishlab chiqilgan rejalar va siyosatlarni monitoringlab borish bo‘lib, quyidagi javobgarliklarni o‘z ichiga oladi:

– sozlanishlarni boshqarish jarayoniga bog‘liq barcha muzokaralarda ishtirok etish;

– axborot texnologiyalari komponentlari qaydlarini saqlash;

– axborot tizimlarida barcha o‘zgarishlarni va ularning ta’sirlarini tadqiqlash;

– barcha tizimlar uchun xavfsizlik holati bo‘yicha hisobotlarni tayyorlash;

– axborot tizimlarini himoyalash uchun zarur bo‘lgan xavfsizlik nazoratini yangilab borish;

– doimiy ravishda xavfsizlikka oid hujjatlarni yangilab borish;

– mavjud xavfsizlik nazoratining samaradorligini taminlash bo‘yicha tekshirish va baholash.

Biznes va funksional menejerlar. Mazkur lavozim egalari tashkilotdagi barcha boshqaruv jarayonlarini madadlash uchun javobgar va bu vazifani bajarishlarida tashkilot rahbariyati tomonidan qo‘llab quvvatlanadi. Funksional menejeri turlari:

– rivojlantirish jamoasi menejeri;

– savdo menejeri;

– mijozlarga xizmat ko‘rsatuvchi menejer.

Xavfsizlik bo‘yicha murabbiy. Xavfsizlik bo‘yicha murabbiy tashkilotda tayyorgarlik va o‘quv kurslarini amalga oshiradi. Bu vazifaning, odatda, soha mutaxassislari tomonidan bajarilishi tavsiya etiladi.

Muhim risk ko‘rsatkichlari. Muhim risk ko‘rsatkichlari risklarni samarali boshqarish jarayonida asosiy tashkil etuvchi bo‘lib, dastlabki bosqichlarda harakatlarning xavflilik darajasini ko‘rsatadi. U tashkilotdagi risk ehtimolini ko‘rsatuvchi o‘lchov sifatida quyidagilarni amalga oshirishda yordam beradi:

- hodisa ta’sirini aniqlash;

- chegara qiymatda ogohlantirish;

- risk hodisalarini qayta ko‘rish.

Muhim risk ko‘rsatkichi aniqlik bilan hisoblanishi va tashkilotning amalga oshirish ko‘rsatkichlariga salbiy ta’sirlarni aks ettirishi kerak.

Risklarni boshqarish bosqichlari. Risklarni boshqarish uzluksiz jarayon va har bir bosqichning muvaffaqqiyatli amalga oshirilishi talab etiladi. U aniqlangan va faol ishlaydigan xavfsizlik dasturidan foydalangan holda xavfni maqbul darajada oldini oladi. Risklarni boshqarish jarayoni quyidagi asosiy to‘rtta bosqichga ajratiladi:

1. Risklarni aniqlash.

2. Risklarni baholash.

3. Risklarni bartaraf etish.

4. Risk monitoringi va qayta ko‘rib chiqish.

Har bir tashkilot risklarni boshqarish jarayonida yuqorida keltirilgan bosqichlarni bosib o‘tadi.

Risklarni aniqlash. Risklarni boshqarishdagi dastlabki qadam bo‘lib, uning asosiy maqsadi riskni tashkilotga zarar yetkazmasidan oldin aniqlash hisoblanadi. Risklarni aniqlash jarayoni mas’ul mutaxassislar qobiliyatiga bog‘liq bo‘lganligi tufayli, turli tashkilotlarda turlicha bo‘ladi. Risklarni aniqlash o‘zida tashkilot xavfsizligiga ta’sir qiluvchi ichki va tashqi risklarning manbasini, sabablarini, natijasini va h. aniqlashni mujassamlashtirgan. Risklar odatda quyidagi 4 ta muhim sohalarda vujudga keladi:

- *Muhit*. Muhitga aloqador bo‘lgan risklar o‘zida ish joyidagi kamchiliklar, turli halaqitlar, issiq/ sovuq muhit, tutun, past yoritilganlik va elektr xavflari kabilarni birlashtiradi.

- *Jihoz*. Jihozga aloqador risklar sifatida jihozlarning past ta’mirlanishi muhitini, ishlamasligini, mavjud bo‘lmasligini va vazifaga nomutanosibligini keltirish mumkin.

- *Mijoz*. Mijozlar bilan bog‘liq risklar odatda muhim o‘zgarishlar, kutilmagan ko‘chishlar va zaif aloqa natijasida yuzaga keladi.

- *Vazifalar*. Vazifalarga aloqador bo‘lgan risklarga yetarli bo‘lmagan bajarish vaqti, takroriy vazifalar, ishni loyihalash va xodimlar sonini yetarli bo‘lmasiligi orqali paydo bo‘luvchi risklar misol bo‘la oladi.

Riskni aniqlash risklarni boshqarish jarayonidagi turli og‘ishlarni kamaytiradi va bu, o‘z navbatida, kelajakda ta’sir qiluvchi omillar ehtimolini kamaytiradi. Aksariyat risklarni aniqlash jarayoni maxsus shakllantirilgan jamoa tomonidan amalga oshiriladi. Risklarni aniqlash jarayoni bir qancha omillarga, masalan, tarmoqning holati va jamoa a’zolarining risklarni boshqarishdagi qobiliyatlariga asoslanadi.

Risklarni baholash. Risklarni baholash bosqichida tashkilotdagi risklarga baho beriladi va bu risklarning ta’siri yoki yuzaga kelish ehtimoli hisoblanadi. Risklarni baholash - uzluksiz davom etuvchi jarayon riskka qarshi kurashish rejalarini amalga oshirish uchun imtiyozlarni belgilaydi. Risklarni baholash ularning miqdoriy va sifatiy qiymatini aniqlaydi. Har bir tashkilot risklarni aniqlash, darajalarga ajratish va yo‘q qilish uchun o‘zining riskni baholash jarayonini qabul qilishi kerak.

Risklarni baholash taqdim etilgan risk turini, riskning ehtimoli va miqdorini, uning darajasini hamda uni nazoratlash uchun rejani aniqlaydi. Tashkilotlar risklarni baholash jarayonini odatda xavf aniqlanganida va uni zudlik bilan nazoratlay olmaganlarida amalga oshiradilar. Riskni baholashdan so‘ng ma’lum vaqt mobaynida barcha axborot vositalarini yangilash talab etiladi.

Risklar baholanganidan so‘ng, ular tashkilotga keltiradigan miqdoriy zararga ko‘ra darajalanadi. Darajalarga ajratish risklarga qarshi kurashishga va resurslarni joylashtirishga yordam beradi. Taqdim etilgan risklarning darajalari ularning miqdoriga bog‘liq bo‘ladi:

– darajasi 1-2 ga teng bo‘lgan risklarni zudlik bilan bartaraf etish yoki bartaraf etish imkoni bo‘lmasa, nazorat harakatlari orqali uning xavflilik darajasini tushirish talab etiladi.

– darajasi 3-4 ga teng bo‘lgan risklarni qandaydir biror vaqt mobaynida bartaraf etish yoki xavfni nazoratga olish zarur hisoblanadi.

– darajasi 5-6 ga teng risklarni imkoni bor bo‘lgan vaqtda bartaraf etish yoki imkoni bo‘lmasa xavfni nazoratga olish zarur.

Risklarni baholash quyidagi ikki bosqichda amalga oshiriladi:

Riskni tahlillash: risk tabiatini aniqlash va uning paydo bo‘lishi darajasini hisoblash bosqichi, risklarni nazoratlashga yordam beradi.

Riskni darajalarga ajratish: risklarni tahlillash jarayonida ularning miqdoriy jihatdan reytingini aniqlash va qarshi choralarni loyihalash bosqichi.

Risklarni bartaraf etish. Risklarni bartaraf etish jarayoni aniqlangan risklarni modifikatsiyalash maqsadida mos nazoratni tanlash va amalga oshirishni ta’minlab, miqdoriy darajasi yuqori bo‘lganlariga birinchi murojaat qilinadi. Risklarni yo‘q qilishdan oldin quyidagi axborotni to‘plash talab etiladi:

- mos himoya usulini tanlash;
- himoya usuli uchun javobgar shaxsni tayinlash;
- himoya narxini inobatga olish;
- himoya usulining afzalligini asoslash;
- muvaffaqqiyatga erishish ehtimolini aniqlash;
- himoya usulini o‘lchash va baholash usulini aniqlash.

Agar aniqlangan risklarni bartaraf etish talab etilsa, risklarni boshqarish rejasini doimiy qayta ko‘rib chiqish va ishlab chiqish zarur bo‘ladi. Turli himoya usullari riskdan qochish, ularni kamaytirish va ular uchun javobgarliklarni boshqaga o‘tkazish kabi imkoniyatlarni taqdim etadi.

Xodimlardan risklarni kamaytirish yoki minimallashtirish uchun quyidagilarni amalga oshirishlari talab etiladi:

- risklarni nazoratlash rejasini ishlab chiqish;
- ko‘rsatilayotgan xizmatga risklarni ta’sirini aniqlash;
- risklarni nazoratlash rejasini tugallash uchun qat’iy cheklovlarni qo‘yish;
- risklarni nazoratlash strategiyasini amalga oshirish;
- risklarni nazoratlashda mijoz harakatini aniqlash;
-risklarni nazoratlash mobaynida madadlovchi xodimlar bilan aloqani o‘rnatish;

- risklarni nazoratlash jarayonining bir qismi risklarni nazoratlash rejasini to‘liq hujjatlashtirish.

Risk monitoringi va qayta ko‘rib chiqish. Samarali risklarni boshqarishning rejasi risklarni aniqlashni va baholashni kafolatli amalga oshirishda risk monitoringi va qayta ko‘rib chiqishni talab etadi. Risk monitoringi quyidagi imkoniyatlarni beradi:

- yangi risklarni paydo bo‘lish imkoniyatini aniqlaydi;

-riskni bartaraf etuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi;

- shuningdek, risk monitoringi riskning ehtimoli, ta’siri, holati va oshkor bo‘lishini o‘z ichiga oladi.

Riskni qayta ko‘rib chiqish:

- orqali amalga oshirilgan risklarni boshqarish strategiyasining samaradorligi baholanadi;

- yuqori ehtimollik risklardan ogoh bo‘lishni boshqarishni kafolatlaydi.

Tashkilotda risklarni boshqarishning freymworki (strukturasi) (Enterprise Risk Management Framework, ERM Framework). Risklarni boshqarish freymworki tashkilotning risklarni boshqarish usuliga amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo‘yicha faoliyatni birlashtiruvchi tarkibiy jarayonni ta’minlaydi.

Amalda tashkilotda risklarni boshqarish freymworklari sifatida NIST ERM, COSO ERM va COBIT ERM kabilardan keng foydalaniladi.

Risklarni boshqarishning axborot tizimlari (Risk Management Information Systems, RMIS). RMIS bu – boshqaruv axborot tizimi bo‘lib, axborotni saqlashni boshqarish, tahlillash va tashkilot tarmog‘i uchun risk to‘g‘risida ma’lumot olish imkoniyatini taqdim qiladi. Tashkilotlar risklarni boshqarish jarayonini optimallashtirish uchun RMIS bilan risklarni boshqarish freymworkini birlashtiradi. RMIS tizimlari quyidagi afzalliklarga ega:

- ma’lumot ortiqchaligi va xatoligini kamaytirish orqali ma’lumot ishonchligini yaxshilaydi;

- RMIS orqali xabarlar boshqaruvining yaxshilanishi natijasida tashkilotdagi xarajatlar kamayadi;

- RMIS, tashkilotning standartlariga muvofiq, risklarni boshqarish siyosatidan samarali foydalanishda yordam beradi.

RMIS turli omillar bo‘yicha hisobotlarni shakllantiradi va ushbu hisobotlar tashkilotda tarmoq risklari to‘g‘risida yaxlit tasavvurga ega bo‘lishga hamda ularni boshqarishga imkon beradi. RMIS quyidagi turdagi hisobotlarni shakllantiradi:

- *Standart hisobotlar*: yuborilgan umumiy so‘rovlarga javob sifatida standart hisobotlarni shakllantiradi. Ushbu hisobot guruhga ajratilgan ma’lumotlardan tashkil topmaydi.

- *Maxsus hisobotlar*: maxsus so‘rovlarga nisbatan turli guruhga tegishli ma’lumotlardan tashkil topgan maxsus javoblarni generatsiyalaydi.

Amalda RMIS tizimining turli ko‘rinishidagi vositalaridan keng foydalaniladi. Ularga misol sifatida, Aon Enterprise Risk Management, Stars RMIS, RiskEnvision, RiskonnectRMIS, INFORM, Traveler’s e-CARMA vositalarini keltirish mumkin.

Nazorat savollari

1. Kompyuter tarmog‘i va uning turlari.
2. Tarmoq topologiyasi va uning turlari.
3. Tarmoq qurilmalari va ularning asosiy vazifalari.
4. Tarmoq xavfsizligiga qaratilgan hujum turlari.
5. Razvedka hujumlarining asosiy maqsadi.
6. Zararli dasturiy vositalarga asoslangan hujumlarning asosiy maqsadi nima?
7. Tarmoqlararo ekran vositasining asosiy vazifasi.
8. Tarmoqlararo ekran vositalarining tasniflanishi.
9. VPN tarmoq va uning asosiy vazifasi.
10. VPN tarmoqni qurish usullari.
11. Risk matritsasi va uning asosiy vazifasini tushuntiring.
12. Risklarni boshqarish va uning asosiy bosqichlari.

