O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

SAMARQAND IQTISODIYOT VA SERVIS INSTITUTI

JOMONQULOVA FAZILAT ESIRGAPOVNA

KIBER XAVFSIZLIK

DARSLIK

SAMARQAND - 2024

UO‘K: 004.056(075.8)
J 16
KBK: 32.81ya73

F.E.Jomonqulova
Kiber xavfsizlik [Matn]: **darslik** / Samarqand iqtisodiyot va servis instituti – Samarqand.: “STEP-SEL” MCHJ nashriyoti, 2024 - 238 bet.

Darslikda talabalarga kiber xavfsizlik asoslari fani bo‘yicha bilimlarning nazariy asoslarini, kiber xavfsizlikning asosiy tushunchalari va kategoriyalarini, kiber xavfsizlik tamoyillarini o‘rgatish hamda ularni amaliyotda tatbiq etish ko‘nikmasini hosil qilishdan iborat.

Darslik oliy o‘quv yurtlari bakalavriat ta’lim yo‘nalishining 60310100 – Iqtisodiyot (tarmoqlar va sohalar bo‘yicha), hamda 60310400 - Iqtisodiy xavfsizlik talabalari uchun mo‘ljallangan bo‘lib, undan shu soha o‘qituvchilari, magistrlar, kasb-hunar maktablari o‘qituvchi va talabalari, nazariy bilimlar, amaliy ko‘nikmalar, ishlab chiqarish korxonalarida va davlat organlarida kerakli ma’lumotlarni himoyalash va kompyuter virusiga qarshi kurashishni, ma’lumotlar bazasini xavfsizligini boshqarish va axborotlarga bo‘lgan xavflar to‘g‘risida strategiyali tasavvurga ega bo‘lishlari mumkin.

Taqrizchilar:

D.Q.Yakubjanova – TATU SF O‘quv ishlari bo‘yicha direktor o‘rinbosari, dotsent;
S.M.Xolmonov – SamDU “Suniy intellekt va axborot tizimlari” kafedrasi dotsenti.

Darslik institut Kengashining 2024 - yil 30 - yanvardagi majlisda muhokama qilingan va nashrga tavsiya etilgan. (6-sonli majlis bayoni).

ISBN: 978-9910-753-76-3

© F.E.Jomonqulova, 2024 y.
©“STEP-SEL” MChJ nashryoti. 2024 y.

KIRISH

Kishilik jamiyati hayotining hozirgi bosqichida kiberxavfsizlikni ta’minlash aspektlarini huquqiy, tashkiliy va texnik sathlari, kiberxavfsizlik sohasida xalqaro, milliy va idoraviy me’yoriy-huquqiy baza, kiberxavfsizlik arxitekturasi, strategiya, kiberxavfsizlik siyosati va uni amalga oshirish, axborotni himoyalashda zarur bo‘ladigan axborot xavfsizligini baholash mezonlari, axborot xavfsizligiga bo‘ladigan tahdidlar, hujumlar darajasini aniqlash, axborot xavfsizligini tashkil etuvchilari va ularning ahamiyati, axborotni himoyalashda kriptografiyaning o‘rni, identifikatsiya va autentifikatsiya tushunchasi, parollarga bo‘ladigan hujumlar, ma’lumotlarni butunligini ta’minlashda elektron raqamli imzoning ahamiyati, axborotga nisbatan foydalanish huquqlarini boshqarish, kompyuter tarmog‘i asoslari va unga bo‘ladigan hujumlar, tarmoqlararo ekran va himolangan virtual tarmoq texnologiyalari, zararkunanda dasturlardan himoyalanish, axborotga bo‘ladigan risklarni boshqarish kabi tushunchalarni o‘z ichiga olgan.

Ayniqsa, bugungi kunda asrimizning global muammolari qatoriga yangidan-yangi turlari bilan tilga olinayotgan kiberjinoyatchilik kirib kelganiga ham ancha bo‘ldi. Uning bizga ma'lum bo‘lgan virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag‘larni o‘zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo‘hton, ma'naviy buzuq ma'lumotlarni tarqatish bilan bashariyat hayotiga katta xavf solayotganidan ko‘z yuma olmaymiz.

«Kiberjinoyatchilik» tushunchasi axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, ma'lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o‘g‘irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi.

Shu o‘rinda kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko‘lami ham oshib borayotganini ta'kidlash joiz. Kiberterroristik harakat (kiberhujum) - komp`yuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog‘lig‘iga bevosita xavf tug‘diradigan yoki potentsial xavf tug‘dirishi mumkin bo‘lgan, moddiy ob'ektlarga katta zarar etkazishi yoki shunga olib kelishi mumkin bo‘lgan, ijtimoiy xavfli oqibatlarning

boshlanishi yoki maqsadi bo‘lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog‘liq.

Ekspertlarning xulosasiga ko‘ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko‘maklashish, umuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta'sir o‘tkazish, ularni turli yo‘llar bilan o‘z maqsadlari sari bo‘ysundirish orqali amalga oshirilmoqda.

Afsuski, bu jarayonda kiberhujumlarni uyushtirish, bu yo‘lda internet global tarmog‘ining mislsiz imkoniyatlaridan «samarali» foydalanishga urinishlar tobora avj olmoqda.

Internetda mavjud ijtimoiy tarmoqlar, ularning ishlab chiqaruvchilari va homiylarining suveren davlat ichki ishlariga «aralashishlari» qanday rol` o‘ynashi oxirigacha o‘rganilmaganligi bois ba'zan bunday «aralashuv» mazkur davlatga qarshi ekanligi hali hanuz e'tirof etilgani yo‘q.

Ijtimoiy tarmoqlar egalari ushbu tarmoqlar sahifalarida davlat tuzumini ag‘darishga da'vat qilingani uchun javobgarlikka tortilishining xalqaro miqyosdagi huquqiy asoslari yaratilmagan. Vaholanki, har bir qilingan jinoiy xatti-harakat yoki harakatsizlik mazmun-mohiyatiga ko‘ra, albatta, javobsiz va jazosiz qolmasligi kerak.

Internet saytlari to‘satdan paydo bo‘lib, ko‘pincha formatini, so‘ngra manzilini o‘zgartiradi. Shu bois ayrim ekspertlar internetning butkul ochiqligi kabi dastlabki kontseptsiyalardan voz kechib, uning yangi tizimiga o‘tishni taklif etmoqda.

Yangi modelning asosiy mohiyati tarmoqdan foydalanuvchilarning anonimligidan voz kechishdir. Bu tarmoqning jinoiy tajovuzlardan yanada ko‘proq himoyalangan bo‘lishini ta'minlashga imkon berdi.

Misol tariqasida, yopiq tarmoq tizimiga o‘tgan Xitoy davlatini va bunday jarayonga tayyorgarlik ko‘rayotgan Rossiya davlatini keltirishimiz mumkin.

Jahon hamjamiyatiga integratsiyalashayotgan mamlakatimizda axborot kommunikatsiya texnologiyalari, axborot tizimlari va zamonaviy komp`yuter texnologiyalaridan samarali foydalanish bo‘yicha izchil davlat siyosati olib borilmoqda.

Bugungi kunda mamlakatimizda joriy etilayotgan zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar va imkoniyatlar eshigini ochmoqda.

Mazkur jarayon bilan bir qatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta'minlash muammosi ham mavjud, albatta.

Bu eng dolzarb masalalardan biri - kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo‘lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Kundan-kunga takomillashib ketayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta'minlashda quyidagi asosiy talablarni bajarish orqali ulardan himoyalanish, ya'ni kiberxavfsizlikni ta'minlashimiz mumkin:

xodimlarga axborot xavfsizligi asoslarini o‘rgatish;

foydalanayotgan dasturiy mahsulotlarning zaifliklarini doimiy sinovdan o‘tkazish;

ishonchli antivirus dasturidan foydalanish;

litsenziyalangan rasmiy dasturlardan foydalanish;

axborot tizimlarini himoyalashda ko‘p faktorli autentifikatsiyadan foydalanish;

parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish;

muntazam ravishda komp`yuter qattiq disklaridagi ma'lumotlarni shifrlash.

Shu o‘rinda, mamlakatimizda kiberjinoyatlarning oldini olish va unga qarshi kurashni olib boruvchi vakolatli davlat idoralariga ham muayyan vazifalar yuklanishini alohida ta'kidlash lozim.

Xususan, ular kiberjinoyatchilikka qarshi kurash faoliyatida O'zbekiston Respublikasi va uning xalqini axborot texnologiyalari va kommunikatsiyalari orqali amalga oshirilayotgan yoki bunga imkon berayotgan shaxs, jamiyat va davlat xavfsizligini va ularning manfaatlari tashqi hamda ichki kibertahdidlardan himoya qilinishini ta'minlash, mazkur sohada qonuniylik va qonun ustuvorligini mustahkamlash, kiberjinoyatlar va kiberhuquqbuzarliklarning oldini olish, ularni aniqlash va barham berish kabi vazifalarni amalga oshirishi darkor.

Shuningdek, kiberjinoyatlar va kiberhuquqbuzarliklarni tergov qilish va ularni aniqlash, bartaraf etish hamda oldini olish bo‘yicha zarur qarorlar qabul qilish, kiberjinoyatchilikka qarshi kurashish

bo‘yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqishda ishtirok etish, kiberterrorizm, kiberekstremizm, uyushgan jinoyatchilikka qarshi kurashish, davlat organlari manfaatlariga hamda kiberxavfsizligiga tahdid soluvchi kiberhatarlarni aniqlash va ularga qarshi kurashish, kiberjinoyatlar bo‘yicha tergovga qadar tekshiruv va dastlabki tergovni o‘tkazish, tezkor-qidiruv faoliyatini amalga oshirish, fuqarolarning huquq va erkinliklariga tahdid soluvchi kiberjinoyatlarning sodir etilishiga imkon yaratuvchi sabablar hamda shart-sharoitlarni aniqlash va bartaraf etish kabi muhim vazifalarni bajarishlari lozim.

I BOB. KIRISH. KIBER XAVSIZLIKNING ASOSIY TUSHUNCHALARI VA TARIXI

1.1. Asosiy tushunchalar

Kiberxavfsizlik

Kiberxavfsizlik hozirda kirib kelgan yangi tushunchalardan biri bo‘lib, unga turli berilgan turli ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force (CSEC2017 JTF) kiberxavfsizlikka quyidagicha ta’rif bergan: *kiberxavfsizlik – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan jaroitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. U o‘zi ichiga xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlil qilish va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jixatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi.*

Tarmoq bo‘yicha faoliyat yuritayotgan *Cisco* tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: *Kiberxavfsizlik – tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo‘q qilishni; foydalanuvchilarni pul undirishni; yoki normal ish faoliyatini uzub qo‘yishni maqsad qiladi. Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar sonining ko‘pligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.*

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfrem kompyuterlar ishlab chiqarilgandan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalarni va ular xizmat qilgan missiyalarni himoyasini uchun ko‘p qatlamli xavfsizlik amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini ortishi natijasida kompleks va texnologik tomondan murakkab bo‘lgan ishonchli xavfsizlik paydo bo‘ldi.

1.2. Axborotning xavfsizlikka oid xususiyatlari

Hozirgi kunda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassis kiberxavfsizlikning fundamental bilimlariga ega bo‘ligi talab etiladi. Xususan, shundan kelib chiqib kiberxavfsizlik fan sohasini tuzulishini quyidagicha tasvirlash mumkin (1.1-rasm).



1.1-rasm. Kiberxavfsizlik fan sohasining tuzulishi

Kiberxavfsizlikni fundamental terminlarini aniqlashning turli yondashuvlari mavjud. Xususan, CSEC2017 JTF manbasida mualliflar tomonidan kiberxavfsizlikni quyidagi 6 termini keltirilgan:

1. Konfidensiallik. Tizim ma'lumoti va axborotiga faqat vakolatga ega subyektlar foydalanishi mumkinligini ta'minlovchi qoidalar. Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan "o'qilishini" ta'minlaydi.

2. Yaxlitlik (butunlik). Ma'lumotni aniq va ishonchli ekanligiga ishonch hosil qilish. Ya'ni, axborotni ruxsat etilmagan o'zgartirishdan yoki "yozish"dan himoyalash.

3. Foydalanuvchanlik. Ma'lumot, axborot va tizimdan foydalanishning mumkinligi.

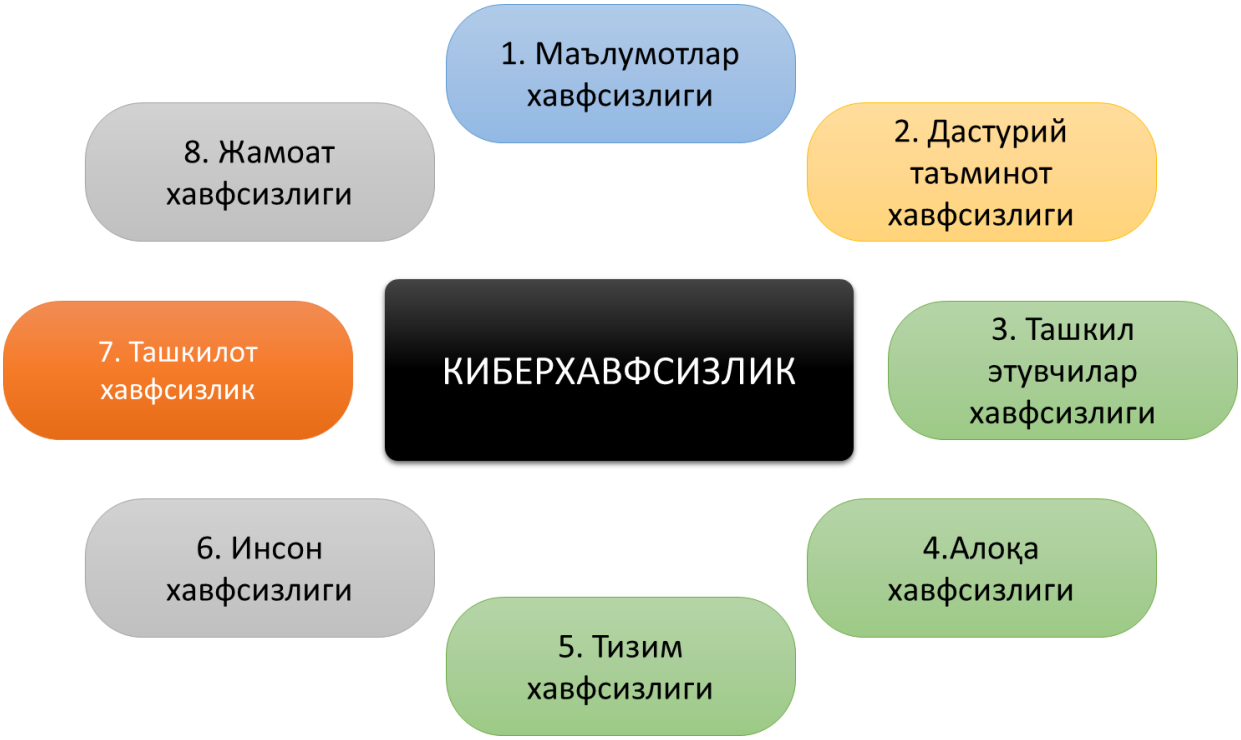
4. Risk. Potensial foyda yoki zarar.

5. Hujumchi kabi fikrlash. Bo'lishi mumkin bo'lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni.

6. Tizimli fikrlash. Kafolatlangan amallarni ta'minlash uchun ijtimoiy va texnik cheklovlarni o'zaro ta'sirini hisobga oladigan fikrlash jarayoni.

1.3. Kiberxavfsizlikning bilim sohalari

CSEC2017 JTF manbasiga ko‘ra kiberxavfsizlikni 8 ta bilim sohasiga ajratilgan bo‘lib, o‘z o‘rnida ularning har biri qism sohalarga bo‘linadi (1.2-rasm).



1.2-rasm. Kiberxavfsizlik bilim sohalari

“Ma’lumotlar xavfsizligi” bilim sohasi ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi. Mazkur bilim sohasi himoyani to‘liq amalga oshirish uchun matematik va analitik algoritmlardan foydalanishni talab etadi.

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

“Tashkil etuvchilar xavfsizligi” bilim sohasi katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi. Tizim xavfsizligi gohida tashkil etuvchilar xavfsizligidan farq qiladi. Tashkil etuvchilar xavfsizligi ular qanday loyihalanganligi, yaratilganligi, sotib olinganligi, boshqa tarkibiy qismlarga ulanganligi, qanday ishlatilganligi va saqlanganligiga bog‘liq.

“Aloqa xavfsizligi” bilim sohasi tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.

“Tizim xavfsizligi” bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun nafaqat, uning tarkibiy qismlari va ulanishini tushunishni, balki butunlikni hisobga olishni talab qiladi. Ya’ni, tizimni to‘liqligicha ko‘rib chiqishni talab qiladi. Mazkur bilim sohasi “Tashkil etuvchilar xavfsizligi” va “Aloqa xavfsizligi” bilim sohalari bilan bir qatorda, ushbu bilim sohasi tashkil etuvchilar ulanishining xavfsiligi va undan katta tizimlarda foydalanish masalasini hal qiladi.

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

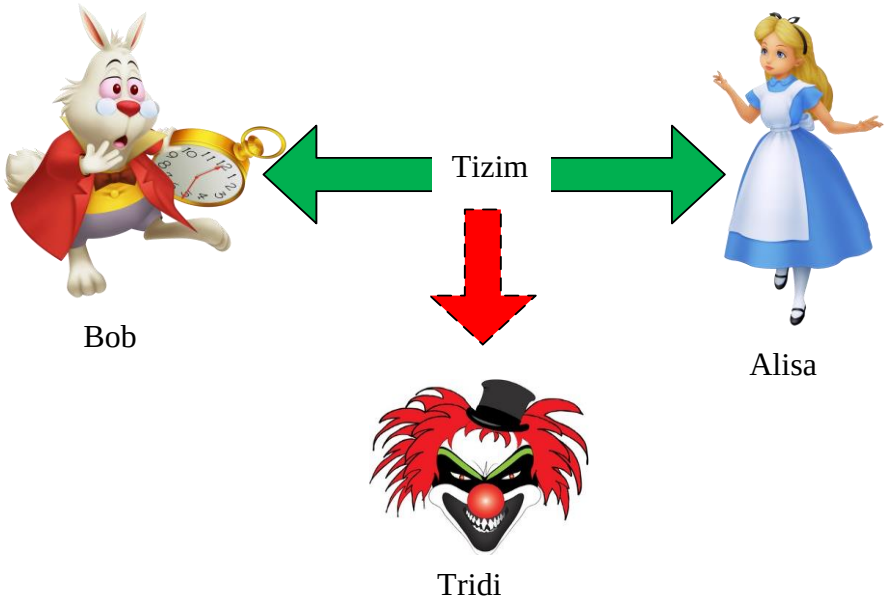
“Tashkilot xavfsizligi” bilim sohasi tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini madadlash uchun risklarni boshqarishga e’tibor qaratadi.

“Jamoat xavfsizligi” bilim sohasi u yoki bu darajada jamiyatda 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.

Shundan kelib chiqib aytish mumkinki, “Kiberxavfsizlik asoslari” kursi axborot texnologiyalari mutaxassisligi uchun eng muhim sohalar va bilimlar to‘g‘risida asosiy bilimlarni qamrab oluvchi umumiy kurs hisoblanadi.

Axborot xavfsizligining hayotiy timsollari

Axborot xavfsizligi hayotda mavjud bo‘lgan timsollarga asoslanadi. Hayotda faqat qonuniy tomondan faoliyat olib boruvchi shaxslar mavjud bo‘lib, ular 1.3-rasmda **Alisa** va **Bob** timsolida akslantirilgan. Biroq hayotda qonuniy faoliyat yurituvchi insonlarni faoliyatiga ruxsatsiz qiziquvchi, ularni ishiga xalaqit beruvchi insonlar ham mavjud va ular 1.3-tasvirda **Tridi** timsolida akslantirilgan. Tridi timsoli barcha g‘arazli niyatlarni amalga oshiruvchi shaxsni ifodalaydi.

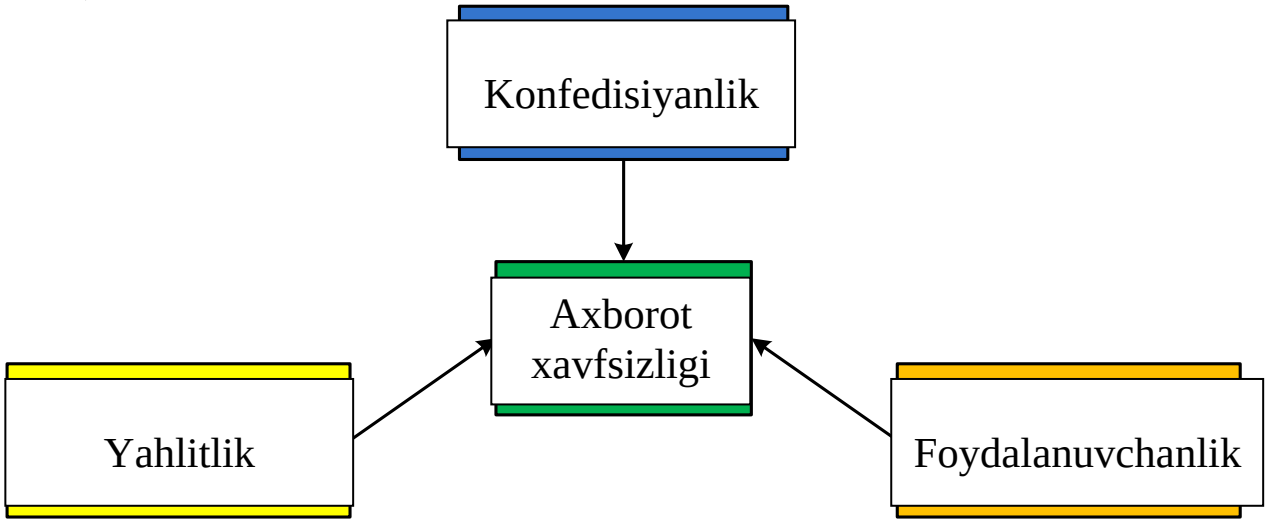


1.3-rasm. Axborot xavfsizligini hayotdagi timsollari

Ma’ruzani keyingi qismlarini yoritish uchun quyidagi hayotiy senariyni qaraylik. Ushbu hayotiy senariy *Alisaning onlayn banki (AOB)* deb ataladi. Bunga ko‘ra, Alisa onlayn bank biznesi faoliyatini boshlagan. Mazkur seneriyda Alisaning xavfsizlik muammosi nima? Alisaning mijozi bo‘lgan Bobda xavfsizlik muammosichi? Alisa va Bobni xavfsizlik muammolari bir xilmi? Tridi nuqtai nazaridan qaraganda, qanday xavfsizlik muammosi mavjud?

Axborotning konfidensialligi, butunligi va foydalanuvchanligi

Axborot xavfsizligi (information security) – axborotning konfidensialligini, butunligini va foydalanuvchanligini saqlashidir (1.4-rasm).



1.4-rasm. Axborot xavfsizligining tashkil etuvchilari

Konfidensiallik (Confidentiality) **–** axborotni ruxsat etilmagan o‘qishdan himoyalash bilan shug‘ullanadi. AOB senariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob Tridini o‘z balansida qancha pul borligini bilishni istamaydi. Shuning uchun Bob uchun balans haqidagi ma’lumotlarni konfidensialligini ta’minlash muhim hisoblanadi.

Yaxlitlik (Integrity) **–** axborotni ruxsatsiz “yozish”dan (ya’ni, ma’lumotni o‘zgartirishdan) himoyalash yoki kamida o‘zgartirilganligini aniqlash bilan shug‘ullanadi. AOB senariysida Alisaning banki Tridan qayd yozuvi butunligini himoyalashi shart, aytaylik, Bob akkauntida balansning o‘zgarishi yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Bu o‘rinda shunga e’tibor berish kerakki, konfidensiallik va butunlik bir narsa emas. Masalan, Tridi biror ma’lumotni o‘qiy olmagan taqdirda ham uning sezilmaydigan darajada o‘zgartirish mumkin.

Foydalanuvchanlik (availability) **–** axborotni (yoki tizimni) boshqarish imkoniyatini kamaytirishni oldini olish bilan shug‘ullanadi. AOB senariysida Alisaning banki va Bob uchun AOB veb saytidan foydalanib bo‘lmaslik, foydalanuvchanlik muammosi hisoblanadi. Sababi, mazkur holda Alisa pul o‘tkazmalaridan daromad ola olmaydi va Bob esa o‘z biznesini amalga oshira olmaydi. Foydalanuvchanlikni buzushga qaratilgan hujumlardan eng mashhuri – Xizmat ko‘rsatishdan vos kechishga undash hujumi (Denial of service) hisoblanadi.

Risk

Risk – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilsa, unda risk paydo bo‘ladi.

Masalan, universitetga kirish jarayonini olsak. Umumiy holda ushbu holatni o‘zi risk hisoblanmaydi. Ammo, agar abituriyent hujjatlarni topshirib kirish imtihonlarini topshirsa, u o‘qishga kirishi yoki kirmasligi mumkin. Bu o‘z navbatida qabul qilinish riskini yoki qabul qilinmaslik riskini yuzaga kelishiga olib keladi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklar salbiy ko‘rinishda qaraladi.

Riskga ISO tomonidan berilgan ta’rif quyidagicha:

Risk – bu noaniqlikning maqsadlarga ta’siri.

Maqsad – u yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz hisoblanadi. So‘ngi keltirilgan misolda abituriyentning maqsadi – bu universitetga kirishdan iborat.

Noaniqlik – hozisaga, uning oqibatlari yoki uning ehtimolini bilishga aloqador axborotni yoki bilimlarni etishmasligi yoki qisman yetishmasligi holati. So‘ngi keltirilgan misolda, murojaat etuvchini o‘qishga kirish yoki kirmasligi noma’lum. Bundan tashqari o‘qishga kirsa yoki kirmasa uni nima kutayotgani ham no‘malum.

Ta’sir – kutilgan yoki xoxlagan hodisani salbiy yoki ijobiy tomonga og‘ishi. So‘ng misolda aytaylik, talaba “shartnoma” asosiy o‘qishni kutayotgan bo‘lsin. Bu holda kutilganidan salbiy og‘ish bo‘lganda, o‘qishga kira olmaydi, agar kutilganidan ijobiy tomonga og‘ish kuzatilsa byudjetga kiradi.

Risk ko‘p hollarda voqyea oqibatlari va yuzaga kelish ehtimoli bilan bog‘liq holda na’moyon bo‘ladi.

Axborot xavfsizligi riski tashkilotga zarar yetkazishi mumkin bo‘lgan axborot aktivlari yoki aktivlar guruhidagi mavjud zaiflikdan foydalanish orqali amalga oshiriladi.

Aktiv – tashkilot uchun qadrli bo‘lgan ixtiyoriy narsa bo‘lib, axborot xavfsizligiga bog‘liq holda aktiv sifatida tashkilotning muhim ahborotini keltirish mumkin.

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. Tahdid tashkilotning aktivlariga qaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror saqlaguvchi hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin.

Zaiflik – bu bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik hisoblanadi. So‘ngi keltirilgan misolda, xonada saqlangan tashkilot hujjatini qo‘g‘oz ko‘rinishda bo‘lgani sabab, uni yonishi mumkinligidir.

Boshqarish vositasi (*Control*) – bu riskni o‘zgartiradigan harakatlar bo‘lib, boshqarish natijasi zaiflik yoki tahdidga ta’sir qiladi. Bundan tashqari boshqarish vositasining o‘zi turli tahdidlar uchun foydalanililishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin. Tashkilotda saqlangan qog‘oz ko‘rinishidagi axborotni yong‘inga qarshi himoyalash uchun yong‘inni o‘chirish vositalarini boshqarish vositasi sifatida ko‘rish mumkin. Bundan tashqari, yong‘in bo‘lganda xodimlarni o‘zini tutishlari va yong‘inni oldini olish uchun o‘tkazilgan chora tadbirlar ham boshqarish vositasi bo‘lishi mumkin. Yong‘inga

qarshi kurashish tizimining ishlammay qolish holati esa boshqarish vositasidagi kamchilik sifatida xizmat qiladi.

1.4. Kiberjinoyatchilik.

Kiberjinoyatchilik bu – kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. Kiberjinoyatchilikning eng keng tarqalgan turlari bu: kompyuter qaroqchiligi, onlayn firibgarlik, kompyuter tizimlariga hujum qilish, shaxsiy ma'lumotlarni o'g'irlash va noqonuniy yoki taqiqlangan ma'lumotlarni tarqatish.

Kiberjinoyatni amalga oshirganda quyidagilar asosiy maqsad sifatida qaraladi:

- pul, qimmatli qog'ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko'chmas mulk, yoqilg'i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy olish;
- soliq va turli yig'imlarni to'lashdan bosh tortish;
- jinoiy daromadlarni legallashtirish;
- qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuqlar uchun kassa chiptalarini qalbakilashtirish yoki tayyorlash;
- shaxsiy yoki siyosiy maqsadlarda maxfiy ma'lumotlarni olish;
- ma'muriyat yoki ishdagi hamkasblar bilan shaxsiy dushmanlik munosabatlari asosida qasos olish;
- shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish;
- mamlakatdagi vaziyatni, hududiy ma'muriy tuzulishni beqarorlashtirish yoki siyosiy maqsadlar uchun tartibga solish;
- talonchilik, raqibni yo'q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ishini tartibga solmaslik;
- boshqa jinoyatlarni yashirish uchun;
- tadqiqot masalalarida;
- shaxsiy intelektual qobiliyat yoki ustunlikni namoyish qilish uchun.

Kiberjinoyatlar hajmini keskin oshishiga quyidagilar motiv bo'lib xizmat qilmoqda:

- moliyaviy qiyinchilikdan chiqish;
- jinoyatchidan qarzdorligini kechikmasdan jamiyatdan olish;
- kompaniyadan va ish beruvchidan o'ch olish;
- o'zini tengsizligini ko'rsatish uchun.

1.5. Kiberqonunlar

Kiberjinoyatchilikning turlari

Kiberjinoyat turlarini qat'iy bir klassifikasiyalashning imkoni yo‘q. Shuning uchun, quyida kriminologiya sohasida aloqador holda kiberjinoyatlarni turlari bilan tanishib o‘tiladi. Kriminologiya sohasiga oid adabiyotlarda kiberjinoyatchilikning quyidagi turlari keltirilgan:

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

Iqtisodiy kompyuter jinoyatlari amalda ko‘p uchraydi. Ular jinoyatchilarga miliionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiridi. Ular orasida keng tarqalgani bu – firibgarlik. Firibgarlik asosan bank hisobraqamlari va bank kartalari orqali amalga oshiriladi. Xalqaro amaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yoki o‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardan foydalanish, karta taqdim etmasdan bank hisobvarag‘i ma'lumotlarini olish va noqonuniy foydalanish bilan, shuningdek karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

Kiberjinoyatlarning yana bir turi bu – inson va fuqorolarning huquqlari va erkinliklariga qarshi jinoyatlar, "kompyuter qaroqchiligi"dir. Ushbu jinoyatlar dasturiy ta'minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi. Bu dasturiy ta'minot va ma'lumotlar bazasini yaratish bilan bog‘liq huquqiy munosabatlarga (mualliflik huquqi) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta'minot kompaniyalariga katta moliyaviy yo‘qotishlarni keltirib chiqaradi.

"Maykrosoft Armaniston" kompaniyasining direktori Grigor Barsegyanning takidlashicha, "kompyuter qaroqchiligi" ishlab chiqaruvchilarga etkazgan zarari yiliga 66 mlrd. dollarni tashkil qiladi. Uning so‘zlariga ko‘ra Armanistonlik istemolchilar o‘zlarining moliyaviy resurslarini tejash uchun viruslarni yuqtirish xavfi yuqori bo‘lgan dasturlardan ongli ravishda foydalanadilar.

Kompyuter jinoyatchiligining oxirgi turi bu – jamoat yoki davlat xavfsizligiga qarshi kompyuter jinoyati bo‘lib, ularga davlat yoki jamoat xavfsizligiga qaratilgan jamoat uchun xavfli xatti - harakatlar kiradi va ular ko‘pincha ma'lumot uzatish qoidalarini buzilishi,

mamlakat mudofaa tizimining yoki uning tarkibiy qismlarining buzilishi bilan bog‘liq bo‘ladi.

1.6. Kiberetika

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

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

Mulk

Axborotdan foydalanishdagi etikaga oid munozaralar uzoq vaqt davomida mulkchilik tushunchasini tashvishga solmoqda. Bu kiberetika sohasidagi ko‘plab to‘qnashuvlarga sabab bo‘ldi. Egalikka oid nizolar egalik huquqi buzilgan yoki noaniq bo‘lgan hollarda yuzaga keladi.

Intellektual mulk huquqlari

Internet tarmog‘ining doimiy ravishda o‘sib borishi va turli ma’lumotlarni siqish texnologiyalarining (masalan, mp3) paydo bo‘lishi “peer-ro-peer” fayl almashinuviga katta yo‘l ochdi. Bu texnologiya dastlab foydalanuvchilar Napster kabi dasturlarga paydo bo‘lgan bo‘lsa, endilikda BitTorrent kabi ma’lumotlarni uzatish protokollarida foydalaniladigan fayllarni bir-biriga anonim uzatish imkoniyatini beradi. Uzatilgan musiqalarning aksariyati mualliflik huquqi bilan himoyalangan bo‘lsada, bu usul boshqalarga tarqatishni noqonuniy holga keltirgan.

Hozirgi kunda aksariyat elektron ko‘rinishdagi media fayllar (musiqa, audio va kinolar) intelektual mulk huquqlariga rioya qilmasdan ommaga tarqalmoqda. Masalan, aksariyat katta mablag‘

sarflangan kinolarning peratiskiy versiyasi chiqishi natijasida, o‘z sarf xarajatini qoplay olmaslik holatlari kuzatilmoqda.

Bu holatni dasturiy ta’minotlar uchun ham ko‘rish mumkin. Masalan, aksariyat dasturlar lisenziyaga ega hisoblansada, turli usullar yordamida ularning “crack” qilingan versiyalari amalda keng qo‘llaniladi. Masalar, lisenziyaga ega bo‘lmagan Windows 10 OT, antivirus dasturiy vositalari, ofis dasturiy vositalari va hak.

Mualliflik huquqini himoyalashning texnik vositalari

Mualiflik huquqini ta’minlashda turli himoya usullaridan foydalaniladi. Bular CD/DVD disklardagi ma’lumotlarni ruxsatsiz ko‘chirishdan himoyalashdan tortib, oddiy PDF fayllarni tahrirlash imkoniyatini cheklash kabi jarayonlarni o‘z ichiga olishi mumkin. Biroq, boshqa toifadagi insonlar agar men lisenziyaga ega CD diskni sotib olsam, undan ko‘chirish imkoniyatiga ham ega bo‘lishim kerak deb fikrlaydilar.

Xavfsizlik

Internet tarmog‘idagi axborotdan foydalanganda xavfsizlik anchadan beri axloqiy munozaralar mavzusi bo‘lib kelgan. Bu birinchi navbatda jamoat faravonligini himoya qilish yoki shaxs huquqini himoya qilish degan savolni o‘rtaga qo‘yadi. Internet tarmog‘ida foydalanuvchilar sonini ortishi, shaxsiy ma’lumotlarni ko‘payishi natijasida ularning o‘g‘irlanishi va kiberjinoyatlar soni ortmoqda.

Aniqlik

Internetning mavjudligi va ba’zi bir shaxs yoki jamoalar tabiati tufayli ma’lumotlarning aniqligini bilan shug‘ullanish muammoga aylanmoqda. Boshqa so‘z bilan aytganda Internetdagi ma’lumotlarning aniqligiga kim javob beradi? Bundan tashqari Internetdagi ma’lumotlarni kim to‘ldirib boradi, undagi xatolar va kamchiliklar uchun kim javobgar bo‘lishi kerakligi to‘g‘risidagi tortishuvlar mavjud.

Foydalanuvchanlik, senzura va filterlash

Foydalanuvchanlik, senzura va axborotni filterlash mavzulari kiberetika bilan bog‘liq ko‘plab axloqiy masalalarni ko‘taradi. Ushbu masalalarning mavjudligi bizning maxfiylik va shaxsiylikni tushunishimizga va jamiyatdagi ishtirokimizga shubha tug‘diradi. Agar biror qonun qoidaga asosan ma’lumotlardan foydalanishni cheklash yoki filterlash asosida ushbu ma’lumotni tarqalishi yoki foydalanuvchanligiga ta’sir qilish mumkin. Hozirda ushbu holatlar amalda keng qo‘llanilmoqda. Senzura ham past darajada (masalan, kompaniya o‘z xodimlari uchun) yoki yuqori darajada (hukumat

tomonidan xavfsizlikni ta’minlash uchun amalga oshirilgan) bo‘lishi mumkin. Mamlakatga kiruvchi ma’lumotlarni boshqarishning eng yaxshi misollaridan biri bu “Buyuk Xitoy Fayrvoli” nomi bilan mashhur bo‘lgan loyihadir.