6 BOB. FOYDALANUVCHANLIKNI TAMINLASH USULLARI

6.1. Foydalanuvchanlik tushunchasi va zaxira nusxalash

Foydalanuvchanlik. Kompyuter xavfsizligi axborot va axborot tizimlarini ruxsatsiz foydalanish, ochish, buzish, o‘zgartirish yoki yo‘q qilishdan himoya qilishni anglatib, uning eng muhim maqsadi axborot konfidensialligini, yaxlitligini va foydalanuvchanligini taminlashdir. Kompyuter tizimlaridan ma’lumotlarni saqlash va ishlash uchun foydalanilsa, xavfsizlikni nazoratlash vositalari ma’lumotlarning suiste’mol qilinishidan himoyalashda ishlatiladi. O‘z navbatida, axborot tizimlarining o‘z maqsadiga erishishiga imkon beruvchi foydalanuvchanlikni taminlash muhim hisoblanadi.

Foydalanuvchanlik tushunchasiga turli soha korxonalari va olimlar tomonidan turlicha ta’riflar keltirilgan, xususan:

- konfidensial ma’lumotlarga yoki manbalarga ehtiyoji bo‘lganlar uchun foydalanish imkonini berish;

- vakolatli foydalanuvchilarning ma’lumotlardan va axborot tizimlaridan o‘z vaqtida va ishonchli foydalanish imkoniyati;

- obyektlardan qonuniy foydalanish imkoniga ega vakolatli shaxslarning tizimga kirishiga to‘sqinlik qilmaslik;

- tizimlarning tezkor ishlashini va qonuniy foydalanuvchilarga rad etilmaslikni kafolatlash.

Hozirda barcha sohalarda axborot texnologiyalarining keng joriy qilinishi tashkilot yoki korxonalar faoliyatini yuritishda muhim ahamiyat kasb etayotgan bo‘lsada, tashkilotda axborot tizimlari bilan bog‘liq muammo kuzatilsa, uning faoliyati katta yo‘qotishlarga duch kelishi mumkin. Faraz qilaylik, xosting provayderlarida xizmat ko‘rsatishda 99% foydalanuvchanlik ta’minlangan bo‘lsin. Bu qiymat ko‘rinishdan katta bo‘lsada, bir yilda 87 soat (3.62 kun) xizmat ko‘rsatilmaganligini anglatadi. Bu vaqt ichida tashkilot, xizmat ko‘rsatish hajmiga bog‘liq, turlicha zarar ko‘rgan bo‘lishi mumkin. Yuqoridagi holda, hattoki 99.9% xizmat ko‘rsatishda foydalanuvchanlikka erishilgan bo‘lsada, yiliga 9 soat yo‘qotish kuzatiladi.

Xizmat ko‘rsatishdagi mazkur zararlarni kamaytirish nafaqat Facebook yoki Amazon kabi yirik korporasiyalar uchun, balki barcha tashkilotlar uchun ham muhim hisoblanadi.

Foydalanuvchanlik o‘zida quyidagi 3 ta omilni birlashtiradi:

- xatolarga bardoshlilik: bu omil tizimda xatolik kuzatilgan taqdirda ham ishlamay qolmaslik shartini ko‘rsatadi;

- taqdim etilayotgan xizmatlarning kafolati: xizmatlar, shuningdek, tizimlar ham har doim mavjud bo‘lishi kerak;

- ma’lumotlar xavfsizligi: infrastruktura tarkibidagi ma’lumotlar yaxlitligi, undagi jarayonlar va xodimlar ishlamay qolgan taqdirda ham ta’minlanishi shart.

Yuqori darajadagi foydalanuvchanlik o‘zida birorta ham xatolikni qamrab olmaydi. Boshqacha aytganda, hosting provayderlarining yuqori foydalanuvchanlikni taminlashi uchun o‘zidagi biror tarmoq qurilmasi (masalan, marshrutizator yoki tarmoqlararo ekran) ishlamay qolishini oldini olish talab etiladi.

Tizim yoki xizmat foydalanuvchanligini buzilishiga olib keluvchi hujum – xizmat ko‘rsatishdan voz kechishga undash (DoS) hujumi hisoblanib, mazkur hujumning asosiy maqsadi tizim yoki tarmoqni qonuniy foydalanuvchilar uchun xizmat ko‘rsatishini to‘xtatishidan iborat. Ushbu hujum turli usul va vositalardan foydalanilib, turli tizim va muhit xususiyati asosida amalga oshiriladi.

Xizmat ko‘rsatishdan voz kechishga undash hujumini oldini olish va foydalanuvchanlikni taminlash uchun kompleks himoya choralarini ko‘rish tavsiya etiladi.

Zaxira nusxalash. Hozirgi kunda ma’lumotlarning yo‘qolishi tashkilotlar uchun asosiy xavfsizlik muammolaridan biri bo‘lib, buning natijasida tashkilot katta zarar ko‘rishi mumkin.

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

− zarar yetkazilganidan so‘ng tizimni normal ish holatiga qaytarish;

− tizimda saqlanuvchi muhim ma’lumotlarni yo‘qolganidan so‘ng uni qayta tiklash.

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

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

- Inson xatosi: qasddan yoki tasodifan ma’lumotlarning o‘chirib yuborilishi, ma’lumotlarni saqlash vositasini to‘g‘ri joylashtirilmaganligi yoki ma’lumotlar bazasini xatolik bilan boshqarilganligi.

- G‘arazli hatti-harakatlar: tashkilotdagi muhim ma’lumotlarning modifikatsiyalanishi yoki o‘g‘irlanishi.

- Tabiiy sabablar: energiyaning o‘chishi, dasturiy ta’minotning tasodifiy o‘zgarishi yoki qurilmaning zararlanishi.

- Tabiy ofatlar: zilzila, yong‘in va h.

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

- muhim ma’lumotlardan yo‘qolgan va zararlangan taqdirda ham foydalanish;

- tashkilotlarni o‘z faoliyatining to‘xtatilishidan himoyalash va ma’lumotlarni ixtiyoriy vaqtda tiklash;

- tashkilotdagi yo‘qolgan ma’lumotlarni tiklash.

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

- ma’lumotlarni zaxira nusxalash strategiyasi ixtiyoriy tashqi qurilmalardan ma’lumotlarni tiklash imkoniyatiga ega bo‘lishi shart. Ushbu qurilmalarga misol sifatida serverlar, host mashinalar, noutbuklar va boshqalarni ko‘rsatish mumkin.

- agar tabiiy ofat natijasida ma’lumot yo‘qolsa, zaxira nusxalash strategiyasi faqat chekli sondagi insidentlarga qarshi himoya bilan cheklanmasligi zarur. Tabiiy ofat yuz bergan taqdirda ham strategiya o‘zida ma’lumotlarni tiklash usullarini mujassamlashtirishi shart;

- strategiya dastlabki bosqichlarda ma’lumotlarni qayta tiklash uchun muhim qadamlardan iborat bo‘lishi kerak;

- zaxira nusxalash narxining qimmat bo‘lmasligi tashkilot uchun moliyaviy madad hisoblanadi;

- inson tomonidan bo‘lishi mumkin bo‘lgan xatoliklarni tezlik bilan oldini olish uchun ma’lumotlarni zaxira nusxalash avtomatik tarzda amalga oshirilishi kerak.

Tashkilotlarda zaxira nusxalarni saqlovchilarni tanlash umumiy muammolardan biri hisoblanib, mos bo‘lmagan zaxira saqlovchi vositaning tanlanishi ma’lumotlarning sirqib chiqishiga olib kelishi mumkin.

Hozirda ma’lumotlarni zaxira nusxalarini saqlashda quyidagi vositalardan foydalanilmoqda:

Optik disklar (DVD, Blu-ray). DVD disklar 8.55 GBaytgacha ma’lumotlarni saqlash imkoniyatiga ega bo‘lib, ularda faqat o‘qish imkoniyati mavjud.

Ko‘chma qattiq disklar/ USB xotiralar. Ko‘chma qattiq disklar DVD, Blu-ray disklarga qaraganda kichikroq hajmli zaxira ma’lumotlarini saqlash uchun yaxshi vosita hisoblanadi.

Lentali disklar. Lentali disklar ma’lumotlarni zaxira saqlash uchun eng mos saqlagichlar bo‘lib, tashkilot sathida ma’lumotni zaxira nusxalashni amalga oshiradi. Ushbu zaxira saqlagichi olib yurish uchun qulay, foydalanuvchi ishtirokini talab etmaydi va to‘liq avtomatlashgan tarzda amalga oshiriladi. Uning asosiy kamchiligi oddiy foydalanuvchilar uchun qimmatligi va oddiy kompyuterlardan foydalanishi uchun qo‘shimcha apparat va dasturiy vositani talab qilishi.

6.2. Ma’lumotlarni zaxiralash texnologiyalari va usullari

Aksariyat tashkilotlar muhim ma’lumotlarini RAID texnologiyasi asosida zaxira nusxalashni amalga oshiradilar. RAID texnologiyasida ma’lumotlar bir qancha disklarning turli sohalarida saqlangani bois, IO (kirish/ chiqish) amallarining bajarilishi osonlashadi. RAID texnologiyasi ko‘plab qattiq disklarni bitta mantiqiy disk sifatida o‘rnatish orqali ishlaydi. Ushbu texnologiya odatda serverlarda ma’lumotlarni saqlashga mo‘ljallangan, shaxsiy kompyuterlardan foydalanish zaruriyati mavjud emas.

RAID texnologiyasida amallarni samarali bajarish uchun 6 ta sath mavjud: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10 va RAID 50.

RAIDning har bir sathi quyidagi xususiyatlarga ega:

- xatoga bardoshlilik: agar biror disk ishlashdan to‘xtasa, boshqa disklar normal ishlashini davom ettiradi;

- unumdorlik: RAID ko‘plab disklar bo‘ylab o‘qish va yozishda yuqori unumdorlik darajasiga ega.

Disklarning ma’lumotlarni saqlash imkoniyati mos RAID sathini tanlashga asoslanadi. Saqlash hajmi individual RAID disklar o‘lchamining bir xil bo‘lishini talab etmaydi. Barcha RAID sathlari quyidagi saqlash usullariga asoslanadi:

- bloklash: ma’lumotlar ko‘plab bloklarga ajratiladi. Mazkur bloklar keyinchalik RAID tizimi orqali yoziladi. Bloklash ma’lumotlarni saqlanishini yaxshilaydi.

- akslantirish: akslantirish ma’lumotlarning nusxalanishini va RAID bo‘ylab uzluksiz saqlanishini amalga oshiradi. Bu usul xatoga bardoshli va amalga oshirilishining yuqori darajasiga ega.

- nazorat qiymati: nazorat qiymati ma’lumotlar bloki yaxlitligini tekshirish funksiyasini amalga oshirishda bloklash funksiyasidan foydalanadi. Disk buzilganida nazorat qiymati xatolikni tuzatish funksiyasi yordamida ma’lumotlarni tiklashga harakat qiladi.

RAID tizimlari sathga bog‘liq holda o‘ziga xos afzalliklar va kamchiliklarga ega.

RAID tizimlarining afzalliklari. *Unumdorlik va ishonchlilik*: RAID texnologiyasi disklarda ma’lumotlarni o‘qish va yozish unumdorligini oshiradi. Ushbu texnologiya IO jarayonini taqsimlash orqali unumdorlikni yaxshilaydi va jarayon tezligi, yagona diskda ma’lumotlarni saqlashga qaraganda, yuqori bo‘ladi.

Xatolikni nazoratlash: buzilgan diskda saqlangan ma’lumotlarni qolgan diskdagi ma’lumotlar bilan taqqoslash orqali ularni tiklashni yoki tuzatishni amalga oshiradi.

Ma’lumotlar ortiqchaligi (ma’lumotlarni nusxalash): diskning buzilishi istalgan vaqtda yuzaga kelishi mumkin. RAID texnologiyasi qurilma buzilganida ma’lumotlarni nusxalash orqali uning qayta tiklanishini ta’minlaydi.

Disklarni navbatlanishi: ma’lumotlarni o‘qish/ yozish unumdorligini oshiradi. Ma’lumotlar kichik bo‘laklarga bo‘linib, bir qancha disklar bo‘ylab tarqatiladi. RAID tizimida ma’lumotlarni o‘qish va yozish bir vaqtda bajariladi.

Tizimning ishlash davomiyligi: ushbu o‘lchov kompyuterning ishonchligini va barqarorligini belgilaydi. Tizimning ishlash davomiyligi tizimning avtomatik ishlash vaqtini belgilaydi.

RAID tizimlarining kamchiliklari. *Tarmoq drayverlarini yozish*: RAID texnologiyasi asosan serverlarda foydalanish uchun loyihalangani bois, uning asosiy kamchiligi - barcha tarmoq drayverlarini yozish.

Mos kelmaslik: tizimlar turli RAID drayverlarini madadlaydi. Muayyan apparat yoki dasturiy komponent serverda sozlangan RAID tizimi bilan mos kelmasligi mumkin. Mos kelmaslik RAID tizimining o‘z vazifasini to‘g‘ri amalga oshirilmasligiga olib kelishi mumkin.

Ma’lumotlarning yo‘qolishi: RAID drayverlari mexanik muammolar tufayli o‘z funksiyalarini bajara olmasliklari mumkin. Disklar ketma-ket buzilishga uchraganida ma’lumotlarning yo‘qolishi xavfi ortadi.

Qayta tiklashning uzoq vaqti: katta hajmli disklardan foydalanish ma’lumotlarni uzatish tezligini ortishiga olib keladi. Biroq, katta hajmli disklarda ma’lumotlarni tiklash va buzilgan disklarni qayta sozlash uzoq vaqt talab etadi.

Narxining yuqoriligi: RAID texnologiyasini amalga oshirish iqtisodiy jihatdan katta mablag‘ni talab etadi. Bundan tashqari, tizim ishini yaxshilash uchun qo‘shimcha RAID kontrollerlarini va qurilma drayverlarini sotib olish talab etiladi.

Mos RAID sathini tanlash tashkilot zaruriyatidan kelib chiqqan holda va har bir sathning taqdim qilayotgan imkoniyatlariga asoslanishi zarur. RAID sathini tanlashda ularni xususiyatlariga ham e’tibor berish talab etiladi (6.1-jadval).