Axborot erkinligi

Axborot erkinligi, ya’ni so‘z erkinligi, shu bilan birga ma’lumot qidirish, olish va uzatish erkinligi kiberhujumda kimga va nimaga yordam beradi degan savol tug‘iladi? Axborot erkinligi huquqi, odatda, ta’sirlangan mamlakat, jamiyat yoki madaniyatga ta’sir ko‘rsatadigan cheklovlarga bog‘liq. Cheklovlar turli ko‘rinishlarda bo‘lishi mumkin. Masalan, ayrim mamlakatlarda Internet ommaviy axborot vositalariga kirishning bir shakli hisoblanadi va undan barcha davlat rezidentlari foydalanadi. Bundan tashqari, ayrim davlatlarda Internetdan foydalanish bo‘yicha cheklovlar shtatlar kesimida farq qilishi mumkin.

Raqamli to‘siqlar

Axborot erkinligi bilan bog‘liq axloqiy masalalardan alohida muammo raqamli to‘siq deb ataladi. Bu raqamli va axborot texnologiyalaridan, masalan, kiberfazodan foydalanish imkoniyati cheklangan yoki kirish 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 kontentlardan voyaga yetmaganlar tomonidan foydalanish doim axloqiy munozaralarga sabab bo‘lmoqda. Ayrim davlatlarda bunday kontentlardan foydalanish qattiq taqiqlansa, ayrim davlatlarda bunga ruxsat berilgan.

Qimor o‘yinlari

Bu muammo ham etik masaladagi munozaralardan biri bo‘lib, uni kimlardir zarar deb hisoblasa, yana kimlardir ularga qonun aralashuvini yoqlamaydilar. O’z navbatida ushbu tomonlar orasidagi munozaralar qaysi turdagi o‘yinlarga ruxsat berish kerak? Ular qayerda o‘tkazilishi kerak? degan savollar keng muzokaralarga sabab bo‘lmoqda. Hozirda aksariyat davlatlarda bu turdagi o‘yinlarga qonuniy ruxsat berilgan bo‘lsa, qolganlariga qat’iy cheklovlar mavjud.

Kompyuterlan foydalanish etikalari

Kompyuter etikasi instituti notijoriy tashkilot bo‘lib, vazifasi texnologiyani axloqiy nuqta nazardan targ‘ib qilishdir. Ushbu tashkilot tomonidan quyidagi 10 ta etika qoidalari keltirib o‘tilgan:

- Shaxsiy kompyuteringizdan boshqalarning zarariga foydalanmang.
- Boshqa foydalanuvchilarning kompyuter ishlariga xalaqit bermang.
- Boshqa odamlarning kompyuter fayllariga qaramang.
- O'g'irlik uchun kompyuterdan foydalanmang.
- Yomonlik uchun kompyuterdan foydalanmang.
- O'zingiz pul to'lab sotib olmagan dasturdan foydalanmang va nusxa ko'chirmang.
- Birovni kompyuterini ruxsatsiz foydalanmang.
- Birovlarni intellektual mehnati samarasiga zarar etkazmang.
- Siz yaratgan dasturni ijtimoiy oqibati haqida o'ylang.
- O'z kompyuteringizdan boshqalarga nisbatan ongli va hurmat bilan foydalaning.

Axborotdan oqilona foydalinish kodeksi

Axborotdan oqilona foydalanish kodeksi buxgalteriya tizimiga qo'yiladigan talablarni ta'kidlaydigan besh tamoilga asoslanadi. Ushbu talablar AQSh sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligin tomonidan 1973 yilda kiritilgan:

- Shaxsiy ma'lumotlarni to'playdigan tizimlar bo'lmasligi kerak. Biroq, bu haqiqat sirdir.
- Har bir kishi tizimda u to'g'risida qanday ma'lumotlar saqlanishini va undan qanday foydalanilishini boshqarishi kerak.
- Har bir kishi u to'g'risida to'plangan ma'lumotlardan bitta maqsadda, boshqa maqsadlarda foydalanilishini oldini olish imkoniyatiga ega bo'lishi kerak.
- Har kim o'zi haqidagi ma'lumotlarni to'g'irlashi kerak.
- Shaxsiy ma'lumotlar sirasiga kiruvchi ma'lumotlar to'plamini yaratish, saqlash, ishlatish yoki tarqatish bilan shug'ullanadigan har bir tashkilot ushbu ma'lumotlardan faqat ular belgilangan maqsadlar uchun foydalanilishini ta'minlash va ulardan boshqa maqsadlarda foydalanilishiga qarshi choralar ko'rishi kerak.

Milliy qonunlar

2002 yil 12 dekabrda O'zbekiston Respublikasining 439-II – sonli "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi qonuni qabul qilindi. Ushbu qonun 16 moddadan iborat. Xususan unda quyidagilar belgilangan:

1-modda. Ushbu Qonunning asosiy vazifalari

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

4-modda. Axborot erkinligi

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

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

6-modda. Axborotning ochiqligi va oshkoraligi

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

Maxfiy axborotga quyidagilar kirmaydi:

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

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

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

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

10-modda. Axborot berishni rad etish

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

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

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

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

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

11-modda. Axborotni muhofaza etish

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

Axborotni muhofaza etish:

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

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

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

13-modda. Shaxsning axborot borasidagi xavfsizligi

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

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

Jismoniy shaxsning roziligisiz uning shaxsiy hayotiga taalluqli axborotni, xuddi shuningdek shaxsiy hayotiga taalluqli sirini,

yozishmalar, telefondagi so‘zlashuvlar, pochta, telegraf va boshqa muloqot sirlarini buzuvchi axborotni to‘plashga, saqlashga, qayta ishlashga, tarqatishga va undan foydalanishga yo‘l qo‘yilmaydi, qonun hujjatlarida belgilangan hollar bundan mustasno.

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

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

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

14-modda. Jamiyatning axborot borasidagi xavfsizligi

Jamiyatning axborot borasidagi xavfsizligiga quyidagi yo‘llar bilan erishiladi:

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

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

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

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

15-modda. Davlatning axborot borasidagi xavfsizligi

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

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

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

O’zbekiston Respublikasining jahon axborot makoniga va zamonaviy telekommunikasiyalar tizimlariga integrasiyalashuvi;

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

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

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

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

Javobgarliklar:

O’ZBEKISTON RESPUBLIKASINING MA’MURIY JAVOBGARLIK TO’G’RISIDAGI KODEKSI

155-modda. Axborotdan foydalanish qoidalarini buzish

- Axborot tizimidan foydalanish maqsadida unga ruxsatsiz kirib olishda ifodalangan axborot va axborot tizimlaridan foydalanish qoidalarini buzish —

- fuqarolarga eng kam ish haqining uchdan bir qismidan bir baravarigacha, mansabdor shaxslarga esa — bir baravaridan uch baravarigacha miqdorda jarima solishga sabab bo‘ladi.

- Axborot tizimlarining ishini buzishga olib kelgan xuddi shunday huquqbuzarlik, xuddi shuningdek kirish cheklangan axborot tizimlarini axborot-hisoblash tarmoqlariga ulash chog‘ida tegishli himoya choralarini ko‘rmaganlik —

- fuqarolarga eng kam ish haqining bir baravaridan uch baravarigacha, mansabdor shaxslarga esa — uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.

- Yuridik va jismoniy shaxslarning axborot tizimlarini xalqaro axborot tarmoqlariga qonunga xilof ravishda ulash, bu tarmoqlarga tegishli himoya choralarini ko‘rmasdan ulanish, xuddi shuningdek ulardan ma’lumotlarni qonunga xilof ravishda olish —

- fuqarolarga eng kam ish haqining ikki baravaridan besh baravarigacha, mansabdor shaxslarga esa — besh baravaridan yetti baravarigacha miqdorda jarima solishga sabab bo‘ladi.

- O’zganing elektron hisoblash mashinalari uchun yaratilgan dasturi yoki ma’lumotlar bazasini o‘z nomidan chiqarish yoxud qonunga xilof ravishda undan nusxa olish yoki bunday asarlarni tarqatish —

- fuqarolarga eng kam ish haqining bir baravaridan uch baravarigacha, mansabdor shaxslarga esa — uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.

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

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

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

O’ZBEKISTON RESPUBLIKASI JINOYaT KODEKSI

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

- Xat-yozishmalar, telefonda so‘zlashuv, telegraf xabarlari yoki boshqa xabarlarning sir saqlanishi tartibini qasddan buzish, shunday harakatlar uchun ma’muriy jazo qo‘llanilgandan keyin sodir etilgan bo‘lsa, —

- eng kam oylik ish haqining yigirma besh baravarigacha miqdorda jarima yoki uch yilgacha muayyan huquqdan mahrum qilish yoki uch yuz oltmish soatgacha majburiy jamoat ishlari yoxud uch yilgacha axloq tuzatish ishlari bilan jazolanadi.

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Risk nima?
2. Kiberhujum nima?
3. Hujumchi kabi fikrlash qanday amalga oshiriladi?
4. Kiberjinoyatchilik nima?
5. Kiberqonunlarga qaysi qonunlar kiradi?
6. Kiberetika deganda nimani tushunasiz?

II BOB. AXBOROTNING KRIPTOGRAFIK HIMOYASI

2.1.Kriptografiya bo‘limlari

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

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

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

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

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

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

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

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

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

Quyida keyingi bayonlarda ishlatiluvchi asosiy atamalarga oydinlik kiritiladi.

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

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

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

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

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

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

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

2.2. Kriptografiya tarixi

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

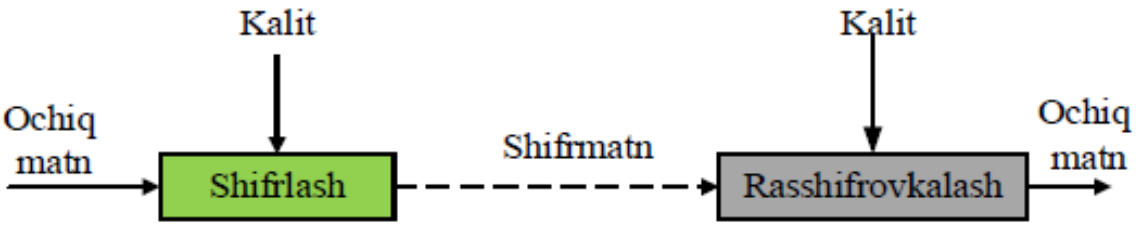
Kriptotizim (cryptosystem) – ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o‘zgartirishlar oilasi.

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

Kriptotizimning “qora quti” sifatidagi ko‘rinishi 2.1 – rasmda keltirilgan.

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.



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

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

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

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

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 aksariyat adabiyotlarda bir necha davrlarga ajratib, turli yondashuvlarga asoslanib o‘rganilgan. Masalan, ba’zi manbalarda hisoblash qurilmalari yaratilgunga qadar foydalanilgan shifrlar – klassik shifrlar davriga tegishli deb olingan.

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

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

2. O‘rta davr (o‘rta davr klassik shifrlari). Ushbu davrda shifrlar asosan ko‘p alfavitli o‘rniga qo‘yishga asoslangan bo‘lib, ularga Vijiner, Atbash usullarini misol sifatida keltirish mumkin. Ushbu davrdagi shifrlarning, birinchi davr shifrlariga qaraganda, bardoshligi yuqori bo‘lgan.

3. 1 va 2 – jaxon urushlari davri (1 va 2- jaxon urushlari davridagi klassik shifrlar). Ushbu davr kriptotizimlari asosan elektromexanikaga asoslangan bo‘lib, radioto‘lqin orqali shifrmatnni uzatish (Morze alifbosi) amalga oshirilgan. Mazkur davrga oid shifrlash usullariga Zimmermann telegrammi, Enigma shifri, SIGABA mashinalarini misol sifatida keltirish mumkin.

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

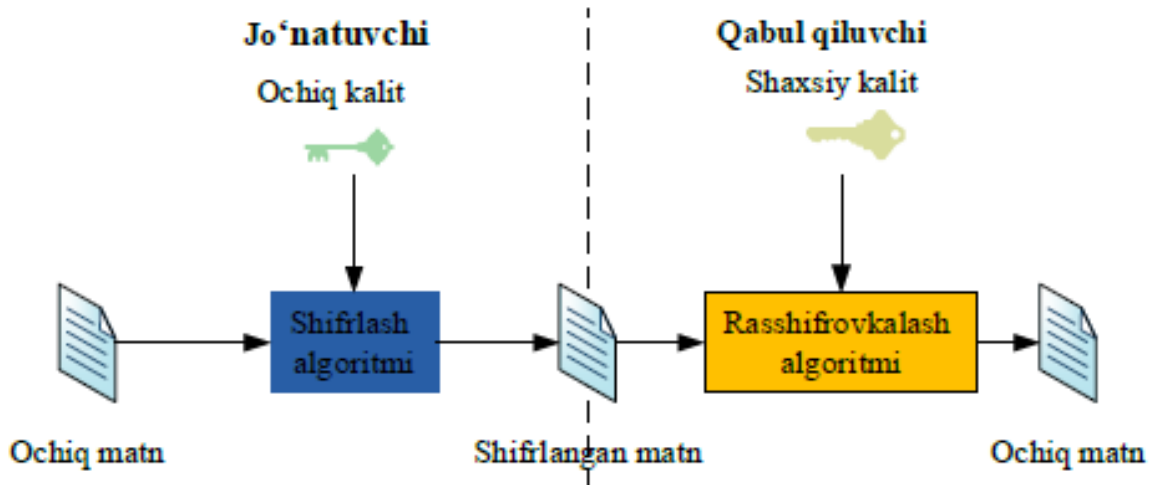
Kriptografiyaning asosiy bo‘limlari.

Kriptografiyani quyidagi bo‘limlarga ajratish mumkin:

1. Simmetrik kalitli kriptografiya. Simmetrik kalitli kriptografiyaning umumiy ko‘rinishi 2.2-rasmdagi kabi bo‘lib, ma’lumotni shifrlash va rasshifrovkalashda yagona kalitdan (simmetrik kalitdan) foydalaniladi. Shuning uchun simmetrik kalitli kriptotizimlarni – bir kalitli kriptotizimlar deb ham yuritishadi. Demak, simmetrik kalitli shifrlash algoritmlaridan foydalanish uchun har ikkala tomonda bir xil kalit mavjud bo‘lishi zarur. Simmetrik kalit odatda bir

tomonda hosil qilinadi va maxsus usullar asosida ikkinchi tomonga xavfsiz tarzda yetkaziladi.

2. Ochiq kalitli kriptografiya. Ochiq kalitli kriptografiyada (yoki asimmetrik kriptografiya deb ham ataladi) ma’lumotni shifrlash qabul qiluvchining ochiq kaliti bilan amalga oshirilsa, uni rasshifrovkalash qabul qiluvchining shaxsiy kaliti bilan amalga oshiriladi. Shuning uchun ham ochiq kalitli kriptotizimlarni ikki kalitli kriptotizimlar deb ham yuritishadi. Ochiq kalitli kriptografiyaning umumiy ko‘rinishi 2.2-rasmda keltirilgan.



2.2-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.

2.3. Kriptografik akslantiishlar

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

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

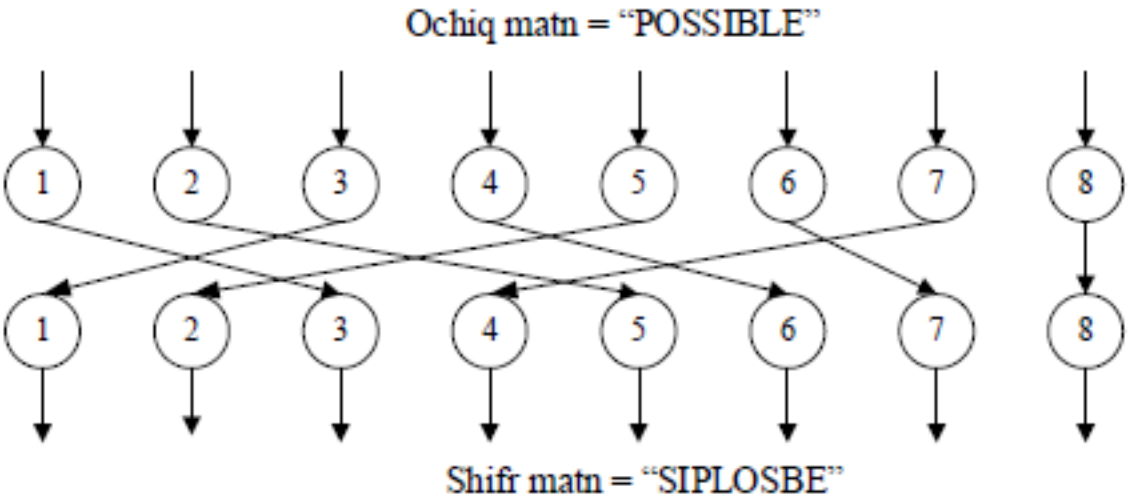
Sodda ko‘rinishda olingan o‘rniga qo‘yish akslantirish amali asosida shifrlash uchun olingan matn quyida keltirilgan. Ushbu sodda shifrlash usuli Sezar nomi bilan mashhur. Masalan, agar ochiq matn “HELLO” ga teng bo‘lsa, unga mos holda shifrmatn “KHOOR” ga teng bo‘ladi. Mazkur holda shifrmatn alfaviti ochiq matn alfavitidan 3 ta pozisiyaga surish natijasida hosil qilingan va shuning uchun shifrlash kalitini 3 ga teng deb hisoblash mumkin (5.1-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.

2.1-jadval

O‘rniga qo‘yish akslantirishiga misol

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

O‘rin almashtirish akslantirishi. Ushbu akslantirishga ko‘ra, ochiq matn simvollarining o‘rni biror qoidaga ko‘ra o‘zaro almashtiriladi. Bunda ochiq matnda ishtirok etgan simvollar shifrmatnda ham ishtirok etib, faqat ularning o‘rni almashgan bo‘ladi (2.3-rasm).



2.3-rasm. Sodda o‘rin almashtirish usuliga misol

Bir martali bloknot. Bir martali bloknot (one time pad) yoki “Vernam shifri” nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanib, tarixda keng foydalanilgan bo‘lsada, ko‘p hollarda amalga oshirishning imkoniyati mavjud bo‘lmagan. Uning bir martali deb atalishiga asosiy sabab, undagi kalitning (bloknotning) bir marta foydalanilishi bo‘lib, uni aksariyat hollarda amalga oshirishning imkoni bo‘lmaydi. Masalan, ushbu shifrlash algoritmi 8 ta simvoldan iborat bo‘lgan alfavit bo‘lsin. Olingan alfavit simvollari va unga mos bo‘lgan binar qiymatlar 2.1 - jadvalda keltirilgan. Alfavit simvollari va ularga mos bit qiymatlari barcha uchun ochiq va sir saqlanmaydi.

Ochiq matn chun tanlangan alfavit

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

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

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

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

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

Jadvaldan, $xx \oplus yy \oplus yy = xx$ tenglik o‘rinligini ko‘rish mumkin. Bu esa bir martali parol bilan rasshifrovkalashda shifrmatnga kalitni XOR amalida bajarilishining o‘zi yetarligini ko‘rsatadi: $PP = CC \oplus KK$.

Faraz qilaylik, A tomon 2.2-jadvaldagi ochiq matn uzunligiga teng bo‘lgan quyidagi kalitga ega bo‘lsin:

111 101 110 101 111 100 000 101

A tomon ushbu kalit asosida shifrmatnni quyidagicha hisoblaydi:

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

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

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

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

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.

III BOB. SIMMETRIK SHIFRLAR. ASSIMMETRIK SHIFRLAR

3.1. Simmetrik kriptografik algoritmlar

Quyida simmetrik kriptotizimlar, shuningdek ularning ikki turi:

oqimli va blokli simmetrik shifrlash algoritmlariga to‘xtalib o‘tiladi. Simmetrik shifrlash algoritmlarida ma’lumotlarni shifrlash va rasshifrovkalashda yagona kalitdan foydalaniladi. Ma’lumotlarni shifrlash va rasshifrovkalash jarayonlarini amalga oshirish tartibi foydalanilayotgan tizim xususiyatiga asosan tanlanadi.

Simmetrik kriptotizimlarning ishlashi bilan tanishishda quyidagi belgilashlar kiritiladi:

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

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

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

3.2. Oqimli simmetrik shifrlash algoritmlari

Oqimli simmetrik shifrlash algoritmlari bir martali bloknotga asoslangan, farqli jihati – bardoshligi yetarlicha pastligi va boshqariladigan kalitning mavjudligi. Ya’ni, kichik uzunlikdagi kalitdan ochiq matn uzunligiga teng bo‘lgan ketma-ketlik hosil qilinadi va undan bir martali bloknot sifatida foydalaniladi.

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

Oqimli shifrni quyidagicha sodda ko‘rinishda yozish mumkin:

StreamCipher(K) = S

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

Agar berilgan ketma-ketlik $S=s_0,s_1,s_2,\ldots$, va ochiq matn $P=S_0,S_1,S_2,\ldots$, berilgan bo‘lsa, XOR amali yordamida shifrmatnning mos bitlari $C= c_0,c_1,c_2,\ldots$, ni quyidagicha hosil qilish mumkin.

$c_0 = S_0 \oplus s_0, c_1 = S_1 \oplus s_1, c_2 = S_2 \oplus s_2$,…

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

$S_0 = c_0 \oplus s_0, S_1 = c_1 \oplus s_1, S_2 = c_2 \oplus s_2$,…

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

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

A5/1 shifrlash algoritmi uchta *chiziqli siljitish registr*laridan iborat, ular mos holda X,Y va Z kabi belgilanadi. X registr o‘zida 19 bit (x_0,x_1,…,x_{18}), Y registr 22 bit (y_0,y_1,…,y_{21}) va Z registr 23 bit (z_0,z_1,…,z_{22}) ma’lumotni saqlaydi. Uchta registrning bunday o‘lchamdagi bitlarni saqlashi bejiz emas. Sababi, chiziqli siljitish registrlari o‘zida jami bo‘lib 64 bitni saqlaydi. A5/1 shifrlash algoritmida foydalaniluvchi kalit K ning uzunligi 64 bitga teng va ushbu kalitdan registrlarni dastlabki to‘ldirish uchun foydalaniladi. So‘ngra oqimli shifrlash algoritmi asosida talab etilgan uzunlikdagi (ochiq matn uzunligiga teng bo‘lgan) ketma-ketliklar generasiyalanadi. Ketma- ketliklarni generatsiyalash tartibini o‘rganishdan oldin, registrlar xususidagi ba’zi ma’lumotlar quyida keltirilgan.

X siljitish registrida quyidagi amallar ketma-ketligi bajariladi:

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

S= 18,17,16,…,1 $uchun\ x_i = x_{i-1}\ x_0 = S$

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

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

va

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

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

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

− agar $x_8 = S$ ga teng bo‘lsa, X siljitiladi;

− agar $y_{10} = S$ ga teng bo‘lsa, Y siljitiladi;

− agar $z_{10} = S$ ga teng bo‘lsa, Z siljitiladi.

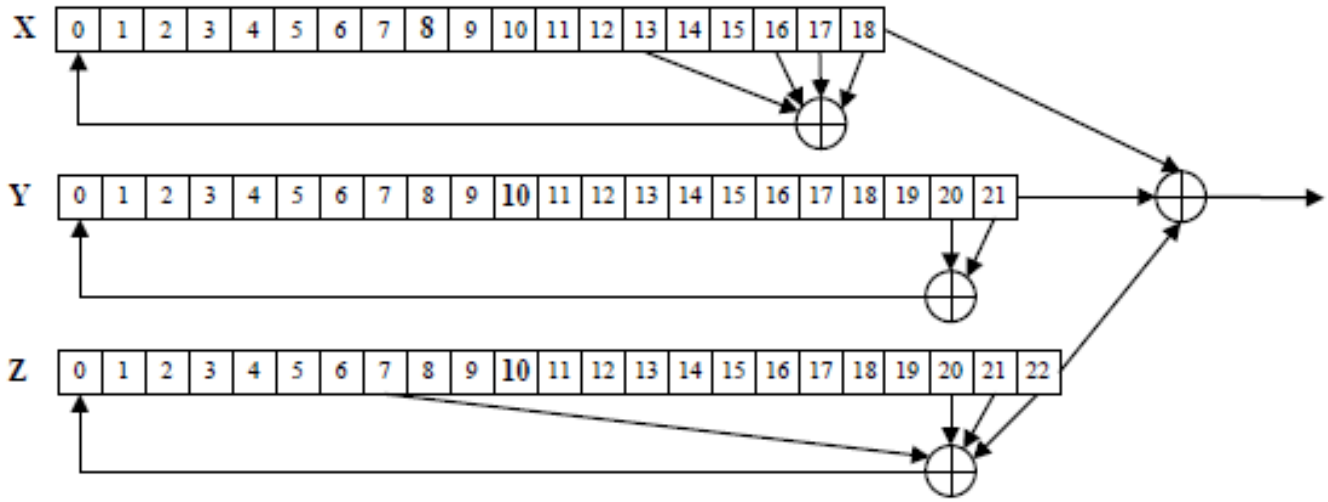
Ketma-ketlikning bir biti s quyidagicha generatsiyalanadi:

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

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

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

A5/1 oqimli shifrlash algoritmi murakkab ko‘rinsada, qurilmada amalga oshirilganida yuqori tezlik qayd etiladi. Umumiy holda A5/1 oqimli shifrni 3.1 - rasmdagi kabi ifodalash mumkin.



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

Hisoblash qurilmalari hozirgi kundagi kabi rivojlanmagan vaqtlarda oqimli shifrlash algoritmlari juda ham mashhur bo‘lgan,

hozirgi kunda esa ularning o‘rnini simmetrik blokli shifrlar egallamoqda. Biroq, shunday holatlar mavjudki, oqimli shifrlar shubhasiz zarur bo‘ladi. Masalan, real vaqt tizimlaridan biri GSM tarmog‘ida ma’lumotlarni shifrlashda blokli simmetrik shifrlarni qo‘llashning imkoni yo‘q. Sababi, shifrlash uchun zarur bo‘lgan bir blokni (blok uzunligi kamida 64 bit bo‘ladi) ma’lum vaqtda to‘plash talab etiladi. Bu esa so‘zlashuvda to‘xtalishlarga olib keladi. Bundan tashqari, ma’lumotni shifrlab uzatish jarayonida shifrmatnda bo‘lgan o‘zgarishga (tashqi ta’sirlar natijasida) simmetrik oqimli shifrlash bardoshli sanaladi. Masalan, oqimli shifrlashda shifrmatndagi bir bitning o‘zgarishi ochiq matnning ham bir bitining o‘zgarishiga olib keladi. Simmetrik blokli shifrlarda esa bir bitning o‘zgarishi bir blokning (masalan, 64 bit) o‘zgarishiga olib keladi. Bundan tashqari, simmetrik oqimli shifrlash, blokli shifrlarga qaraganda, kichik qurilmalarda amalga oshirilishi mumkin.

3.3. Blokli simmetrik shifrlash algoritmlari

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

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

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

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

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Simmetrik kriptografiyaning axborotni himoyalashdagi o‘rni.
2. Ochiq kalitli kriptografiyaning axborotni himoyalashdagi
3. Xesh funksiya, unga qo‘yilgan talablar va uning axborot himoyalashdagi o‘rni.

IV БОБ. FOYDALANISHNI NAZORATLASH

4.1. Bir tomonlama funksiya

Assimetrik shifrlash algoritmlari

Simmetrik kriptotizimlarga bag‘ishlangan ma’ruzada ko‘rib o‘tilgani kabi, mazkur kriptozimlarga mavjud muammolardan biri bu – maxfiy kalitni xavfsiz uzatish va saqlashdir. Ushbu ma’ruzada esa o‘zida kalitlarni uzatish va xavfsiz saqlash bilan bog‘liq muammolarni bartaraf etgan assimetrik yoki ochiq kalitli kriptotizimlar bilan tanishib chiqiladi.

Ochiq kalitli kriptotizimlarda maxlumotni shifrlash bir kalit bilan amalga oshirilsa (ochiq kalit deb ataladi), uni deshifrlash boshqa bir kalit (shaxsiy kalit deb ataladi) bilan amalga oshiriladi. Shuning uchun, ochiq kalitli kriptotizimlar simmetrik kriptotizimlarda mavjud bo‘lgan kalitlarni taqsimlash muammosini o‘zida bartaraf etgan. Biroq, ochiq kalitli kriptografik tizimlarning ham o‘ziga xos muammosi mavjud bo‘lib, uni ma’ruza davomida tahlil qilib o‘tamiz.

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

Simmetrik kalitli shifrlarda ochiq matn P ni shifrlaymiz va shifrmatn C ni hosil qilsak, ochiq kalitli shifrlash tizimlarida xabar M shifrlab, C shifrmatnni hosil qilamiz.

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

Modul arifmetikasi

Ochiq kalitli kriptotizimlarni chuqur o‘rganishdan oldin ularning asosi hisoblangan sonlar nazariyasi bilan yaqindan tanishib chiqish muhim hisoblanadi. Ochiq kalitli kriptotizimlar asosan modul arifmetikasiga asoslangani bois, dastlab ularga to‘xtalib o‘tamiz.

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

Quyidagi qoldiq arifmetikasiga oid misollar bilan tanishib chiqiladi:

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

$-7mod3 \equiv (-7 + 3)mod3 \equiv -4mod3 \equiv (-4 + 3)mod3 \equiv$
$-1mod3 \equiv (-1 + 3)mod3 \equiv 2$

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

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

Misol tariqasida 3 sonining 7 maydondagi teskarisini topish talab etilsin. Ya’ni, x ni topish talab etilsin: $3^{-1}mod7 \equiv x$. Yuqoridagi tenglik $(3 * x)mod7 \equiv 1$ dan foydalanib, x ning o‘rniga son qo‘yib natijani hisoblash mumkin. Lekin ushbu jarayon ko‘p vaqt talab etadi (ayniqsa katta sonlarda juda ham ko‘p vaqt talab etadi).

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

Kengaytirlgan Yevklid algoritmi. Kengaytirlgan Yevklid algoritmi RSA kriptotizimi ochiq kaliti «*ye*» - ni topishda

$d * e \equiv 1 (mod\, \varphi(n))$ taqqoslama tenglamaga duch kelinib, uni yechish bevosita $ax + by = d,\ \ d = ЭКУБ(a,b)$ tenglama butun yechimlarini topish masalasiga ekvivalent hamda bu algoritmga ko‘ra berilgan a – soniga modn bo‘yicha teskari elementni topish imkonini beradi. Shuning uchun ham bu algoritm ishlash prinsiplarini keltirib o‘tamiz.

Teorema. Aytaylik, a va b natural sonlar, $d = ЭКУБ(a, b)$ bo‘lsin. U holda shunday α va β butun sonlar topiladiki

$\alpha * a + \beta * b = d$

tenglik o‘rinli bo‘ladi.

Demak, bu algoritm nafaqat ikkita natural sonning EKUB –ni, balki yoyilmadagi α va β koeffisentlarni ham topish imkonini berar ekan.

Shunisi bilan ham aslida Yevklid algoritmidan farqlanadi.

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

$\alpha * a + \beta * b = d$

butun yechimlari hisoblanadi. Bu esa esa bizga RSA algoritmi ochiq va maxfiy kalitlarini topish imkonini yaratadi. Shu sababli bu algoritm ishlash qadamlari bilan yaqindan tanishib chiqamiz.

Faraz qilaylik, a va b sonlarning EKUB - ni topishda quyidagi ketma-ketlik qaralayotgan bo‘lsin:

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

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

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

…… ……..

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

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

Biz, bu yerda

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

sonlarini topishimiz kerak. Bu sonlar quyidagi formula yordamida topiladi:

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

bu yerda

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

Kerakli malumotlarni quyidagi jadval orqali berish mumkin

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

Jadvalda keltirilgan oxirgi ustundagi ikki qiymat biz izlayotgan alfa va betta koeffisentlardir, yani $\alpha = x_{n-1}$, $\beta = u_{n-1}$ teng bo‘ladi.

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

Yevklid algoritmi qadamlariga muvofiq:

6188=4709*1+1479, ya’ni r_1=1479

4709=1479*3+272, ya’ni r_2=272

1479=272*5+119, ya’ni r_3=119

272=119*2+34, ya’ni r_4=34

119=34*3+17, ya’ni r_5=17

34=17*2+0, ya’ni r_6=0

demak,

r_5=17

soni 6188 va 4709 sonlarining EKUB-deb e’lon kilinadi, ya’ni

EKUB (6188,4709)=17 .

Kengaytirilgan Yevklid algoritmiga ko‘ra:

6188*α + 4709 *β=17

α=?, β=? topaylik:

yuqorida keltirilgan ifodani quyidagicha yozib olamiz:

17=119 – 34*3

34=272 – 119*2

119=1479 – 272*5

272=4709 – 1479*3

1479=6188 – 4709*1

yoki:

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

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

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

ya’ni

6188*121+4709* (- 159)=17; demak, α=121; β= - 159

Javob: α=121, β= - 159.

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

$7 = 3 * 2 + 1$

$$3 = 1 * 3 + 0$$

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

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

Yuqoridagi tenglikni ikki tomonini modulga $(mod7)$ olinsa quyidagi tenglikga ega bo‘linadi: $\big((7 * 1)mod7 + (-2 * 3)mod7\big)mod7 \equiv 1mod7$

yoki $(-2 * 3)mod7 \equiv 1mod7 \equiv 1$. Ushbu tenglikni $(3 * x)mod7 \equiv 1$ taqqoslash orqali $x = -2$ ga tengligini yoki $-2mod7 = 5$ ligini topish mumkin. Ya’ni, $(3 * 5)mod7 \equiv 1$ tenglikni qanoatlantiradi.

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

4.2. RSA algoritmi

RSA ochiq kalitli shifrlash algoritmi mualliflari bo‘lgan uchta olimlar, Rivest, Shamir va Adleman, sharafiga qo‘yilgan. RSA algoritmi yuqorida keltirilgan katta sonlarni faktorlash muammosiga asoslanadi.

RSA algoritmida ochiq va shaxsiy kalitlar juftini generasiya qilish uchun ikkita katta uzunlikdagi p va q sonlari tanlanadi va ularning ko‘paytmasi hisoblanadi: $N = p * q$. Shundan so‘ng $\varphi(N) = (p - 1) * (q - 1)$ bilan o‘zaro tub bo‘lgan, e soni tanlanadi ($\varphi(N)$ funksiya ma’nosi quyida keltirilgan). Shundan so‘ng $\varphi(N)$ modulda e sonining teskarisi hisoblanadi va u d ga teng bo‘ladi. Shundan so‘ng bizda, ikkita tub sonlarning (p ва q) ko‘paytmasi N va $ed = 1\ mod\ \varphi(N)$ shartni qanoatlantiruvchi e va d sonlari mavjud. Shundan so‘ng, p ва q larni esdan chiqaramiz (o‘chirib tashlaymiz).

Bu yerda, N modul hisoblanib, (N, e) ochiq kalit juftini va d maxfiy kalitni tashkil etadi. RSA algoritmida shifrlash va deshifrlash

modul bo‘yicha darajaga oshirish asosida bajariladi. RSA algoritmida shifrlash uchun M xabarni son ko‘rinishida ifodalash talab etiladi va N modul bo‘yicha e darajaga ko‘tariladi, ya’ni

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

C ni deshifrlash uchun uni va N modul bo‘yicha shaxsiy kalit d darajaga ko‘tarish talab etiladi:

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

RSA algoritmi to‘g‘ri ishlashining tasdig‘i

Boshqa so‘z bilan aytganda RSA algoritmida xabar ochiq kalit bilan shifrlansa va shaxsiy kalit deshifrlansa, u holda $M = C^d \ mod \ N = \ M^{ed} \ mod \ N$ tenglik to‘g‘riligini isbotlash zarur?

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

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

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

Ushbu tengliklardan esa, RSA algoritmi to‘g‘ri ishlashini tasdiqlash mumkin:

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

.

Misol

Keling, RSA algoritmida ma’lumotni shifrlash va deshifrlash amallarini tanlab olingan ($p = 11$ ва $q = 3$) “katta” sonlar ustida amalga oshirib ko‘ramiz. Mazkur holda modul $N = p * q = 33$ ga teng bo‘ladi va $\varphi(N) = (p-1)(q-1) = 20$ ga teng bo‘ladi. U holda shifrlash uchun zarur bo‘lgan daraja e ni ($e = 3$) ga teng deb olamiz. Sababi, 3 soni $\varphi(N) = 20$ bilan o‘zaro tubdir. Shundan so‘ng, Evklidning kengaytirilgan algortmi asosida deshifrlash kalitini ($d = 7$) aniqlaymiz, ya’ni, $ed = 3 * 7 = 1 \ mod \ 20$. U holda A tomonning ochiq kalit jufti $(N, e) = (33,3)$ va shaxsiy kaliti esa $d = 7$ ga teng.

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

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

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

va uni A tomonga yuboradi.

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

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

Agar RSA algoritmida kichik tub sonlardan (p ва q учун) foydalanilgan taqdirda, hujumchi ochik bo‘lgan N ni osonlik bilan ikkita tub sonning ko‘paytmasi ko‘rinishiga yozish mumkin. Shundan so‘ng, ochiq kalitning ikkinchi qism e dan foydalangan holda, shaxsiy kalit d ni hisoblay oladi. Shuning uchun RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida 2048 bit bo‘lishi talab etiladi. Bundan tashqari, RSA algoritmini buzish faqat faktorlash muammosiga bog‘liqligi isbotlanmagan. Boshqa so‘z bilan aytganda, RSA algoritmini buzishning faktorlash muammosini yechishdan tashqari biror usuli aniqlanmagan.

4.3. Ochiq kalitli kriptotizimlardan foydalanish

Ochiq kalitli kriptgrafik tizimlardan foydalanish masalasini ko‘rib chiqishdan oldin, quyidagi belgilanishlarini bilish maqsadga muvofiqdir.

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

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

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

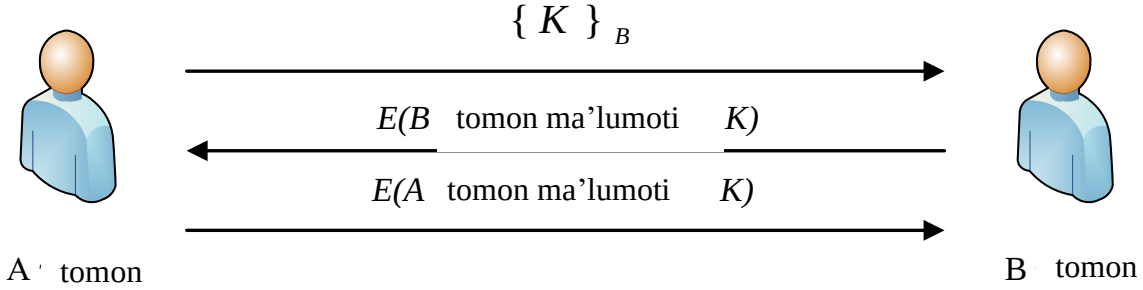
Simmetrik shifrlar bilan bajargan ixtiyoriy amalingizni, ochiq kalitli shifrlash algoritmlari bilan ham amalga oshirish mumkin. Biroq, jarayon ko‘proq vaqt talab etadi. Masalan, tarmoqda ma’lumotni uzatishda va xavfsiz bo‘lmagan muhitda axborot konfidensialligini ta’minlashda simmetrik shifrlash algoritmlarining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

Bundan tashqari simmetrik kriptotizimlar kabi ochiq kalitli kriptotizimlardan ham ma’lumotni butunligini ta’minlashda foydalanish

mumkin. Mazkur masala bilan keyingi ma’ruzada batafsil tanishib chiqiladi.

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

Har ikkala kriptotizimlarning afzalliklarini birlashtirish imkoniyati mavjudmi? Ya’ni, ma’lumotni shifrlashda yuqori samaradorlikka ega bo‘lgan va kalitlarni taqsimlashda muammosi bo‘lmagan kriptotizimni yaratish mumkinmi? Albatta, buning imkoniyati mavjud va bunday tizimlar *gibrid* kriptotizimlar deb ataladi. Gibrid kriptotizimlarda simmetrik shifrlash algoritmining kaliti ochiq kalitni shifrlash orqali yetkazilsa, ma’lumotning o‘zi esa simmetrik shifrlash orqali himoyalanadi. Gibrid kriptotizim 4.1-rasmda aks ettirilgan.



4.1-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. Bundan oldingi ma’ruzada simmetrik kriptotizimlar uchun ushbu masalaga to‘xtalib o‘tilgandi. Simmetrik va ochiq kalitli kriptotizimlarning matematik asosi turlicha bo‘lgani bois, ular bir xil bardoshlik darajasida bo‘lganda turli kalit uzunliklariga ega bo‘ladilar (4.1-jadval).

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

4.1-jadval

Simmetrik va ochiq kalitli kriptotizimlar bir xil bardoshlikka ega bo‘lganda ulardagi kalitlarning uzunliklari

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

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

4.2-jadval

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

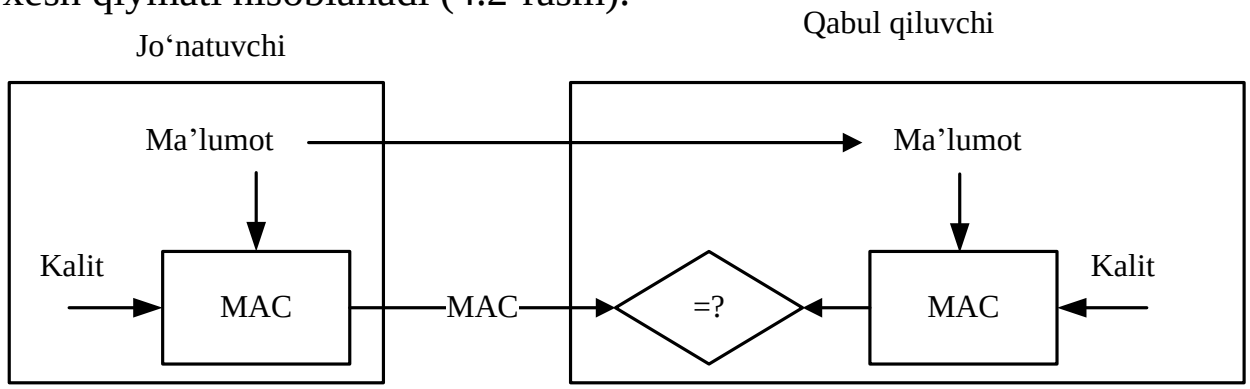
Yuqoridagi keltirilgan ma’lumotlardan shuni ko‘rish mumkinki, hisoblash qurilmalari imkoniyatining ortishi kriptografik algoritmlarning bardoshligini kamayishiga olib keladi. Bu ta’sir har ikkala simmetrik va ochiq kalitli kriptotizimlarga ham tegishlidir.

4.4. Simmetrik shifrlash algoritmlaridan ma’lumot butunligini tekshirish

Bundan oldingi ma’ruzalarda har ikkala shifrlash algoritmlaridan (simmetrik va ochiq kalitli) faqat ma’lumotni konfidensiyalligini ta’minlashda foydalanish haqida aytib o‘tildi. Mazkur ma’ruzada esa ulardan ma’lumotni butunligini tekshirishda foydalanish tartibi bilan tanishib o‘tiladi.

Oldingi ma’ruzada xesh – funksiyadan foydalanib ma’lumotni butunligini tekshirishning sodda usuli keltirilgan edi. Biroq, ushbu

usulda jiddiy xavfsizlik muammosi bo‘lgani bois, undan amalda foydalanilmaydi. Ushbu muammoni bartaraf etuvchi – *xabarlarni autentifikasiyalash kodi (message authentication code, MAC)* tizimlari mavjud bo‘lib, unga ko‘ra biror maxfiy kalit asosida ma’lumotning xesh qiymati hisoblanadi (4.2-rasm).



4.2-rasm. MAS tizimi

MAC tizimlarini ishlab chiqishda blokli shifrlardan ham foydalanish mumkin. Buning uchun blokli shifrni CBC rejimida foydalanish va eng oxirgi shifrmatn blokini olishning o‘zi yetarli (qolganlari tashlab yuboriladi). Ushbu oxirgi shifrmatn bloki *MAC* sifatida xizmat qiladi. Mazkur holda N blokdan iborat bo‘lgan ma’lumot bloklari, $P_0, P_1, P_2, \dots, P_{N-1}$ uchun MAC quyidagi formula orqali hisoblanadi:

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

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

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

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

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

Faraz qilaylik hujumchi birinchi blok P_1 ni o‘zgartirdi (uni Q deb belgilaymiz) va bu holda B tomon MAC ni quyidagicha hisoblaydi:

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

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

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

4.5. Xesh – funksiyalar asosida ma’lumot yaxlitligini tekshirish

Yuqorida M ma’lumot butunligini 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 butunligini ta’minlashda bevosita foydalanilmaydi. Boshqa so‘z bilan aytganda, xesh funksiyalardan ma’lumot butunligini ta’minlashda hisoblangan xesh qimatni o‘zgartira olmaslikni kafolatlash maqsad qilinadi. Buni amalga oshirish uchun balki xesh qiymatni simmetrik kalitli shifrlar asosida shifrlash zarurdir (ya’ni, $E(h(M), K)$). Biroq, buni amalga oshirishning soddaroq usuli – *xeshlangan MAS* (hashed MAC yoki HMAC) mavjud.

Bunga ko‘ra, xesh qiymatn shifrlashning o‘rniga, xesh qiymatni hisoblash jarayonida kalitni bevosita ma’lumotga biriktirish amalga oshiriladi. HMAC tizimida kalitlar qanday biriktiriladi? Umumiy holda ikki usul: kalitni matnni oldidan qo‘yish ($h(K, M)$) yoki kalitni matndan keyin qo‘yish ($h(M, K)$) mavjud bo‘lsada, ularning har ikkalasida jiddiy xavfsizlik muammosi mavjud.

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

HMAC tizimida kalit ma’lumotga quyidagicha biriktiriladi. Dastlab xesh funksiyadagi blokning uzunligi baytlarda aniqlanadi. Masalan. MD5 xesh fuknsiyasida blok uzunligi $B = 64$ baytga teng. Olingan kalit (K) uzunligi ham blok uzunligiga olib kelinadi. Bunda 3

ta holat bo‘lishi mumkin: (1) agar kalitning uzunligi 64 baytga teng bo‘lsa, hyech qanday o‘zgarish amalga oshirilmaydi, (2) agar kalitning uzunligi 64 dan kichik bo‘lsa, u holda etmagan baytlar o‘rni nollar bilan to‘ldiriladi, (3) agar kalit uzunligi blok uzunligidan katta bo‘lsa, kalit dastlab xeshlanadi va hosil bo‘lgan xesh qiymatning o‘ng tomonidan blok uzunligiga yetguncha nollar bilan to‘ldiriladi. Shu tariqa, kalit uzunligi blok uzunligiga moslashtiriladi.

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

$ipad = 0x36$ ни B марта такрорлаш натижасида

$opad = 0x5c$ ни B марта такрорлаш натижасида

Bu holda HMAC quyidagicha hisoblanadi:

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

Tenglikdan ko‘rinib turibdiki, HMAC da ikki marata xeshlash amalga oshirilmoqda. Kalit K faqat ikki tomonga (yuboruvchi 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 qiluvch tomonidan osonlik bilan aniqlanadi.

4.6. Elektron raqamli imzo

Ochiq kalitli shifrlash algoritmlari asosida ma’lumot butunligini tekshirish va rad-etishdan himoyalash

Mazkur bo‘limda ochiq kalitli kriptotizimlar va xesh funksiyalar asosida ishlovchi – *elektron raqamli imzo* tizimlari bilan tanishib o‘tiladi. O’zbekiston Respublikasining Elektron raqamli imzo to‘g‘risidagi qonunida elektron raqamli imzoga quyidagicha ta’rif berilgan:

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

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

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

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

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

Agar A tomon xabar M ga imzo qo‘ygan bo‘lgan u holda imzo $S = [M]_A$ shaklida ifodalanadi (xuddi ochiq kalitli kriptografiyada shaxsiy kalit bilan deshifrlash kabi). ERI tizimlari ikkita jarayondan iborat: *ERIni shakllantirish* va *ERIni tekshirish*.

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

ERIni tekshirish jarayoni. Faraz qilinsin, B tomondan M' xabarga qo‘yilgan imzo S ni tekshirish talab etilsin. Buning uchun B tomon dastlab xabar M' ni xesh qiymatini hisoblaydi: $H' = h(M')$. A tomonning ochiq kaliti bilan S ni “deshifrlaydi” (bu haqiqiy deshifrlash emas, shunchaki ochiq kalit bilan S ustiga biror amal bajargan holda H tiklash) va H ni hosil qiladi. Agar ikki xesh qiymatlar (H ва H') o‘zaro teng bo‘lsa, ERI to‘g‘ri deb topiladi (demak xabar butun).

Rad – etishdan himoyalashni tushunishdan oldin, MAS asosida butunlikni ta’minlashga bir sodda misol olsak. Faraz qilaylik A tomon o‘zining sevimli dalloli B tomonga 100 ta aksiyasini olishga buyurtma berdi. Berilgan buyurmani butunligina ta’minlash uchun A tomon B tomon bilan taqsimlangan kalit K_{AB} yordamida MAS ni hisobladi.

Ma’lum vaqt o‘tgandan so‘ng, buyurtmalar tayyor bo‘ladi. Biroq, A tomon to‘lovni amalga oshirishdan oldin aksiyalarning narxi tushib ketadi. Bu vaqtda esa, A tomon buyurtmani men bermadim deb turib oladi va ni rad etadi. Sababi, butunlikni ta’minlash uchun hisoblangan MAC ni har ikkala tomon ham hosil qila oladi.

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

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

Faraz qilinsin, A va B tomonlar ochiq kalitli kriptotizimlardan foydalanish imkoniyati mavjud hamda A tomon B tomonga M xabarni yuborishni istaydi. Agar konfidensiallikni ta’minlash uchun A tomoni B tomonning ochiq kaliti bilan xabar M ni shifrlasa, butunlik va rad etishdan himoyalash uchun A tomon shaxsiy kaliti bilan M xabarga imzo qo‘yadi. Biroq, faraz qilinsin, A tomon ma’lumotni konfidensialligi va rad etishdan himoyalanishini istaydi. Buning uchun esa A tomon shunchaki shifrlash yoki imzolash bilan muammoni yecha olmaydi.

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

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

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

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

Xo‘sh? Yuqoridagilardan qay biri masalaga to‘g‘ri yechim bo‘la oladi. Keling, yuqoridagi holatlar uchun misollar qarab chiqaylik.

Birinchi holat. Farz qilaylik A va B tomonlar orasida ishqiy munosabat bo‘lsin va A tomon B tomonga quyidagi xabarni yuborishga qaror qildi:

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

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

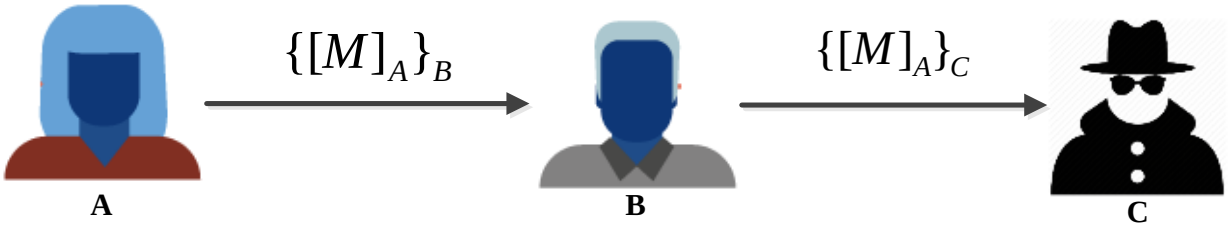
$$\{[M]_A\}_B$$

Shundan so‘ng, A va B tomonlar orasida ozgina kelishmovchilik kelib chiqadi va B tomon janjal boshlamoqchi bo‘ladi. Buning uchun qabul qilingan xabarni deshifrlaydi va $[M]_A$ ga ega bo‘ladi va uni

uchinchi C tomonning ochiq kalitidan foydalanib shifrlaydi va C yuboradi (4.4-rasm):

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

Albatta mazkur holatda, C tomon A tomon uni yaxshi ko‘rarkan deb o‘ylaydi va bu ikkala A va C tomonlar uchun muammo olib kelsa, B tomon esa bundan huzur qiladi.



4.3-rasm. Imzo qo‘yish va shifrlash sxemasi muammosi

Mazkur holatdan xulosa chiqargan A tomon konfidensiallikni ta’minlash uchun imzolash va shifrlash sxemasi mos emasligini biladi. Shuning uchun bundan keyin mazkur holatlarda shifrlash va keyin imzolash sxemasidan foydalanishni qaror qiladi.

Ma’lum vaqtdan so‘ng, A va B tomonlar o‘zaro kelishib olishdi. Shundan so‘ng A tomon bir yangi nazariyani yaratdi va B tomon bilan ulanishni istadi. Mazkur holatda xabar quyidagicha bo‘lsin:

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

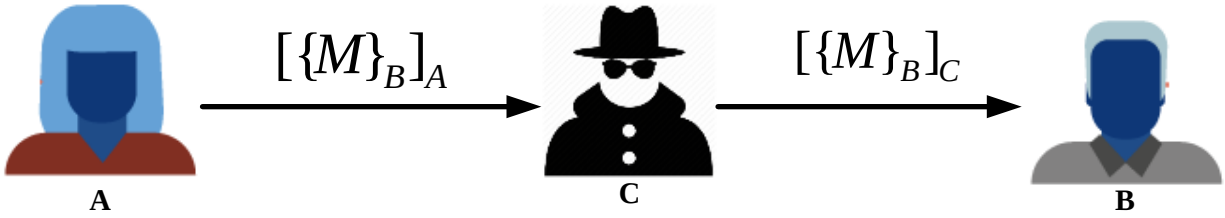
A tomon xabarni yuborishda shifrlash va imzolash sxemasidan foydalandi:

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

Bu vaqtda kelib, C tomon A va B tomonlar bilan xanuzgacha xafa va ulardan “o‘ch olishni” istaydi hamda A va B tomonlar orasida joylashib, barcha o‘tuvchi xabarlarni to‘sib qoladi. Bundan tashqari, C tomon A tomon shu kunlarda bir yangilik ustida ish olib borayotganidan xabardor. Shuning uchun A tomondan uzatiladigan har bir xabarni muhim deb hisoblaydi. C tomon A tomondan uzatilgan shifrlangan va imzolangan xabarni muhim deb hisoblaydi va uni tutib oladi. Shundan so‘ng shifrlangan xabar $\{M\}_B$ ga o‘z nomidan imzo qo‘yadi (8.4-rasm):

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

B tomon mazkur xabarni qabul qilgandan so‘ng, uni C tomon yuborganini aniqlaydi va deshiflagandan so‘ng C tomon haqiqatda yangi nazariyani yaratgan deb hisoblaydi va C tomonni rag‘batlantiradi. Bu holatdan so‘ng, A tomon shifrlash va imzolash sxemasi ham o‘rinli emasligini aniqlaydi.



4.4-rasm. Shifrlash va imzolash sxemasidagi muammo

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

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

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

Ochiq kalitlar infratuzilmasi (Public key infrastructure, PKI)

Ochiq kalitli kriptografiya bilan bog‘liq bo‘lgan muammolardan yana biri bu - ochiq kalitning kimga tegishli ekanligini aniqlashdir. Faraz qilaylik, A tomon biror maxfiy xabar M ni B tomonga yubormoqchi. Buning uchun A tomon B tomonning ochiq kalitidan foydalanadi. Biroq, g‘arazli niyatda bo‘lgan C tomon o‘z 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.

Mazkur muammoni oldini olish uchun ochiq kalitli kriptografik tizimlarda *ochiq kalitlar infratuzilmasi*dan foydalaniladi.

Ochiq kalitlar infratuzilmasi yoki PKI real hayotda ochiq kalitli kriptotizimlardan xavfsiz foydalanish uchun talab etiluvchi barcha narsani o‘z ichiga oladi. PKI tarkibidan barcha narsalarning birgalikda ishlashi juda ham murakkab jarayon bo‘lib, quyida ularning ayrim tashkil etuvchilari va PKI ning asosiy vazifalari bilan tanishib chiqiladi.

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

$M = (\text{A томон номи}, A \text{ томонинг очиқ калити})$ va $S = [M]_{CA}$.

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

CA tomoni odatda *ishonchli uchunchi tomon (trusted third party* yoki *TTP)* sifatida qaraladi. Ya’ni, odatda A foydalanuvchi uchun shaxsiy va ochiq kalitlar juftini generasiya qiladi. Shaxsiy kalitni A tomoning o‘ziga taqdim etadi va o‘zidan o‘chirib tashlaydi. Ochiq kalitni esa sertifikat shaklida taqdim etadi. Agar B tomon A tomonga biror ma’lumotni shifrlab yubormoqchi bo‘lsa, uning sertifikatidan foydalanadi. Buning uchun sertifikatdagi imzoni tekshirishi talab etadi. Bu esa o‘z navbatida B tomonga CA ni ochiq kalitini (ya’ni, unga teng bo‘lgan sertifikatni) bilishni talab etadi. Bundan kelib chiqadiki, CA tomoning ochiq kaliti (yoki sertifikati) oldindan foydalanilayotgan tizimda mavjud bo‘ladi va bu haqida barcha ma’lumotga ega bo‘ladi.

4.7. Apparat-dasturiy shifrlash

Axborotni kriptografik himoyasi, hususan shifrlash algoritmlaridan amalda keng qo‘llaniladi. Masalan, saqlash qurilmalarida ma’lumotlarni shifrlash orqali saqlash yoki tarmoq bo‘ylab uzatiladigan axborotni shifrlab uzatishni misol keltirish mumkin. Umuman olganda ma’lumotni shifrlashda ma’lum algoritmdan foydalaniladi. Ushbu algoritm biror bir operasion tizim uchun (masalan, Windows OT, Linux OT, Android OT) mo‘ljallangan dastur ko‘rinishida yoki maxsus qurilmada (masalan, maxsus prosessorlar, USB token, smart karta va hak.) yozilishi mumkin.

Apparat shifrlash – bu shifrlash jarayoni bo‘lib, buning uchun maxsus ishlab chiqilgan hisoblash qurilmasidan foydalaniladi. Unga misol qilib, ruToken USB shifrator qurilmasini olish mumkin (4.6 - rasm).



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

ruToken USB shifrator qurilmasi – rossiyada ishlab chiqariluvchi qurilma bo‘lib, unda asosan Rossiya federasiyasining kriptografik algoritmlari amalga oshirilgan. Masalan, rutoken S qurilmasining umumiy xarakteristikalari keltirilgan:

- shifrlash kalitlari, ERI kalitlari va turli sertifikatlarni xavfsiz saqlash uchun foydalaniladi;
- ushbu tokendan foydalanish uchun PIN kodni kiritish talab etiladi;
- diskdagi ma’lumotlarni shifrlash uchun qo‘llaniladi;
- tokenda mehmon, foydalanuvchi va administrator darajalari mavjud;
- Microsoft Windows 9/8.1/2012R2/8/2012/7/2008R2/ Vista/2008/XP/2003, GNU/Linux, Apple macOS/OSX muhitlarida foydalanish mumkin;
- 32, 64 va 128 KB xotiraga ega EEPROM;
- USB 1.1 va undan yuqori interfeysga ega;
- 58x16x8mm (mikro-token 17,8x15,4x5,8mm) o‘lchamga ega;
- 6,3g (mikro-token 1,6g) og‘irlikka ega.

Apparat shifrlash o‘ziga xos quyidagi xususiyatlarga ega:

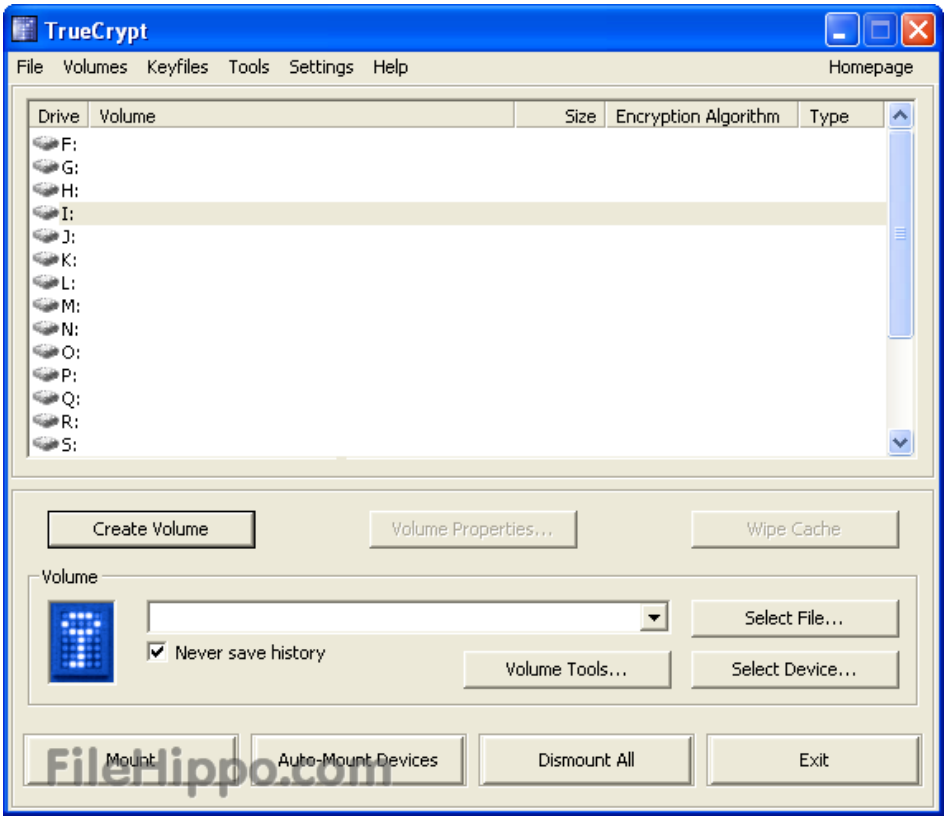
- saqlagishda (qurilmada) joylashgan maxsus prosessordan foydalanadi;

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

Dasturiy shifrlash – bu kompyuter vositasi yordamida disklarni, fayllarni, kataloglarni, turli ma’lumot saqlash vositalaridagi axborotni shifrlash va deshifrlash jarayonini amalga oshiradi. Umumiy holda dasturiy shifrlash vositalarini quyidagi guruhlarga ajratish mumkin:
- Diskni shifrlash dasturiy vositalari (Disk encryption software);
- Fayl/ katalogni shifrlash dasturiy vositalari (File/folder encryption);
- Ma’lumotlar bazasini shifrlash dasturiy vositalari (Database encryption);
- Aloqani shifrlash dasturiy vositalari (Communication encryption software).

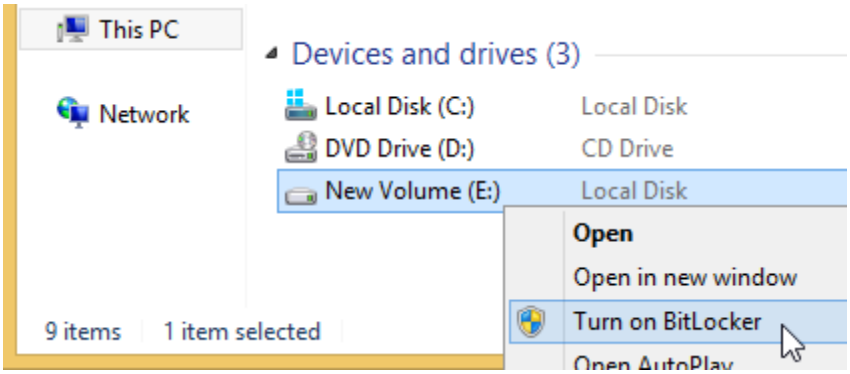
Masalan, quyidagi 4.7-rasmda diskni shifrlashda foydalaniluvchi TrueCrypt dasturiy vositasining ko‘rinishi keltiralgan. Ushbu dasturlash vositasi quyidagi xususiyatlarga ega:
- C, C++, Assembly dasturlash tillaridan foydalanib yozilgan;
- Windows, macOS, Linux OTlarida foydalanish mumkin;
- 3.30 MB hajmga ega;

- ushbu dasturiy vosita AES, Serpent, va Twofish blokli shifrlash algoritmlaridan foydalaniladi.



4.6-rasm. TrueCrypt dasturiy vositasi

Bundan tashqari TrueCrypt dasturiy vositasiga o‘rinbosar sifatida Windows OTda BitLocker dasturiy vositasidan foydalaniladi.



4.7-rasm. BitLocker dasturiy vositasi

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

- shifrlash uchun boshqa dasturlar bilan bir vaqtning o‘zida kompyuter resursidan foydalanadi;

- kompyuterning himoyalanganlik darajasi saqlagichning himoyalanganlik darajasini belgilaydi;

- foydalanuvchi tomonidan kiritilgan parol ma’lumotni shifrlash kaliti sifatida f+
- oydalaniladi;
- dasturni yangilab turish talab etilishi mumkin;
- katta bo‘lmagan tashkilotlar uchun foydalanish yuqori iqtisodiy samaradorlik beradi;
- ixtiyoriy ma’lumotni saqlash turlari uchun shifrlashni amalga oshirish imkoniyati mavjud;
- parolni to‘liq tanlash hujumi yoki parolni topishga qaratilgan boshqa hujumlarga bardoshsiz;
- apparat shifrlashga qaraganda kam sarf xarajat talab etadi.

4.8. Disk va fayl tizim sathida shifrlash

Diskni shifrlash. Bu jarayon turli ma’lumotni saqlash vositalarida (qattiq disk, yumshoq disk, USB disk va bosh.) saqlangan ma’lumot konfidensialligini ta’minlash uchun amalga oshiriladi. Bunda diskni shifrlashning apparat yoki dasturiy vositasidan foydalanilib, diskning yoki uning bir bo‘limining (masalan, D disk) har bir biti shifrlanadi. Ushbu jarayon ruxsat etilmagan foydalanishdan nazoratlashni maqsad qiladi.

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

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

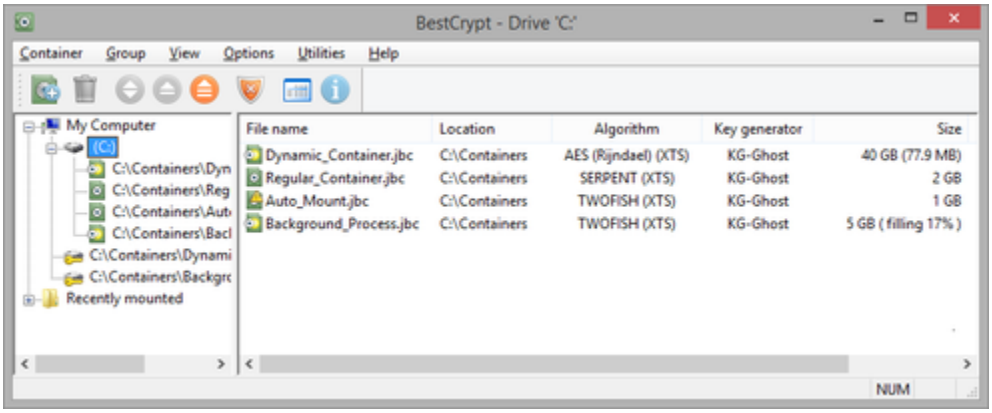
Qurilmaga asoslangan FDE ikki tashkil etuvchidan: qurilmaga asoslangan shifrlash vositasidan va ma’lumotni saqlash qismidan. Qurilmaga asoslangan FDE ning hozirda uchta ko‘rinishi amalda keng qo‘llaniladi:

1. Hard disk drive (HDD) FDE.

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

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

Ba'zi diskni shifrlovchi dasturiy vositalar tomonidan *shaffof shifrlash (Transparent encryption)* usuli foydalaniladi. Bu usulga ko'ra shifrlash kaliti taqdim etilgandan so'ng avtomatik ravishda diskning barcha sektorlari (fayl nomini, katalog nomini, fayl kontentini va boshqa meta ma'lumotlarni o'z ichiga olgan holda) shifrlanadi. Dasturiy vosita ko'rinishadagi diskni shirflash vositalariga *Aloaha Crypt Disk*, *BestCrypt Volume Encryption*, *BitArmor DataControl*, *BitLocker*, *Bloombase Keyparc*, *Cryptic Disk*, *USBCrypt* va hak.larni misol keltirish mumkin. Dasturiy ko'rinishdagi diskni shifrlash vositalari haqida batafsil https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software manzilidan ma'lumot olish mumkin.



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

Diskni to'liq shifrlash usuli alohila fayl/ katalogni shifrlash usuliga qaraganda quyidagi afzalliklarga ega:

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

Encryption ishga tushirish uchun shifrlanmagan soha qoldiradi va qolgan sohalarni to‘liq shifrlaydi.

- Ushbu usul foydalanuvchi shaxsiy xabarlarni alohida shifrlashni unutgan vaqtlarda juda qo‘l keladi.

- Zudlik bilan ma’lumotlarni yo‘q qilish, masalan, kriptografik kalitni yo‘q qilish mavjud ma’lumotni foydasiz holatga keltiradi. Biroq, kelajakdagi bo‘lishi mumkin bo‘lgan ma’lumotlarni tiklash usullariga bardoshli bo‘lishi uchun diskni fizik yo‘q qilish tavsiya etiladi.

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

- asosiy fayl tizimining ustida joylashgan kriptografik fayl tizimidan foydalanish (masalan, ZFS, EncFS);

- shifrlashni amalga oshiruvchi yagona umumiy maqsadli fayl tizimi.

- Fayl/ katalogni shifrlash usuli quyidagi afzalliklarga ega:

- faylga asoslangan holda kalitlarni boshqarish, ya’ni, har bir fayl uchun turli kalitlardan foydalanish;

- shifrlangan fayllarni alohida boshqarish butun shifrlangan diskni boshqarishdan ko‘ra osonroq;

- foydalanishni boshqarish ochiq kalitli kriptografik tizimlar yordamida amalga oshirilishi mumkin;

- faqat kriptografik kalitlar xotirada saqlanib, shifrlangan fayllar ochiq holatda saqlanadi.

Ma’lumotni yo‘q qilish usullari

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

Qog‘oz ko‘rinishdagi hujjatlar

Odatda qog‘oz ko‘rinishdagi hujjatlarni yo‘q qilishda quyidagi usullardan foydalaniladi:

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

Maydalash. Tashkilotda rahbariyat ruxsati bilan xodimlar qo‘lida bo‘lgan qog‘oz ko‘rinishidagi hujjatlar vaqti o‘tib o‘z kuchini yoqotadi yoki ularda arzimas ma’lumotlar saqlangani bois ularni yo‘q qilish zaruriyati tug‘uladi. Biroq, mazkur holda qimmat ma’lumot bo‘lsa ularni to‘liq yo‘q qilish talab etiladi. Maydalash jarayoni ushbu vazifani bajarishda keng qo‘llaniladigan usullardan biri hisoblanadi. Bunda ofis maydalagichi qog‘ozni turli kesishlar orqali ularni maydalaydi (4.9-rasm).

Maydalash usulining afzalligi quyidagilar:

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



4.9-rasm. Shreder Rexel Auto+ 90X

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

- tashkilot ichida yoki tashqarichida qog‘ozlarini yoqish uchun maxsus joy bo‘lishi talab etiladi;
- agar yonish yuqori sharoitda maxsus qozonxonalarda amalga oshirilmasa, qattiq bosilgan papkalarni saqlanish ehtimoli mavjud;
- olovni yoqish va yuklash-tushirish amallari hisobida ortiqcha xarajat talab etadi.

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

Kimyoviy ishlov berish. Yuqori maxfiylik darajasiga ega hujjatlarni yo‘q qilishda yuqorida keltirilgan usullari to‘liq kafolatni bermaydi. Kimyoviy usul esa qog‘oz ko‘rinishidagi axborotni 90% ishonchlik bilan yo‘q qilish imkonini beradi. Buning uchun maxsus kimyoviy modda va suvdan foydalaniladi. Hosil qilingan massani tiklashning umuman imkoni mavjud emas. Ushbu usulning yagona kamchiligi uning narxi yuqoriligi va maxsus joy talab etilishidir.