6.1-jadval

RAID texnologiyalarining tahlili

RAID	Diskdan foydalanish	Buzilishga bardoshligi	Katta ma’lumotlar transferi	IO darajasi	Ma’lumot foydalanuvchanligi	Asosiy kamchiligi
Yagona disk	Bir xil 100%	Yo‘q	Yaxshi	Yaxshi	Yagona diskning MTBF davri	Disk buzilsa, ma’lumot yo‘qoladi
RAID 0	A’lo 100%	Ha	Juda yaxshi	Juda yaxshi	Diskning past MTBF davri	
RAID 1	O‘rtacha 50%	Ha	Yaxshi	Yaxshi	Yaxshi	Disk hajmidan 2 marta kam foydalanish
RAID 3	Yaxshi-juda yaxshi	Ha	Juda yaxshi	Yaxshi	Yaxshi	Disk buzilsa, ma’lumot yo‘qoladi
RAID 5	Yaxshi-juda yaxshi	Ha	Yaxshi-juda yaxshi	Yaxshi	Yaxshi	Disk buzilsa, kam o‘tkazuvchanlik
RAID 0+1	O‘rtacha 50%	Ha	Yaxshi	Juda yaxshi	Yaxshi	Disk hajmidan 2 marta kam foydalanish
RAID 1+0	O‘rtacha 50%	Ha	Juda yaxshi	Juda yaxshi	Juda yaxshi	Juda qimmat, keng ko‘lamli emas
RAID 30	Yaxshi-juda yaxshi	Ha	Juda yaxshi	A’lo	A’lo	Juda qimmat
RAID 50	Yaxshi-juda yaxshi	Ha	Yaxshi-juda yaxshi	A’lo	A’lo	Juda qimmat

Izoh: MTBF – Mean Time Between Failures (buzilishlar o‘rtasidagi o‘rtacha vaqt).

Zaxira nusxalash usullari. Tashkilot o‘zining moliyaviy imkoniyati va AT infrastrukturasi asosida zaxira nusxalash usulini tanlaydi. Ma’lumotlarni zaxira nusxalashning quyidagi usullari mavjud.

Issiq zaxiralash. Ma’lumotlarni zaxira nusxalashning mazkur usuli amalda keng qo‘llaniladi va dinamik yoki aktiv zaxira nusxalash usuli deb ham ataladi. Ushbu usulga binoan foydalanuvchi tizimni boshqarayotgan vaqtida zaxira nusxalash jarayonini ham amalga oshirishi mumkin. Mazkur zaxiralash usulini

amalga oshirish tizimning harakatsiz vaqtini kamaytiradi. Zaxiralash davomida ma’lumotlardagi o‘zgarish yakuniy zaxira nusxasiga ta’sir qilmaydi. Ravshanki, zaxiralashni amalga oshirish vaqtida tizimning ishlash jarayoni sekinlashadi.

Sovuq zaxiralash. Ushbu zaxiralash usuli offlayn zaxiralash deb ham atalib, tizim ishlamay turganida yoki foydalanuvchi tomonidan boshqarilmagan vaqtda amalga oshiriladi. Ushbu usul zaxiralashning xavfsiz usuli bo‘lib, ma’lumotlarni nusxalashda turli tahdidlardan himoyalaydi.

Iliq zaxiralash. Ushbu zaxiralashda tizim muntazam yangilanishni amalga oshirish uchun tarmoqqa bog‘lanishi kerak bo‘ladi. Bu ma’lumotlarni akslantirish yoki nusxalash hollarida muhim hisoblanadi. Zaxira nusxalashda ma’lumotlarni saqlash manzilini tanlash muhim hisoblanadi. Zaxira nusxalarni quyidagi manzillarda saqlash mumkin.

Ichki (onsite) zaxiralash. Ushbu zaxiralash usuli tashkilot ichida amalga oshirilib, tashqi qurilmalar, lentali saqlagichlar, DVD, qattiq disk va boshqa saqlagichlardan foydalaniladi. Ichki zaxiralash qurilmalari zaxira saqlanuvchi ma’lumotlar hajmiga muvofiq tanlanadi.

Tashqi (offsite) zaxiralash. Tashqi zaxiralash mosofadagi manzilda amalga oshirilib, fizik disklarda ma’lumotlarni saqlash onlayn yoki uchinchi tomon xizmati orqali amalga oshirilishi mumkin.

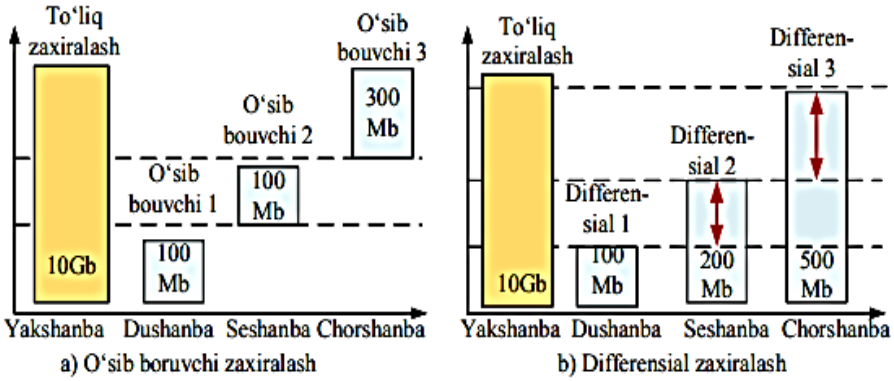
Bulutli tizimda zaxiralash. Ushbu zaxiralash usuli onlayn usuli deb ham ataladi. U zaxiralangan ma’lumotlarni ochiq tarmoqda yoki ma’lum serverda saqlaydi. Odatda ma’lum server vazifasini uchinchi tomon xizmati amalga oshirishi mumkin.

Zaxiralash turlari. Mos zaxiralash turi tarmoqqa ortiqcha yuklama qo‘shmaydi hamda narx, vaqt va resursni kam talab qiladi. Amalda uchta turdagi zaxiralash turlari mavjud: to‘liq, differensial va o‘sib boruvchi.

To‘liq zaxiralash: ushbu usul normal zaxiralash deb ham atalib, jadvalga ko‘ra avtomatik tarzda amalga oshiriladi. Bunda, barcha fayllar nusxalanadi va zichlangan tarzda saqlanadi. Ushbu usul nusxalangan ma’lumotlar uchun samarali himoyani ta’minlaydi.

O‘sib boruvchi zaxiralash: ushbu usulga ko‘ra zaxiralanuvchi ma’lumotlarga nisbatan o‘zgarish yuz berganida zaxiralash amalga oshiriladi. Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usulidan foydalanish mumkin. Shuning uchun, o‘sib boruvchi zaxiralashni amalga oshirishdan oldin, tizim to‘liq zaxiralashni amalga oshirishi shart.

Faraz qilaylik, zaxira nusxalash jadvaliga ko‘ra to‘liq zaxiralash yakshanba kuniga, ortib boruvchi zaxiralash esa seshanbadan shanbagacha amalga oshirilishi belgilangan bo‘lsin. Yakshanba kuni to‘liq zaxiralash amalga oshirilganidan so‘ng, dushanba kunidagi o‘zgarishlar seshanba kuni o‘sib boruvchi usul asosida amalga oshiriladi. Ushbu jarayoni shanbagacha davom ettiriladi (6.1 – rasm “a”)



6.1-rasm. Zaxiralash turlari

Differensial zaxiralash: ushbu zaxiralash usuli to‘liq va o‘sib boruvchi usullarning mujassamlashgan ko‘rinishi bo‘lib, oxirgi zaxiralangan nusxadan boshlab bo‘lgan o‘zgarishlarni zaxira nusxalash amalga oshiriladi.

Masalan, yuqoridagi misolni qaraylik. To‘liq zaxiralash yakshanba kuni, differensial nusxalash esa shanbagacha amalga oshirilishi jadvalda keltirilgan bo‘lsin. Yakshanba kuni to‘liq zaxira nusxalash amalga oshirilganidan so‘ng, dushanba kuni differensial zaxiralash kun o‘tishi bilan amalga oshiriladi. Bu holat o‘sib boruvchi zaxiralashga o‘xshab ketadi. Biroq, seshanbada, zaxira nusxalash yakshanba va dushanbadagi o‘zgarishlar uchun amalga oshiriladi. Shundan so‘ng, chorshanbada zaxiralash yakshanba, dushanba va seshanba kunlari uchun amalga oshiriladi (6.1 – rasm “b”).

6.3. Ma’lumotlarni qayta tiklash va hodisalarni qaydlash

Ma’lumotlarni qayta tiklash. Ma’lumotlarning yo‘qolishi har qanday tashkilot uchun jiddiy muammo hisoblanadi. Shu sababli, ma’lumotlarni qayta tiklash usullaridan foydalanish talab etiladi. Ushbu jarayon ma’lumotlarning qanday yo‘qolganiga, ma’lumotlarni qayta tiklash dasturiy vositasiga va ma’lumotlarni tiklash manziliga bog‘liq.

Ma’lumotlarni eltish vositalarida, USB xotirada, qattiq diskda, DVD va boshqa saqlagichlarda ma’lumotlarni qayta tiklash mumkin. Qayta tiklash jarayonining muvaffaqqiyatli amalga oshirilishi foydalanuvchining malakasiga bog‘liq. Ma’lumotlarni qayta tiklash jarayonida bilim va to‘g‘ri tanlangan vosita muhim hisoblanadi.

Ma’lumotlarni qayta tiklash har doim ham muvaffaqiyatli bo‘lmasligi mumkin. Agar saqlagichda xatolik mavjud bo‘lsa yoki unga ko‘p zarar yetgan bo‘lsa, ma’lumotlarni tiklashning imkoni bo‘lmasligi mumkin. Ma’lumotlarning qayta tiklanishi ehtimoli ularning yo‘qolishi sababiga bog‘liq. Ma’lumotlarni yo‘qolishiga sabab bo‘luvchi hollar quyidagilar:

Faylni o‘chirish: agar fayl o‘chirilsa, ushbu soha qaytadan yozilgunga qadar saqlagichda mavjud bo‘ladi. Ma’lumotlar saqlangan sohadagi kichik xotiraga ma’lumotlar yozilishi butun ma’lumotlarni tiklanmasligiga sababchi bo‘lishi mumkin.

Faylning zararlanishi: agar OT zararlansa, ma’lumotlarni diskning qismlar jadvali yordamida tiklash mumkin. Agar diskning qismlar jadvali ham zararlangan bo‘lsa, qayta tiklashning maxsus vositalaridan foydalanishga to‘g‘ri keladi.

Qattiq diskning fizik zararlanishi: qattiq diskka fizik ta’sir bo‘lishi , faylni zararlanishiga qaraganda, katta yo‘qotishlarga sabab bo‘lishi mumkin. Bu esa ma’lumotlarni qayta tiklashning maxsus sathidan foydalanishni talab etadi. ***Ma’lumotlarni qayta tiklashda quyidagilarni esda saqlash zarur***:

- ma’lumotlar yo‘qolgan qattiq diskga qayta tiklangan ma’lumotlarni yozmaslik;

- turli zaxira nusxalarni amalga oshirish va ularni turli manzillarda saqlash;

- ma’lumotlarni qayta tiklash har doim ham 100% samara bermasligi.

Amalda saqlagichlardagi yo‘qolgan ma’lumotlarni tiklashda maxsus dasturiy vositalardan foydalaniladi. Ularga Recovery My Files, EASEUS Data Recovery Wizard, Advanced Disk Recovery, Handy Recovery, R-Studio, Data Recovery Pro, Recuva, Total Recall, Pandora Recovery kabilarni misol sifatida keltirish mumkin.

Hodisalarni qaydlash. Xatolik yuz berganida, tizim ma’muri yoki madadlash xodimi xatoning sababini aniqlashi, yo‘qolgan ma’lumotlarni qayta tiklashga urinishi va xatoning takrorlanishiga yo‘l qo‘ymasligi lozim. Ilovalar, operatsion tizim va boshqa tizim xizmatlari muhim voqealarni, masalan, xotira hajmining kamligi yoki diskdan foydalanishga haddan tashqari ko‘p urinishlarni qayd etishi muhim hisoblanadi. Keyinchalik tizim ma’muri xato sababini aniqlashi va u sodir bo‘lgan kontekstni aniqlash uchun hodisalar jurnalidan (log fayl deb ataladi) foydalanishi mumkin.

Hodisalarni qaydlash quyidagilarni o‘z ichiga olishi shart:

operatsion tizim hodisalari:

– tizimni ishga tushirish va o‘chirish;

– xizmatni boshlash va tugatish;

– tarmoq ulanishidagi o‘zgarishlar yoki muvaffaqiyatsizliklar;

– tizim xavfsizligini sozlash va boshqarish vositalarini o‘zgartirishga urinishlar.

OT audit yozuvlari:

– tizimga kirishdagi urinishlar (muvaffaqiyatli yoki muvaffaqiyatsiz);

– tizimga kirgandan so‘ng bajariladigan funksiyalar (masalan, muhim faylni o‘qish yoki yangilash, dasturni o‘rnatish);

– qayd yozuvini o‘zgartirish (masalan, yozuvni yaratish va yo‘q qilish, imtiyozlarni tayinlash);

– imtiyozli qayd yozuvidan muvaffaqiyatli / muvaffaqiyatsiz foydalanish. ilova qayd yozuvi to‘g‘risidagi ma’lumot:

– ilovani muvaffaqiyatli va muvaffaqiyatsiz autentifikatsiya qilishga urinishlar;

– hisob qaydnomasidagi o‘zgartirishlar (masalan, qayd yozuvini yaratish va yo‘q qilish, qayd yozuvi imtiyozlarini tayinlash);

– dastur imtiyozlaridan foydalanish.

ilova amallari:

– dasturni ishga tushirish va o‘chirish;

– dastur xatolari;

– dastur konfigurasiyasidagi asosiy o‘zgarishlar.

Har bir hodisa uchun qaydlangan tafsilotlar farqlanadi, ularni quyidagi parametrlar bo‘yicha qaydlash tavsiya qilinadi:

– vaqt belgisi;

– hodisa, holat va / yoki xatolik kodlari;

– servic / buyruq / ilova nomi;

– foydalanuvchi yoki tizim bilan bog‘liq voqea;

– amaldagi qurilma (masalan, IP va manba manzili, terminal sessiyasi identifikatori, web brauzer va h.).

Audit jurnallarida barcha harakatlar qaydlangani bois, niyatibuzuqlar ularni tahrirlash orqali o‘z faoliyatini yashirishi mumkin. Shuning uchun, audit jurnalidan foydalanishlarni nazoratlash muhim vazifa hisoblanadi.

Windows OTda hodisa turlari. Windows OTda besh turdagi hodisa ro‘yxatga olinadi. Bularning barchasi uchun aniq belgilangan ma’lumotlar mavjud bo‘lib, biror bir hodisa haqidagi xabar faqat bitta turga tegishli bo‘ladi (6.2-jadval).

6.2-jadval

Windows OT hodisalari turlari

Hodisa	Tavsifi
1	2
Xatolik	Ma'lumotlarni yoki funksionallikni yo'qotish kabi muhim muammoni ko'rsatadigan hodisa. Masalan, biror xizmat ishga tushirishi paytida yuklanmasa, mazkur xatolik hodisasi qayd etiladi.
Ogohlantirish	Hodisa juda ahamiyatli bo'lmasada, kelajakda yuzaga kelishi mumkin bo'lgan muammolarni ko'rsatishi mumkin. Masalan, diskda bo'sh joy kam bo'lsa, ogohlantirish hodisasi qayd etiladi.
Axborot	Ilova, drayver yoki xizmatning muvaffaqiyatli ishlashini tavsiflaydigan hodisa. Masalan, tarmoq drayveri muvaffaqiyatli yuklanganida, hodisalarni axborot qaydlaydi.
1	**2**
Muvaffaqiyatli audit	Muvaffaqiyatli tekshirilgan xavfsizlikka oid kirish urinishlarini yozib boradigan hodisa. Masalan, foydalanuvchining tizimga kirishga muvaffaqiyatli urinishi muvaffaqiyatli audit hodisasi sifatida qaydlanadi.
Muvaffaqiyatsiz audit	Tekshirilgan xavfsizlikdan foydalanishga urinish muvaffaqiyatsiz tugaganida, bu hodisa qaydlanadi. Masalan, agar foydalanuvchi tarmoq drayveriga kirishida muvaffaqiyatsizlikka uchrasa, bu hodisa qaydlanadi.

Quyidagi hodisalar qaydlanishi shart. Xotirani ajratishda xatolik yuz bergan taqdirda ogohlantirish hodisasini qaydlash kam xotirali vaziyatning sababini ko'rsatishga yordam beradi.

Uskuna bilan bog'liq muammolar. Tarmoq kartasi, qattiq disk, tezkor xotira va boshqa qurilma drayveri bilan bog'liq hodisalar qaydlanishi shart.

Axborot hodisalari. Server dasturi (masalan, ma'lumotlar bazasi serveri) foydalanuvchining ro'yxatdan o'tkazilishi, ma'lumotlar bazasidagi amallar va boshqa hodisalar qaydlanishi shart.

Windows XP/2000 operatsion tizimlarda hodisalarni qaydlash jurnalida turli qayd yozuvlari uchun berilgan imtiyozlar mavjud (6.3-jadval).

6.3-jadval

Windows XP/2000 operatsion tizimda hodisa jurnalida mavjud imtiyozlar

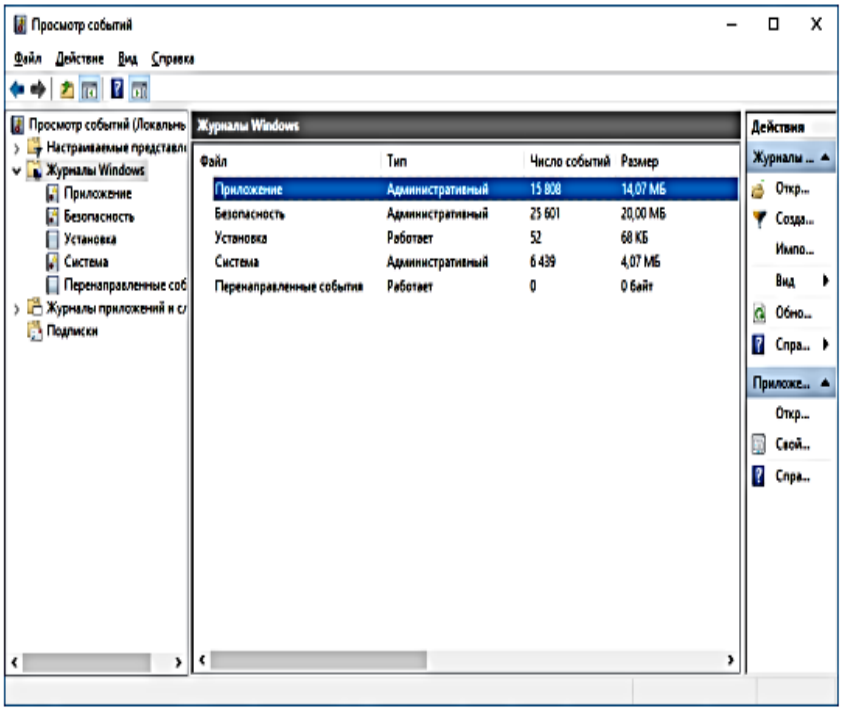
Log	Qayd yozuvi	O‘qish	Yozish	Tozalash
Ilovaga tegishli	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-
Tizimga tegishli	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	-	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	-	-
Tanlovga ko‘ra yaratilgan log fayl	Ma’murlar (tizim)	+	+	+
	Ma’murlar (domen)	+	+	+
	Lokal tizim	+	+	+
	Interaktiv foydalanuvchi	+	+	-

Windows OT da hodisalarni qaydlash fayllarini (log faylni) ko‘rish uchun quyidagi ketma-ketlik amalga oshiriladi:

1. Kompyuterda Win+R tugmalar kombinatsiyasi bosiladi.

2. Hosil bo‘lgan oynadagi maydonda eventvwr kiritiladi va Enter tugmasi bosiladi.

3. Hosil bo‘lgan hodisalarni ko‘rish oynasidan Windows Logs bandi tanlanadi (6.2-rasm).



6.2-rasm. Windows OTning hodisalar jurnali oynasi

Nazorat savollari

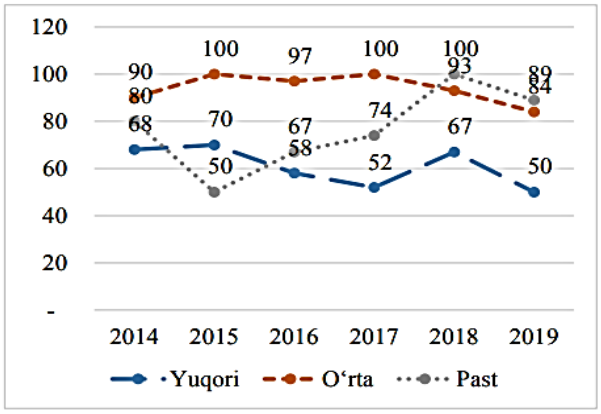
1. Foydalanuvchanlik tushunchasi va uning tizim uchun muhimligi.
2. Zaxira nusxalash va uning turlari.
3. Ma’lumotlarni yo‘qolishiga olib keluvchi asosiy sabablar.
4. Zaxira nusxalashda bajariluvchi vazifalar ketma-ketligi.
5. Zaxira nusxalarni saqlovchi vositalar va ularning xususiyatlari.
6. RAID texnologiyasi va uning asosiy xususiyatlari.
7. Zaxiralash turlari va ularning afzalliklari va kamchiliklari.

7 BOB. DASTURIY VOSITALAR XAVFSIZLIGI

7.1. Dasturiy vositalardagi xavfsizlik muammolari

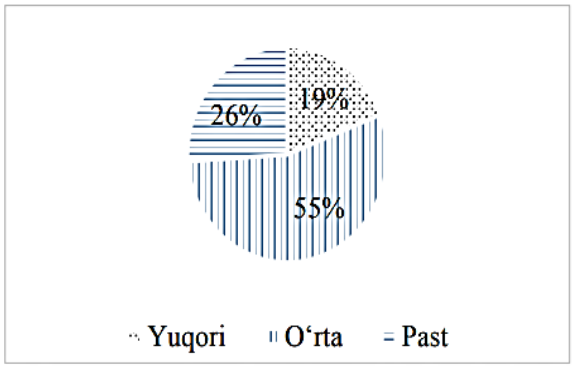
Hozirda dasturiy vositalar xavfsizligi axborot xavfsizligining kriptografiya, foydalanishni nazoratlash va xavfsizlik protokollari kabi muhim sohalardan hisoblanadi. Bunga sabab - axborotning virtual xavfsizligi dasturiy vositalar orqali amalga oshirilishi. Dasturiy vosita tahdidga uchragan taqdirda xavfsizlik mexanizmi ham ishdan chiqadi.

So‘nggi yillarda ushbu zaiflik muammolarining soni va jiddiylik darajasi ortib bormoqda. Xususan, 7.1-rasmda Positive Technologies tashkiloti tomonidan veb-saytlardagi turli darajadagi zaifliklarni yillar bo‘yicha ortib borishi keltirilgan.



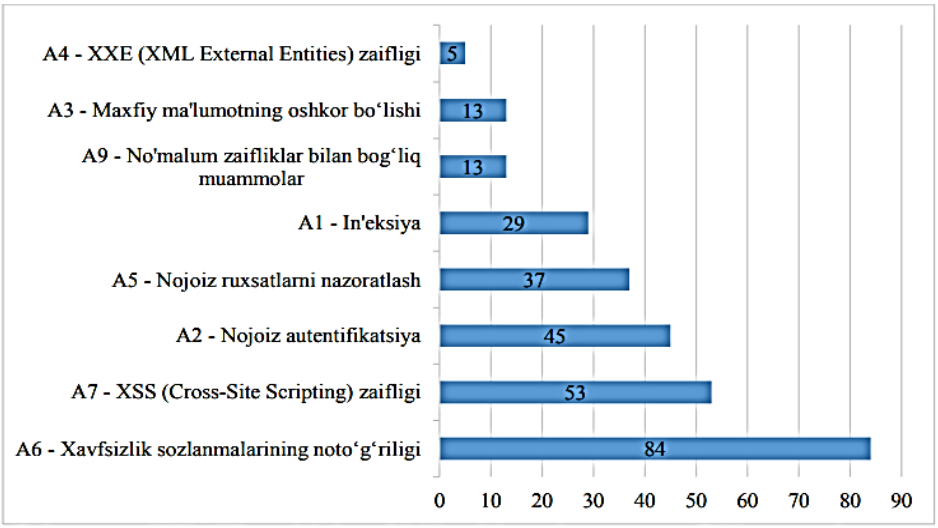
7.1-rasm. Turli darajadagi zaifliklarga ega Web-saytlar soni

2019 yilda aniqlangan web-saytlardagi muammolarning jiddiyligi bo‘yicha taqsimoti 7.2-rasmda keltirilgan.



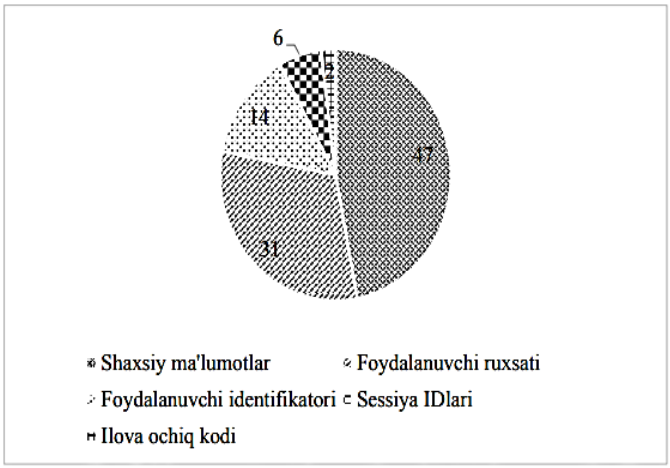
7.2-rasm. Web-sayt muammolarining jiddiyligi bo‘yicha taqsimoti

2019 yilda veb-saytlarda keng tarqalgan zaifliklar va ularning ulushi, OWASP (Open Web Application Security Project) tomonidan berilgan ma’lumotga ko‘ra, quyidagicha bo‘lgan (7.3-rasm).



7.3-rasm. OWASP tashkiloti 2019 yilda uchragan zaifliklar va ularning ulushi

Yuqorida keltirilgan zaifliklar natijasida turli ma'lumotlarni hujumchilar tomonidan qo'lga kiritish maqsad qilingan (7.4-rasm).



7.4-rasm. Zaifliklar natijasida qo'lga kiritishga mo'ljallangan ma'lumotlar

Dasturiy vositalardagi mavjud tahdidlar, odatda, dasturlash tillari imkoniyatlari bilan belgilanadi. Masalan, nisbatan quyi dasturlash tillari dasturchidan yuqori malakani talab etgani bois, ularda ko'plab xavfsizlik muammolari paydo bo'ladi. C# va Java dasturlash tillarida ko'plab muammolar avtomatik tarzda kompilyasiya jarayonida aniqlanganligi sababli, C yoki C++ dasturlash tillariga nisbatan, xavfsiz hisoblanadi.

Odatda zararli dasturiy vositalar ikki turga bo'linadi:

– dasturlardagi zaifliklar (atayin yaratilmagan);

– zararkunanda dasturlar (atayin yaratilgan).