4.9. Hujjatlarni yo‘q qilish usullari

Elektron hujjatlarni yo‘q qilish

Elektron shaklda saqlanadigan shaxsiy va tashkilotga tegishli ma’lumotlarga noqonuniy kirish usullarining ko‘payishi sababli elektron ommaviy axborot vositalariga ishonish muammosining dolzarbligi oshmoqda. Bunga misol qilib, Markaziy razvedka boshqarmasi va AQSh milliy xavfsizlik agenti Edvard Snoudenga tegishli yangiliklarni olish mumkin. Xususan, 2013 yil iyun oyining boshida u NSAga tegishli hujjatlarni oshkor qildi. Bunga ko‘ra G20 sammitining chet ellik mehmonlari, shu jumladan Dmitriy Medvedovni Amerika va Buyuk Britaniya razvedka idoralari tomonidan kuzatilayotgani aytilgan. Maxfiy agentlar PRISM dasturidan foydalanib, noutbuk va telefonlarda saqlanayotgan shaxsiy ma’lumotlarga kirishni uddasidan chiqishgan. Buyuk Birtaniya hukumati aloqa markazining xodimlari BlackBerry kodini buzib,

qo‘ng‘iroqlarni tinglash va sammit ishtirokchilarining yozishmalarini o‘qish imkoniyatiga ega bo‘lishgan.

O’chirish degani bu yo‘q qilish degani emas

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

Hozirgi kunda amalda elektron hujjatlarni saqlagichlar sifatida quyidagi turdagi vositalardan foydalanib kelinmoqda:

- qattiq disklar: noutbuk va kompyuterdagi qattiq disklar;
- magnit lentalar (zaxira nusxalashdagi);
- Floppi-disk: 3.5, 5.25 dyumli va boshqa;
- ZIP disklar;
- Optik disklar: CD, DVD, Blue Ray va HD DVD;
- Flesh xotiralar va hak.

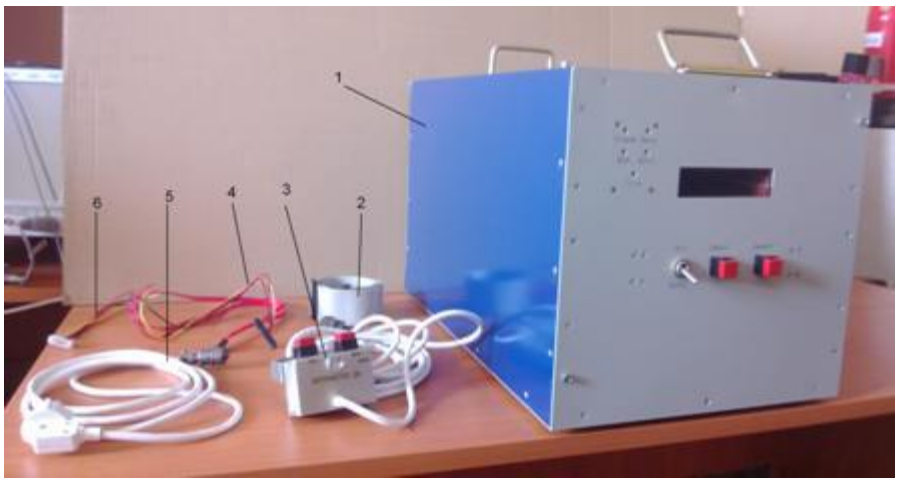
AQSh hukumatida konfidensial axborotni saqlash va o‘chirib tashlash bo‘yicha qator normativ hujjatlar ishlab chiqilgan (Code of Federal Regulations). Masalan, AQShning markaziy arxiv markazlarida elektron saqlagichdagi ma’lumotni yo‘q qilishning quyidagi uchta usulidan amalda foydalaniladi:

Shredirlash. Kuchli sanoat maydalagichlari deyarli barcha ko‘chma saqlaguvchilarni: CD, DVD, disket, magnit lentalar va hak. Maydalash natijasida buyumlar 25 mmli qismlarga bo‘lib tashlanadi (4.10-rasm).

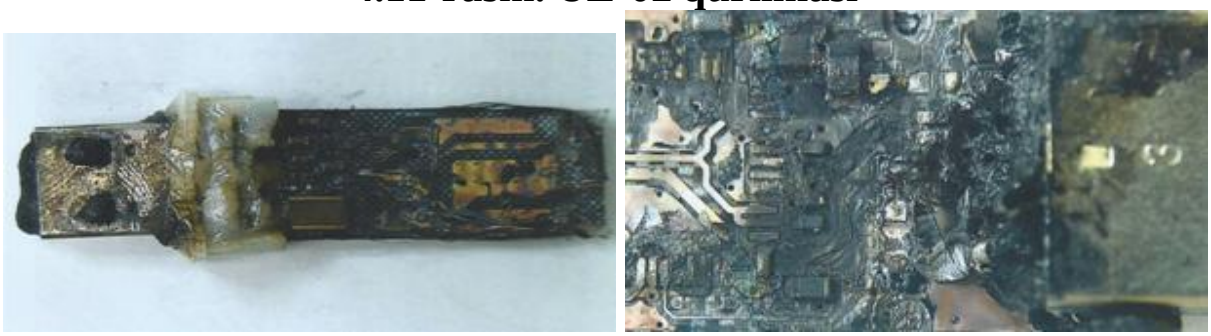


4.10-rasm. Shredirlash jarayoni

Magnitsizlantirmoq. Maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o‘zgartiriladi va shu bilan o‘qib bo‘lmasligi ta’minlanadi. Agar kuchli magnitsizlantirish amalga oshirilsa ma’lumotlar saqlagichdan o‘chiriladi va saqlagichning o‘zi neytral mannit holatiga kiradi. Ushbu ma’lumotni yo‘q qilish usuli dattiq disklarni va bazi ko‘chma qurilmalar uchun qo‘llaniladi (4.11-rasm).



4.11-rasm. UE-02 qurilmasi



4.12-rasm. Kuchli magnit maydoni natijasida USB flesh saqlagichining o‘zgarishi

Yanchish. Shredirlash jarayonidan tashqari AQSh federal arxiv markazlari tomonidan qattiq diskni yanchish orqali uni jismonan yo‘q qilish usuli ham mavjud. 5.5 tonna tosh ostida kompyuter va noutbuklarning qattiq diskalari tamomila yo‘q qilinadi. Ushbu mexanizm maksimal hajmi 2.5x9x15sm bo‘lgan, 3.5, 2.5 va 1 dyumli disklar (SATA, PATA, SCSI) ni maydalash uchun mo‘ljallangan.

Yuqorida keltirilgan usullarning aksariyati ma’lumot tashuvchini fizik yo‘q qilishni maqsad qiladi. TOP SECRET bo‘lmagan axborot saqlangan holda esa saqlagichlardan qayta foydalanish talab etiladi. Buning uchun quyidagi usullardan foydalaniladi:

- xotiraga bir necha marta takroran yozish;
- maxsus dasturlar yordamida saqlagichni tozalash (formatlashdan oldin ma’lumotni o‘chirish).

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

AQShning Cornell kompaniyasi tomonidan elektron axborotni saqlovchilardan qayta foydalanish uchun va ularni yo‘q qilish uchun quyidagi tavsiyalar beriladi.

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

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

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Simmetrik kriptotizimlarda qanday xavfsizlik muammolari mavjud va ular ochiq kalitli kriptotizimlarda qanday bartaraf etilgan.
2. Ochiq kalitli kriptotizimlarda bir tomonlama funksiyalardan foydalanishdan asosiy maqsad nima.
3. Agar bir tomonlama funksiya sifatida faktorlash amali olinsa, uning murakkabligi nimada?
4. Ochiq kalitli kriptotizimlarda foydalanilgan muammolarini (masalan, faktorlash) qanday yechimi mavjud?

5. RSA ochiq kalitli shifrlash algoritmi va unda kalitlar qanday generasiya qilinadi.
6. CBC shifrlash rejimining qanday xususiyati undan MAC tizimlarini qurishda foydalanilishini ta’minlaydi.
7. CBC rejimida qurilgan MAC tizimi va HMAC tizimlari orasida qanday farq va o‘xshashliklar mavjud.
8. Ma’lumotni uzatishda “rad etish” holati nima va unga misol keltiring.
9. ERIga ta’rif bering va uning asosiy vazifalarini keltiring.
10. Apparat-dasturiy shifrlash nima
11. Disk va fayl tizim sathida shifrlash qanday amalga oshiriladi
12. Hujjatlarni yo‘q qilish usullari haqida gapirib bering

V BOB. AUTENTIFIKASIYA

5.1. Identifikasiya

Identifikasiya, autentifikasiya, avtorizasiya va ruxsatlarni nazoratlash.

Tizim resurslarini boshqarish bilan bog‘liq bo‘lgan ixtiyoriy xavfsizlik muammosi uchun biz *ruxsatlarni nazoratlash* terminini “soyabon” sifatida foydalansak bo‘ladi. Mazkur sohaga oid tushuntirishlarni olib borganda 3 ta asosiy muhim bo‘lgan soha mavjud: *identifikasiya, autentifikasiya* va *avtorizasiya.*

Identifikasiya – shaxsni kimdir deb davo qilish jarayoni. Masalan, siz telefonda o‘zingizni tanitishingizni identifikasiyadan o‘tish deb aytish mumkin. Bunda siz o‘zingizni, masalan, “Men Bahodirman” deb tanitasiz. Bu o‘rinda “Bohodir” sizning *identifikatoringiz* bo‘lib xizmat qiladi. Shunday qilib, *identifikasiya* – subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni hisoblanadi. Bundan tashqari, elektron pochta tizimida ham pochta manzilni – *identifikator* sifatida qarash mumkin. Pochta manzilini taqdim etish jarayonini esa *identifikasiyalash* jarayoni sifatida qarash mumkin. Elektron pochta tizimida pochta manzili takrorlanmas yoki unikal bo‘ladi. Shundan kelib chiqib aytish mumkinki, foydalanuvchining identifikatori tizim ichida unikal va takrorlanmasdir.

Autentifikasiya – foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni. Masalan, foydalanuvchini shaxsiy kompyuterdan foydalanish jarayonini olsak. Dastlab kirishda foydalanuvchi o‘z identifikatorini (ya’ni, foydalanuvchi nomini) kiritadi va u orqali tizimga o‘zini tanitadi (identifikasiya jarayonidan o‘tadi). Shundan so‘ng, tizim foydalanuvchidan taqdim etilgan identifikatorni haqiqiyligini tekshirish uchun parolni so‘raydi. Agar identifikatorga mos parol kiritilsa (ya’ni, autentifikasiyadan o‘tsa), foydalanuvchi kompyuterdan foydalanish imkoniyatiga ega bo‘ladi. Boshqa so‘z bilan aytganda, autentifikasiyani foydalanuvchi yoki subyektni haqiqiyligini tekshirish jarayoni deb aytish mumkin.

Autentifikasiyadan o‘tgandan so‘ng foydalanuvchi tizim resursidan foydalanish imkoniyatiga ega bo‘ladi. Biroq, autentifikasiyadan o‘tgan foydalanuvchiga tizimda ixtiyoriy amallarda bajarishga ruxsat berilmaydi. Masalan, autentifikasiyadan o‘tgan – imtiyozga ega foydalanuvchi uchun dasturlarni o‘rnatish imkoniyatini

berilishi talab etilsin. Xo‘sh, autentifikasiyadan o‘tgan foydalanuvchiga qanday qilib ruxsatlarni cheklash mumkin? Mazkur masalalar bilan aynan, avtorizasiya sohasi shug‘ullanadi.

Avtorizasiya – identifikasiya, autentifikasiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayonidir.

Demak, autentifikasiya binar qaror – ya’ni, ruxsat beriladi yoki yo‘q. Avtorizasiya esa tizimning turli resurslariga foydalanishni cheklash uchun foydalaniluvchi qoidalar to‘plami haqidagi barcha narsa.

Xavfsizlik sohasida terminlar standartlashtirilgan ma’nolaridan ayri qo‘llaniladi. Xususan, ruxsatlarni nazoratlash ko‘p hollarda avtorizasiyaga sinonim sifatida ishlatiladi. Biroq, mazkur kursda ruxsatlarni nazoratlash kengroq qaraladi. Ya’ni, avtorizasiya va autentifikasiya jarayonlari ruxsatlarni nazoratlashning qismlari sifatida qaraladi.

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

Identifikasiya – siz kimsiz?

Autentifikasiya – siz haqiqatdan ham sizmisiz?

Avtorizasiya – sizga buni bajarishga ruxsat bormi?

5.2. Autentifikasiya

Parolnaya avtorizasiya Yozish kerak

Autentifikasiya

Autentifikasiyada yoki identifikasiya jarayonlarida subyektlar inson ko‘rinishida yoki qurilma (kompyuter) ko‘rinishida bo‘lishi mumkin. Ya’ni, inson insonni autentifikasiyadan o‘tkazishi mumkin, mashina insonni autentifikasiyadan o‘tkazishi mumkin yoki mashina mashinani autentifikasiyadan o‘tkazishi mumkin. Mazkur ma’ruzada mashina insonni yoki mashina mashinani autentifikasiyadan o‘tkazish senariylariga asosiy e’tibor qaraladi.

Mashina insonni quyidagi “narsalar” asosida autentifikasiyadan o‘tkazishi mumkin:

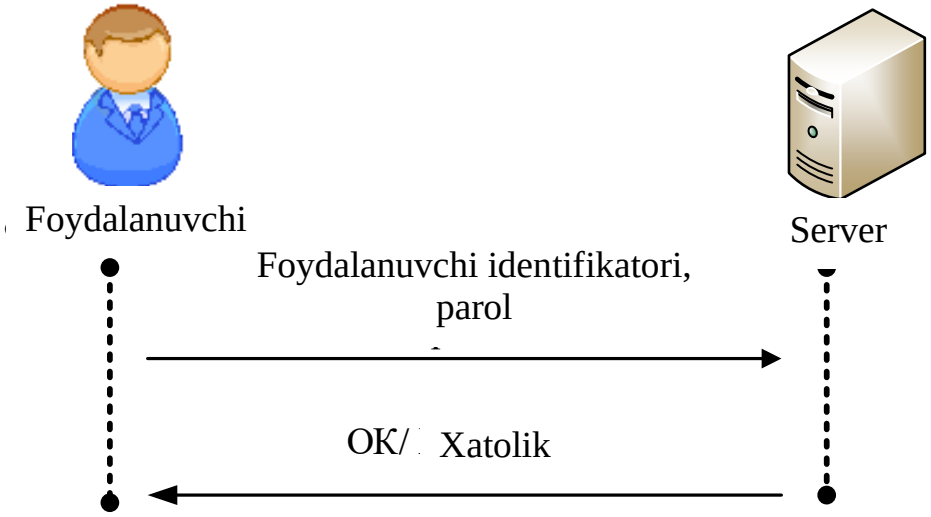
- siz bilgan biror narsa (something you know);
- sizda mavjud biror narsa (something you have);
- sizning biror narsangiz (something you are).

“Siz bilgan biror narsa” holatiga parol misol bo‘la oladi. “Sizda mavjud biror narsa” holatiga esa smartkartalar, token, mashinaning

pulti yoki kaliti misol bo‘la oladi. “Sizning biror narsangiz” holati odatda biometrik parametrlarga sinonim sifatida qaraladi. Masalan, hozirda siz noutbuk sotib olib, undagi barmoq izi skaneri orqali autentifikasiyadan o‘tishingiz mumkin.

Parol

Parol – faqat foydalanuvchiga ma’lum va biror tizimda autentifikasiya jarayonidan o‘tishni ta’minlovchi biror axborot. Parol amalda autentifikasiya jarayonida keng qo‘llaniluvchi parametr hisoblanadi. Masalan, biz o‘z shaxsiy kompyuterlarimizdan foydalanish huquqini olish uchun talab etilgan parolni kiritishimiz talab etiladi. Mazkur holatni mobil telefonlar uchun ham ishlatish mumkin. Parolga asoslangan holatdagi autentifikasiyalash jarayonining umumiy ko‘rinishi 5.1-rasmda keltirilgan.



5.1-rasm. Parolga asoslangan mashina-insonni autentifikasiyalash jarayoni

- Parolga asoslangan autentifikasiyalash quyidagi xususiyatlarga ega:

- parolga asoslangan autentifikasiyani amalga oshirish qulay (sarf xarajati kam, almashtirish oson);

- foydalanuvchi paroli odatda unga aloqador ma’lumot bo‘ladi (masalan, uning yaxshi ko‘rgan futbol komandasi, telefon raqami va hak.) (***123456, 12345, qwerty***) va shuning uchun “hujumchilar” tomonidan aniqlanishi oson;

- murakkab parollarni esda saqlash murakkab (masalan, ***jfIej(43jEmmL+y***);

- parolga asoslangan autentifikasiya usuli amalda keng qo‘llaniluvchi usul.

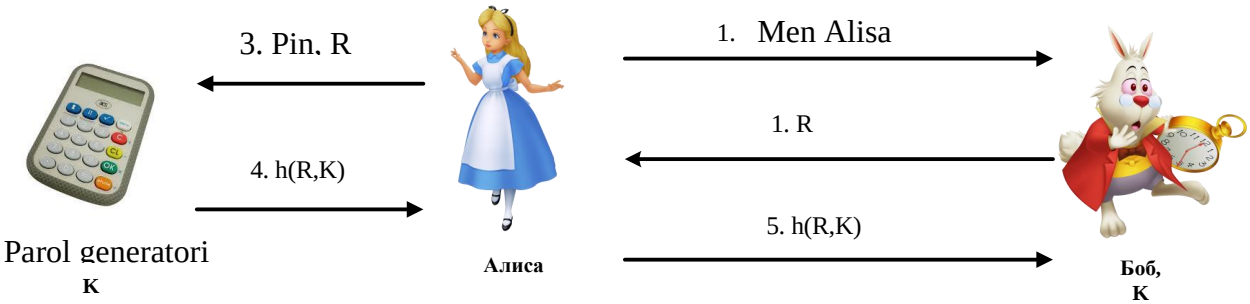
Smartkarta yoki token

Smartkartalar yoki qurilma ko‘rinishidagi tokenlar autentifikasiyalash uchun qo‘llaniladi. *Smartkarta* – kredit karta o‘lchamidagi qurilma bo‘lib, kichik hajmdagi xotira va hisoblash imkoniyatiga ega. Smartkarta odatda o‘zida biror maxfiy kattalikni, kalit yoki parolni, saqlaydi va hattoki biror hisoblashni amalga oshiradi. 5.2-rasmda maxsus maqsadli smartkarta va uni o‘quvchi qurilma (smartkarta o‘quvchi qurilma) aks ettirilgan.



5.2-rasm. Smartkarta va smartkarta o‘quvchi

Biror narsa asosida autentifikasiyalash usullarini turli ko‘rinishlarda amalga oshirish mumkin. Masalan, parollar generatorini misol qilib olaylik. Parollar generatori kichik qurilma bo‘lib, tizimda kirishda qo‘llaniladi. Faraz qilaylik Alisada parol generatori mavjud va undan foydalanib Bobdan autentifikasiyadan o‘tmoqchi. Buning uchun Bob biror tasodifiy son R ni (“savolni”) Alisaga yuboradi. Alisa qabul qilingan R sonini va parol generatoridan foydalanish uchun talab qilingan PIN ni parol generatoriga kiritadi. Parol generatori esa Alisaga javobni taqdim etadi va u Bobga uzatiladi. Agar javob to‘g‘ri bo‘lsa, Alisa autentifikasiyadan o‘tadi, aks holda o‘ta olmaydi. Mazkur senariyning umumiy ko‘rinishi 5.3-rasmda keltirilgan.



5.3-rasm. Tokenga asoslangan autentifikasiya jarayoni

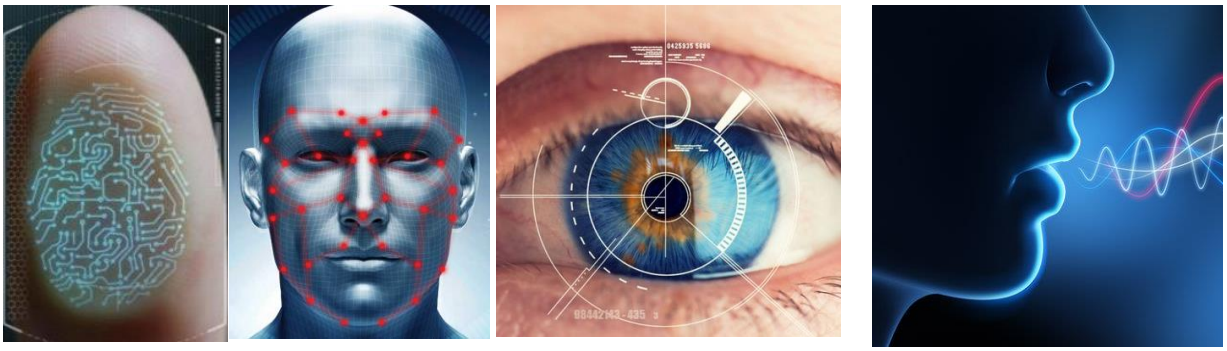
Keltirilgan sxemaga ko‘ra, Bob va parol generatorida taqsimlangan kalit K bo‘lishi shart. Ushbu sxemada “savol-javob” mexanizmi ishlatilgan. Ya’ni, savol sifatida Bob Alisaga R sonini uzatadi va unga mos bo‘lgan javob - $h(R,K)$ ni qabul qiladi. Qabul qilgan ma’lumotni tekshirish orqali Bob Alisani haqiqiyligini tekshiradi.

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

- smartkartaga asoslangan autentifikasiyada biror narasani esda saqlashni talab etilmaydi;
- amalga oshirish va qurilma narxi yuqori (xususan, token yo‘qolgan taqdirda uni almashtirish qimmatga tushadi);
- token yoki smartkartani yo‘qotib qo‘yish muammosi mavjud;
- token xavfsiz olib yurilsa yuqori xavfsizlik darajasini ta’minlaydi.

Biometrik parametrlarga asoslangan autentifikasiya

Biometrik parametrga asoslangan autentifikasiya usulida biometrik parametr insonning o‘zi uchun kalit sifatida xizmat qiladi. Juda ham ko‘plab biometrik parametrlar mavjud, masalan, barmoq izi, yuz tasviri, ko‘z qorachig‘i, ovoz, harakat tarzi, quloq shakli, qo‘l shakli va hak. Biometrik parametrlarga asoslangan autentifikasiya usuli amalda keng qo‘llaniladi. Masalan, qo‘p qavatli uylarni kirish eshiklarida yoki tashkilotlarga kirishda barmoq iziga asoslangan autentifikasiya usuli, noutbuklarda va mobil telefonlarda yuz tasviriga asoslangan yoki barmoq iziga asoslangan autentifikasiyadan keng qo‘llaniladi (5.4-rasm).



Barmoq izi Yuz tasviri Ko‘z qorachig‘i Ovoz

5.4-rasm. Biometrik na’munalarga misollar

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

- biometrik parametrga asoslangan usul o‘zida esda saqlash va birga olib yurish zaruriyatini talab etmaydi;
- biometrik parametrga asoslangan autentifikasiyani amalga oshirish parolga asoslangan usuldan qimmat va tokenga asoslangan usuldan arzor hisoblanadi (ba’zi, istisno holatlar mavjud);
- biometrik parmetrni almashtirish imkoniyati mavjud emas, ya’ni, agar biometrik parametr qalbakilashtirilsa, u holda autentifikasiya tizimi shu foydalanuvchi uchun to‘liq buzilgan hisoblanadi;
- turli biometrik parametrlarga asoslangan autentifikasiya usullari insonlar tomonidan turli darajada qabul qilinadi.

Autentifikasiya sohasida foydalanish uchun ideal biometrik parametr quyidagilarni qanoatlantirishi shart:

- *universal bo‘lishi* – biometrik parametr barcha foydalanuvchilarda bo‘lishi shart;
- *farqli bo‘lish* – tanlangan biometrik parametr barcha insonlar uchun farq qilishi shart;
- *o‘zgarmaslik* – tanlangan biometrik parametr vaqt o‘tishi bilan o‘zgarmay qolishi shart;
- *to‘planuvchanlik* – fizik xususiyat osonlik bilan to‘planuvchi bo‘lishi shart. Amalda fizik xususiyatni to‘planuvchanligi, insonning jarayonga e’tibor berishiga ham bog‘liq bo‘ladi.

Biometrik parametr nafaqat autentifikasiya masalasini echishda balki, identifikasiyalashda ham keng qo‘llaniladi. Ya’ni, “Siz kimsiz?” degan savolga javob bera oladi. Masalan, FBI da jinoyatchilarga tegishli barmoq izlari bazalari mavjud. Ushbu bazada barmoq izlari ***(barmoq izi tasviri, foydalanuvchi nomi)*** shaklida saqlanadi va bu orqali biror insonni jinoyatchilar ro‘yxatida bor yo‘qligini tekshira oladi. Buning uchun, tekshiriluvchi insondan barmoq izi tasviri olinadi va u FBI bazasida mavjud bo‘lsa, u holda *tekshiriluvchi insonning nomi* ***barmoq izi tasviri***ga mos ***foydalanuvchi nomi*** bilan bir xil bo‘ladi.

Bir tomonlama va ikki tomonlama autentifikasiya

Agar tomonlardan biri ikkinchisini autentifikasiyadan o‘tkazsa, *bir tomonlama autentifikasiya* deb ataladi. Agar har ikkala tomon bir-birini autentifikasiyadan o‘tkazsa, u holda *ikki tomonlama autentifikasiya* deb ataladi. Masalan, elektron pochtadan foydalanish davomida faqat server foydalanuvchini haqiqiyligini tekshiradi (parol orqali) va shu sababli uni *bir tomonlama autentifikasiyalash* deb atash mumkin. Elektron to‘lovlarni amalga oshirishda esa ham server foydalanuvchini autentifikasiyadan o‘tkazadi ham foydalanuvchi serverni autentifikasiyadan o‘tkazadi. Shuning uchun mazkur holatni *ikki tomonlama autentifikasiyalash* deb aytish mumkin.

5.3. Ko‘p omilli autentifikasiya

Ko‘p faktorli autentifikasiya

Yuqorida keltirilgan barcha autentifikasiya senariylarida faqat bitta omil o‘yicha haqiqiylikni tekshirish amalga oshirildi. Masalan, pochtada kirishda faqat parolni bilsangiz siz autentifikasiyadan o‘ta olasiz yoki kirishda barmoq izini to‘g‘ri kiritsangiz, eshik ochiladi. Ya’ni, server faqat foydalanuvchidan parolni yoki barmoq izini to‘g‘ri bo‘lishini istayapti. Mazkur ko‘rinishdagi autentifikasiya – *bir faktorli autentifikasiya* deb ataladi. Bir faktorli autentifikasiyada tekshirish faqat bitta faktor bo‘yicha (masalan, parol) amalga oshiriladi.

Biroq, bir faktorli autentifikasiyalashni amalda joriy qilish natijasida yuqori xavfsizlikni ta’minlash mumkin emas. Masalan, ovozga asoslangan autentifikasiya tizimini olaylik. Agar hujumchi foydalanuvchini ovozini diktafonga yozib olib, uni autentifikasiyadash o‘tish jarayonida taqdim etsa, osonlik bilan autentifikasiya tizimini aldab o‘tishi mumkin. Sababi, faqat bitta faktor (ovoz) bo‘yicha tekshirish amalga oshirilmoqda. Shunga o‘xshash holatni parolga

asoslangan yoki tokenga asoslangan autentifikasiya jarayonida ham kuzatish mumkin.

Mazkur muammoni bartaraf etish uchun, birinchi faktorga qo‘shimcha qilib, yana boshqa faktorlardan foydalanish mumkin. Masalan, ovozga asoslangan autentifikasiyalashda qo‘shimcha qilib paroldan foydalanish mumkin. Ya’ni, foydalanuvchi dastlab tizimga o‘z ovozi orqali autentifikasiyadan o‘tadi va udan so‘ng parol bo‘yicha autentifikasiyadan o‘tkaziladi. Har ikkala bosqichda ham autentifikasiyadan muvaffaqqiyatli o‘tilganda, foydalanuvchi tizimdan foydalanish imkoniyatiga ega bo‘ladi. Ko‘p faktorli autentifikasiyalashdan foydalanishda hayotimizda ham ko‘plab misollar keltirish mumkin. Masalan, plastik kartadan to‘lovni amalga oshirishda. Plastik kartadan to‘lovni amalga oshirishdagi autentifikasiya jarayoni o‘zida “*sizda mavjud biror narsa*” va “*siz bilgan biror narsa*” usullarini birlashtirgan. Ya’ni, dastlab foydalanuvchida plastik kartani o‘zini bor bo‘lishini talab etadi va ikkinchidan uni PIN kodini bilishni talab etadi. Shu sababli, ushbu usulni *ko‘p faktorli autentifikasiyalash* deb aytish mumkin.

Ko‘p faktorli autentifikasiya usuli faktorlardan bittasi qalbakilashtirilgan taqdirda ham autentifikasiya jarayonini buzilmasligiga olib keladi.

OTR yozish kerak

Autentifikasiya usullariga qaratilgan hujumlar

Mavjud autentifikasiya usullarini buzishda ko‘plab hujum usullaridan foydalaniladi. Ushbu hujum usullarini autentifikasiya usullariga mos ravishda quyidagicha tavsiflash mumkin:

1. **Siz bilgan biror narsa.** Autentifikasiyalashning mazkur usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

a. **Parollar lug‘atidan foydalanishga asoslangan hujum.** Bunga ko‘ra statistika bo‘yicha eng ko‘p qo‘llaniluvchi parollar yordamida autentifikasiyadan o‘tishga harakat qilinadi.

b. **Parollarni barcha variantlarini ko‘rib chiqish.** Ushbu usulda parolning bo‘lishi mumkin bo‘lgan barcha variantlari generasiya qilinadi va ular tekshirib ko‘riladi.

c. **“Elka orqali qarash” hujumi.** Ushbu hujum foydalanuvchi parolni kiritish jarayonida yonida turib qarab turish orqali bilib olishni maqsad qiladi.

d. **Zararli dasturlar asosida hujum.** Shunday maxsus dasturiy vositalar mavjudki ular foydalanuvchi kompyuterida o‘rnatilib, klaviatura orqali kiritilgan barcha ma’lumotlarni serveriga uzatadi. Ushbu zararli dasturiy vositalar “*keylogger*” deb ataladi.

2. Sizda mavjud biror narsa. Autentifikasiyaning mazkur usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

a. **Fizik o‘g‘irlash.** Hujumning mazkur turi tokenni yoki smart kartani o‘g‘irlashni maqsad qiladi. Mazkur hujum bu toifdagi autentifikasiya uchun eng xavfli hujum hisoblanadi.

b. **Dasturiy ko‘rinishdagi tokenlarning zararli dasturlarga bardoshsizligi.** Ba’zi tokenlar dasturiy ko‘rinishda bo‘lib, mobil qurilmalarda ishlaydi va shu sababli zararli dastur tomonidan boshqarilishi mumkin.

3. Sizning biror narsangiz. Autentifikasiyaning mazkur usulini buzish uchun quyidagi hujum usullaridan foydalaniladi:

a. **Qalbakilashtirish.** Hujumning mazkur turi biometrik parametrni qalbakilashtirishni maqsad qiladi. Masalan, yuzlari o‘xshash bo‘lgan Hasan o‘rniga Xusan autentifikasiyadan o‘tishi yoki sifati yuqori bo‘lgan foydalanuvchi yuz tasviri mavjud rasm bilan tizimni aldashni misol qilish mumkin.

b. **Ma’lumotlar bazasidagi biometrik parametrlarni almashtirish.** Ushbu hujum bevosita foydalanuvchilarni biometrik parametrlari (masalan, barmoq izi tasviri, yuz tasviri va hak) saqlangan bazaga qarshi amalga oshiriladi. Ya’ni, tanlangan foydalanuvchini biometrik parametrlari hujumchini biometrik parametrlari bilan almashtiriladi.

Autentifikasiya usullariga qaratilgan hujumlarni oldini olish uchun har bitta usulda o‘ziga xos qarshi choralari mavjud. Umumiy holda mazkur hujumlarni oldini olish uchun quyidagi himoya usullari va xavfsizlik choralari tavsiya etiladi:

1. ***Murakkab parollardan foydalanish.*** Aynan ushbu usul parolni barcha variantlarini tekshirib ko‘rish va lug‘atga asoslangan hujumlarni oldini olishga katta yordam beradi.

2. ***Ko‘p faktorli autentifikasiyadan foydalanish.*** Mazkur usul yuqorida keltirilgan barcha muammolarni bartaraf etishda katta amaliy yordam beradi.

3. ***Tokenlarni xavfsiz saqlash.*** Ushbu tavsiya biror narsaga egalik qilishga asoslangan autentifikasiya usulidagi mavjud muammolarni oldini olish uchun samarali hisoblanadi.

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

O‘z-o‘zini nazorat va muhokama qilish uchun savollari

1. Identifikasiya, autentifikasiya va avtorizasiya jarayonlarini tushuntirib bering

2. Bir tomonlama va ikki tomonlama autentifikasiya nima?

3. Ko‘p omilli autentifikasiya qanday amalga oshiriladi?

VI BOB. MA’LUMOTLARNING FIZIK XAVFSIZLIGI. MA’LUMOTLARDAN FOYDALANISHNING MANTIQIY NAZORATI. FORMAL MODELLAR.

6.1. Fizik xavfsizlik, uning zaruriyati

Axborot xavfsizligini ta’minlashda amalga oshiriladigan dastlabki choralardan biri bu – fizik xavfsizlik hisoblanadi. Ruxsat etilmagan fizik boshqarishni, shaxs tomonidan amalga oshiriladigan tahdidlarni va muhitga bog‘liq tahdidlarni oldini olish uchun tashkilotlar mos fizik xavfsizlik boshqaruvini sharoitida bo‘lishi shart. Tizim administratori fizik xavfsizlikga qaratilgan tahdidlardan saqlanish uchun fizik xavfsizlik choralari o‘rnatilgani va to‘g‘ri ishlayotganini kafolatlashi shart.

Fizik xavfsizlik fizik qurilmalarni, shaxslarni, tarmoq va ma’lumotni hujumlardan himoyalash bilan shug‘ullanadi. Ma’lumot, tarmoqlar va qurilmalar xavfsizligi o‘zida tabiiy va sun’iy (inson tomonidan qilingan) tahdidlardan himoyalashni mujassamlashtiradi. Tashkilotlar fizik xavfsizlikni ta’minlash uchun mos himoya vositalaridan foydalanishlari zarur. Bunda, tashkilotlar o‘z infratuzilmasi va axborot tizimlarining fizik xavfsizligiga ta’sir qiluvchi barcha yo‘llarni inobatga olishi shart.

Fizik xavfsizlik – tashkilot axborot xavfsizligi dasturining muhim qismlaridan biri. O’tgan davrda, insonlar fizik xavfsizlik bilan kalitlar, qo‘riqchilar, to‘siqlar, eshiklar va hak. orqali tushunchaga egalar. Hozirgi kunda, fizik xavfsizlikning ko‘rinishi esa tamomila o‘zgardi va tashkilotlardan ishchi kuchlar, aktivlar va ko‘chmas mulklar nazoratini talab etmoqda. Mazkur aktivlarning fizik xavfsizligini ta’minlash tashkilot uchun muhim vazifalardan biriga aylanmoqda. Tashkilot uchun fizik xavfsizlikni loyihalashda binoning qurilishini rejalashtirishga, jixozlarni sotib olishga, ishchi kuchini jalb etishga, tabbiy hodisalarga, quvvat manbaiga, haroratni nazoratlashga va hak.larga e’tibor qaratish talab etiladi.