Birinchi turga, dasturchi tomonidan yo‘l qo‘yilgan xatolik natijasidagi dasturlardagi muammolar misol bo‘lsa, ikkinchi turga buzg‘unchilik maqsadida yozilgan maxsus dasturiy mahsulotlar (masalan, viruslar) misol bo‘la oladi.

Dasturiy vositalarda xavfsizlik muammolarining mavjudligi quyidagi omillar orqali belgilanadi:

– dasturiy vositalarning ko‘plab dasturchilar tomonidan yozilishi (komplekslilik);

– dasturiy mahsulotlar yaratilishida inson ishtiroki; – dasturchining malakasi yuqori emasligi;

– dasturlash tillarining xavfsiz emasligi.

Dasturiy vositalarning bir necha million qator kodlardan iborat bo‘lishi xavfsizlik muammosini ortishiga sababchi bo‘ladi (7.1-jadval). Boshqacha aytganda, katta hajmli dasturiy vositalar ko‘plab dasturchilar tomonidan yoziladi va yakunida biriktiriladi. Dasturchilar orasidan bittasining bilim darajasi yetarli bo‘lmasligi, butun dasturiy vositaning xavfsizligini yo‘qqa chiqarishi mumkin.

7.1 – jadval

Turli OTlar kodlarining uzunligi

Tizim	Dasturdagi kod uzunligi
Netscape	17 mln.
Space Shuttle	10 mln.
Linuxkernel 2.6.0	5 mln.
Windows XP	40 mln.
Mac OS X 10.4	86 mln.
Boeing 777	7 mln.

Tahlillar natijasi har 10 000 ta qator kodda 5 ta bag mavjudligini ko‘rsatadi. Boshqacha aytganda, o‘rtacha 3kbayt .exe faylda 50 tacha bag bo‘ladi.

Dasturiy vositalar injineriyasida dasturning o‘z vazifasini kafolatli bajarishiga harakat qilinsa, xavfsiz dasturiy vositalar injineriyasida esa o‘z vazifasini xavfsiz bajarishi talab etiladi. Biroq, amalda butunlay xavfsiz dasturiy vositaning bo‘lishi mumkin emas.

Dasturiy mahsulotlarda zaiflikka tegishli quyidagi tushunchalar mavjud.

Nuqson. Dasturni amalga oshirishdagi va loyihalashdagi zaifliklarning barchasi nuqson hisoblanadi va uning dasturiy vositalarda mavjudligi yillar davomida bilinmasligi mumkin.

Bag. Baglar dasturiy ta’minotni amalga oshirish bosqichiga tegishli muammo bo‘lib, ularni osongina aniqlash mumkin. Misol sifatida dasturlashdagi buferning to‘lib-toshishi (Buffer overflow) holatini keltirish mumkin.

Xotiraning to‘lib-toshishi. Amalda ko‘p uchraydigan dasturlash tillaridagi kamchiliklar, odatda, taqiqlangan formatdagi yoki hajmdagi ma’lumotlarning kiritilishi natijasida kelib chiqadi. Bu turdagi tahdidlar ichida keng tarqalgani – xotiraning to‘lib-toshishi tahdidi.

Agar buzg‘unchi tomonidan o‘ziga “kerakli” ma’lumot kiritilsa, bu o‘z navbatida kompyuterning buzilishiga olib keladi.

Quyida C dasturlash tilida yozilgan kod keltirilgan, agar bu kod kompilyasiya qilinsa, xotiraning to‘lib-toshishi hodisasi sodir bo‘ladi.

```
int main()
   {
   int buffer [10];
   buffer [20] =37;
   }
```

Bu yerda mavjud muammo - 10 bayt o‘lchamli xotiraga 20 baytli ma’lumot yozilishi. Bu esa xotiraning ruxsat etilmagan manziliga ham murojaatga sabab bo‘ladi.

7.2. Dasturiy vosita xavfsizligining fundamental prinsiplari

Dasturiy ta’minot yaratilganida va foydalanilganida qator prinsiplarga amal qilish talab qilinadi. Quyida OWASP tashkiloti tomonidan taqdim etilgan prinsiplar keltirilgan:

Hujumga uchrashi mumkin bo‘lgan soha maydonini minimallashtirish. Dasturiy ta’minotga qo‘shilgan har bir xususiyat dasturga ma’lum miqdordagi xavf darajasini ham qo‘shadi. Dasturni xavfsiz amalga oshirishning maqsadi – hujumga uchrashi mumkin bo‘lgan sohani toraytirish orqali umumiy dasturdagi xavfni kamaytirish. Masalan, web saytlarda onlayn yordamini amalga oshirish uchun

qidirish funksiyasi mavjud. Biroq, ushbu imkoniyat web saytga SQL – inyeksiya hujumi bo‘lishi ehtimolini keltirib chiqarishi mumkin. Qidiruv imkoniyati autentifikatsiyadan o‘tgan foydalanuvchilar uchun bo‘lsa, hujum bo‘lishi ehtimoli kamayadi. Agar qidiruv ma’lumotlari markazlashgan tarzda tekshirilsa, ushbu hujum ehtimoli yanada kamayadi.

Xavfsiz standart sozlanmalarini o‘rnatish. Amalda, aksariyat dasturiy ta’minotlarda va operatsion tizimlarda ko‘plab xavfsizlik sozlanmalari standart tartibda o‘rnatilgan bo‘ladi. Biroq, bu foydalanuvchilar tomonidan yaxshi qabul qilinmaydi va shuning uchun, aksariyat hollarda, ushbu sozlanmalarni o‘chirib qo‘yish amalga oshiriladi. Masalan, operatsion tizimlarda parollarni eskirish vaqti standart holda o‘rnatilgan bo‘lsada, aksariyat foydalanuvchilar tomonidan ushbu sozlanma o‘chirib qo‘yiladi.

Minimal imtiyozlar prinsipi. Axborot xavfsizligi, informatika, dasturlash va boshqa sohalarda keng qo‘llaniluvchi minimal imtiyozlar prinsipi (Principle of least privilege) – hisoblash muhitidagi u yoki bu abstraksiya darajasida resurslarga murojaatni tashkil qilish. Bunga ko‘ra har bir modul o‘z vazifasini to‘laqonli bajarishi uchun zarur bo‘lgan resurs yoki axborotdan minimal darajada foydalanish talab etiladi.

Bu prinsip foydalanuvchi yoki dasturchiga faqat o‘z vazifasi uchun zarur bo‘lgan imtiyozlarga ega bo‘lishi kerakligini anglatadi. Masalan, vaqt o‘tkazish uchun ishlab chiqilgan turli mobil o‘yin dasturlari SMS xabarni o‘qish yoki qo‘ng‘iroq qiluvchilar ro‘yxatini bilish imkoniyatiga ega bo‘lishi shart emas. Masalan, dasturlash tillarida (Java dasturlash tilida keltirilgan) obyektlardan foydanishni cheklash uchun turli kalit so‘zlardan foydalaniladi (7.2-jadval).

7.2-jadval

Java dasturlash tilidagi foydalanuvchi imtiyozlari

Imtiyoz / Xususiyat	Default	Private	Protected	Public
Bir xil klass	+	+	+	+
Bir paket qismklassi	+	-	+	+
Bir paket qismklassi bo‘lmagan	+	-	+	+
Turli paket qismklasslari	-	-	+	+
Turli paket qismklassi bo‘lmagan	-	-	-	+

Teran himoya prinsipi. Ushbu prinsipga binoan, bitta nazoratning bo‘lishi yaxshi, ko‘plab nazoratlardan foydalanish esa yaxshiroq deb qaraladi. Teran himoyada foydalanilgan nazoratlar turli zaiflik orqali bo‘lishi mumkin bo‘lgan tahdidlarni oldini oladi. Xavfsiz dastur yozish orqali esa, foydalanish qiymatini tekshirish, markazlashgan auditni boshqarish va foydaluvchilarning barcha sahifalardan foydalanishlari ta’minlanishi mumkin.

Agar to‘g‘ri ishlab chiqilgan ma’mur interfeysi, tarmoqdan foydalanish qoidalarini to‘g‘ri bajarsa, foydalanuvchilarning avtorizatsiyasini tekshirsa va barcha holatlarni qaydlasa, u anonim hujumga bardoshsiz bo‘lishi mumkin emas.

Xavfsizlikning buzilishi. Ilovalar, amalga oshirilishi jarayonida turli sabablarga ko‘ra, buzilishlarga uchraydi. Masalan, quyida e’tiborsizlik oqibatida qoldirilgan xavfsizlik holati keltirilgan.

```
isAdmin = true;
try {
codeWhichMayFail();
isAdmin = isUserInRole( “Administrator” ); }
catch (Exception ex) {
log.write(ex.toString());
}|
```

Mazkur holda codeWhichMayFail() yoki isUserInRole() funksiyalarida xatolik bo‘lsa yoki biror Exception kuzatilgan taqdirda ham foydalanuvchi ma’mur rolida qolaveradi. Bu ko‘rinib turgan xavfsizlik riski hisoblanadi.

Xizmatlarga ishonmaslik. Hozirgi kunda ko‘plab tashkilotlar uchinchi tomon, sheriklarining hisoblash imkoniyatidan foydalanadi. Masalan, Payme yoki shunga o‘xshash ilovalar bir necha bank kartalaridagi ma’lumotlarni taqdim qiladi.

Vazifalarni ajratish. Firibgarlikni oldini olishga qaratilgan asosiy chora – vazifalarni ajratish. Masalan, tashkilotda kompyuter olish bo‘yicha talab yuborgan odam tomonidan uni qabul qilinmasligi shart. Sababi, bu holda u ko‘plab kompyuterlarni so‘rashi va qabul qilib olganini rad qilishi mumkin.

Xavfsizlikni noaniqlikdan saqlash. Noaniqlikka asoslangan xavfsiz – zaif xavfsizlik bo‘lib, birinchi nazoratning o‘zida xatolikka uchraydi. Bu biror sirni saqlash yomon g‘oya ekanligini anglatmasada, xavfsizlikning muhim jihatlari tafsilotlarining yashirin bo‘lishiga asoslanmasligini bildiradi.

Xavfsizlikni soddaligi. Hujumga uchrash soha maydoni va soddalik bir-biriga bog‘liq. Ba’zi dasturiy ta’minot muhandislari kodning sodda ko‘rinishidan ko‘ra murakkabligini afzal ko‘radilar. Biroq, sodda va tushunishga oson ko‘rinish tezkor bo‘lishi mumkin. Shuning uchun, dasturiy ta’minotni yaratish jarayonida murakkablikdan qochishga harakat qilish zarur.

Dasturiy mahsulotlarga qo‘yiladigan talablar uch turga bo‘linadi:

- vazifaviy talablar:

tizim amalga oshirilishida kerak bo‘lgan vazifalar. - novazifaviy talablar:

tizimning xususiyatlariga qo‘yilgan talablar.

Vazifaviy talablar. Bu talablar quyidagilarni o‘z ichiga oladi:

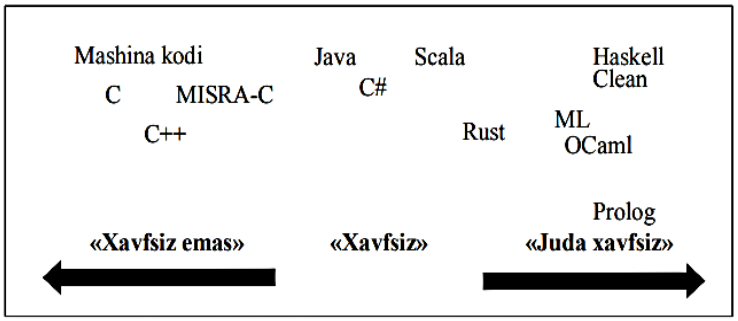
- tizim kutgan kirishga qo‘yilgan talablar;
- tizimdan chiqqan natijaga qo‘yilgan talablar;
- kirish va chiqishga aloqador bo‘lgan talablar.

Novazifaviy talablarga quyidagilar taalluqli:

- audit qilish imkoniyati;
- kengaytirish mumkinligi;

- foydalanishga qulayligi;
- bajarilishi;
- ixchamligi;
- ishonchliligi;
- xavfsizligi;
- testlash imkoniyati;
- foydalanuvchanligi va h.

Dasturlash tiliga asoslangan xavfsizlik. Turli dasturlash tillari o‘ziga xos imkoniyatlarga ega, dasturlash sathida xavfsizlikni taminlash muhim ahamiyat kasb etadi. Mavjud dasturlash tillarini xavfsiz yoki xavfsiz emas turlariga ajratish nisbiy tushuncha bo‘lib, ularni quyidagicha tasvirlash mumkin (7.5-rasm).



7.5 – rasm. Dasturlash tillarining xavfsizlik darajasining sodda ko‘rinishi

7.3. Kompyuter viruslari va virusdan himoyalanish muammolari

Kompyuter virusining ko‘p ta’riflari mavjud. Birinchi ta’rifni 1984 yili Fred Koen bergan: “Kompyuter virusi – boshqa dasturlarni, ularga o‘zini yoki o‘zgartirilgan nusxasini kiritish orqali, ularni modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko‘payish qobiliyatini saqlaydi”. Virusning o‘z-o‘zidan ko‘payishi va hisoblash jarayonini modifikatsiyalash qobiliyati bu ta’rifdagi tayanch tushunchalar hisoblanadi.