Fizik xavfsizlik dasturiy ta’minot va qurilmalarni o‘z ichiga olgan tashkilot binosini va aktivlarini o‘g‘irlikdan, bosqinchilikdan, tabiy ofatlardan, iqlim o‘zgarishlaridan, muhit o‘zgarishlaridan va inson tomonidan amalga oshiriluvchi turli tahdidlardan himoyalashni maqsad qiladi. Mos joyda ko‘p sathli amalga oshirilgan xavfsizlik tashkilotni turli fizik tahdidlardan himoyalaydi. Xavfsizlikning birinchi sathi tashkilot binolariga tashqaridan kirishni nazoratlash va tashqi transport

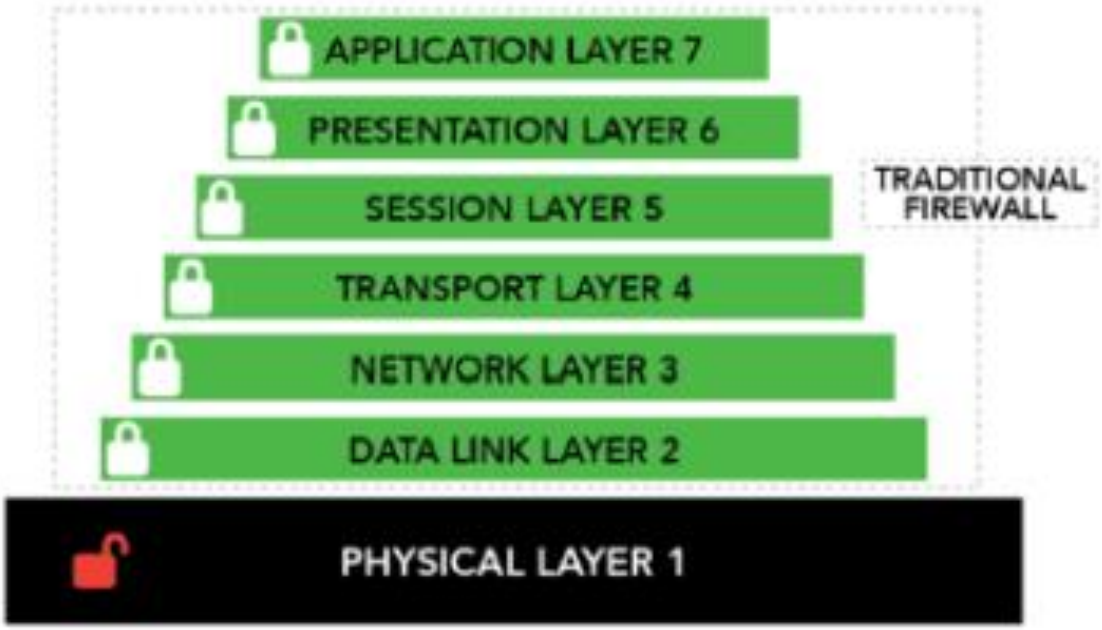
vositalarining harakati bilan shug‘ullanadi. Mazkur himoya sathi tashqaridan keluvchini yoki buzg‘unchini tashkilot binosiga ruxsatsiz kirishini oldini oladi va tashkilotni dastlabki sathda bo‘lishi mumkin bo‘lgan xavfni kamaytiradi. Himoyaning keyingi sathi transportlarni, insonlarni va boshqa tashilot aktivlarini ichki va tashqi xavflardan himoyalash bilan shug‘ullanadi. Ushbu sathda quvvat manbai tizimini xavfsiz joyda o‘rnatish, uni yong‘in o‘chirish tizimi va zaxira tizimi bilan ta’minlash amalga oshiriladi. Bundan tashqari, tashkilot asosiy binosini mashinalar to‘xtash joyidan ajratish, to‘g‘ri ventilyasiya tizimiga ega yaxshi jixozlangan suv quvur tizimini mos joyga o‘rnatish, ogohlantirish tizimlari va hak. ushbu bosqichda amalga oshiriladi. Keyingi sath fizik sathning eng muhim qismi bo‘lib, bunda tashqaridan va ichkaridan (xodimlar) kiruvchilarni nazoratlash amalga oshiriladi. Ushbu sathda, agar buzg‘unchi fizik aktivga hujumni amalga oshirsa, u tashkilotga aloqador maxfiy axborotni qo‘lga kiritishi mumkin bo‘ladi.

Fizik xavfsizlining zaruriyati

Kiberxujumlarning murakkablashishi natijasida hujumchilar tashkilot fizik xavfsizligini buzishda turli usullardan foydalanmoqda. Hujumchilar tashkilotning fizik xavfsizlik tizimidagi bo‘shliqlardan foydalangan holda o‘z harakatlarini amalga oshirishadi. AQShning Department of Health and Human Services Breach Portal tashkiloti tomonidan 2015 yilda tashkilotlarda eng ko‘p yuzaga kelgan xavfsizlik insidentlari fizik xavfsizlikni buzishga uringani aniqlangan.

Fizik xavfsizlikni buzilishi boshqa xavfsizlik buzilishlaridan tamomila farq qiladi. Ular texnik ma’lumotsiz juda ham kam hollarda amalga oshirilishi mumkin. Ana’naviy xavfsizlik choralari, masalan, tarmoqlararo ekran, IDS va bosh. fizik xavfsizlikka ishonmagan hollarda, haqiqiy fizik xavfsizlik muammolari ortadi. Masalan, tarmoqlararo ekran vositasi OSI modelining turli sathlarida ishlaydi va himoyani tashkil etadi. Biroq, tashkilotning fizik xavfsizligiga ta’sir eta olmaydi (6.2-rasm).

Fizik himoya tarmoq, ilova yoki ma’lumotlar bazasi xavfsizligi sohalariga o‘xshash amallarni bajarmaydi. Ya’ni, fizik xavfsizlik OSI modelining fizik sathida himoyani ta’minlash bilan shug‘ullanadi.



6.1-rasm. Tarmoqning fizik sathi ananaviy tarmoqlararo ekran yordamida himoyalanmaydi

Fizik sath quyidagilarni o‘z ichiga oladi:

- barcha kabel va tarmoq tizimlari;
- tizim va kabellarni fizik nazoratlash;
- tizim va kabel uchun quvvat manbai;
- tizimni madadlash muhiti.

6.2. Fizik xavfsizlikka ta’sir qiluvchi omillar

Fizik xavfsizlikka ta’sir qiluvchi faktorlar

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

Tabiiy tahdidlar*:*

Toshqinlar. Toshqinlar odatda kuchli yomg‘ir va muzlarning erishi natijasida yuzaga keladi. Toshqinlar natijasida tashkilotning elektr quvvatiga va server xonalariga zarar etishi mumkin. Odatda tashkilotda server xonalari tashkilot binosining podvalida joylashganligi sababli, toshqin yanada ko‘proq zarar etkazishi mumkin.

Yong‘inlar. Yong‘inlar odatda qisqa tutashuvlar va eski bino materiallari sababli yuzaga keladi. Yong‘in natijasida tashkilotning kompyuter xonalari va ishchi binolariga zarar etkazilishi mumkin. Yong‘in qurilmalar, kabellar va boshqa muhim tashkil etuvchilarga to‘liq zarar yetkazishi mumkin.

Zilzila. Zilzila Yer qobig‘ida seysmik terbanishni yaratuvchi kuchli energiya natijasida to‘satdan yuzaga keladi. U tashkiloning fizik infratuzilmasiga ta’sir qiladi. Zilzila natijasida tashkilot ichidagi xavfsiz muhitda saqlangan kompyuter qurilmalari, boshqa qurilmalar va hujjatlarga jiddiy ziyon yetadi.

Chaqmoq va momaqaldiroq. Chaqmoq va momaqaldiroq muhitning o‘zgarishi natijasida yuzaga keladi. Buning natijasida barcha tashqi faoliyat to‘xtatiladi. Chaqmoq va momaqaldiroq natijida elektr quvvati o‘zgaradi va bu ish faoliyatiga tasir qiladi. Bu esa, o‘z navbatida tashkilotdagi qurilmalarning xotira qismlariga tasir qiladi. Bundan tashqari, chaqmoq va momaqaldiroq natijasida kabellarda va boshqa ulanish tizimlarda qisqa tutashuvlar yuzaga kelishi mumkin.

Harorat va namlik. Hisoblash qurilmalari ishlashi uchun ularni ma’lum haroratli muhitda bo‘lishi talab etiladi. Kompyuter vositalari yuqori haroratga ishlashga mo‘ljallanmagan. Kompyuterlarda sovutish tizimlari mavjud bo‘lsada, tashqi harorat ularning ish faoliyatiga salbiy ta’sir ko‘rsatadi. Tashkilotdagi elektr va elektron jixozlar namlikni o‘zgarishiga ta’sir ko‘rsatadi. Yuqori namlik o‘z navbatida karroziyaga, qisqa tutashuvlarga sababchi bo‘ladi yoki magnetik va optiq saqlovchilarga jiddiy ta’sir qiladi.

Sun’iy tahdidlar. Fizik komponentlarga va tarmoqqa bo‘ladigan eng katta ta’sir insonlar xatosi natijasida yuzaga keladi. Bu xatolik insonlar tomonidan bilmasdan yoki ataylabdan amalga oshirilishi mumkin. Insonlar tomonidan amalga oshirluvchi fizik xavfsizlik tizimiga bo‘ladigan quyidagi tahdidlar mavjud:

Vandalizim. Norozi xodimlar yoki eski ishchilar tizim komponentlarini buzish yoki zarar etkazish orqali tizimni obro‘sizlantirishga harakat qiladi.

Qurilmaning yo‘qolishi. Ruxsat etilmagan nazoratlash muhim axborot yoki qurilmani yo‘qolishiga sababchi bo‘ladi. Agar qurilma himoyasi to‘g‘ri amalga oshirilmagan bo‘lsa, uning o‘g‘irlanishiga sababchi bo‘ladi.

Fizik qurilmalarni buzulishi. Qurilmaning noto‘g‘ri ishlashi, masalan, qurilmani yoki ma’lumotni qanday tutib turilganligi, zararlangan qurilmalarni almashtirilmaganligi va zaif kabellar natijasida fizik qurilmalarga jiddiy zarar yetkazilishi mumkin.

O’g‘irlash. Xavfsizlik tizimidagi kamchilik natijasida jixozlar o‘g‘irlanishi mumkin.

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

Sosial injineriya. Sosial injineriya shaxsiy axborotni boshqa shaxslar tomonidan noqonuniy qo‘lga kiritish harakati sifatida qaraladi. Hujumchi tashkilot xodimlaridan sosial injineriya orqali ruxsat etilmagan fizik nazoratlashdan daromad ko‘radi.

Tizimlarni ruxsat etilmagan nazoratlash. Har ikkala, ichki va tashki foydalanuvchilar ham tashkilot haqidagi axborot yoki tizimni ruxsatsiz boshqarishga harakat qilib ko‘radi.

6.3. Fizik xavfsizlikni nazoratlash

Mos xavfsizlik nazoratisiz, biror fizik xavfsizlikni amalga oshirish qiyin. Fizik xavfsizlik nazorati bardoshli fizik xavfsizlik muhitini yaratishi uchun turli darajalarda amalga oshirilishini talab etadi. Fizik xavfsizlik nazoratini qaysi darajada amalga oshirilishiga qarab, ular quyidagicha tasniflanadi:

Ma’muriy nazorat. Ushbu nazorat turi xavfsizlikni nazoratlashda inson faktorini mujassamlashtiradi. Xodimlarning barcha darajalari ma’muriy nazoratni qurishda inobatga olinishi kerak. Ma’muriy nazorat har bir foydalanuvchi boshqarishi mumkin bo‘lgan resurslar va axborotga asoslanadi. Ma’muriy nazorat boshqaruv cheklanishlarini, amaliy muolajalarni, qayd yozuvini amalga oshirish muolajalari va axborot tizimi uchun mos himoya darajasini o‘z ichiga oladi. U asosan insonni boshqarish uchun shaxsga qaratilgan usullarni amalga oshiradi.

Fizik nazorat. Fizik nazorat tashkilotdagi fizik tizimlarga zarar yetishini oldini olish bilan shug‘ullanadi. U o‘z ichiga qurilmalarni, bino yoki biror maxfiy muhitni ruxsatsiz boshqarishdan himoyalashni qamrab olgan. Bundan tashqari, fizik xavfsizlikni nazoratlash fizik tahdidlar: qurilmaning yo‘qolishi yoki o‘g‘irlanishi, tasodiy tufayli zararlanishi va yo‘q qilinishi, yong‘indan himoyalash yoki tabiiy ofatlardan himoyalash bilan shug‘ullanadi.

Texnik nazorat. Texnik nazorat mantiqiy nazorat kabi qaraladi. Texnik nazorat tashkilotdagi fizik avtivlarga yoki binolarga ruxsatlarni nazoratlash uchun texnologiyalardan foydalanadi. U odatda taqiqlangan hududda ruxsatlarni nazoratlash uchun kompyuter qurilmalari, dasturlar, amallar va ilovalardan foydalanadi.

Fizik xavfsizlikni nazoratlash: joylashuv va arxitektura

Tashkilotlar o‘zlari uchun bino sotib olishdan yoki ijaraga olishdan oldin fizik xavfsizligiga ta’sir qilishi mumkin bo‘lgan ko‘plab omillarni e’tiborga olishi shart. Bu omillar o‘z ichiga binoning joylashuvi, qo‘shni binolar, elektr va suv manbalari, kanalizasiya tizimi, kichik va katta yo‘llarga yaqinligi, transport masalasi, tez yordam ko‘rsatish holati, shifoxona, ayeroportga yaqinligi, mazkur hududda mahalliy holatda jinoyatchilar ko‘rsatkichi yoki turli xavfsizlik insidentlarini mavjudligi va h.k.larni oladi. Tanangan hudud tabiiy ofatlardan, masalan, toshqinlar, tarnadolar, yer silkinishi, dovul, yong‘inlar va hak.lardan xoli bo‘lishi kerak.

Binoning joylashuvi haqida yetarlicha axborotga ega bo‘lingandan so‘ng, ichki tuzilma va arxitekturani loyihalash va rejalashtirish amalga oshiriladi. Joylashuv arxitekturasini loyihalash va rejalashtirish vaqtida, tashkilot tomondan binodagi barcha aktivlarning ro‘yxati tayyor bo‘lishi lozim.



6.2-rasm.

Tashkilot infratuzilma va arxitekturani loyihalash vaqtida quyidagi joxatlarga yetibor berishi lozim:

- binoga kirish eshiklarining sonini, asosiy kirish, zinalar, lift, mashina stoyankasi, o‘tish yo‘laklari va qabul qilish hududini o‘z ichiga olgan holda, aniqlashtirish;

- joylashgan hududingizga yaqin qo‘shni binolarni topish va ular uchun ichki va tashqi arxitekturani tekshirish. Atrofdagi narsalar

haqida qo‘shimcha ma’lumot olish uchun binolarning egasi va menedjerlari bilan suhbatlashish.

- katastropik buzilishlar va tashqi tomondan aktivlarni ko‘rinishi orqali zarar etuvchi aktivlarni tahlil qilish;

- agar bino boshqa tashkilotlar bilan sheriklikda foydalanilsa, ularni sizning shaxsiy ma’lumotlaringizga va muhim aktivlaringizga ta’siri haqida o‘ylang;

- fizik xavfsizlikni, maxfiy ma’lumotni saqlash va tashkilot ishlarini samarali amalga oshirish yo‘lga qo‘yishni boshqarish uchun talab etilgan muhim infratuzilmani aniqlashtirish.

Fizik xavfsizlikni nazoratlash: yong‘inga qarshi tizimlar

Yong‘inga qarshi tizimlar fizik xavfsizlikni ta’minlashda muhim omil hisoblanadi. Yong‘in yuzaga kelganini avtomatlashgan yoki avtomatlashmagan shakllarda aniqlash mumkin.



6.3-rasm. Yong‘inga qarshi himoya vositalari

Turli yong‘inga qarshi tizimlar o‘zida aktiv yong‘inga qarshi himoyani va passiv yong‘inga qarshi himoyani mujassamlashtirgan.

Aktiv yong‘inga qarshi himoya. Aktiv yong‘inga qarshi himoya tashkilotda yong‘in yuzaga kelgani haqida ogohlantirishni ta’minlaydi. Mazkur turdagi himoya tizimi odatda tijoriy joylarda, ishlab chiqarish joylaridi va savdo uylarida o‘rnatiladi. Ushbu himoya usulining asosiy maqsadi yong‘inni binoning boshqa qismlarini tarqalmasligini oldini olish hisoblanadi. Ushbu himoya tizimi yong‘inga qarshi chora ko‘rishda ma’lum ishlarni amalga oshirishi talab etiladi. Mazkur harakatlar avtomatik yoki avtomatik bo‘lgan tarzda amalga oshiriladi.

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

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

- *Yong‘inni aniqlash tizimi:* ushbu tizim yong‘in tarqalishidan oldin uni aniqlashga yordam beradi. Ushbu tizim *tutunni aniqlovchilar, alangani aniqlovchilar* va *issiqlikni aniqlovchilarni* o‘z ichiga oladi.

- *Yong‘inni bartaraf etish tizimlari:* ushbu tizimlar inson aralashuvisiz yong‘inni dastlabki bosqichlarida uni bartaraf etish bilan shug‘ullanadi. Ushbu tizimlar zararni kamaytirishga va qurilmalarni yo‘q bo‘lishidan himoyalaydi. Yong‘inni bartaraf etish tizimlari avtomatik va avtomatik bo‘lgan turlarga ajratiladi. Ushbu tizimlarga: *o‘to‘chirgich (ognetushiyet), suv purkash tizim*larini misol keltirsa bo‘ladi.

Yong‘inga qarshi passiv himoya. Yong‘inga qarshi passiv himoya tizimlari bino bo‘ylab yong‘inni tarqalishini oldini olishga foydalaniladi. Yong‘inga qarshi eshiklar, oynalar va devorlar passiv yong‘inga qarshi himoya usuli sifatida foydalanilishi mumkin. Ushbu himoya tizimi boshqa biror tizim tomonidan ishga tushurilishni talab etmaydi.

Passiv yong‘inga qarshi himoya usuli amaliyotda quyidagi usullar asosida oshiriladi:

- minimal darajada yonuvchan materiallardan foydalanish;
- binoga yong‘inni tarqalishini oldini olish uchun qo‘shimcha yetaj yoki xonalarni qurish;
- binoga istiqomat qiluvchilarni yong‘in sodir bo‘lganda qilinishi zarur bo‘lgan ishlar bilan tanishtirish;
- yong‘inga aloqador tizimlarni to‘g‘ri madadlar;
- yetarli sondagi qo‘shimcha chiqish yo‘llarining mavjudligi.

Fizik xavfsizlikni nazoratlash: fizik to‘siqlar

Fizik xavfsizlikni ta’minlashda tashkilotda ruxsatsiz kirishlarni oldini olish muhim hisoblanadi. Bu vazifani bajarishda odatda turli fizik to‘siqlardan foydalaniladi. Fizik to‘siqlar fizik chegarani umumiy hududdan taqiqlangan hududga ajratadi. Ushbu to‘siqlarni joylashuv o‘rniga ko‘ra: tashqi, o‘rta va ichki to‘siqlarga ajratish mumkin. Tashqi to‘siqlar odatda *zabor, devor* va boshqalarni o‘z ichiga oladi. O’rta to‘siqlar odatda olamon va insonlarni taqiqlash uchun foydalaniladi. Ichki to‘siqlarni esa eshiklar, derazalar, reshyotkalar, oynalar, pardalar va hak.lar tashkil etadi.

Bino ichida foydalaniluvchi fizik to‘siqlarni quyidagi turlari mavjud:

- *Zaborlar/ elektr zaborlar/ metal to‘siqlar.* Ushbu to‘siqlar odatda taqiqlangan hududlarni, nazoratlangan hududlarni va ruxsat etilmagan kirishdan himoyalani belgilashda foydalaniladi. Fizik to‘siqlarni amalga oshirishdan asosiy maqsad:

- hujumchini bloklash va ushlab qolish;
- tashkilot chegarasini belgilash;
- xavfsiz hududni tashqi hujumlardan himoyalash;
- transportlarni kirishidan himoyalash;
- portlovchi hujumlardan himoyalash.

- *Tumba.* Ushbu to‘siq kichik vertikal shakldagi tumba shaklida bo‘lib, avtomabillarni kirishidan himoyalashda foydalaniladi.

- *Turniketlar.* Turniketlar bir vaqtda bir shaxsni ichkariga kirishini yoki chiqishini ta’minlaydi. Bunda tizim shaxs tomonidan mos tanga, bilet, barmoq izi yoki token ko‘rsatilganda kirishga ruxsat beradi.

- *Boshqa to‘siqlar.* Fizik himoyani tashkil qilishda bundan tashqari turli eshiklar, oynalar, reshyotkalar, oynalar, deraza pardalaridan foydalaniladi.



-





6.4-rasm. To‘siqlarga misollar

Fizik xavfsizlikni nazoratlash: xavfsizlik xodimi

Xavfsizlik xodimi/ qo‘riqchi tashkilot fizik xavfsizligini amalga oshirish, monitor qilib borish va madadlashni amalga oshiradi. Ular maxfiy axborotni yo‘qolishidan, o‘g‘irlanishidan, noto‘g‘ri foydalanishidan himoyalash uchun xavfsizlik tizimini o‘rnatish, baholash va ishlab chiqishga javobgardirlar. Yuqori malakali va tajribaga ega xodim ixtiyoriy tashkilotning xavfsizligiga muhim ro‘y o‘ynaydi. Tashkilotda xodimlar tomonidan amalga oshirilgan himoya 24x7x365 tartibida amalga oshirilishi zarur. Fizik xavfsizlikka jalb etilgan shaxslar quyidagilar:

Qo‘riqchilar. Qo‘riqchilar odatda asosiy kirish eshigidan va darvozadan kiruvchilarni va xoimlarni nazoratlashga javobgardir. Ular xususan, begona shaxslarning tashkilot hududida kirmasligini, turli

taqiqlangan paketlar va jixozlarni olib kirmaslikni ta’minlashi talab etiladi. Tashkilotdagi barcha kirish eshiklaridagi holatlar qo‘riqchilar tomonidan CCTV kameralar yordamida yozib va saqlanib boriladi.

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

Xavfsizlik xodimi. Ushbu shaxsning vazifasi tashkilot atrofida o‘rnatilgan xavfsizlikka aloqador jixozlarni amalga oshirish va boshqarishdan iborat bo‘lib, ularni to‘g‘ri ishlayotganini kafolatlashi shart.

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

Ruxsatlarni nazoratlash: autentifikasiya usullari

Tashkilotdagi o‘rta to‘siqlar vazifasini o‘tovchi turniketlar odatda shaxslarni autentifikasiyalash vazifasini ham o‘taydi yoki bu vazifa qo‘riqchilar tomonidan ham amalga oshirilishi mumkin. Shaxslarni autentifikasiyadan o‘tganda turli axborotdan foydalaniladi va ular quyidagilar:

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

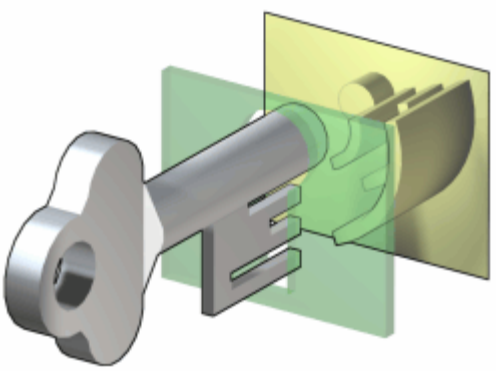
Fizik xavfsizlikni nazoratlash: fizik qulflar

Ruxsatsiz fizik kirishlarni cheklashda turli qulflar mavjud. Har bir tashkilot o‘zining xavfsizik talabidan kelib chiqqan holda ulardan mosini tanlashi shart. Quyidagi turdagi fizik qulflar mavjud:

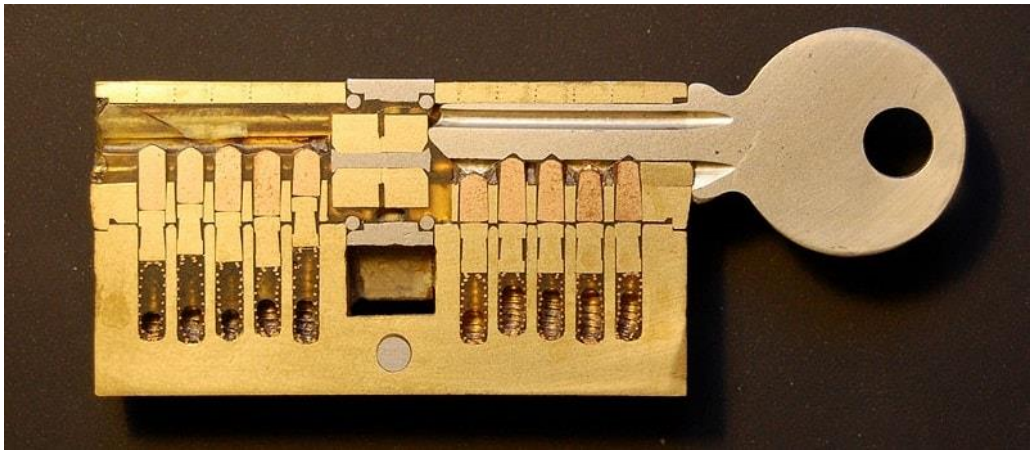
Mexanik qulflar: tashkilotda fizik ruxsatlarni cheklashning eng oson usuli hisoblanadi. Ushbu qulflar kalitli yoki kalitsiz bo‘lishi mumkin. Mexanik qulflarning ikki turi mavjud:

- O’ralgan qulflar, - Tumbler qulfi

Raqamli qulflar: raqamli qulflarda yeshikni ochish uchun barmoq izi, smart karta yoki PIN kodni kiritishi talab etiladi. Ular ochish uchun biror narsani (kalitni) olib yurishni talab etmaydi va oson foydalaniladi.



6.5-rasm. O’ralgan qulflar



6.6-rasm. Tumbler ulfi

Elektr/ elektromagnetik qulflar: elektr qulflar yoki elektron qulflash tizimi elektr quvvatni kamaytiradi va natijada eshik ochiladi. U odatda magnit va motor asosida qulfni aktivlashtiradi va deaktivlashtiradi. Ushbu qulflar ochish uchun kalitni talab etmaydi.

Kombinasion qulflar: ushbu qulflar raqam va belgilar kombinasiyasidan iborat bo‘ladi. Foydalanuvchi uni ochishi uchun ularning kombinasiyasidan iborat bo‘lgan maxfiy sirni kiritishi talab etiladi.

Fizik xavfsizlikni nazoratlash: Yashirin qurol/ kontrabanda qurilmalarini aniqlash moslamasi

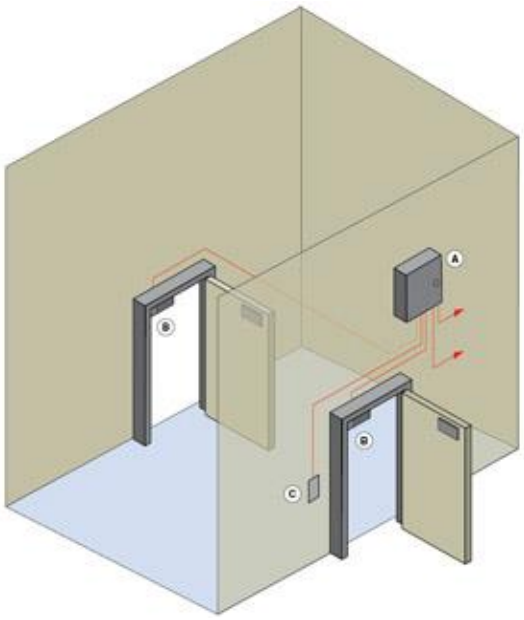
Tashkilotlarda odatda shaxslar tomonidan olib kiriladigan jixozlar yoki vositalar maxsus skanelarlar yordamida tekshiruvdan o‘tkaziladi. Bunda turli qurollar yoki kontrabanda vositalarini, bombalar, otish qurilmalarini aniqlash amalga oshiriladi. Mazkur skanerlarga misol qilib, metalni aniqlovchilar, X-ray aniqlash tizimlari va harakat bo‘ylab metalni aniqlash tizimlarini keltirish mumkin.



6.7-rasm. X-Ray metal detektorlar

Fizik xavfsizlikni nazoratlash: qopqon

Qopqon chegarani buzib o‘tuvchini tutuvchi va fizik xavfsizlikni nazoratlash vositasi hisoblanadi. Ushbu vosita odatda xavfsiz hududni xavfsiz bo‘lmagan hududdan ajratadi. Qopqon mexanik qulflashga asoslangan kichik soha bo‘lib, ikkita kirish eshigi mavjud. Ikkinchi eshik ochilishidan oldin birinchi eshik yopilgan holatda bo‘ladi. Shaxsni autentifikasiyalash smart karta, PIN kod yoki biometrik usullar asosida amalga oshirilishi mumkin.



6.8-rasm. Qopqon

Fizik xavfsizlikni nazoratlash: xavfsizlik yorliqlari va ogohlantiruvchi signallar

Xavfsizlik yorliqlari yuqori va past xavfsizlik sohasida axborotga bo‘lgan murajaatni cheklash uchun foydalaniladi. Ushbu yorliqlar foydalanuvchilar tomonidan oson tushuniladi va ular ma’lumotdan foydalana olishlari mumkin yoki mumkin emasligini bilishadi. Buning uchun tashkilotdagi ma’lumotlar dastlab xavfsizlik yorliqlari bilan ta’minlanadi. Odatda quyidagi turdagi xavfsizlik yorliqlari mavjud:

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

Axborotga murojaat qilishdan oldin uning yorlig‘iga qarab, ruxsat bor yoki yo‘qligini aniqlash va ruxsat bo‘lsa undan foydalanish amalga oshiriladi.

Ogohlantiruvchi signallar odatda tashkilotda ruxsat etilmagan harakatlarni amalga oshirni kamaytirish uchun foydalaniladi. Ushbu signallar tashkilotda katta hajmli hodimlarni cheklash uchun katta amaliy yordam beradi. Odatda ogohlantiruvchi signallar sifatida “TAQIQLANGAN HUDUD” (RESTRICTED AREA), “OGOHLANTIRISh” (WARNING), “XAVFLI” (DANGER) iboralardan foydalaniladi.



6.10-rasm. Ogohlantiruvchi belgilar

Fizik xavfsizlikni nazoratlash: video kuzatuv vositalari

Video kuzatuv tashkilotning fizik xavfsizligini ta’minlashda muhim komponent hisoblanadi. Ushbu tizimlar tashkilot aktivlarini bosqinchilardan, o‘g‘rilardan himoyalashda muhim ahamiyatga ega. Video kuzatuv moslamalari odatda tashkilotning kirish eshiklarida, zallarda va ishchi sohalarida o‘rnatiladi. Ushbu vositalar tashkilotga kirishdagi va chiqishdagi harakatlarni kuzatishda yordam beradi. Hozirgi kundagi video kuzatuv vositalari nafaqat harakatlarni qayd etishda balki, bo‘layotgan harakatlarni aniqlash imkonini beradi. Masalan, taqiqlangan jixoz olib kirayotgan yoki chiqayotgan holatni aniqlaydi va ogohlantirish signalini yuboradi yoki janjal bo‘layotgan holatni aniqlab, zarur signalni yuboradi. Video kuzatuv vositalari sifatida odatda, quyidagi kameralar amalda foydalanib kelinmoqda:



Dome CCTV Bullet CCTV C-mount CCTV Day/ night CCTV

6.10-rasm. Kuzatuv kameralari

Fizik xavfsizlikni nazoratlash: fizik xavfsizlik siyosati va muolajalari

Har bir tashkilot samarali fizik xavfsizlikni amalga oshirish uchun talab qilingan fizik xavfiszlik siyosatini va muolajalarini amalga oshirishi shart. Fizik xavfsizlik siyosati turli tashkilotlar uchun turlicha bo‘ladi.

Xususan, tashkilot fizik xavfsizligining siyosati o‘zida quyidagilarni mujassamlashtiradi:

- tashkilotni fizik xavfsizligi nuqtai-nazaridan;
- xodimlarning vazifalari va majburiyatlari;
- foydalanishlarni boshqarishni nazoratlash;
- qaydlash va auditlash.
- Fizik xavfsizlik muolajasi o‘qida quyidagilarni oladi:
- qulflash tizimini boshqarish;
- suqilib kirish insidentlarini qaydlash;
- tashrif buyuruvchilarni boshqarish;

- konfidensial materiallarni yo‘q qilish;
- qog‘oz ko‘rinishidagi axborot uchun *toza stol* siyosatini va axborotni ishlashda *toza ekran* siyosatini amalga oshirish.

Toza stol siyosatiga ko‘ra tashkilot uchun muhim bo‘lgan axborotni xodimlar tomonidan qarovsiz qoldirilmasligi yoki ovqatlanganda oshxonalarga olib kirilmasligi zarur. Toza ekran siyosatiga ko‘ra esa xodim o‘z kompyuteridan foydalanish davomida uni qarovsiz qoldirmaslikka e’tibor qaratadi.

Boshqa fizik xavfsizlik choralari: yoritish tizimlari

Yoritish tizimlari tashkilot binosi xavfsizligini ta’minlashda muhim ahamiyat kasb etadi. Tashkilot binolarining atrofida yetarlicha yoritish amalga oshirilmaganligi boshqa xavfsizlik vositalarining vazifasiga salbiy ta’sir o‘tkazadi. Masalan, agar tashkilotning kirishida, mashina turar joyida yoki kuzatuv kamerasi o‘rnatilgan hududlarda yoritish tizimi yetarlicha ishlamasa, u holda ushbu hududlardagi obyektlar va insonlarni aniqlash imkoniyati kamayadi. Muhitning yoritish tizimi holat va sezuvchanlikga aloqador holda quyidagilarga bo‘linadi:

- *doimiy yoritish tizimlari* – tashkilot binosi atrofida har doim o‘rnatiluvchi yoritish vositalari.
- *kutish rejimidagi yoritish tizimlari* – biror ogohlantiruvchi signal asosida avtomatik yoki avtomatik bo‘lmagan shaklda ishlaydi.
- *harakatlanuvchi yoritish tizimlari* – qo‘lda boshqariluvchi yoritish tizimlari bo‘lib, kechasi va zarur bo‘lganda yoritish uchun foydalaniladi.
- *favqulotda yoritish tizimlari* – elektr quvvati manbalari ishdan chiqqanda yoki elektr energiyasi uzilganda vaqtinchalik tashkilot binolarini yoritish bilan shug‘ullanadi.

Quvvat manbalari nafaqat tashkilotning axborot texnologiyalari tizimiga balki, fizik xavfsizlikni ta’minlash tizimlariga ham katta ta’sir qiladi. Yetarli darajada quvvatning bo‘lmasligi va tez tez uzilib qolishi natijasida jixozlarga zarar yetishi mumkin. Tashkilotlarda quvvat manbaini uzulishi yuzaga kelganda quyidagi xavfsizlik choralari amalga oshirilishi zarur:

- quvvat tebranishlariga tayyor turish;
- quvvat uzilishi kuzatilganda uzluksiz quvvat manbalaridan (UPS – Unintrruptible power supply) foydalanish;
- muhitni tahdidlardan himoyalash tizimlari;

- ish joylarida statik elektrga g‘arazli ta’sir qilishdan himoyalash tizimlari;
- elektr quvvatidan foydalanuvchi vositalarni to‘g‘ri foydalanish.



6.10-rasm. Boshqa fizik xavfsizlik choralari: quvvat manbalari

Ish joyining xavfsizligi: qabulxona

Tashkilotning qabulxonasi har doim mehmon va tashkilot o‘rtasida aloqa o‘rnitishda muhim soha hisoblanadi. Qabulxona mehmonlar uchun oson foydalanishni ta’minlagani bois, fizik nuqta nazardan zaif bo‘lishi mumkin. Tashkilotda har kuni turli mehmonlar, hamkorlar, xodimlar va hak.lar kelishadi. Shu sababli, qabulxonada o‘tiruvchilar ularni har birini tanib olishga harakat qilishi shart. Bundan tashqari qabulxonada har bir kiruvchini qayd etish lozim.



6.12-rasm. Ish joyining xavfsizligi: Server/ zaxira nusxalash qurilmalarining xavfsizligi

Har bir tashkilot o‘z serverini va zaxira nusxalash vositalarining fizik xavfsizligini ta’minlashga e’tibor berishi lozim. Ushbu vositalarni fizik nazoratlash cheklangan bo‘lishi lozim. Faqat, ruxsat etilgan shaxs undan foydalana olishi kerak. Server va zaxira nusxalash qurilmalarini fizik xavfsizligini ta’minlash uchun quyidagilar amalga oshiriladi:

- Server va zaxira nusxalash qurilmalarini alohida honada saqlash. Bu chora ushbu qurilmalarni nomalum va ruxsat etilmagan xodimlar tomonidan boshqarilishini cheklaydi.
- Server va zaxira nusxalash vositalari joylashgan xonani yoki muhitga kuzatuv kameralarini o‘rnatish, smart karta yoki biometrik parametrga asoslangan autentifikasiyani amalga oshirish.
- Serverlarni maxsus tagliklarga o‘rnatish. Bu serverni o‘g‘irlinishidan va zarar yetishidan himoyalaydi.
- Turli quvvat o‘zgarishini oldini olish uchun serverlar UPS vositasiga ulangan bo‘lishi.
- Qurilmalarni qulflanuvchi xona va kabinetlarda saqlash.
- Xodimlar tomonidan ixtiyoriy zaxira nusxalash va server vositalarini olib chiqib ketmasligini ta’minlash.