Viruslarni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

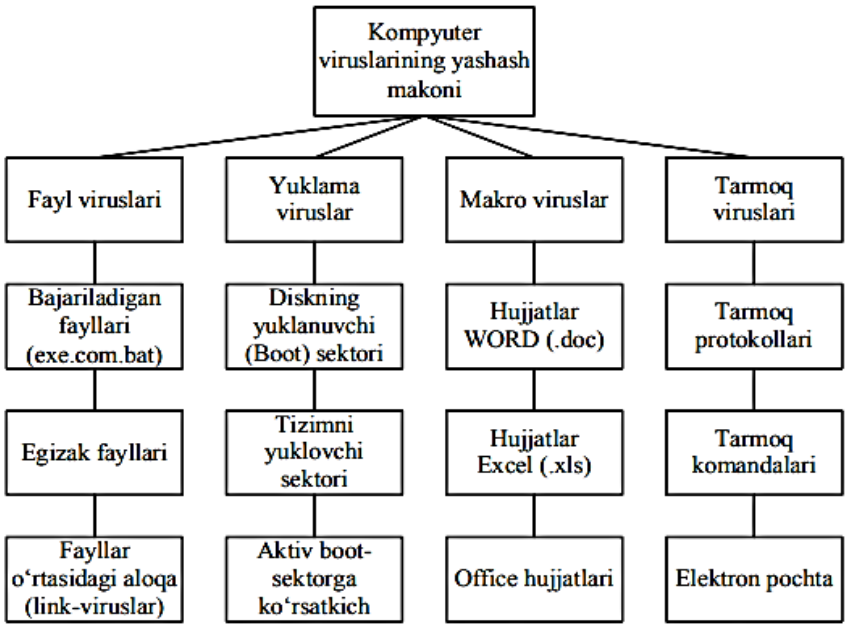
– yashash makoni;

– operatsion tizim;

– ishlash algoritmi xususiyati;

– destruktiv imkoniyatlari.

Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo‘yicha turkumlash keng tarqalgan (7.6-rasm). Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko‘p tarqalgan viruslar xili), yoki fayl-egizaklarni (kompanon viruslar) yaratadi yoki faylli tizimlarni (link-viruslar) tashkil etish xususiyatidan foydalanadi. Yuklama viruslar o‘zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (MasterBootRecord) bo‘lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.



7.6-rasm. Yashash makoni bo‘yicha kompyuter viruslarining turkumlanishi

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan Microsoft Word, Microsoft Excel va h. kabi ommaviy muharrirlarning fayl-hujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba’zida tarmoq viruslarini “qurt” xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo‘yicha tarqaladi), IRC-qurtlarga (chatlar, InternetRelayChat) bo‘linadi.

Kompyuter viruslarining ko‘pgina kombinasiyalangan xillari ham mavjud, masalan – tarmoqli makrovirus tahrirlanuvchi hujjatlarni zaxarlaydi, hamda o‘zining nusxalarini elektron pochta orqali tarqatadi. Boshqa bir misol sifatida fayl-

yuklama viruslarini ko‘rsatish mumkinki, ular fayllarni hamda disklarning yuklanadigan sektorini zaharlaydi.

Viruslarning hayot davri.Har qanday dasturdagidek kompyuter viruslari hayot davrining ikkita asosiy bosqichini - saqlanish va bajarilish bosqichlarini ajratish mumkin.

Saqlanish bosqichi virusning diskda u kiritilgan obyekt bilan birgalikda shundaygina saqlanish davriga to‘g‘ri keladi. Bu bosqichda virus virusga qarshi dastur ta’minotiga zaif bo‘ladi, chunki u faol emas va himoyalanish uchun operatsion tizimni nazorat qila olmaydi.

Kompyuter viruslarining bajarilish davri, odatda, beshta bosqichni o‘z ichiga oladi:

1. Virusni xotiraga yuklash.
2. Qurbonni qidirish.
3. Topilgan qurbonni zaharlash.
4. Destruktiv funksiyalarni bajarish.
5. Boshqarishni virus dastur-eltuvchisiga o‘tkazish.

Virusni xotiraga yuklash. Virusni xotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi obyekt bilan bir vaqtda amalga oshiriladi. Masalan, agar foydalanuvchi virus bo‘lgan dasturiy faylni ishga tushirsa, ravshanki, virus kodi ushbu fayl qismi sifatida xotiraga yuklanadi. Oddiy holda, virusni yuklash jarayoni-diskdan operativ xotiraga nusxalash bo‘lib, so‘ngra boshqarish virus badani kodiga uzatiladi. Bu harakatlar operatsion tizim tomonidan bajariladi, virusning o‘zi passiv holatda bo‘ladi. Murakkabroq vazifalarda virus boshqarishni olganidan so‘ng o‘zining ishlashi uchun qo‘shimcha harakatlarni bajarishi mumkin. Bu bilan bog‘liq ikkita jihat ko‘riladi.

Birinchisi viruslarni aniqlash muolajasining maksimal murakkablashishi bilan bog‘liq. Saqlanish bosqichida ba’zi viruslar himoyalanishni taminlash maqsadida yyetarlicha murakkab algoritmdan foydalanadi. Bunday murakkablashishga virus asosiy qismini shifrlashni kiritish mumkin. Ammo faqat shifrlashni ishlatish chala chora hisoblanadi, chunki yuklanish bosqichida

rasshifrovkani ta’minlovchi virus qismi ochiq ko‘rinishda saqlanishi lozim. Bunday holatdan qutilish uchun viruslarni ishlab chiquvchilar rasshifrovka qiluvchi kodni “mutatsiyalash” mexanizmidan foydalanadi. Bu usulning mohiyati shundan iboratki, obyektga virus nusxasi kiritilishida uning rasshifrovka qilinishiga taalluqli qismi shunday modifikatsiyalanadiki, original bilan matnli farqlanish paydo bo‘ladi, ammo ish natijasi o‘zgarmaydi.

Ikkinchi jihat rezident viruslar deb ataluvchi viruslar bilan bog‘liq. Virus va u kiritilgan obyekt operatsion tizim uchun bir butun bo‘lganligi sababli, yuklanishdan so‘ng ular, tabiiy, yagona adres makonida joylashadi. Obyekt ishi tugaganidan so‘ng u operativ xotiradan ishlay boshlaydi.

Rezident bo‘lmagan viruslar faqat faollashgan vaqtlarida xotiraga tushib zaharlash va zarakunandalik vazifalarini bajaradi. Keyin bu viruslar xotirani butunlay tark etib yashash makonida qoladi.

Ta’kidlash lozimki, viruslarni rezident va rezident bo‘lmaganlarga ajratish faqat fayl viruslariga taalluqli. Yuklanuchi va makroviruslar rezident viruslarga tegishli.

Qurbonni qidirish. Qurbonni qidirish usuli bo‘yicha viruslar ikkita sinfga bo‘linadi. Birinchi sinfga operatsion tizim funksiyalaridan foydalanib faol qidirishni amalga oshiruvchi viruslar kiradi. Ikkinchi sinfga qidirishning passiv mexanizmlarini amalga oshiruvchi, ya’ni dasturiy fayllarga tuzoq qo‘yuvchi viruslar taalluqli.

Topilgan qurbonni zaharlash. Oddiy holda zaharlash deganda qurbon sifatida tanlangan obyektda virus kodining o‘z-o‘zini nusxalashi tushuniladi.

Avval fayl viruslarining zaharlash xususiyatlarini ko‘raylik. Bunda ikkita sinf viruslari farqlanadi. Birinchi sinf viruslari o‘zining kodini dasturiy faylga bevosita kiritmaydi, balki fayl nomini o‘zgartirib, virus badani bo‘lgan yangi faylni yaratadi. Ikkinchi sinfga qurbon fayllariga bevosita kiruvchi viruslar taalluqli. Bu viruslar kiritilish joylari bilan xarakterlanadi. Quyidagi variantlar bo‘lishi mumkin:

1. Fayl boshiga kiritish. Ushbu usul MS-DOSning com-fayllari uchun eng qulay hisoblanadi, chunki ushbu formatda xizmatchi sarlavhalar ko‘zda tutilgan.

2. Fayl oxiriga kiritish. Bu usul eng ko‘p tarqalgan bo‘lib, viruslar kodiga boshqarishni uzatish dasturning birinchi komandasi (com) yoki fayl sarlavhasini (exe) modifikatsiyalash orqali ta’minlanadi.

3. Fayl o‘rtasiga kiritish. Odatda bu usuldan viruslar strukturasi oldindan ma’lum fayllarga (masalan, Command.com fayli) yoki tarkibida bir xil qiymatli baytlar ketma-ketligi bo‘lgan, uzunligi virus joylashishiga yetarli fayllarga tatbiqan foydalaniladi.

Yuklama viruslar uchun zaharlash bosqichining xususiyatlari ular kiritiluvchi obyektlar – qayishqoq va qattiq disklarning yuklanish sektorlarining sifati va qattiq diskning bosh yuklama yozuvi (MBR) orqali aniqlanadi. Asosiy muammo-ushbu obyekt o‘lchamlarining chegaralanganligi. Shu sababli, viruslar o‘zlarining qurbon joyida sig‘magan qismini diskda saqlashi, hamda zaharlangan yuklovchi original kodini tashishi lozim.

Beziyon viruslar - o‘z-o‘zidan tarqalish mexanizmi amalga oshiriluvchi viruslar. Ular tizimga zarar keltirmaydi, faqat diskdagi bo‘sh xotirani sarflaydi xolos.

Xavfsiz viruslar – tizimda mavjudligi turli taassurot (ovoz, video) bilan bog‘liq viruslar, bo‘sh xotirani kamaytirsada, dastur va ma’lumotlarga ziyon yetkazmaydi.

Xavfli viruslar – kompyuter ishlashida jiddiy nuqsonlarga sabab bo‘luvchi viruslar. Natijada dastur va ma’lumotlar buzilishi mumkin.

Juda xavfli viruslar – dastur va ma’lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o‘chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar.

Boshqarishni virus dastur – eltuvchisiga o‘tkazish. Ta’kidlash lozimki, viruslar buzuvchilar va buzmaydiganlarga bo‘linadi.

Viruslardan tashqari zarar keltiruvchi dasturlarning quyidagi xillari mavjud:

– troyan dasturlari;

– mantiqiy bombalar;

masofadagi kompyuterlarni yashirincha ma’murlovchi xaker utilitalari;

– Internetdan va boshqa konfidensial axborotdan foydalanish parollarini o‘g‘rilovchi dasturlar.

Ular orasida aniq chegara yo‘q: troyan dasturlari tarkibida viruslar bo‘lishi, viruslarga mantiqiy bombalar joylashtirilishi mumkin va h.

Troyan dasturlar o‘zlari ko‘paymaydi va tarqatilmaydi. Tashqaridan troyan dasturlar mutlaqo beozor ko‘rinadi, hatto foydali funksiyalarni tavsiya etadi. ammo foydalanuvchi bunday dasturni kompyuteriga yuklab, ishga tushirsa, dastur bildirmay zarar keltiruvchi funksiyalarni bajarishi mumkin. Ko‘pincha troyan dasturlar viruslarni dastlabki tarqatishda, Internet orqali masofadagi kompyuterdan foydalanishda, ma’lumotlarni o‘g‘rilashda yoki ularni yo‘q qilishda ishlatiladi.

Mantiqiy bomba – ma’lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari. Mantiqiy bomba, masalan, ma’lum sana kelganida yoki ma’lumotlar bazasida yozuv paydo bo‘lganida yoki yo‘q bo‘lganida va h. ishga tushishi mumkin. Bunday bomba viruslarga, troyan dasturlarga va oddiy dasturlarga joylashtirilishi mumkin.

Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari. Kompyuterlar va korporativ tarmoqlarni himoyalovchi samarador tizimni yaratish uchun qayerdan xavf tug‘ilishini aniq tasavvur etish lozim. Viruslar tarqalishning juda xilma-xil kanallarini topadi. Buning ustiga eski usullarga yangisi qo‘shiladi.

Tarqatishning klassik (mumtoz) usullari. Fayl viruslari dastur fayllari bilan birgalikda disketlar va dasturlar almashishda, tarmoq kataloglaridan, Web- yoki FTP – serverlardan dasturlar yuklanishida tarqatiladi. Yuklama viruslar kompyuterga foydalanuvchi zaharlangan disketani diskovodda qoldirib, so‘ngra operatsion tizimni qayta yuklashida tushib qoladi.

Makrokomanda viruslari Microsoft Word, Excel, Access fayllari kabi ofis hujjatlarining zaxarlangan fayllari almashinishida tarqaladi.

Agar zaharlangan kompyuter lokal tarmoqqa ulangan bo‘lsa virus osongina fayl-server disklariga tushib qolishi, u yerdan kataloglar orqali tarmoqning barcha kompyuterlariga o‘tishi mumkin. Shu tariqa virus epidemiyasi boshlanadi. Virus

tarmoqda shu virus tushib qolgan kompyuter foydalanuvchisi xuquqlari kabi xuquqqa ega ekanligini tizim ma’muri unutmasligi lozim.

Elektron pochta. Hozirda Internet global tarmog‘i viruslarning asosiy manbai hisoblanadi. Viruslar bilan zaharlanishlarning aksariyati MicroSoftWord formatida xatlar almashishda sodir bo‘ladi. Elektron pochta makroviruslarni tarqatish kanali vazifasini o‘taydi, chunki axborot bilan bir qatorda ko‘pincha ofis hujjatlari jo‘natiladi. Viruslar bilan zaharlash bilmasdan va yomon niyatda amalga oshirilishi mumkin.

Troyan Web-saytlar. Foydalanuvchilar virusni yoki troyan dasturni Internet saytlarining oddiy kuzatishda, troyan Web-saytni ko‘rganida olishi mumkin. Foydalanuvchi brauzerlaridagi xatoliklar ko‘pincha troyan Web-saytlari faol komponentlarining foydalanuvchi kompyuterlariga zarar keltiruvchi dasturlarni kiritishiga sabab bo‘ladi.

Lokal tarmoqlar. Lokal tarmoqlar ham tezlikda zaharlanish vositasi hisoblanadi. Agar himoyaning zaruriy choralari ko‘rilmasa, zaharlangan ishchi stansiya lokal tarmoqqa kirishda serverdagi bir yoki bir necha xizmatchi fayllarni zaharlaydi. Bunday fayllar sifatida Login.com xizmatchi faylni, firmada qo‘llaniluvchi Excel-jadvallar va standart hujjat-shablonlarni ko‘rsatish mumkin.