6.14-rasm. Ish joyining xavfsizligi: Kritik aktivlar va olib yuriluvchi qurilmalar

Tashkilot har doim o‘zining server va zaxira nusxalash vositalarining xavfsizligiga e’tibor berishi lozim. Shu bilan bir vaqtda, ular boshqa kritik aktivlar, ishchi stansiyalar, rouiterlar va svitchlar,

printerlar, boshqa tarmoq qurilmalari, olib yuriluvchi vositalar va hak.lar xavfsizligiga ham e’tibor berishi lozim.

Bundan tashqari tashkilot tarmoq kabellarining joylashuvi va ularning xavfsizligiga ham jiddiy e’tibor berishi lozim. Sababi, tashkilotga kiruvchi va chiquvchi barcha ma’lumotlar aynan ushbu axborot tarmog‘i orqali harakatlanadi.

Ish joyining xavfsizligi: olib yuriluvchi vositalar

Hozirgi kunda har bir tashkilotda turli olib yuriluvchi vositalar xizmatidan foydalanilmoqda. Ularga laptoplar, planshetlar, proyektorlar va hak. misol bo‘lib, ularni osonlik bilan o‘g‘irlanishi, yo‘qolishi, zarar yetishi mumkin. Ushbu vositalarni fizik xavfsizligini ta’minlashda turli mexanik qulflardan foydalanish yoki ularni xavfsiz xonalarda saqlash choralarini ko‘rish talab etiladi.



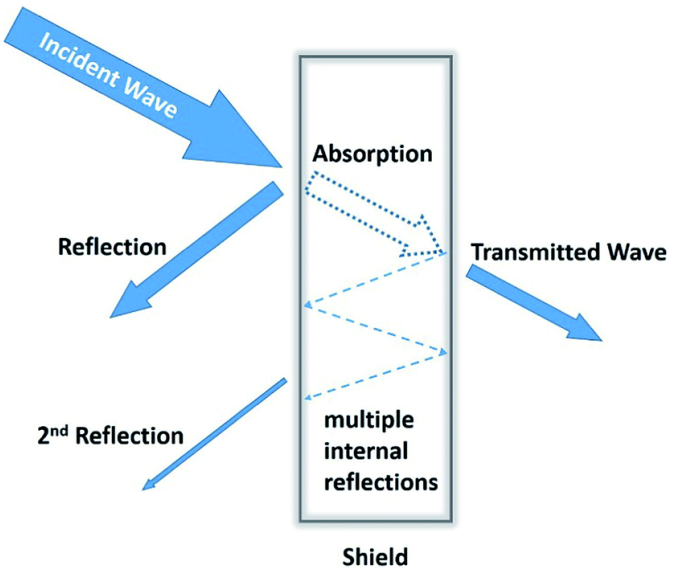
Muhitni nazoratlash: isitish, ventilyasiya va havoni sovitish tizimlari (Heating, ventilating and air-conditioning system, HVAC)

Mazkur tizimlar xona yoki bino ichidagi muhitni nazoratlash uchun ishlatiladi va tashkilotdagi qurilmalar ishlashi uchun zurur bo‘lgan muhitni yaratishga xizmat qiladi. Ba’zi HVAC tizimlarida muzlatish tizimini ham mavjud bo‘lib, ular HVAC&R (Refrigeration) tizimlari deb ataladi. Ular nafaqat qurilmalar ishlovchi mos sharoitni yaratish uchun balki xodimlar ishlashi va tashkilot faoliyati uchun zarur bo‘lgan muhitni yaratish uchun ham qo‘lliniladi.



6.14-rasm. Muhitni nazoratlash: elektromagnit shovqinlarni ekranlash

Tashkilotda bir elektron qurilmadan hosil bo‘lgan elektromagnit shovqinlar atrofdagi boshqa qurilmalar ishiga ta’sir etishi mumkin. Elektrmagnit shovqinlarni ekranlashda elektron vositalar metal bilan qoplanadi va tarqaluvchi elektr to‘lqini boshqa vositaga ta’sir etishiga yo‘l qo‘yilmaydi. Bundan tashqari qurilmalarni maxsus materiallar bilan to‘sish orqali boshqa qurilmalardan ajratish mumkin. Tashkilotlarda elektron qurilmalar ko‘p bo‘lgan hollarda (masalan, telekommunikasiya yoki shifoxonalarda) ularni ekranlash zaruriyati yanada ortadi.



6.15-rasm. Fizik xavfsizlik: ogohlik / o‘qitish

Yaxshi o‘qitilgan va malakaga ega bo‘lgan xodim tashkilot fizik xavfsizligiga bo‘lgan risklarni minimallashtirishi mumkin. Tashkilot o‘z xodimlarini fizik xavfsizlikni to‘g‘ri amalga oshirish uchun ogohlik mashg‘ulotlarini amalga oshirishi lozim. Ogohlantirish yoki o‘qitish dasturiy quyidagilarni mujassamlashtirgan bo‘lishi shart:

- hujumlarni kamaytiruvchi usullarni ta’minlashi;
- maxfiy axborotni olib yurishdagi risklar;
- xavfsizlik xodimlarining muhimligini;
- barcha qurilma va ma’lumotlarga bo‘lishi mumkin bo‘lgan hujum ehtimolini ko‘rib chiqish.

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

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

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

1. Ruxsatsiz kirishlarni oldini olish uchun mos ruxsatlarni nazoratlash usullarini o‘rnatilgani.
2. Muhim hududlar to‘g‘ri yoritish tizimi asosida kuzatilayotgani.

3. Turli tahdidlar, yong‘in, tutun, elektr, suv va hak.lar uchun aniqlovchi ogohlantiruvchi tizimlar o‘rnatilgani va ularni to‘g‘ri ishlayotgani.

4. To‘g‘ri eshiklarni qulflash tizimi o‘rnatilgani va ularni to‘g‘ri ishlayotgani.

5. Tashkilot binosi va hududini yetarli sondani qo‘riqchilar tomonidan qo‘riqlanayotgani.

6. Xavfsizlik xodimlarini to‘g‘ri o‘quv mashg‘ulotlariga yuborilgani.

7. Xavfsizlik xodimlarini ishonarli agentliklardan olingan.

8. Tashkilotdagi kuzatuv kameralari to‘g‘ri o‘rnatilgani va uzluksiz ishlayotgani.

9. Fizik xavfsizlik insidentlarini aniqlash va qayd qilish uchun to‘g‘ri muolajalar amalga oshirilgani.

10. Favqulotda vaziyatlar uchun xodimlar bilan aloqa o‘rnatuvchi axborotni mavjudligi.

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Fizik xavfsizlik, uning zaruriyati nimada?
2. Fizik xavfsizlikka ta’sir qiluvchi omillar qaysilar?
3. Fizik xavfsizlikni nazoratlash qanday amalga oshiriladi?

VII BOB. PAROLLARGA HUJUMLAR VA PAROLLARNI SAQLASH. MA’LUMOTLAR BUTUNLIGI.

7.1. Tarmoq topologiyalari

Kalit so‘zlar: Tarmoq turlari, tarmoq topologiyalari, OSI modeli, tarmoqqa qo‘yiladigan talablar, TCP/IP modeli, tarmoq vositalari. Zaiflik, tahdid, hujum, ichki tahdid, tashqi tahdid, razvedka hujumlari, kirish hujumlari, zararli hujumlar, xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari.

Kompyuter tarmoqlari

Kompyuter tarmoqlari bu – bir biriga osonlik bilan ma’lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi. Kompyuter axborotni ma’lumot yo‘llari orqali uzatadi. Keng tarqalgan kompyuter tarmog‘i bu – Internet. Kompyuter tarmoqlari quyidagi xususiyatlarga ega:

- bir kompyuterdan boshqasiga resurlarni taqsimlashga imkon beradi;
- bir kompyuterda fayllarni va boshqa axborotni saqlash va bulardan boshqa kompyuterdan turib foydalanish imkonini beradi;
- tarmoq orqali kompyuterga ulangan ixtiyoriy qurilma unda saqlangan fayllardan foydalanishi mumkin.

Ko‘plab sohalarda, elektrik injiniring, telekommunikasiya, Computer science, axborot texnologiyalarida kompyuter tarmoqlari konsepsiyasidan foydalaniladi. Bular foydalanuvchilar orasida osonlik bilan muloqot o‘rnatish imkonini beradi.

7.2. Tarmoqqa qo‘yiladigan talablar

Open System Interconnection (OSI) Model

OSI modeli tarmoq bo‘ylab ma’lumotlar almashinuvini aniqlashtirish uchun taqdim etilgan model. U qolib bo‘lib, bir qurilmadan tarmoq orqali boshqa qurilmaga ma’lumot oqib o‘tishini tasvirlaydi. OSI modeli ikki nuqta orasidani aloqani 7 ta turli sathlar guruhiga ajratadi. Ushbu modelda manba kompyuterdan ma’lumot pastki satha qarab harakatlansa, masafadagi kompyuterda esa pastdan yuqori sathga qarab harakatlanadi.

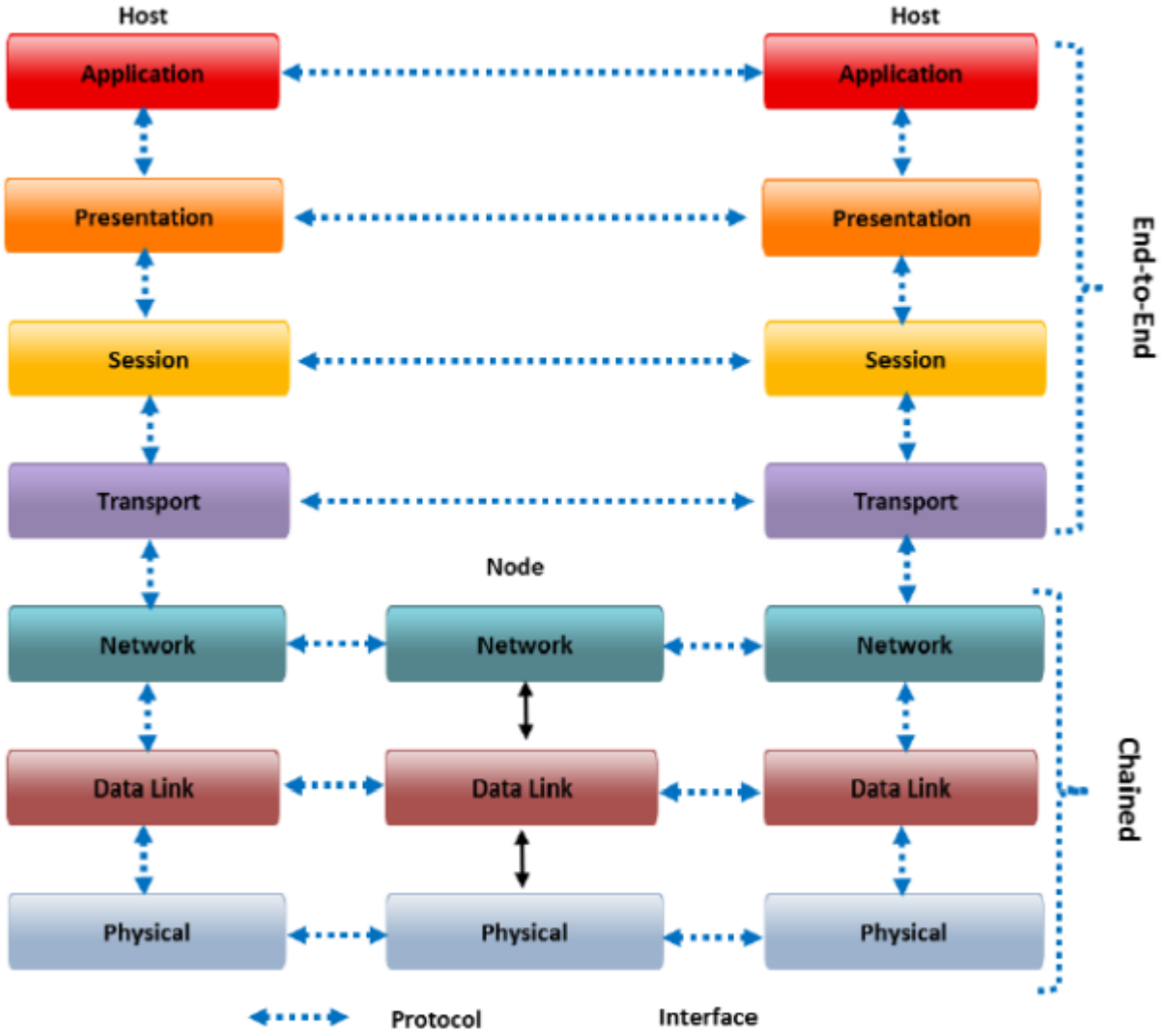
OSI modeli quyidagi xususiyatlarga ega:

- tarmoq bo‘ylab amalga oshirilgan aloqani oson tushunilishini ta’minlaydi;
- dasturlar va qurilmalar ishlashini ko‘rsatadi;

- foydalanuvchilarga yangi topologiyani tushunishga yordam beradi;

- turli tarmoqlar orasidagi funksional boqliqliklarni oson solishtirish imkoniyatiga ega.

OSI modelida protokollar to‘plami mavjud bo‘lib, bir tomonni boshqa tomon bilan aloqasini ta’minlash imkonini beradi (7.1-rasm).



7.1-rasm. OSI modeli

OSI modelining har bir sathida turli darajali qoidalar mavjud bo‘lib, ular turli vazifalarni bajaradilar. 7 qatlamli OSI modelini ishlab chiqishda foydalanilgan prinsiplar quyidagilar:

- Har bir sath turli tushunchalarga va umumiy ko‘rinishlarga ega bo‘lishi mumkin. Shuning uchun har bir sathni yaratish abstraksiya darajasiga asoslanadi.

- Har bir sath turli vazifani bajarishga muhtoj.

- Har bir sathda amalga oshirluvchi vazifa ushbu sathda ishlovchi standart protokollarga asoslanishga mavjur.
- Barcha vazifalar bir xil sathda taqdim etilmasligi zarur. Sathni tanlinishi amalga oshiriluvchi funksiyalar soniga bog‘liq bo‘ladi.

7.3. TCP/IP modeli

TCP/IP modeli 4 sathli protokol bo‘lib, Department of Defense (DOD) tomonidan ishlab chiqilgan. Ushbu modeldagi har bir sath turli vazifalarni bajaradi va ma’lumotni yuboruvchi qurilmada ma’lumot 4 sathdan birinchi sathgi qarab harakatlansa, qabul qiluvchi mashina uchun uning teskarisi. TCP/IP modeli ikkit mashina orasidagi nuqtadan-nuqtaga aloqasini tasvirlaydi va shuning uchun ma’lumotni addreslash, marshrutlash va uzatish masalalarini qamrab oladi. 4 sathli TCP/IP modeli o‘zida quyidagilarni qamrab oladi:

- Ilova sathi (Application layer, 4-sath): ilovalar uchun ma’lumotlardan foydalanishni ta’minlaydi.
- Transport sathi (Transport layer, 3-sath): host-host aloqasini boshqaradi.
- Tarmoq sathi (Internet layer, 2-sath): o‘zaro ishlashni ta’minlaydi.
- Kanal sathi (Network Access layer, 1-sath): bir xil tarmoqda mavjud bo‘lgan ma’lumotlarni uzatishni ta’minlaydi.

Kanal sathi – 1-sath

Ushbu sath TCP/IP modelning eng quyi sathi bo‘lib, bir xil tarmoqda ikkita hostlar orasida Internet sathi bo‘ylab ma’lumot oqishini ta’minlaydi. Ushbu sath OSI modelidagi ikki sathni: Data Link Layer va Physical Layer, mujassamlashganiga mos. Ushbu sathda apparat manzil ko‘rib chiqiladi va ushbu sathda ishlovchi protokollar ma’lumotni jismoniy uzatishga imkon beradi. Ushbu sathda quyidagi protokollar foydalaniladi: Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.

Tarmoq sathi – 2-sath

Ushbu sath asosan tarmoq bo‘ylab paketlarni uzatish bilan shug‘ullanadi. U manba tarmoqdan masofadagi tarmoqga ma’lumotlarni uzatish bilan tarmoqlararo paket almashinuvini amalga oshiradi. Tarmoq sathi orqali amalga oshiriladigan vazifalar quyidagilar:

- hostga murojaat qilish va identifikasiyalash;
- paketlarni yo‘naltirish.

Tarmoq sathi TCP/IP protokoli doirasini boshqarish uchun to‘liq javobgar. Ushbu protokolda manba tarmog‘idan yuborilgan paketlar ketma-ketligi masofadagi tarmoqda qabul qilinadi. Ushbu sathda IP, ICMP, ARP, RARP protokollaridan foydalaniladi.

Transport sathi – 3-sath

Transport sathi yuboruvchi va qabul qiluvchilar orasida ma’lumot uzatilishi holatini aniqlaydi. Ushbu sathning vazifalari, nuqtadan-nuqtaga aloqani, xatoliklarni nazoratlash, segmentlash, oqimni nazoratlash va ilovalar murojaatini o‘z ichiga oladi. Nuqtadan-nuqtaga aloqa ikki turda: ulanishga yo‘naltirilgan va ulanmaslikka yo‘naltirilgan bo‘lishi mumkin. TCP protokoli ulanishga yo‘naltirilgan ulaninshi ta’minlasa, UDP protokoli ulanmaslikka asoslangan aloqani amalga oshiradi.

Transport sathi ma’lumotlar almashinuvini parallel yo‘ldami yoki yagona yo‘lda paydo bo‘lishini belgilaydi. Ushbu sath ilovalar uchun ma’lumotga sarlavha axborotini qo‘shish orqali o‘ziga yozish va o‘qish imkonini beradi. Transport sathi tarmoq sathi ma’lumotlarni oson qabul qilishi uchun kichik bo‘laklarga ajratgan holda yuboradi. Transport sathida TCP, UDP, RTP protokollaridan foydalaniladi.

Ilova sathi – 4-sath

Ilova sathi turli ilovalar tomonidan foydalaniladigan protokollardan iborat. Mazkur ilovalar foydalanuvchi xizmatlarini va quyi sath protokollari orqali amalga oshirilgan tarmoq bo‘ylab uzatilgan ma’lumotlarni ta’minlaydi. Ilova sathi protokollari mijoz-kliyent ilovalari va boshqa xizmatlar bilan shug‘allanadi. Ushbu sathda HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak. protokollaridan foydalaniladi.

TCP/IP modeli quyidagi afzalliklarga ega:

- ushbu model mijoz-server arxitektrurasi kabi xizmat qiladi;
- u muqtaqil ravishda ishlaydi;
- u ko‘plab marshrutlash protokollaridan iborat;
- ikki kompyuter orasila aloqani amalga oshiradi.

TCP/IP modeli quyidagi kamchiliklarga ega:

- o‘rnatish uchun murakkab;
- transport sathida paketlarni yetkazilishiga kafolat yo‘q;
- protokollarni almashtirish oson vazifa emas;
- xizmatlar, protokollar va interfeyslar orasida ko‘rinarli ajralish yo‘q.

OSI va TCP/IP modellarining taqqosi

OSI model

OSI modelini amalga oshirish orqasidagi bir qancha standart protokollardan foydalangan holda tomonlar ulanishi orasidagi aloqani standartlashtirish va osonlashtirish maqsadi yotadi. U kompyuterlar orasidagi aloqani sathlar kesimida umumlashtiradi. OSI modelida 7 ta sath mavjud. Ushbu modelda, har bir sath o‘zidan yuqori sathga xizmat qiladi va bu yuqoridagi sathni quyi sath bilan birgalikda ishlashi kerakligi xulosasini beradi.

TCP/IP model

Shuningdek, OSI va TCP/IP modellari quyidagi farqlarga ega:

OSI	**TCP/IP**
1. OSI – bu umumiy, protokoldan mustaqi standart bo‘lib, tarmoq va oxirgi foydalanuvchi orasidagi aloqa shlyuzi vazifasini o‘taydi.	1. TCP/IP modeli Internet standartida ishlab chiqilgan standart protokollar asosida yaratilgan. Bu hostlarni tarmoq orqali ulashga imkon beradigan aloqa protokoli.
2. OSI modelida transport sathi paketlarni yetib borishini kafolatlaydi.	2. TCP/IP modelida transport sathi paketlarni yetib borishini kafolatlamaydi. Shuni bilan ham TCP/IP modeli shunchalik ishonchli.
3. Vertikal yondashuvga amal qiladi.	3. Gorizontal yondashuvga amal qiladi.
4. OSI modelida alohida taqdimot va sessiya sathlari mavjud.	4. TCP/IP modelida alohida taqdimot va sessiya sathlari mavjud emas.
5. Transport sathi ulanishga yo‘naltirilgan.	5. Transport sathi ham ulanishga ham ulanmaslikka yo‘naltirilgan.
6. Tarmoq sathi ham ulanishga ham ulanmaslikka yo‘naltirilgan.	6. Tarmoq sathi ulanishga yo‘naltirilgan.
7. OSI - bu tarmoqni qurish imkonini beruvchi etalon model. Odatda u qo‘llanma sifatida ishlatiladi.	7. TCP/IP modeli esa OSI modelini amalga oshirish usulidir.
8. OSI modelida protokollarni modelga moslashtirish muammosi mavjud.	8. TCP/IP modeli ixtiyoriy protokolga ham mom kelavermaydi.
9. OSI modelida protokollar yashiringan va texnologiya o‘zgarishi bilan osonlik bilan almashtirish mumkin.	9. TCP/IP modelida protokolni almashtirish oson emas.
10. OSI modeli xizmatlar, interfeyslar va protokollarni juda aniq belgilaydi va ular o‘rtasida aniq farq qiladi. Bu protokolga bog‘liq emasyu	10. TCP/IP modelida xizmatlar, interfeslar va protokollar aniq ajratilmagan. Bundan tashqari protakolga bog‘liq.
11. Modelda 7 ta sath mavjud.	11. Modelda 4 ta sath mavjud.

TCP/IP aloqa uchun asos protokol sifatida qaraladi. TCP/IP protokol o‘z ilovasini intranet yoki ekstranetda mavjudligini qidiradi. TCP/IP modeli 4 ta sathdan iborat bo‘lib, yuqori sathda haqiqiy xabardagi paketlar birlashmasi boshqarilsa, quyi sathlar har bir paketning manzillar qismini va ularni to‘g‘ri manziliga yetib borishni nazoratlaydi.

OSI va TCP/IP modellarining o‘xshash tomonlari:

- har ikkalasi ham sathlarga asoslangan arxitekturaga ega;
- sathlar bir xil vazifalarni amalga oshirishni ta’minlaydi;
- har ikkalasi ham protokllar to‘plami hisoblanadi;
- har ikkalasi ham etalon model hisoblanadi.

Tarmoqlarning turlari

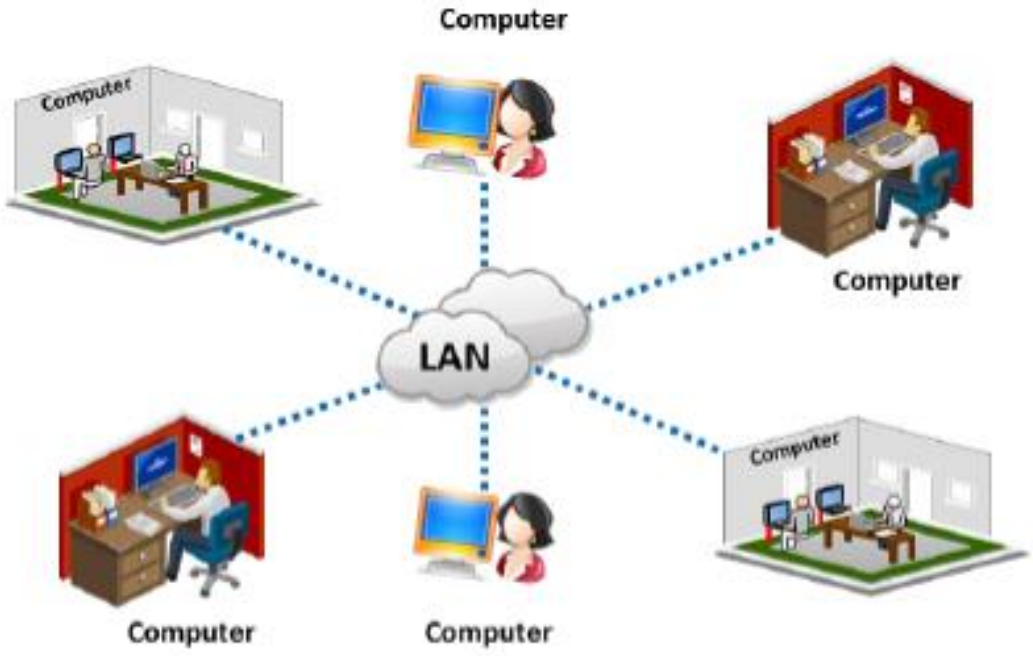
Kompyuter tarmoqlari turli yo‘nalishlarda bir-biridan farq qilishi mumkin. Masalan, o‘lchami bo‘yicha, vazifasi bo‘yicha, geografik masofasi bo‘yicha. Tarmoqlar tomonidan ko‘rsatilayotgan xizmatlar tarmoqlarning tuzilishiga mos holda turlicha bo‘lishi mumkin.

Tarmoq tarqalgan sohaning o‘lchamiga va tarmoqdagi kompyuterlarning soniga ko‘ra quyidagicha guruhlarinishi mumkin:

- Lokal tarmoqlar (Local Area Network, LAN);
- Mintaqaviy tarmoq (Wide Area Network, WAN);
- Shahar tarmog‘i (Metropolitan Area Network, MAN);
- Shaxsiy tarmoq (Personal Area Network, PAN);
- Kampus tarmog‘i (Campus Area Network, CAN);
- Global tarmoq (Global Area Network, GAN).

Lokal tarmoqlar, LAN

LAN tarmog‘i kompyuterlar va ularni bog‘lab turgan qurilmalardan iborat bo‘lib, ular odatda bitta tarmoqda bo‘ladi. LAN tarmoq offis binosi yoki uyning ichida mavjud bo‘lishi mumkin. LAN tarmoqlar yuzlab foydalanuvchilarni o‘zida mujassamlashtirishi mumkin. Hozirda LAN ning ikkita keng tarqalgan texnologiyasi: Ethernet va Wi-Fi keng foydalanilmoqda. LAN tarmog‘ida ko‘plab dasturlardan foydalanish imkoniyati mavjud va foydlanuvchilar LAN tarmog‘idan ularni osonlik bilan yuklab olishlari va foydalanishlari mumkin. Hozirda simli LAN tarmoqlariga ko‘ra sarf xarajatlarni kamligi sababli simsiz LAN tarmoqlari ommalashib bormoqda (7.2-rasm).



7.2-rasm. LAN tarmog‘i

LAN tarmog‘ining afzalliklari:

- uydagi yoki ofisdagi foydalanuvchilar orasida printerlarni birgalikdagi foydalanish imkoniyatini beradi;
- LAN tarmog‘i foydalanuvchiga o‘zidagi ixtiyoriy tarmoqda ishlash uchun imkoniyatni taqdim etadi;
- barcha ma’lumotlarni tarmoqdagi yagona katalogda saqlash va undan foydalanuvchilar tomonidan birgalikda foydalanish imkonini yaratish.

LAN tarmog‘ining kamchiliklari:

- fayllarni taqsimlangan holda foydalanish imkoniyatini taqdim etgani bois, u foydalanishni nazoratlash uchun alohida xavfsizlik choralarini ko‘rishni talab etadi;
- fayl serverdagi kichik nosozlik, server mashinasiga ulangan barcha foydalanuvchilar ishiga salbiy ta’sir qiladi.

Mintaqaviy tarmoq, WAN

WAN tarmog‘i LAN tarmog‘iga qaraganda kengroq sohaga ega va keng miqiyosida foydalaniladi. WAN tarmog‘i odatda ijaraga olingan telekommunikasiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog‘laydi. Ushbu liniyalar tarmoqdagi turli kompyuterlar orqali ma’lumotlarni samarali uzatilishiga yordam beradi. WAN tarmoqdagi turli LANlarga ulana oladi. LANlar WAN

tarmog‘iga tezkor va xavfsiz ma’lumotlar transferini amalga oshirish uchun bog‘lanadi. Biroq, WANlardan ularni boshqarish uchun zarur bo‘lgan ruxsatlar talab etiladi. WAN tarmog‘i quyidagi xususiyatlarga ega (14.3-rasm):

- WAN tarmoqlar odatda keng va maqsadli tarmoq xizmatlarini ta’minlaydi. U har doim biznes talablarga mos bo‘lgan xizmatlarni mujassamlashtirishga xizmat qiladi;
- WAN tarmog‘ida LAN tarmog‘iga qaraganda ma’lumotlarni uzatish darajasi kam bo‘ladi.



7.3-rasm. WAN tarmog‘i

WAN tarmog‘i quyidagi afzalliklarga ega:

- WAN tarmog‘i bir – biridan geografik tomondan alohida bo‘lgan tomonlarni kam xarajat va osonlik bilan ulash imkoniyatini beradi.

WAN tarmog‘ining kamchiliklari:

- tuzilish jaxatidan juda ham murakkab;
- past o‘tkazish qobilyatiga ega va ulanishni uzilish xavfi yuqori.

Shahar tarmog‘i, MAN

Ushbu tarmoq LAN tarmog‘iga qaraganda katta hajmga ega bo‘lsada, WAN tarmog‘idan kichik. Bu tarmoq shahar yoki shaharcha bo‘ylab tarmoqlarning o‘zaro bog‘lanishini nazarda tutadi. Ya’ni, bir nechta LANlar birikib, MANni tashkil qiladi. MAN tarmog‘i optik kabellardan foydalanish orqali samarali va xavfsiz aloqagi ta’minlashi mumkin. MAN tarmoq o‘z foydalanuvchilari uchun taqsimlangan tarmoq ulanishini ta’minlaydi (7.4-rasm).



7.4-rasm. MAN-tarmog‘i

MAN tarmog‘i quyidagi afzalliklarga ega:

- MAN tarmog‘ida kompyuterlarni bog‘lash kanallari yuqori o‘tkazuvchanlik qobilyatiga egaligi sababli, ma’lumotlarni oson taqsimlash imkoniyatini beradi.
- Ko‘plab foydalanuvchilar uchun ma’lumotlarni taqsimlashda teng tezkorlik taqdim etadi.

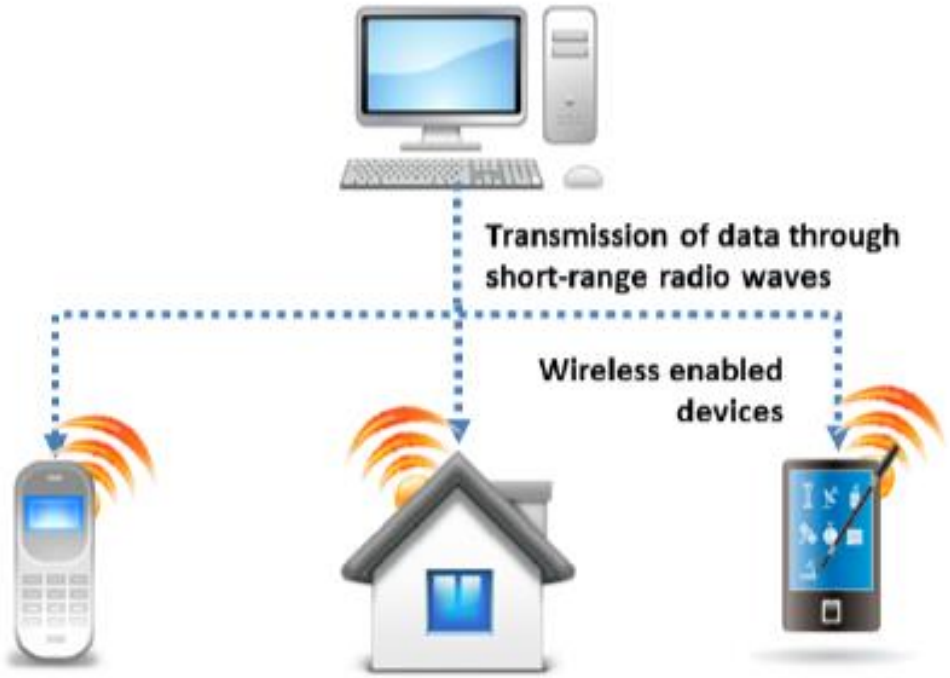
MAN tarmog‘i quyidagi kamchiliklarga ega:

- Birinchi marta foydalanishdan oldin ma’lumot o‘rnatilish va sozlanishlarni talab etadi.
- LAN tarmog‘iga qaraganda yuqori narxga ega.

Shaxsiy tarmoq, PAN

Shaxsiy tarmoq qisqa masofalarda qurilmalar o‘rtasida ma’lumot almashinish imkoniyatini taqdim etadi. Masalan, shaxs noutbuki, mobil telefoni yoki planshetini qisqa masofadagi simsiz tarmoqqa ulanishini olish mumkin. Mazkur tarmoq o‘rnatilgan ulanish orqali qurilmalar

orasida ma’lumot va fayllarni taqsimlash imkoniyatini beradi (7.5-rasm).



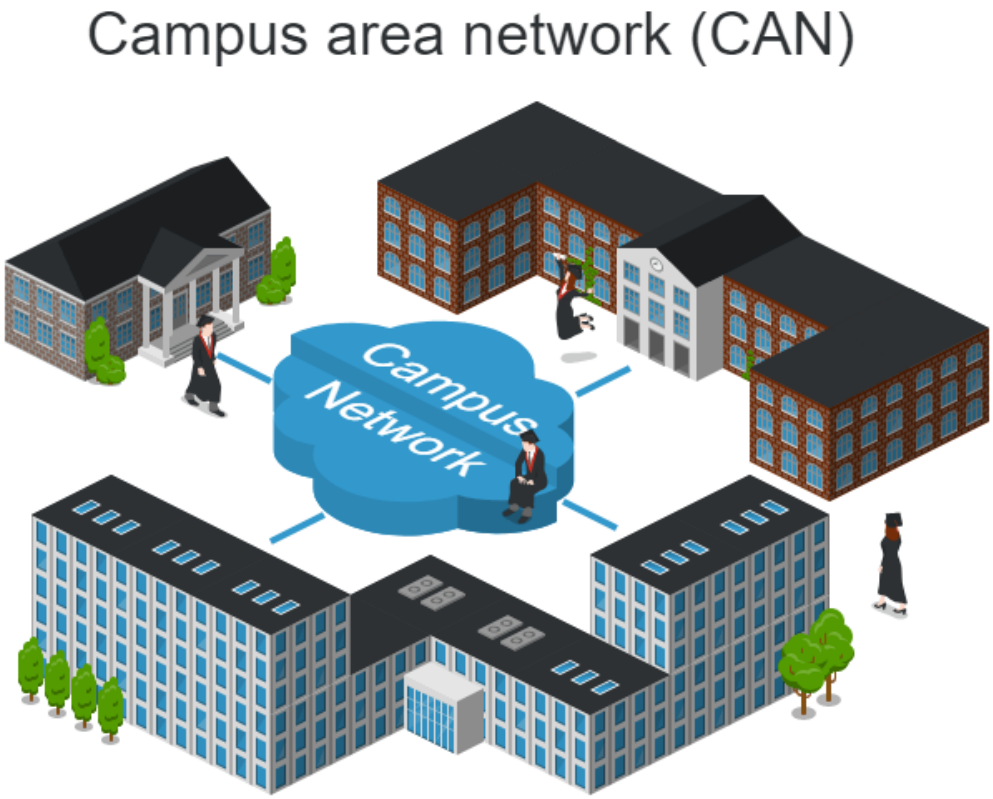
7.5-rasm. PAN-tarmog‘i

Kampus tarmog‘i, CAN

Ushbu tarmoq bir geografik hudud ichida ko‘plab LAN tarmoqlarni birlashtirish natijasida hosil qilanadi. Ko‘plab davlat tashkilotlari va universitetlar o‘zlari uchun CAN tarmoqlarini qurishlari mumkin. CAN tarmog‘ining hajmi MAN va WAN tarmog‘iga qaraganda kichik bo‘lib, tugunlarni o‘zaro ulash uchun optik kabellardan foydalanadilar. Masalan, kampusdagi turli binolar CAN tarmog‘ini qurish orqali o‘zaro ma’lumot almashishlari mumkin. CAN tarmoqlarini amalga oshirish kam xarajatli bo‘lib, iqtisodiy tomondan samarali hisoblanadi. CAN tarmog‘i quyidagi xususiyatlarga ega:

- narx nuqtai nazaridan samarali;
- kampusdagi turli bo‘limlar o‘rtasida o‘zaro aloqa o‘rnatish imkoniyatini beradi;
- ma’lumotlarni taqsimlashda bir xil tezlikni taqdim etadi;
- buzilishga chidamli;
- CAN tarmog‘i keyinchalik o‘zgartirish va rivojlantirishga qulay;

- tarmoqdan foydalanishda foydalanuvchilarni autentifikasiyadan o‘tkazgani bois CAN tarmog‘i yuqori xavfsizlikni ta’minlaydi.