Zarar keltiruvchi dasturlarni tarqatishning boshqa kanallari. Viruslarni tarqatish kanallaridan biri dasturiy ta’minotning qaroqchi nusxalari hisoblanadi. Disketlar va CD-disklardagi noqununiy nusxalarda ko‘pincha turli-tuman viruslar bilan zaharlangan fayllar bo‘ladi. Viruslarni tarqatish manbalariga elektron anjumanlar va FTP va BBS fayl-serverlar ham taalluqli.

O‘quv yurtlarida va Internet-markazlarida o‘rnatilgan va umumfoydalanish rejimida ishlovchi kompyuterlar ham osongina viruslarni tarqatish manbaiga aylanishi mumkin.

Kompyuter texnologiyasining rivojlanishi bilan kompyuter viruslari ham, o‘zining yangi yashash makoniga moslashgan holda, takomillashadi. Yangi viruslar ma’lum bo‘lmagan yoki oldin mavjud bo‘lmagan tarqatish kanallaridan hamda kompyuter tizimlarga tatbiq etishning yangi texnologiyalaridan

foydalanishi mumkin. Virusdan zaharlanish xavfini yo‘qotish uchun korporativ tarmoqning tizim ma’muri, nafaqat virusga qarshi usullardan foydalanishi, balki kompyuter viruslari dunyosini doimo kuzatib borishi shart.

Zararli dasturiy vositalarni aniqlash. Zararli dasturiy vositalarni aniqlashda asosan uchta yondashuvdan foydalaniladi. Birinchisi va eng keng tarqalgani signaturaga asoslangan aniqlash bo‘lib, zararli dasturdagi shablon yoki signaturani topishga asoslanadi. Ikkinchi yondashuv o‘zgarishlarni aniqlashga asoslangan bo‘lib, o‘zgarishga uchragan fayllarni aniqlaydi. O‘zgarishi kutilmagan fayl o‘zgarganida zararlangan deb topiladi. Uchinchi yondashuv anomaliyaga asoslangan, noodatiy yoki virusga o‘xshash fayllarni va holatlarni aniqlashga asoslanadi.

Signaturaga asoslangan aniqlash. *Signatura bu* – faylda topilgan bitlar qatori bo‘lib, maxsus belgilarni o‘z ichiga oladi. Bu o‘rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.

Signaturaga asoslangan aniqlash usuli virus aniq bo‘lganida va umumiy bo‘lgan signaturalar ajratilgan holatda juda yuqori samaradorlikka ega. Bundan tashqari, ushbu usulga binoan foydalanuvchi va ma’murga minimal yuklama yuklanadi va ularga faqat signaturalarni saqlash va uzluksiz yangilash vazifasi qo‘yiladi.

Hozirgi kunda signaturaga asoslangan tanib olish usuli zamonaviy antivirus yoki zararli dasturlarga qarshi himoya vositalarida keng qo‘llaniladi.

O‘zgarishlarni aniqlovchi usul. Zararli dasturlar ma’lum manzilda joylashganligi sababli, tizimdagi biror joyda o‘zgarish aniqlansa, zararlangan joyini ko‘rsatish mumkin. Ya’ni, agar o‘zgarishga uchragan fayl aniqlansa, u virus orqali zararlangan bo‘lishi mumkin.

O‘zgarishlarni qanday aniqlash mumkin? Ushbu muammoni yechishda xesh-funksiyalar mos keladi. Faraz qilaylik, tizimdagi barcha fayllar xeshlanib, xesh qiymatlari xavfsiz manzilda saqlangan bo‘lsin. U holda vaqti-vaqti bilan ushbu faylning xesh qiymatlari qaytadan hisoblanadi va dastlabkilari bilan taqqoslanadi. Agar faylning bir yoki bir nechta bitlari o‘zgarishga uchragan bo‘lsa,

xesh qiymatlar bir biriga mos kelmaydi va fayl virus tomonidan zararlangan hisoblanadi.

Ushbu usulning afzalliklaridan biri shuki, agar fayl zararlangan bo‘lsa, uni to‘liq aniqlash mumkin. Bundan tashqari, oldin noma’lum bo‘lgan zararli dasturni ham aniqlash mumkin.

Biroq, ushbu usul kamchiliklarga ham ega. Tizimdagi fayllar odatda tez-tez o‘zgarib turadi va natijada yolg‘ondan zararlangan deb topilgan holatlar soni ortadi. Agar virus tizimdagi tez-tez o‘zgaruvchi fayl ichiga joylashtirilgan bo‘lsa, ushbu usulni osonlik bilan aylanib o‘tish mumkin. Bu holda ushbu fayldagi o‘zgarishni log fayl orqali aniqlash ko‘p vaqt talab qiladi va bu signaturaga asoslangan usuldagi kabi muammolarga olib keladi.

Anomaliyaga asoslangan aniqlash. Anomaliyaga asoslangan usul noodatiy yoki virusga o‘xshash yoki bo‘lishi mumkin bo‘lgan zararli harakatlarni yoki xususiyatlarni topishni maqsad qiladi.

Ushbu g‘oya IDS tizimlarida ham foydalaniladi. Ushbu usulning fundamental muammosi - qaysi holatni normal va qaysi holatni normal bo‘lmagan deb topish hamda ushbu ikki holat orasidagi farqni aniqlash hisoblanadi. Bundan tashqari, normal holatning o‘zgarishi va tizimning bu holatga moslashish muammosi ham mavjud. Bu esa ko‘plab noto‘g‘ri signallarni paydo bo‘lishiga sabab bo‘ladi. Ushbu usulning afzalligi sifatida oldin noma’lum bo‘lgan zararli dasturlarni aniqlash imkonini ko‘rsatish mumkin.

Antivirus dasturiy vositalarining kamchiligi. Antivirus dasturiy vositasiga kompyuterni himoyalashda amalga oshirilish lozim bo‘lgan zaruriy shart sifatida qaraladi. Umuman olganda, antivirus kompyuter uchun zararli dasturlarni skanerlashni, himoyalashni, karantin holatiga tushirishni va boshqa amallarni bajaradi. Antivirus dasturiy vositalarini CD-disklardan va Internet tarmog‘idan foydalangan holda o‘rnatish mumkin. Antivirus dasturiy vositalari bir biridan ko‘plab o‘ziga xos xususiyatlari bilan ajralib turadi. Masalan, Internet tarmog‘idan foydalanilganda reklamalarni blokirovkalash, Internet tarmog‘idan kirib keluvchi

zararli dasturlarni blokirovkalash va h. Biroq, foydalanuvchilar to‘liq antivirus dasturiy vositalarining imkoniyatilariga ishonib qolmasliklari lozim.

Viruslarni doimiy aniqlash uchun antivirus dasturiy vositalari eng yangi va yangilangan ma’lumotlarni o‘z ichiga olgan namunaviy fayllarga muxtoj. Biroq, antivirus ishlab chiqaruvchilari yangi virus uchun namunaviy fayllar yaratgunlaricha virus ishlab chiqaruvchilari tomonidan katta hajmdagi yangi viruslar yaratiladi. Bu esa, yangi virus uchun vaksinani tayyorlash yyetarlicha ko‘p vaqtni talab qiladi.

Bundan tashqari, antivirus dasturi Rootkit tipidagi zararli dasturlarni aniqlashda foydasi tegmasligi mumkin. Rootkit tipidagi zararli dasturlar kompyuter operatsion tizimining markaziga hujum qilishni maqsad qiladi.

Antivirus dasturiy komplekslari. Har bir antivirus dasturiy vositalar o‘ziga xos afzallik va kamchiliklarga ega. Faqat bir necha antivirus dasturiy vositalaridan kompleks foydalanish to‘liq himoyani taminlashi mumkin. Amalda ko‘plab antivirus dasturiy vositalar mavjud, ularga quyidagilarni misol sifatida keltirish mumkin (7.3-jadval).

7.3-jadval

Turli antivirus dasturlarining xususiyatlari

Mahsulot / Xususiyati	McAfee AntiVirus Plus	Semantec Norton AntiVirus Plus	Kaspersky Anti-Virus	Bitdefender Antivirus Plus	Webroot SecureAnywhere Antivirus	Eset Nod32 Antivirus	Trend Micro Antivirus+ Security	F-secure Anti-Virus	VoodooSoft VoodooShield	The Kure
Narxi	19.99$	19.99$	29.99$	29.99$	18.99$	27.99$	29.95$	39.99$	19.99$	19.99$
Talabga ko‘ra skanerlash	+	+	+	+	+	+	+	+	-	-
Doimiy skanerlash	+	+	+	+	+	+	+	+	+	-
Web saytni baholash	+	+	+	-	+	-	+	-	-	-
Zararli URL ni bloklash	+	+	+	+	+	+	+	+	-	-
Fishingdan himoyalash	+	+	+	+	+	+	+	-	-	-
Xususi-yatga ko‘ra aniqlash	+	+	+	+	+	+	+	+	+	-
Zaifliklarni skanerlash	+	-	+	+	-	-	-	-	-	-

Profilaktik choralar. Viruslar va virus yuqtirilgan fayllarni o‘z vaqtida aniqlash, aniqlangan viruslarni har bir kompyuterda to‘liq yo‘q qilish orqali virus epidemiyasining boshqa kompyuterlarga tarqalishini oldini olish mumkin. Har qanday virusni aniqlaydigan va yo‘q qilinishini kafolatlaydigan mutlaqo ishonchli dasturlar mavjud emas.

Nazorat savollari

1. Dasturiy mahsulotlarda xavfsizlik ta’minlanishining muhimligi.
2. Dasturiy mahsulotlarda xavfsizlik muammolarining kelib chiqish sabablari.
3. Nuqson, bag, xotirani to‘lib toshishi tushunchalari.
4. Dasturiy vosita xavfsizligini fundamental prinsiplari.
5. Dasturiy vositalarga qo‘yilgan talablar.
6. Dasturiy vositalarga qo‘yilgan xavfsizlik talablari.
7. Dasturiy vositalar xavfsizligini taminlashda dasturlash tillarining o‘rni.
8. Xavfsiz va xavfsiz bo‘lmagan dasturlash tillari.
9. Zararli dasturlar va ularning asosiy turlari.
10. Kompyuter viruslari nima?
11. Zararli dasturiy vositalardan himoyalanish usullari va vositalari.
12. Antivirus dasturiy vositalarini tanlashdagi talablar

FOYDALANILGAN ADABIYOTLAR

1. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 140 b.

2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.

3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.

4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –T.: «Aloqachi», 2008, 382 bet.

5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.

6. Марков А. С., Барабанов А. В., Дорофеев А. В., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С.Маркова. –М.: ДМК Пресс, -2017. – 224с.

7. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoyeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 192 bet.

8. Akbarov D.Y. Axborot xavfsizligini taminlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, 394 bet.

9. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.

10. Raef Meeuwisse. Cybersecurity for Beginners (2nd. ed.). Cyber Simplicity Ltd, London, England, 2017, - 224 p.

11. Manjikian M. Cybersecurity ethics: an introduction. – Routledge, 2017, -328 p.

12. Kostopoulos G. Cyberspace and cybersecurity. – CRC Press, 2017, -316 r.

13. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity. – Springer Nature, 2020. – S. 384.

14. Pande J. Introduction to Cyber Security. Uttarakhand Open University, 2017, -152 p.

15. Cybersecurity Fundamentals Study Guide, ISACA 2015, -196 p.

16. Easttom C. Computer security fundamentals. – Pearson IT Certification, 2019, -447 p.

17. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.

18. Shinder D. L., Cross M. Scene of the Cybercrime. – Elsevier, 2008.

19. Scarfone K. et al. Guide to storage encryption technologies for end user devices //NIST Special Publication. – 2007. – T. 800. – S. 111.

20. Curricula Cybersecurity. Curriculum guidelines for postsecondary degree programs in cybersecurity. – 2017.

Internet manbalar

1. ACR39U smart card rader [sayt]: http://smartkardtechnologies.com/productdetails/acr39u-smart-cardrader (murojaat vaqti: 29.10.2020).

2. Certified Network Defender [sayt]: https://iclass.eccouncil.org/our-courses/certified-network-defender-cnd/ (murojaat vaqti: 29.10.2020).

3. 3D Airport Security X-ray Machine [sayt]: https://www.turbosquid.com/3d-models/3d-airport-x-ray-machinesecurity-1405223 (murojaat vaqti: 29.10.2020).

4. Web Applications vulnerabilities and threats: statistics for 2019 [sayt]: https://www.ptsecurity.com/ww-en/analytics/webvulnerabilities-2020/ (murojaat vaqti: 29.10.2020).

5. How to Spot Phishing Emails [sayt]: https://www.nuigalway.ie/itsecurity/howtospotphishingemails/ (murojaat vaqti: 29.10.2020).

6. Beware of fake microsoft security essentials [sayt]: https://techjaws.com/beware-of-fake-microsoft-security-essentials/ (murojaat vaqti: 29.10.2020).

7. The Best Antivirus Protection for 2020 [sayt]: https://www.pcmag.com/roundup/256703/the-best-antivirus-protection (murojaat vaqti: 29.10.2020).

8. Securing Wireless Networks [sayt]: https://www.uscert.gov/ncas/tips/ST05-003 (murojaat vaqti: 29.10.2020).

9. Why High Availability Is Important for Your Business [sayt]: https://blog.layershift.com/why-high-availability-for-your-business/ (murojaat vaqti: 29.10.2020).

10. Rutoken [sayt]: https://www.rutoken.ru/ (murojaat vaqti: 29.10.2020).

11. Comparison of disk encryption software [sayt]: https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software (murojaat vaqti: 29.10.2020).

12. G20 summit: NSA targeted Russian president Medvedev in London [sayt]: https://www.theguardian.com/world/2013/jun/16/nsadmitry-medvedev-g20-summit (murojaat vaqti: 29.10.2020).

13. CRADC Data Destruction and Return of Restricted Data Policy [sayt]: https://ciser.cornell.edu/wpcontent/uploads/2017/01/CRADC_Destruction_and_Return_of_Restrict ed_Data.pdf (murojaat vaqti: 29.10.2020).

14. Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements [sayt]: https://www.fbi.gov/services/information-management/foipa/privacyimpact-assessments/iafis (murojaat vaqti: 29.10.2020).

15. Best Keylogger for Windows 10 in 2020 [sayt]: https://www.pctattletale.com/blog/1505/best-keylogger-softwarewindows-10 (murojaat vaqti: 29.10.2020).

QISQARTMA SO‘ZLAR RO‘YXATI

ABAC - Attribute-based access control

AES - Advanced Encryption Standard

APT - Advanced persistent threats

ASSII – American Standard Code for Information Interchange

AT – Axborot texnologiyalari

CBC - Cipher Block Chaining

CCTV - Closed-circuit television

CDMA - Code Division Multiple Access

CSEC2017 JTF – Cybersecurity Curricula 2017 Joint Task Force

CVE - Common Vulnerabilities and Exposures

DAC - Discretionary access control

DES - Data Encryption Standard

DLP - Data Leakage Prevention,

DoD – Department of Defense

DOS - Denial of service

ECB - Electronic codebook mode

FAR - False Acceptance Rate

FRR - False Rejection Rate

FTP – File Transfer Protocol

GNFS - General Number Field Sieve

GSM – Global System for Mobile Communications

HMAC – hash-based message authentication code

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

IDS - Instrusion Detection System

IPS - Intrusion Prevention System

IPSec - IP Security

ISO – International Organization for Standardization

IV - Initialization Vector

KDC - Key Destribution Center

L2TP - Layer 2 Tunneling Protocol

LAN - Local Area Network

MAC - Mandatory access control

MAC - Message Authentication Code

MAN - Metropolitan Area Network

MITM - Man in the middle attack

NAT - Network Address Translation

OWASP - Open Web Application Security Project

PAN - Personal Area Network

PIN - Personal Identification Number

PKI - Public key infrastructure

PPP – Point-to-Point Protocol

PPTP - Point-to-Point Tunneling Protocol

RAID - Redundant Array of Independent Disks

RBAC - Role-based access control

RFID – Radio Frequency IDentification

SIM - Security Information Management

SSID - Service Set Identifier

SSL - Secure Sockets Layer

TCP/IP – Transmission Control Protocol/Internet Protocol

USB – Universal Serial Bus

UTM - Unifield Threat Management

VPN – Virtual Private Network

WAN - Wide Area Network

WEP - Wired Equivalent Privacy

WLAN - Wireless Local Area Network

WMAN - Wireless Metropolitan Area Network

WPA - Wi-Fi Protected Access

WPAN - Wireless Personal Area Network

WWAN - Wireless Wide Area Network

AOB - Alisaning onlayn banki

ATM – Automated teller machine

MAC - Media access control

OT – Operatsion tizim

ERI - Elektron raqamli imzo

ATAMALARNING RUS, O‘ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG‘ATI

Авторизация - представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.

Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.

Authorization – granting the user certain access rights based on the positive result of authentication in the system.

Администратор защиты - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Himoya ma’muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Security administrator - the subject of the access responsible for the protection of the automated system against unauthorized access to the information.

Администратор системы - лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.

Tizim ma’muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini taminlashga javobgar shaxs.

System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.

Актив - 1. Информация или ресурсы, подлежащие защите. 2. Все, что имеет ценность для организации. 3. Главное приложение, общая система поддержки, высоко авторитетная программа, материальная часть, миссия

критической систем, персонал, оборудование или логически связанная группа систем.

Aktiv - 1. Himoyalanuvchi axborot yoki resurslar. 2. Tashkilot uchun qiymatli barcha narsalar. 3. Bosh ilova, umumiy madadlovchi tizim, yuqori nufuzli dastur, moddiy qism, kritik tizim missiyasi, xodimlar, jihozlar yoki mantiqiy bog‘langan tizimlari guruhi.

Asset - 1. Information or resources that should be protected. 2. Anything that has value to the organization. 3. A major application, general support 206 system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Активная угроза - угроза преднамеренного несанкционированного изменения состояния системы.

Faol tahdid – tizim holatini atayin ruxsatsiz o‘zgartirish tahdidi.

Active threat – a threat that can make a deliberate unauthorized change to the system.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.

Kriptografik algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.

Cryptographic algorithm - the algorithm that implements the calculation of one cryptographic functions.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.

Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Decryption algorithm – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function. Алгоритм хеширования - в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и 207 программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o‘zgartiruvchi algoritm. Chiqish yo‘li satrining har bir simvolining qiymati kirish yo‘li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog‘liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o‘zgartiradi.

Hashing algorithm – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.

Алгоритм цифровой подписи - асимметричный алгоритм, используемый для цифровой подписи данных.

Raqamli imzo algoritmi - ma’lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

Digital signature algorithm – asymmetric algorithm used for digitally signing data.

Алгоритм шифрования RSA - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных. RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo‘ljallangan shifrlash algoritmi.

RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Анализ - изучение значимости полученных данных и доказательственной ценности к случаю.

Tahlil – olingan ma’lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o‘rganish.

Analysis – the examination of acquired data for its significance and probative value to the case.

Анализаторы сетевые (сниффер) - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.

Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini “tinglash”ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.

Network analyzers (sniffer) - programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. Еще - программа, предназначенная для защиты от вирусов,

обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.

Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo‘q qiluvchi dastur. Agar virus yo‘q qilinmasa, zaharlangan dastur yo‘q qilinadi. Yana – viruslardan himoyalashga, zaxarlangan dasturiy modullar va tizimli makonlarni aniqlashga, hamda zaxarlangan obyektlarning dastlabki holatini tiklashga mo‘ljallangan dastur.

Antivirus - the program that detect or detect and remove viruses. If virus remove not possible, then the infected program is destroyed. Another program, designed to protect against viruses, detecting infected software modules and system areas as well as restore the original state of infected object.

Аппаратное средство защиты информации - специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.

Hardware data protection - a special protective device or fixture included in the kit technical tools of information processing.

Апплеты вредоносные - небольшие приложения, которые автоматически загружаются и выполняются, и которые реализуют несанкционированные функции информационной системы.

Zararli appletlar - axborot tizimida ruxsat etilmagan funksiyalarni amalga oshiruvchi, avtomatik yuklanuvchi va bajariluvchi kichik ilovalar. Malicious applets – small application that are automatically downloaded and executed and that perform an unauthorized function on an information system.

Архитектура IT безопасности - описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.

AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.

IT security architecture – a description of security principles and an overall approach for complying with the principles that drive the system design.

Архитектура информационной безопасности - встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информационной безопасности, персональных и организационных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.

Axborot xavfsizligining arxitekturasi - tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo‘linmalarini, ularni tashkilot missiyasi va strategik rejalariga tenglashtirishni ko‘rsatish bilan tavsiflovchi tashkilot arxitekturasining o‘rnatilgan, ajratib bo‘lmas qismi.

Information security architecture – an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans.

Атака «противник в середине» — атака на протокол криптографический, в которой противник C выполняет этот протокол как с участником A, так и с участником B. Противник C выполняет сеанс с участником A от имени B, а с участником B от имени A. В процессе выполнения противник пересылает сообщения от A к B и обратно, возможно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для B под именем A.

«Dushman o‘rtada» xujumi – kriptografik protokolga hujum bo‘lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o‘zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o‘rtada» hujumining

muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o‘zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi.

Attack “the opponent in the middle” - attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack “the opponent in the middle” allows authenticate itself to the enemy in the name of A.

Атака на отказ в обслуживании — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo‘luvchi hujum, ya’ni shunday sharoitlar tug‘diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.

Denial-of-service attack - attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult. Атака пассивная — атака на криптосистему или протокол криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.

Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo‘lib, bunda dushman va/yoki buzg‘unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta’sir etmaydi.

Passive attack - attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate. Атака со словарем паролей — атака на криптосистему, основанная на переборе значений пароля.

Parollar lug‘atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizimga hujum.

Attack with a dictionary of passwords - the attack on the cryptosystem based on iterating the value of a password.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo‘shimcha kod so‘zlari, biometrik ma’lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo‘lishi mumkin.

Authenticator - means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user. Аутентификация - проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации. Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikasiyasini tekshirish; saqlanuvchi va uzatuvchi ma’lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Authentication - checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

Аутентификация биометрическая — способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и

т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.

Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko‘z pardasining to‘ri va h.) asosidagi autentifikatsiyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo‘lmasligi. Ularni esdan chiqarishning, yo‘qotishning yoki boshqa foydalanuvchiga berishning iloji yo‘q.

Biometric authentication - the method of authentication of a subscriber (user), based on a verification of biometric characteristics (fingerprints, hand geometry, face, voice, eye retina image, etc.). The advantages of this method is the inseparability of biometric characteristics from user: they cannot be forgotten, lost or transferred to another user.

Аутентификация двухфакторная — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida. Two-factor authentication - user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

Аутентификация на основе паролей одноразовых — технология аутентификации с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства – токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.

Bir martali parollar aosidagi autentifikatsiya - bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funksiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.

One time password based authentication - technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device – taken, or technology OOB (out of band) based on the transmission password disposable using additional channels, other than where the user accesses the application system.

Аутентификация сообщений - добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.

Xabarlar autentifikatsiyasi – ma’lumotlarda har qanday o‘zgarishlarni aniqlash maqsadida ma’lumotlar blokiga nazorat hoshiyasini qo‘shish. Ushbu hoshiya qiymatini hisoblashda faqat ma’lumotlar priyemnigiga ma’lum kalitlar ishlatiladi.

Message authentication - adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информационной моделью предметной области. База данных, как правило, представляются тремя уровнями абстракции: внешним, концептуальным и внутренним.

Ma’lumotlar bazasi - tatbiqiy dasturlarga bog‘liq bo‘lmagan holda ma’lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy

prinsiplarini ko‘zda tutuvchi, ma’lum qoidalar bo‘yicha tashkil etilgan ma’lumotlar majmui. Predmet sohasining informatsion modeli hisoblanadi. Ma’lumotlar bazasi odatda abstraksiyaning tashqi, konseptual va ichki satxlari orqali ifodalanadi.

Database - a collection of data organized according to certain rules, providing general principles for describing, storing and manipulating data independent of the application programs. An information domain model. The database, usually presented in three levels of abstraction: external, conceptual and internal.

Безопасность - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще - состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Xavfsizlik - ta’siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma’lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko‘rib chiqilishi va modifikatsiyalanishi mumkin bo‘lmagan holat.

Security - the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be 215 used, viewed and modified by unauthorized persons (including the system staff), computers or software.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение; еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее

качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.

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

Information security - status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

Безопасность информационная общества - то же, что и «безопасность, информационная личности» применительно к организованному коллективу людей и к обществу в целом.

Jamiyat axborot xavfsizligi – “shaxs axborot xavfsizligi” kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo‘llaniladi. Society information security - what “safety information personality” when applied to organized team of people and to society as a whole. Безопасность информационной сети - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Axborot tarmog‘i xavfsizligi – axborot tarmog‘ini ruxsatsiz foydalanishdan, me’yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.

Network security - measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами; еще - является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).

Tarmoqlararo ekran – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo‘li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta’minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to‘sig‘i hisoblanadi.

Firewall - a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software). Кибер инфраструктура - включает электронную информацию и коммуникационные системы, и службы и информацию, содержавшуюся в этих системах и службах.

Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o‘z ichiga oladi. Cyber infrastructure – includes electronic information and communications systems and services and the information contained in these systems and services.

Кибер инцидент - действия, использующие компьютерные сети, приводящие к фактическому или потенциальному ущербу в информационной системе и/или содержащейся в ней информации. Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo‘luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.

Cyber incident – actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Кибер-атака - атака, через киберпространство, предназначенная для использования предприятием киберпространства в целях, отключения, уничтожения или злонамеренного контроля вычислительной среды/инфраструктуры.

Kiber-hujum – hisoblash muhiti/ infrastrukturasini, o‘chirish, buzish yoki g‘arazli nazoratlash yoki ma’lumot yaxlitligini buzish yoki nazoratlanuvchi axborotni o‘g‘irlash maqsadida kiberfazodan foydalanuvchi tashkilotga atalgan kiberfazo orqali amalga oshiriluvchi hujum.

Cyber-attack – an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disabling, destroying, or maliciously controlling a computing environment/infrastructure.

Кибербезопасность - возможность охранять или защитить использование киберпространства кибератаками.

Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo‘riqlash yoki himoyalash imkoniyati.

Cybersecurity – the ability to protect or defend the use of cyberspace from cyber-attacks.

Киберпреступность — действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях. Kiberjinoyatchilik - g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Cyber cryme — the actions of individuals or groups aimed at cracking computer security systems, theft or destruction of information for selfish or destructive purposes.

Киберпространство - глобальный домен в информационной среде, состоящий из взаимозависимой сети инфраструктур информационных систем включая Интернет, сети телекоммуникации, компьютерные системы, и встроенные процессоры и контроллеры.

Kiberfazo – Internet, telekommunikatsiya tarmoqlari, kompyuter tizimlari va o‘rnatilgan prosessorlar va kontrollerlarni o‘z ichiga olgan, 218 o‘zaro bog‘langan axborot tizimlari infrastrukturalar tarmog‘idan tashkil topgan axborot muhitidagi global domen.

Cyberspace – a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Кибертерроризм — действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных общественно опасных последствий.

Kiberterrorizm - insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug‘diruvchi kompyuter tizimlarini izdan chiqarish bo‘yicha harakatlar.

Cyber terrorism — action disruption of computer systems, creating a danger of loss of life, significant property damage or other socially dangerous consequences.

Привилегии - права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.