7.6-rasm. CAN-tarmog‘i

Global tarmoq, GAN

GAN tarmog‘i cheklanmagan geografik hudud bo‘ylab turli o‘zaro bog‘langan tarmoqlardan iborat bo‘lib, LAN va WAN tarmog‘iga qaraganda katta geografik hududni o‘z ichiga oladi. GAN tarqog‘i to‘g‘ridan-to‘g‘ri bog‘lanmagan tomonlar orasida ham ma’lumotlar almashinish imkoniyatini beradi. Bunda yuboruvchi markaziy serverga ulanadi yoki ma’lumot qabul qiluvchiga etguncha nuqtadan-nuqtaga uzatish asosida yetkaziladi.

GAN tarmog‘i bir qancha simsiz LANlar uchun mobil ulanishni madadlaydi. GAN tarmog‘i quyidagi afzalliklarga ega:

- GAN tarmog‘i ko‘plab tarmoqlarni o‘zaro bog‘lash imkoniyatini beradi va ma’lumotni o‘zgarmasdan taqsimlash imkoniyatini taqdim etadi;
- Markaziy serverga ma’lumotni saqlash imkoniyati mavjudligi sababli, ulardan turli tarmoqlar bo‘ylab foydalanish mumkin;

- Markaziy serverda saqlangan ma’lumotlar va fayllardan foydalanishni cheklash orqali ularning xavfsizligini ta’minlaydi.

Tarmoq topologiyalari

Tarmoq bo‘ylab kompyuterlar topologiyalardan foydalanib mantiqiy bog‘lanishlari mumkin. Topologiya tarmoqning tuzilishini aniqlab, tarmoqning mantiqiy va fizik joylashuvini hisoblaydi. Fizik topologiya kompyuter tizimlari komponentlarining tuzilishini aniqlasa, mantiqiy topologiya kompyuterlar orasidagi tarmoqda ma’lumotlarni uzatish usullarini aniqlaydi. Quyida keng tarqalgan tarmoq topologiyalari bilan tanishib chiqiladi.

Yulduz topologiyasi

Yulduz topologiya tarmoqdagi kompterlarga kabel orqali ulangan markaziy xabdan (tugun) iborat bo‘lgan. Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog‘langan bo‘ladi. Bunda yangi tugunni tarmoqqa qo‘shish juda ham oson bo‘lib, biror tugun va markaziy tugun orasidagi uzilish qolganlari ishiga ta’sir qilmaydi. Markaziy xabga bo‘lgan biror zarar butun topologiyaga ta’sir qiladi (7.7-rasm).

Bu yerda markaziy xab vazifasini server o‘tashi va unga ulangan kompyuterlar mijoz sifatida bo‘lishi mumkin. Barcha ma’lumotlar markaziy xabdan o‘tadi. Yulduz topologiyada markaziy xab qolganlar uchun bog‘lovchi vazifasini o‘taydi. O’z o‘rnida markaziy xab qolgan tarmoqga ulanishi mumkin. Markaziy tugunga kompyuterlar oddiy Ethernet kabellari yordamida ulanishi mumkin. Quyidagi omillar markaziy xabni aktiv yoki passivligini aniqlaydi:

- markaziy tugun yoki xab ma’lumotni kuchaytirish, yangilash kabi jarayonlarni amalga oshirishi;
- markaziy xab ma’lumotlar ko‘chishini nazoratlashi;
- tarmoq elektr quvvat manbalarini talab qilishi.

Ushbu topologiya quyidagi afzalliklarga ega:

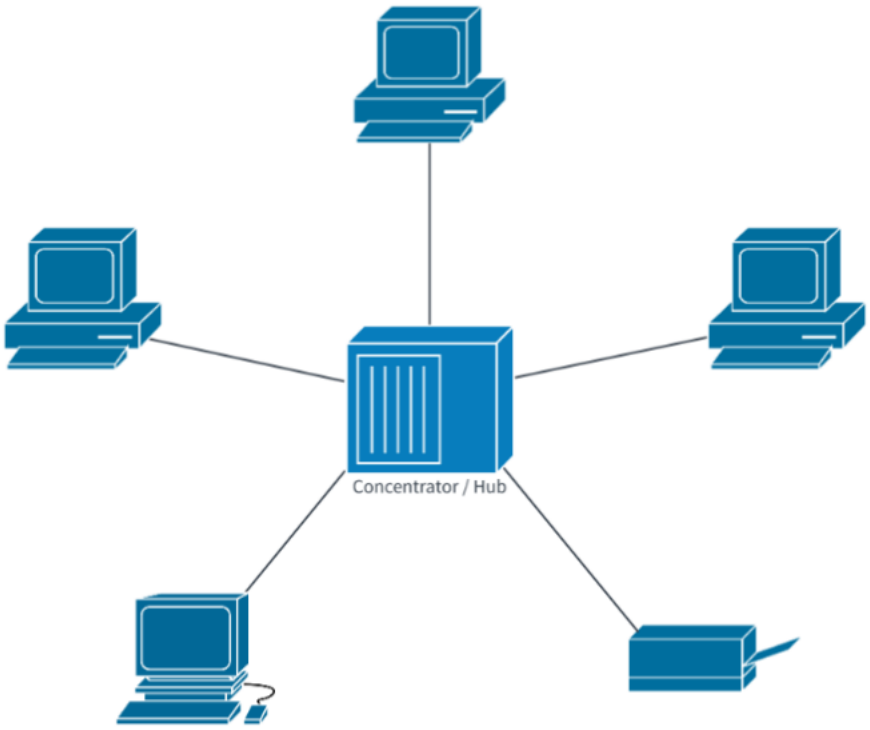
- markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish;
- topologiyaga osonlik bilan yangi tugunni kiritish yoki olib tashlash imkoniyati;
- bir kompyuter tugunining buzilishi qolganlarining ishiga ta’sir qilmaydi;
- tarmoqdagi bo‘lgan uzilishni osonlik bilan aniqlash mumkin va muammoni osonlik bilan bartaraf etish imkonini beradi.

Yulduz topologiya quyidagi kamchiliklarga ega:

- markaziy nuqtadagi bo‘lgan uzilish butun topologiyaga ta’sir ko‘rsatadi;

- markaziy nuqta sifatida router yoki kommutatordan foydalanish tarmoqni amalga oshirish narxini oshiradi;

- yangi tugunni tarmoqqa qo‘shish markaziy tugunni imkoniyatiga bog‘liq bo‘ladi.

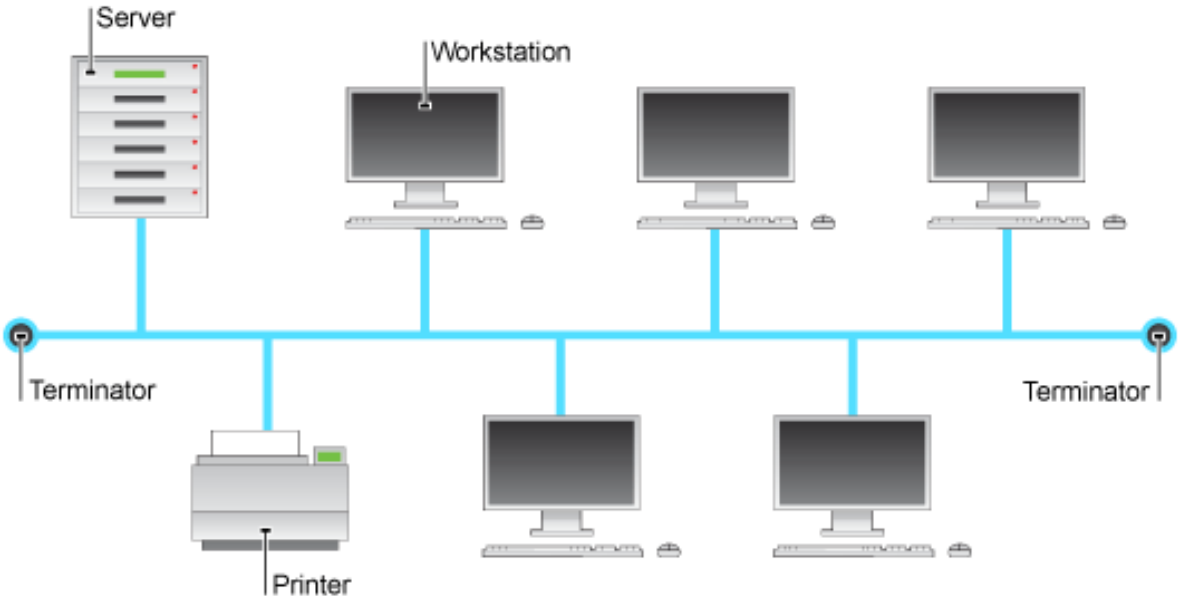


7.7-rasm. Yulduz topologiya

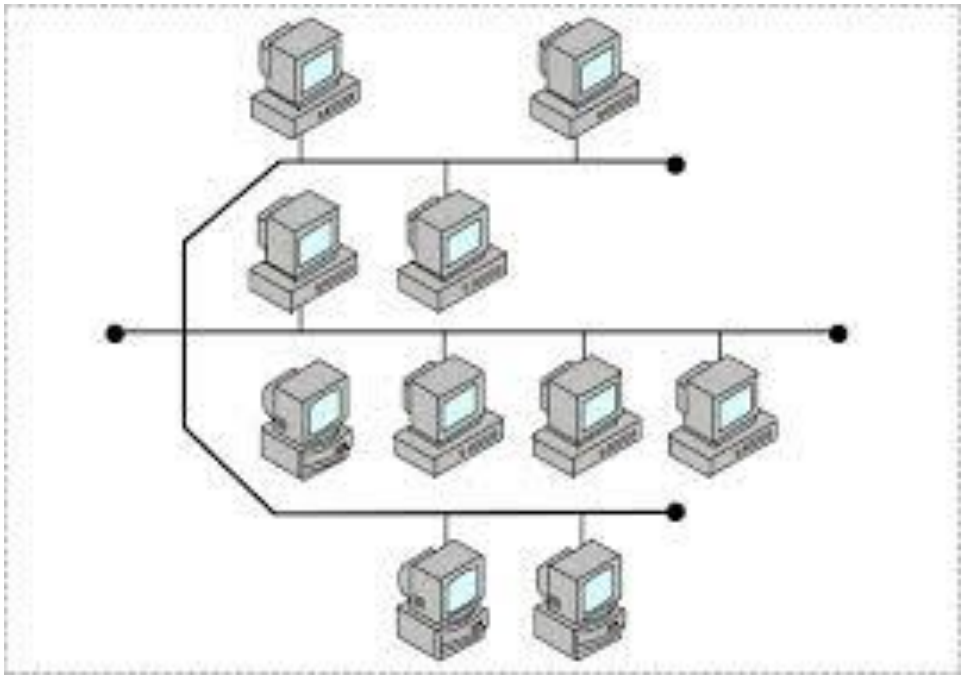
Shina topologiya

Mazkur topologiyada tarmoqda yagona kabel barcha kompyuterlarni o‘zida birlashtiradi. Yagona kabel tarmoqdagi barcha tugunlarga yo‘naltirilgan axborotni o‘tkazadi. Asosiy kabel va tugun orasidagi bo‘lgan ixtiyoriy uzilish kabel orqali o‘tuvchi axborotga ta’sir qilishi mumkin.

Shina topologiyada ixtiyoriy tugun tomonidan tarmoq “salomi” (network broadcast) signali uzatiladi. Ushbu signal kabelga ulangan tarmoqning barcha tugunlariga yetib borishiga imkon beradi. Kabelning har ikkala tomonida terminator mavjud bo‘lib, signalni sakrashini oldini oladi. Shina topologiyaning ikki turi mavjud: chiziqli va taqsimlangan shina topologiya. Chiziqli shina topologiyasida ikki nuqta o‘rtasida faqat yagona kabel o‘tkaziladi. Taqsimlangan shina topologiyada esa tarmoqni hosil qilish uchun birdan ortiq kabel talab etiladi.



7.8-rasm. Chiziqli shina topologiya



7.9-rasm. Taqsimlangan shina topologiya

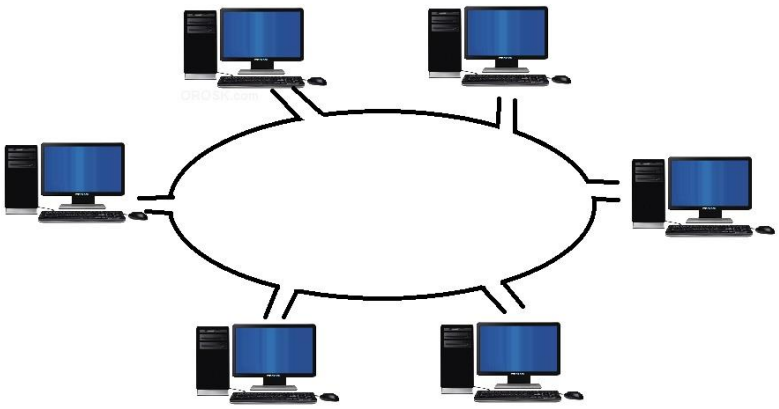
Shina topologiya quyidagi afzalliklarga ega:
- shina tarmoqqa yangi tugunni qo‘shish juda ham oson;
- amalga oshirishda kam xarajatlik;
- kichik tarmoqlarda yaxshi ishlaydi;
- yulduz topologiyaga qaraganda kam kabel talab etiladi.

Shina topologiya quyidagi kamchiliklarga ega:
- yangi tugun kiritish kabelning uzunligiga bog‘liq;

- asosiy kabeldagi biror buzilish butun tarmoq ishiga ta’sir qiladi;
- kabelning har ikkala tomonida terminatorni bo‘lishi shart;
- xizmat ko‘rsatish narxi yuqori;
- yuqori tezlikdagi tarmoqlar uchun o‘rinli emas;
- manbadan uzatilgan signalni barcha tugunlar qabul qilgani kabi, u tarmoqning xavfiszligiga ta’sir qiladi.

Xalqa topologiyasi

Xalqa topologiya tarmoqdagi barcha tugunlarni o‘zaro bog‘laydi. Tarmoqda ma’lumot qabul qiluvchi qabul qilgunicha aylanadi. Tarmoqdagi ixtiyoriy tugunni uzulishi butun tarmoqni buzilishiga olib keladi. Tarmoqda ma’lumotlar bir yo‘nalishda harakat qiladi. Yuboriluvchi va qabul qilinuvchi ma’lumot TOKEN yordamida manziliga yetkaziladi. TOKEN konsepsiyasiga TOKEN ma’lumotni o‘z ichiga olgan ma’lumot manbadan uzatiladi va har bir tugunda yetib kelganda ushbu tugunga tegishli ekanligi tekshiriladi. Odatda maktablarda, ofislarda va kichik binolarda xalqa topologiyasidan foydalaniladi (7.10-rasm).



7.10-rasm. Xalqa topologiyasi

Xalqa topologiyasining afzalliklari:
- bir tomonga yo‘naltirilgan trafik oqimi;
- har bir tugun faqat bo‘sh bo‘lgan vaqtdagina ma’lumotni uzata oladi;
- markazlashgan biror tarmoq serveri talab etilmaydi;
- shina topologiyana qaraganda amalga oshirish qulayligi (trafik hajmi oshmasligi sababli);
- barcha tugunlarni ma’lumotdan foydalanishda bir xil imkoniyatga ega;

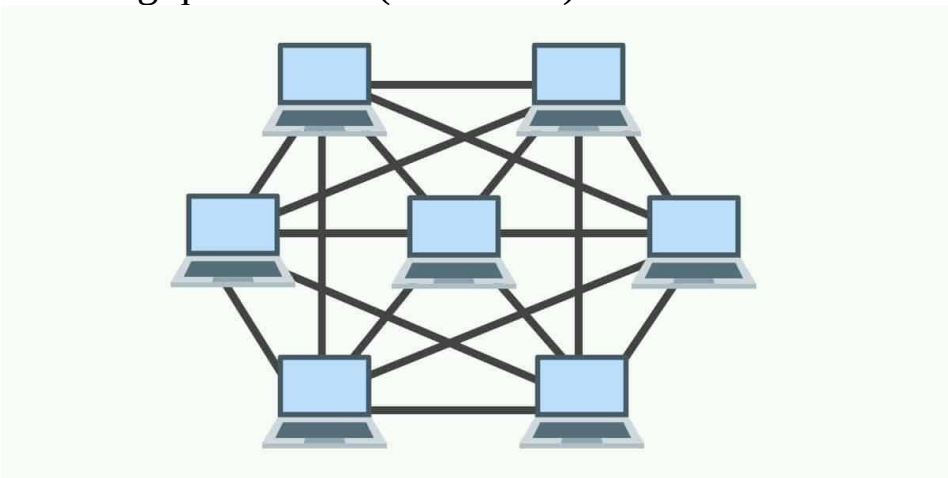
- tarmoqda yangi tugunni qo‘shilishi tarmoqning butun o‘zgarishiga ta’sir qilmaydi.

Halqa topologiyasining kamchiliklari:

- tarmoqda har bir tugundan signalning o‘tishi sekin jarayon;
- ixtiyoriy tugundagi buzilish butun tarmoqning buzilishiga olib keladi;
- tugunlarni ulash uchun ko‘p kabel talab etiladi va bu ortiqcha xarajatni talab etadi;
- trafik barcha tugunlar uchun taqsimlanadi.

Mesh topologiya

Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o‘zaro bog‘langan bo‘ladi. Ushbu topologiya biror kompyuter buzilgan taqdirda ham ma’lumotlar almashinuvini ta’minlashni maqsad qiladi. Biroq, ushbu topologiya amalga oshirishni yuqori narxligi sababli aksariyat tashkilotlarda foydalanilmaydi va uning o‘rniga simsiz tarmoqlarda keng qo‘llaniladi (7.11-rasm).



7.11-rasm. Mesh topologiya

Mesh topologiyasi quyidagi afzalliklarga ega:

- ma’lumotlarni davomli uzatishga imkoniyat beradi;
- yuqori trafikni o‘tkazish imkoniyati mavjud;
- tugunlardan birini buzilishi butun tarmoqqa ta’sir qilmaydi;
- tarmoqni kengaytirish osonlik bilan amalga oshiriladi.

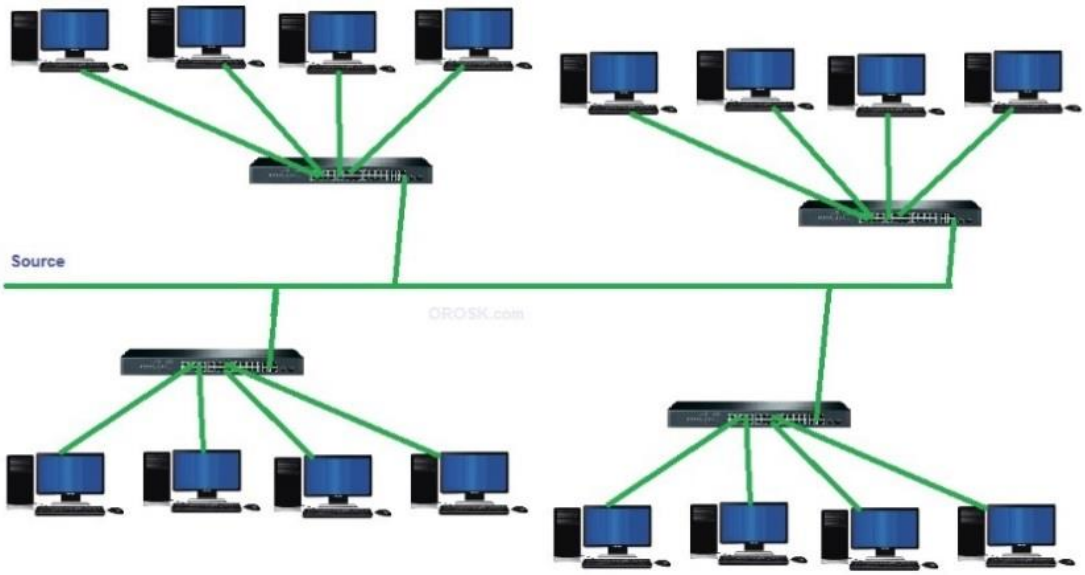
Mesh topologiyasi quyidagi kamchiliklarga ega:

- ko‘plab ulanishlarning mavjudligi sababli yuqori darajali ortiqchalik;
- boshqa tarmoq topologiyalariga qaraganda yuqori narxga egalik;

- tarmoqni qurish uchun ko‘p vaqt va ma’muriy ye’tibor talab qiladi.

Daraxt topologiya

Daraxt topologiya shina va yulduz topologiyalarning kombinasiyasidan tashkil topgan. Ya’ni, daraxt topologiya yulduz topologiyalarni asosiy kabelga ulash orqali hosil qilinadi. Bu topologiyaning boshqacha nomi “kengayltirilgan yulduz topologiya” deb ham ataladi (7.12-rasm).



14.12-rasm. Daraxt topologiya

Ushbu topologiya quyidagi afzalliklarga ega:

- yulduz va shina topologiyalarni amalga oshirish murakkab bo‘lgan holarda foydalanish foydali;
- tarmoqni osonlik bilan kengaytirish imkonini beradi;
- ushbu topologiyada yulduz topologiyani loyihalash tugunlarni osonlik bilan boshqarish imkonini beradi;
- xatoliklarni aniqlash va tuzatish xususiyatlarini ta’minlaydi;
- har bir yulduz kabel asosiy kabelgan kabellar orqali ulanadi;
- yulduz topologiyadagi tarmoqni buzilishi qolgan tarmoqlar ishiga xalaqit bermaydi.

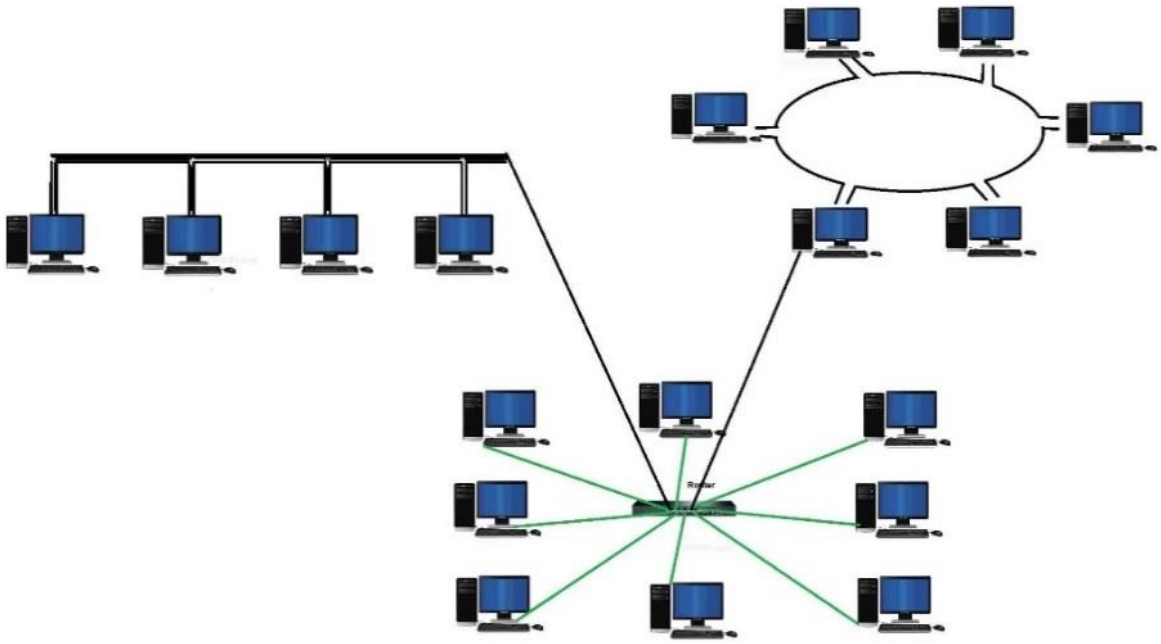
Ushbu topologiya quyidagi kamchiliklarga ega:

- asosiy kabelga yetkazilgan ixtiyoriy buzilish butun tarmoq faoliyatiga ta’sir qiladi;
- ushbu topologiya tarmoqni osonlik bilan kengaytirish imkonini bersada, butun tarmoqni boshqarish murakkab jarayon hisoblanadi;

- tarmoqni kengaytirish imkoniyati foydalanilgan asosiy kabel turiga bog‘liq.

Gibrid topologiya

Gibrid topologiya o‘zida ikkita turli topologiyani mujassamlashtirgan bo‘ladi. Mazkur topologiya odatda WAN tarmog‘ini qurishda keng foydalaniladi. Tashkilot o‘z talablaridan kelib chiqqan holda gibrid topologiya asosida tarmog‘ini quradi. Masalan, tashkilotning bir sektorida yulduz topologiya amalga oshirilgan bo‘lsa, ikkinchi sektorida xalqa topologiya amalga oshirilgan bo‘lsa, u holda ushbu ikki topologiya asosida gibrid topologiya amalga oshiriladi (7.13-rasm).



7.13-rasm. Gibrid topologiya

Gibrid topologiya quyidagi afzalliklarga ega:

- tarmoqning boshqa sektori ishiga ta’sir qilmasdan xatoliklarni aniqlash va tuzatish imkoniyatini ta’minlaydi;
- qo‘shimcha tugunllarni osonlik bilan qo‘shish imkoniyati;
- tashkilotlarga o‘z talabidan kelib chiqib tarmoqni loyihalashtirish imkonini beradi;
- ko‘plab topologiyalarni o‘zida mujassamlashtirish imkoniyatini beradi.

Gibrid topologiya quyidagi kamchiliklarga ega:

- o‘zida ko‘plab topologiyalarni mujassamlashtirgani bois, arxitekturani juda ham aniqlik bilan loyihalash talab etiladi;
- gibrid topologiyada ko‘p sonli tarmoq kabellaridan foydalanilgani bois yuqori narxga ega.

Tarmoqning apparat tashkil etuvchilari

Tarmoq kartasi. (Network Interface Card, NIC). Hisoblash qurilmasining ajralmas qismi bo‘lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Qurilmalar aynan bir elektron mikrosxema asosida simli yoki simsiz tarmoqqa ulanish imkoniyatiga ega bo‘ladilar (7.14-rasm).



7.14-rasm. Tarmoq kartalariga misollar

Repetir. Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi. Repetirlar uzatilish davomida yo‘qolgan analog va raqamli signallarni tiklaydi. Bundan tashqari ushbu qurilmalar turli protokollar tomonidan uzatilayotgan ma’lumotlarni o‘tkazish imkoniyatiga ega. Repetirlarning quyidagi turlari mavjud (7.15-rasm):

- telefon repetirlari;
- optik aloqa repetirlari;
- radio repetirlar.

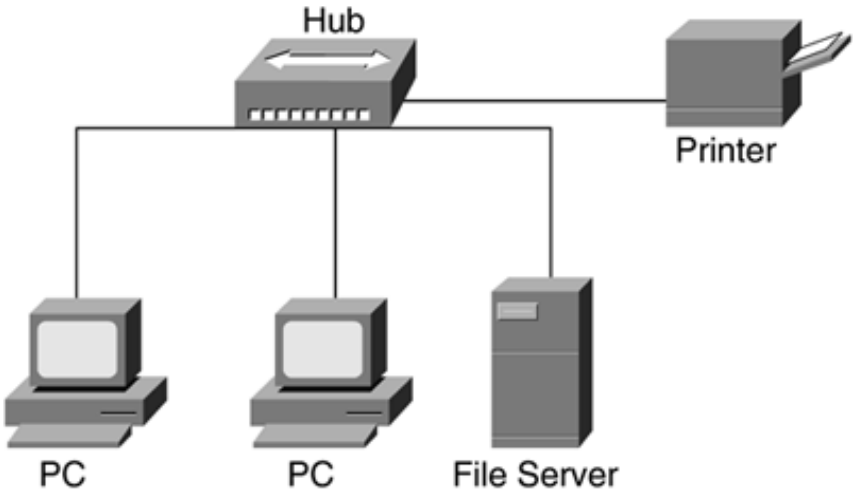


7.15-rasm. Turli repetir qurilmalari

Repetir qurilmasi foydalanishga oson, narxi past bo‘lib, signalni kuchaytirib beradi.

Xab. Xab tarmoq qurilmasi bo‘lib, ko‘plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog‘lash uchun xizmat qiladi. Xabning asosiy vazifasi bir qurilmadan kelgan ma’lumotni qurilmaning boshqa portiga ulangan qurilmaga uzatishdan iborat. Ba’zi xablarla repetir qurilmalari mavjud bo‘lib, signalni kuchaytirish imkoniyatini ham taqdim qiladi. Xabga bir portdan qabul qilingan ma’lumotlar nuxsalangan holda chiqishdagi bir qancha portlar orqali uzatiladi. Xablarga turli sondagi chiqish portlari bo‘lishi mumkin (masalan, 12, 14, 24) (7.16-rasm).



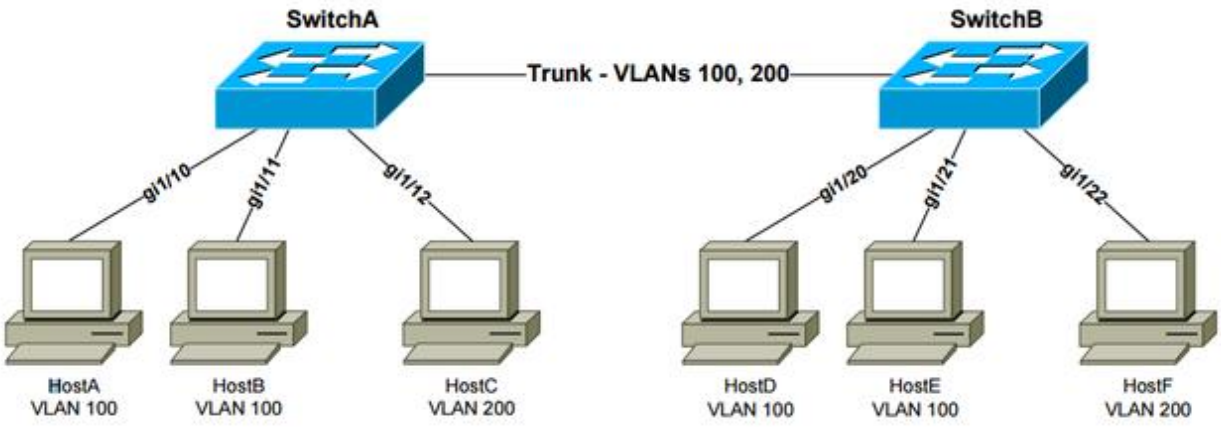


7.16-rasm. Xab va uning tarmoqda joylashuvi

Xablarning bir qancha turlari mavjud bo‘lib, ularga passiv xablarni, aktiv xablarni, intelektual xablarni, ulovchi xablarni, repetir xablarni misol keltirish mumkin. Xablar foydalanishda oson, tarmoqni uzaytirishga imkon bersada, tarmoqni nazoratlash imkoniyatini bermaydi. Bundan tashqari ushbu qurilmalarning o‘rinini hozirda svitchlar ekallab kelmoqda. Xablar OSI modelining birinchi sathida ishlaydi.

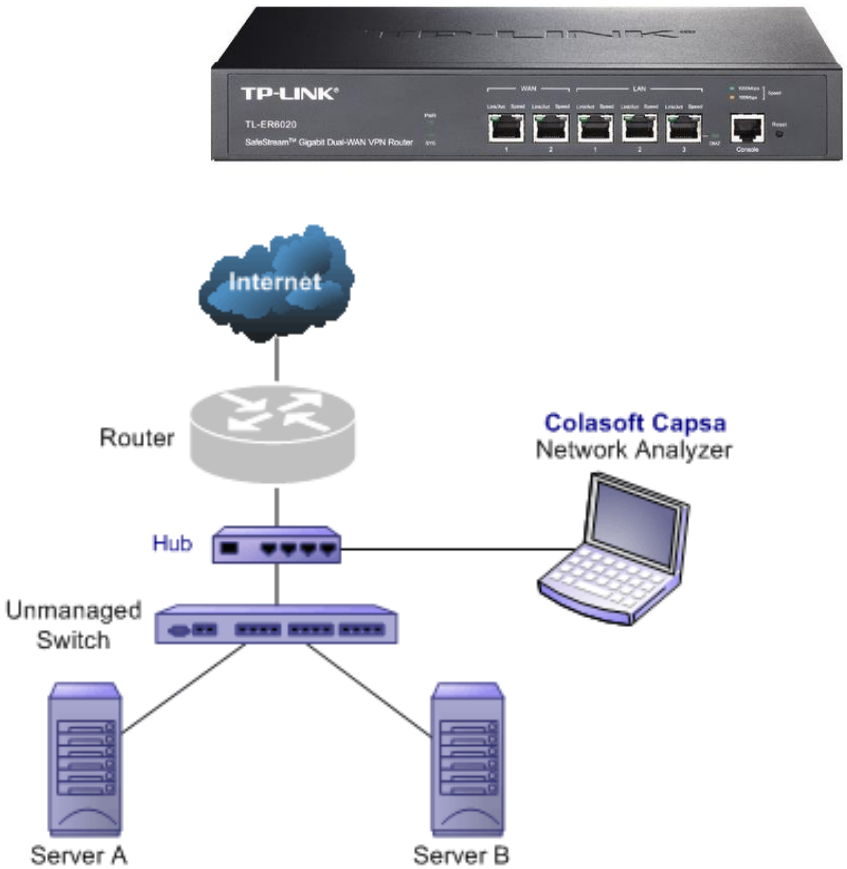
Svitch. Simli va simsiz LANlar uchun tarmoq svitchlari asos qurilma hisoblanadi. U simli va simsiz kabel orqali tarmoqdagi qurilmalardan signalni qabul qiladi. Har ikkala holda ham qabul qilgan signalni LAN orqali kompyuterlarga uzatadi. Svitchlar xablardan farqli qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. Boshqa so‘z bilan aytganda svitchlar OSI modelining 1 va 2 sathlarida ishlaydi (7.17-rasm).





7.17-rasm. Svitch va uning tarmoqda joylashuvi

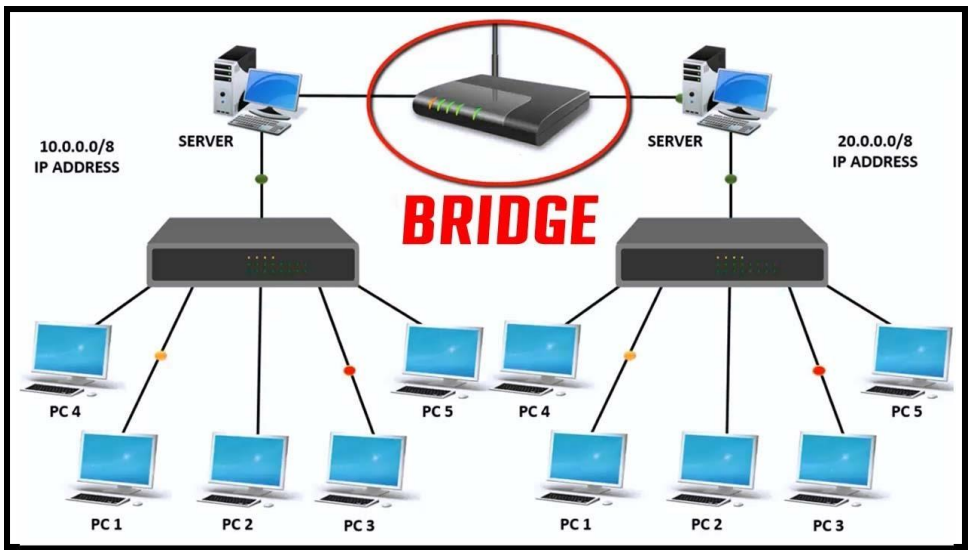
Routerlar. Routerlar yuqorida keltirilgan tarmoq qurilmalariga qaraganda murakkab tuzilishga ega qurilma bo‘lib, OSI sathining tarmoq sathida ishlaydi. Router qabul qilingan ma’lumotlarni tarmoq sathiga tegishli manzillarga ko‘ra (IP manzil) uzatadi. Bundan tashqari routerlar qabul qilingan paketlarni uzatishda ko‘plab protokollar ishlashini madadlaydi va paketlarni filterlash amallarini bajaradi (7.18-rasm).



7.18-rasm. Router va uni tarmoqda joylashuvi

Ko‘priklar. Ko‘priklar tarmoq chegarasida trafikni filterlashni amalga oshiradi. Ko‘prik har bir ma’lumotlar paketidagi MAS manzillarni o‘qib oladi va ularni masofadagi qurilmaga yuboradi. Ko‘priklar mantiqiy qurilma bo‘lib, har bir tarmoq segmentini alohida qaraydi. Ko‘priklar OSI modelini kanal sathida ishlaydi. Ko‘priklarda MAS manzillar saqlanuvchi jadvallar bo‘lib, u asosida qabul qilingan paketlarni yuborishni amalga oshiradi (7.19-rasm).

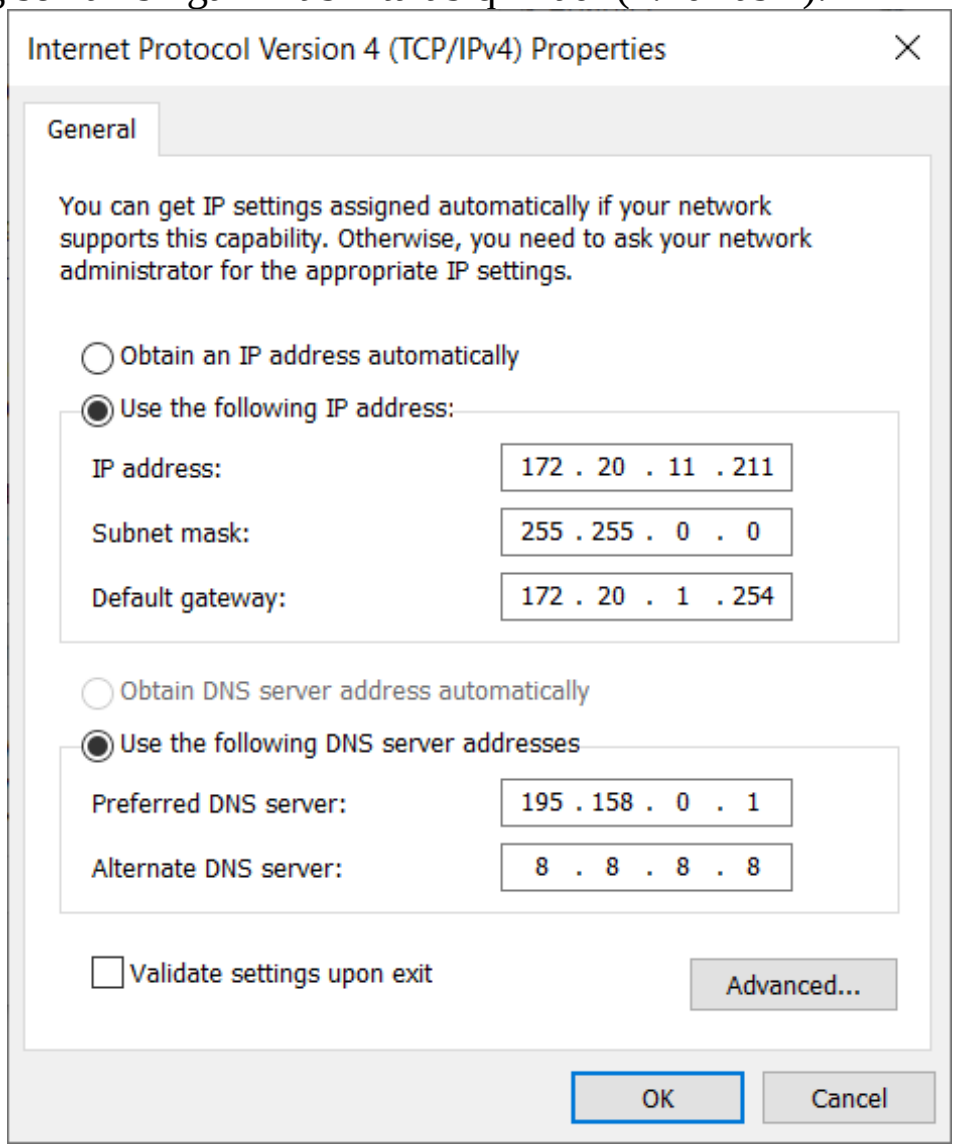




7.19-rasm. Ko‘prik va uning tarmoqda joylashuvi

Shlyuzlar. Shlyuzlar ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini o‘taydi. O’z navbatida tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini o‘taydi. Shlyuz vazifasini ishchi stansiyalar yoki serverlar bajarishi mumkin. OSI modelining ilova va transport sathlari shlyuzni madadlaydi. Shlyuzlar turli protokol va muhitdagi qurilmalarni bir biriga ulash imkoniyatini beradi. Shlyuzlar o‘zidan o‘tuvchi paketlarni filterlash vazifasini bajarmaydi. Ichki tarmoqdagi

qurilmalar tashqi tarmoqqa ulanishi uchun shlyuzning manzilini o‘zining sozlanishiga kiritishi talab qilinadi (7.20-rasm).



7.20-rasm. Shlyuz manzilini ko‘rsatish

7.4. Zaiflik, tahdid, hujum

DNS: Domain name system

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

DNS xizmatlari mijoz-server modelida ishlaydi. Mijoz DNS serverdan javobni qabul qiladi. Bu o‘rinda ikki turdagi so‘rovlar bo‘lishi mumkin:

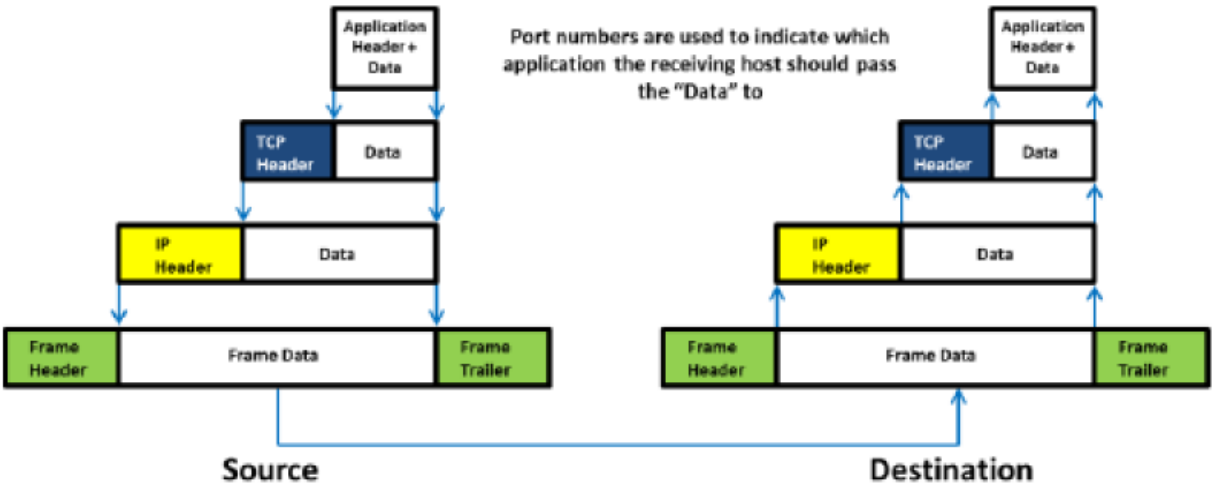
- *Oldinga qaratilgan DNS so‘rovi:* nomdan iborat bo‘lgan so‘rovlar beriladi va natija IP manzil bo‘ladi.

- *Teskari DNS so‘rovi:* IP manzildan iborat bo‘lgan so‘rovlar beriladi va natija nom bo‘ladi.

DNS turli kompyuterlarda mavjud ma’lumotlar bazasidan tashkil topgan. Ma’lumotlar bazasi host va domenlarning IP manzili va nomlaridan iborat.

TCP protokoli: Transmission Control Protocol

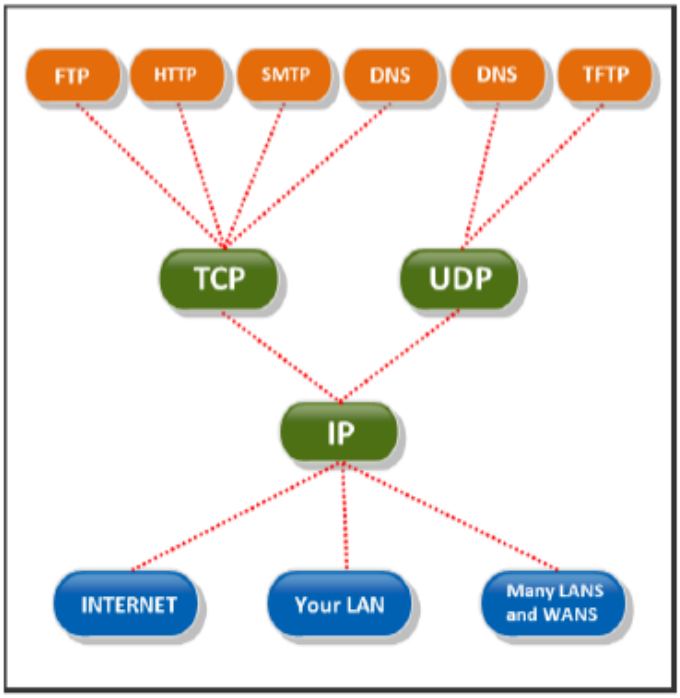
TCP protokoli ulanishga asoslangan protokol bo‘lib, internet orqali ma’lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. TCP mavjud kompyuter bir tarmoqda turgan yoki boshqa tarmoqdagi foydanuvchi kompyuteriga ma’lumotni yuborish imkoniyatiga ega bo‘ladi. TCP protokoli qabul qiluvchi tomonida manbadan uzatilgan barcha xabarlarni qabul qilinganini kafolatlaydi. TCP protokoli xabarni barchaga uzatmaydi (broadcasting imkoniyati mavjud emas). Ya’ni, paket aynan faqat masofadagi foydalanuvchiga yetkaziladi. www, e-mail, masafadan turib boshqarish yoki fayl transferini amalga oshiruvchi ilovalar ishi TCP protokollari asosida amalga oshiriladi. Masalan, HTTP protokoli HTML faylni mijozga uzatish uchun foydalaniladi. Bunda TCP protokoli HTTP protokoliga faylni uzatish va bog‘lanishda ko‘mak beradi. TCP protokoli ma’lumotlarni raqamlangan bir nechta sondagi paketlarga bo‘ladi. Shundan so‘ng ularni uzatish uchun IP sathiga uzatadi. Paketlar ko‘plab marshrutizatorlar orqali o‘tib masofadagi IP manziliga yetkaziladi. Qabul qiluvchi kompyuterida barcha paketlar tartib raqamiga ko‘ra qabul qilinadi. Quyidagi rasmda TCP protokolinnig bajaradigan amallari keltirilgan (7.21-rasm):



7.21-rasm. TCP/IP sathida ma’lumotlar oqimi

UDP protokoli: User Datagram Protocol

UDP ulanmaslikka asoslangan protokol bo‘lib, Internetda ilovalar orasida kam kechikishli va past chidamlilik darajasidagi aloqani ta’minlaydi. TCP protokoliga o‘xshamagan holda, UDP protokoli ma’lumotlarni to‘liq yetib kelishiga kafolat bermaydi. UDP protokoli ma’lumotni raqamlangan paketrlar shaklida emas, balki tarmoq bo‘ylab datagramma shaklida uzatadi. UDP protokolidan odatda o‘yin va video ilovalar tomonidan keng foydalaniladi. Tarmoq bo‘ylab ma’lumotni uzatishda paketlar yo‘qolishi kuzatilsada, bu uzatiluvchi ma’lumotni sifatiga ta’sir qilmaydi. Bunda audio va video signallarni yaxshilash uchun xatoliklarni tuzatish texnologiyasidan foydalaniladi. Quyidagi rasmda turli ilovalar tomonidan ma’lumotlarni TCP va UDP protokollari orqali uzatish jarayoni keltirilgan (7.22-rasm).

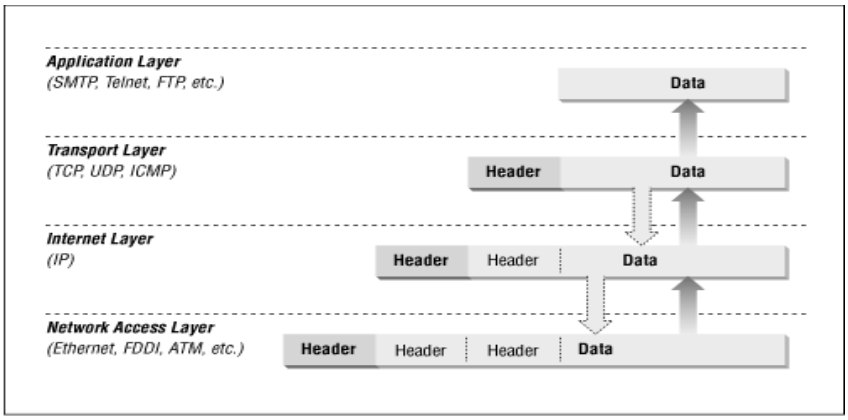


7.22-rasm. TCP/UDP va IP protokollarining ketma-ketligi

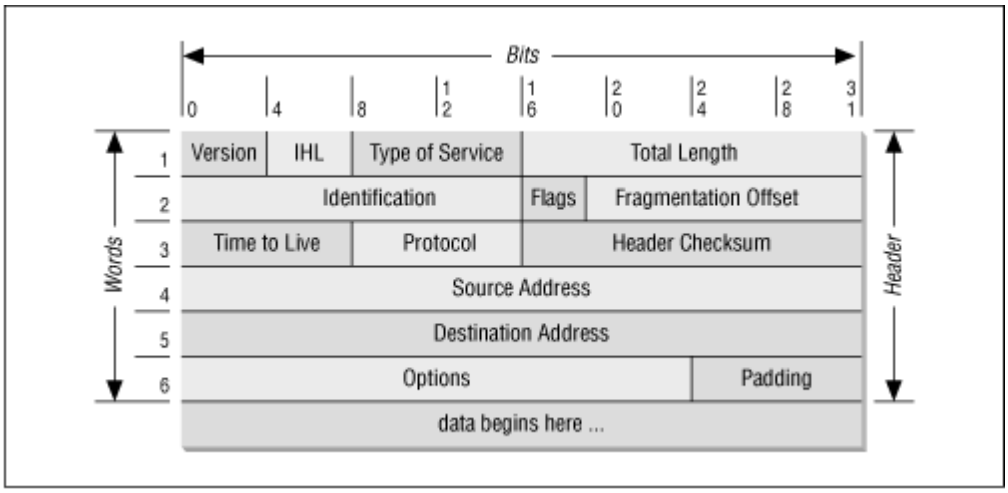
IP protokol: Internet Protocol

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

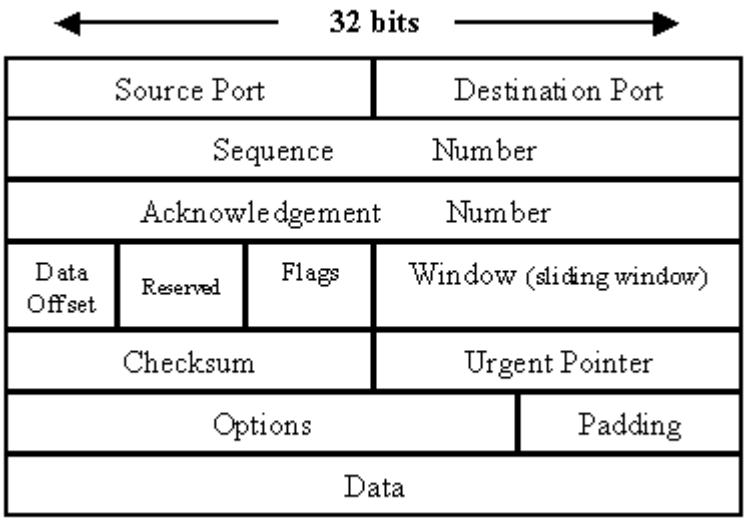
sarlavha IP paketga IP versiyasi, manba qurilmasi IP si, masofadagi qurilma IP, TTL va hak. ma’lumotlarni qo‘shadi.



7.23-rasm. Tarmoq sathlarida mos protokollar



7.24-rasm. IP sarlavha va uning tanasi



7.25-rasm. TCP sarlavha va uning tanasi

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Qanday tarmoq turlari, topologiyalarini bilasiz?
2. OSI modeli, tarmoqqa qo‘yiladigan talablar haqida ayting.
3. TCP/IP modeli nima?
4. Qanday razvedka hujumlarni bilasiz?

VIII BOB. TARMOQ XAVFSIZLIGI

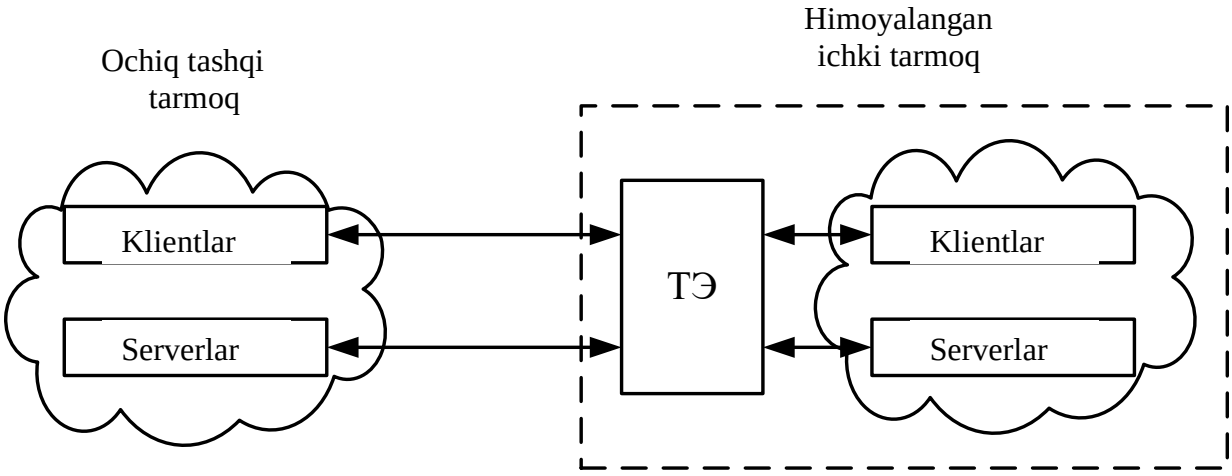
8.1. Tarmoqlararo ekranlash

Tarmoqlararo ekran texnologiyasi

Tarmoqlararo ekran (TE) - maxsus kompleks tarmoklararo ximoya bo‘lib, *braundmauer* yoki *firewall* deb ham yuritiladi. TE umumiy tarmokni ikki qismga: ichki va tashqi tarmokga ajaratadi. Ichki tarmok tashkilotning ichki tarmog‘i - ximoyalanuvchi tarmok va tashqi tarmok global tarmok - Internet. Umumiy xolda TE ichki tarmokni tashqi tarmokdan bo‘ladigan xujumlardan ximoyalaydi (8.1 - rasm).

TE bir vaqtning o‘zida ko‘plab ichki tarmok uzellarini ximoyalaydi va quyidagilarni amalga oshiradi:

- tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash. Bu foydalonuvchilar xakerlar, masofadan foydalonuvchilar, sheriklar va h. lar bo‘lishi mumkin.
- ichki tarmok foydalonuvchilarini tashqi tarmoksha bo‘lgan murojaatlarini chegaralash. Masalan, ishchilarga faqat ruxsat berilgan saytlargagina foydalonishga ruxsat berish.



8.1 - rasm. TE ulanish sxemasi

TElarning hozirgi kunga qadar aniq tayinlangan klassifikasiyasi mavjud bo‘lgan emas. Umumiy xolda ularni quyidacha klassifikasiyalash mumkin:

- OSI modelining funksional sathlari bo‘yicha:
- paket filterlari – tarmoq sathida ishlaydi;
- ekspert paketi filterlari – transport sahida ishlaydi;
- ilova proksilari – ilova sathida.

- foydalanilgan texnologiyasi bo‘yicha:
- protakol holatini nazoratlash;
- vositachi moduli yordamida (proksi).
- bajarilishiga ko‘ra:
- apparat-dasturiy;
- dasturiy.
- ulanish sxemasiga ko‘ra:
- yagona tarmok ximoyasi sxemasi;
- ximoyalangan yopiq va ximoyalanmagan ochiq tarmok segmentli sxema;
- bo‘lingan ximoyalangan yopiq va ochiq segmentli tarmok hamda sxema.

Paket filteri turidagi TE o‘tuvchi axborotni analiz qilishda quyidagi kriteriyalardan foydalonadi:

- xabar paketlarining xizmat maydonlari: tarmok manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar;
- bevosita xabar paketi kontentini tekshirish orqali, masalan, virusga qarshi;
- axborot oqimining tashqi xarakteristikasi bo‘yicha, masalan, vaqt va chastota xarakteristikalari, malumot hajmi va h.

Vositachi moduliga asoslangan TE quyidagi funksiyalarni bajaradi:

- uzatilayotgan axborotni to‘g‘riligini tekshirish;
- xabarlar oqimini filterlash va o‘zgartirish, masalan, virusga qarshi tekshirish va shaffof shifrlash;
- ichki tarmok resursidan foydalonishni cheklash;
- tashqi tarmok resursidan foydalonishni cheklash;
- tashqi tarmokdan so‘ralgan malumotlarni keshlash;
- foydalonuvchini identifikasiyalash va autentifikasiyalash (8.2 - rasm);
- chiquvchi xabar paketlari uchun ichki tarmok manzilini o‘zgartirish;
- hodisalarni ro‘yxatga olish, nazoratlash va analiz qilish.

TE korporativ tarmokdagi barcha xavfsizlik muammolarini barataraf eta olmaydi. Yuqorida keltirilgan imkoniyatlaridan tashqari tarmokda TE hal eta olmaydigan taxdidlar ham mavjud bo‘lgan. Bu cheklanishlar quyidagilar:

- o‘tkazish qobilyatini cheklashi mumkin. Barcha xabarlar oqimi TEdan o‘tganligi sababli, tarmokning o‘tkazish qobiliyati kamayadi;

- viruslarga qarshi ximoyani madadlamaydi. TE vositasi yuklanuvchi turidagi viruslarni ximoyalay olmaydi;

- Internetdagi zararli kontentlardan ximoyalay olmaydi (masalan, Java appletlari);

- foydalonuvchi yoki tizim ma’murini xatosidan yoki bilimini etishmasligidan ximoyalay olmaydi;

- TE faqat bo‘ladigan mavjud bo‘lgan xujumlarni bloklaydi. Yangi turdagi xujumni qaytara olmaydi.

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

Bu turdagi tarmoqlararo ekran samarali bo‘lib, faqat tarmoq sathida ishlaydi va sarlavha ma’lumotlarni tahlillashda katta tezlik beradi. Ammo, bu turdagi tarmoqlararo ekran qator kamchiliklarga ega:

- holatning turg‘unligi mavjud emas, ya’ni har bir paket turlicha bo‘ladi;

- bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi;

- ilova sathi ma’lumotlarni, zararli dasturlarni va hak. tekshirmaydi.

Bu turdagi tarmoqlararo ekran “Ruxsatlarni nazoratlash ro‘yxati (ACL)” yordamida sozlanadi (8.2, 8.3 - rasm).



8.2-rasm. Paket filteri

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

8.3-rasm. Ruxsatlarni nazoratlash ro‘yxatiga misol

Yuqoridagi qoidaga asosan faqat Web uchun kirish va chiqish mavjud bo‘lib, qolgan hollarda harakatlar cheklangan.

Bu sozlanmadan buzg‘unchi qanday qilib foydalanishi mumkin? Buning uchun dastlab buzg‘unchi tarmoqlararo ekranning qaysi porti ochiq ekanligi aniqlash kerak. Boshqa so‘z bilan aytganda portlarni skanerlashni amalga oshirishi kerak.

Ochiq port aniqlangandan so‘ng, u port orqali zararli ma’lumot yuborilishi mumkin. Buni oldini olish uchun odatda, tarmoqlararo ekran mavjud TCP bog‘lanishlarni xotirasida saqlashi kerak va natijada qabul qilingan bog‘lanish oldingi bog‘lanish bilan bir xil yekanligini aniqlaydi.

Ekspert paketi filtrlari. Bu turdagi tarmoqlararo ekran paketni filterlash vazifasini bajaruvchi tarmoqlararo ekranga mavjud kamchiliklarni bartaraf etadi. Bu turga asosan tekshiruv tarmoq va transport sathida amalga oshiriladi. Kamchiligi esa, tekshirish vaqtining ko‘pligi va ilova sathi ma’lumotlarini tekshirish imkoni yo‘qligidir (8.5-rasm.).

Ilova sathi
Transport sathi
Tarmoq sathi
Kanal sathi
Fizik sathi

8.4-rasm. Ekspert paketi filtri

Ilova proksilari. Bu turdagi tarmoqlararo ekran oldingi ikki turga mavjud kamchiliklarni o‘zida bartaraf etadi va ilova sathida ishlaydi (8.5 - rasm).



8.5-rasm. Ilova proksilari

Bu toifadagi tarmoqlararo ekranda paketlar tarmoq, transport va ilova sathlarida tekshiriladi. Ilova sathi uchun paket “buzulib” qaytadan “quriladi”.

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

8.2. Virtual xususiy tarmoqlar

Ximoyalangan virual tarmok (VPN) ximoya mexanizmi

Agar tashkilotlar yagona binoda joylashgan yoki yaqin binolarda joylashgan bo‘lsa, u xolda ular uchun korporativ tarmokni qurishi qiyinchilik tug‘dirmaydi. Ammo, georgafik jixatdan biri - biridan uzoqda joylashgan tashkilot ofislari orasida yagona korporativ tarmokni hosil qilish murakkab vazifa.

Ochiq tarmok orqali ximoyalangan tarmokni qurish va biznes harakatlarini amalga oshirish uchun dastlabki qadamlar 1990 yillarda qo‘yila boshlandi va bu konsepsiya ximoyalangan virtual tarmok - VPN (Virtual Private Network) deb atala boshlandi.

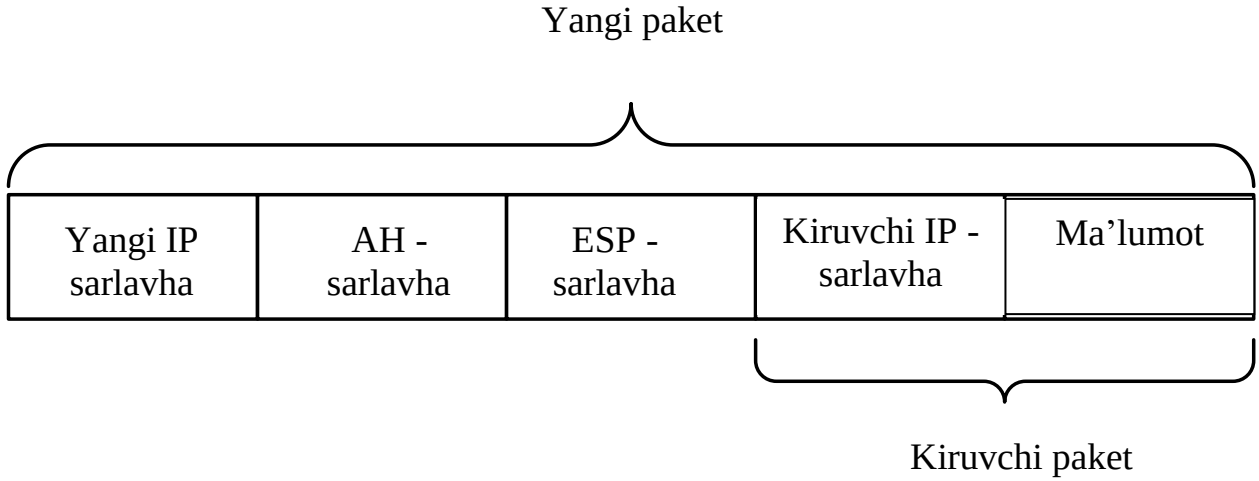
VPNni qurishda juda oddiy g‘oya yotadi. Internet tarmog‘ida malumot almashinish uchun ikkita uzel mavjud bo‘lgan ekan, bu ikki uzel orasida axborotni konfidensiyalligini va butunligini ta’minovchi virtual tarmok qurish kerak. Bu ximoyalangan tarmokdan ixtiyoriy passiv va aktiv xujum hamda ham malumotni olish imkoniyati bo‘lmasin.

Bu qurilgan ximoyalangan kanalni *tunel* ham deb atash mumkin. VPN tarmok orqali bosh ofis va uning masofadagi filiallari orasida ishonchli ravishda axborotni uzatish mumkin.

VPN tunel ochiq kanal yordamida bog‘lanishni amalga oshirib, virtual tarmok orqali kriptografik ximoyalangan xabarlar paketini uzatadi. VPN tunel orqali uzatilgan axborot ximoyasi quyidagilarga asoslanadi:

- tomonlarni autentifikasiyalashga;
- yuboriladigan axborotlarni kriptografik yashirish (shifrlash);
- etkazilgan axborotni butunligini va to‘g‘riligini tekshirish.

Virtual tunelni yaratishda mavjud bo‘lgan paket shifrlangan xolda yangi hosil qilingan mantiqiy paket ichiga kiritiladi. Bundan shunday xulosa kelib chiqadiki, VPN shifrlanuvi paket qismi tegishli bo‘lgan tarmok sathidan past bo‘lishi yoki o‘ziga teng bo‘lishi shart. Odatda mavjud bo‘lgan IP - paket to‘liq shifrlanib, unga yangi IP sarlavha beriladi. (8.6 - rasm).



8.6 - rasm. Tunellash uchun tayorlangan paketga misol

VPN apparat-dasturiy qurilmasi VPN - mijoz, VPN - server va VPN - shlyuz sifatida faoliyat yuritishi mumkin. VPN shlyuz hamda ximoyalangan kanalni qurishda ikkita tomonda ham shlyuz bo‘lishi talab etiladi. Bunda lokal tarmokdan chiquvchi paketga yangi sarlavha beriladi. Eski sarlavha esa shifrlangan xolda bo‘ladi. Ochiq tarmok orqali uzatilganda, qabul qiluvchi shlyuz qabul qilingan paketdan yangi sarlavhani olib tashlaydi va lokal tarmok ichida eski sarlavha hamda paketlarni uzatadi.

Virtual tarmoklarni qurish asosan ikkita sxemaga asoslanadi:

- lokal tarmoklar orasida qurilgan virtual lokal tarmok;

- lokal tarmok va uzel orasida qurilgan virtual lokal tarmok.

VPN texnologiyalar quyidagi belgilariga ko‘ra klassifikasiyalanadi:

- OSI modelining “ishchi sathlari”ga ko‘ra:
- kanal sathidagi VPN (L2F, L2TP va PPTP protakoli yordamida);
- tarmok sathidagi VPN (IPSec protakoli);
- seans sathidagi VPN (TLS protakoli).
- VPNning texnik echim arxitekturasiga ko‘ra:
- korporativ ichidagi VPN;
- masofadan foydaloniluvchi VPN;
- korporativlararo VPN.
- VPN ning texnik amalga oshirilishiga ko‘ra:
- marshrutizator ko‘rinishida;
- tarmoklararo ekran ko‘rinishida;
- dasturiy ko‘rinishda;
- maxsus shifrlash prosessoriga ega apparat vosita.

VPN tarmoklarni axborot tizimlarida axborot xavfsizligini ta’minlashda foydalonishning afzalliklari quyidagilar:

- barcha korporativ tarmokni ximoyalash imkoniyati - yirik lokal tarmok ofislaridan tortib alohida ishchi joylarigacha;
- masshtablashgan ximoya tizimi, ya’ni, alohida foydalonuvchi uchun dasturiy ko‘rinishda, lokal tarmok uchun server ko‘rinishda va korporativ tarmok uchun shlyuz ko‘rinishda amalga oshirish imkoniyati;
- ochiq tarmok yordamida ximoyalangan tarmokni qurish imkoniyati;
- tarmok ishini nazorat ositida olish va barcha axborot manbalarini identifikasiyalash.

VPN texnologiya tarmoqlararo uzatilayotgan axborotni ximoyalashda muhim sanalib, yaqin kelajakda barcha tashkilotlar bu texnologiyadan to‘liq foydalona boshlaydi.

8.3. Simsiz tarmoq turlari

Simsiz tarmoqlar odamlarga simli ulanishsiz o‘zaro bog‘lanishlariga imkon beradi. Bu siljish erkinligini va uy, shahar qismlaridagi yoki dunyoning olis burchaklaridagi ilovalardan foydalanish imkonini ta’minlaydi. Simsiz tarmoqlar odamlarga

o‘zlariga qulay va istagan joylarida elektron pochtani olishlariga yoki Web-saxifalarni ko‘zdan kechirishlariga imkon beradi.

Simsiz tarmoqlarning turli xillari mavjud, ammo ularning eng muhim xususiyati bog‘lanishning kompyuter qurilmalari orasida amalga oshirilishidir. Kompyuter qurilmalariga shaxsiy raqamli yordamchilar (Personal digital assistance, PDA), noutbuklar, shaxsiy kompyuterlar, serverlar va printerlar taalluqli. Odatda uyali telefonlarni kompyuter qurilmalari qatoriga kiritishmaydi. Ammo, eng yangi telefonlar va xatto naushniklar ma’lum xisoblash imkoniyatlariga va tarmoq adapterlariga ega. Yaqin orada elektron qurilmalarning aksariyati simsiz tarmoqlarga ulanish imkoniyatini ta’minlaydi.

Bog‘lanish ta’minlanadigan fizik xudud o‘lchamlariga bog‘liq xolda simsiz tarmoqlarning quyidagi kategoriyalari farqlanadi:

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

Simsiz shaxsiy tarmoqlari uzatishning katta bo‘lmagan masofasi bilan (17 metrgacha) ajralib turadi va katta bo‘lmagan binoda ishlatiladi. Bunday tarmoqlarning xarakteristikalari o‘rtacha bo‘lib, uzatish tezligi odatda 2Mb/s dan oshmaydi.

Bunday tarmoq, masalan, foydalanuvchi PDAsida va uning shaxsiy kompyuterida yoki noutbukida ma’lumotlarni simsiz sinxronlashni ta’minlashi mumkin. Xuddi shu tariqa printer bilan simsiz ulanish ta’minlanadi. Kompyuterni tashqi qurilmalar bilan ulovchi simlar chigalliklarining yo‘qolishi yetarlicha jiddiy afzallik bo‘lib, buning evaziga tashqi qurilmalarning boshlang‘ich o‘rnatilishi va keyingi, zaruriyat tutilganda joyining o‘zgartirilishi anchagina osonlashadi.

Simsiz shaxsiy tarmoqlarning aksariyat uzatuvchi-qabul qiluvchilari (transceiver) kam quvvat is’temol qiluvchi va ixcham mikroprosessorlar bilan ta’minlangan. Bu esa katta bo‘lmagan foydalanuvchi qurilmalarini samarali madadlashga hamda kompyuter qurilmasini uzoq vaqt mobaynida bitta batareyada (yoki akkumulyatorda) ishlashiga imkon beradi. Undan tashqari, kam quvvat iste’mol qilinishi simsiz shaxsiy tarmoqlarni uyali telefonlarga, PDAlarga va naushniklarga tatbiq etishga sabab bo‘ldi.

8.1-jadval

Simsiz tarmoq usullari

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

Simsiz shaxsiy tarmoqlar Internetga va ilovalarga ulanishda noutbuklar va shaxsiy kompyuterlarning o‘zaro aloqasini ta’minlashi mumkin. Bu ta’sir doirasi bitta xona bilan chegaralangan tarmoqlarga to‘g‘ri keladi.

Shaxsiy simsiz tarmoqlarning keng tarqalgan turiga Bluetooth texnologiyasi misol bo‘la oladi.

Bluetooth. Ushbu texnologiya qisqa masofalarda simsiz tarmoqni tashkil etish texnologiyasi hisoblanib, 2.4 - 2.485 Ggs oraliqda ishlaydi. Ushbu texnologiya 1994 yilda Ericsson kompaniyasi tomonidan yaratilgan. Ushbu texnologiyaga IEEE tashkiloti tomonidan IEEE 802.15.1 standarti berilgan. Ushbu texnologiyada ma’lumot paket ko‘rinishada 79 ta kanaldan biri orqali yuboriladi. Ya’ni har bir kanal uchun 1 Mgs dan chastota berilgan. Bluetooth 4.0 da esa 2 Mgs.dan chastota berilib, kanallar soni esa 40 ta bo‘ladi. 79 kanal bo‘lgan holda birinchi kanal 2402 Mgs.dan boshlanib, 2480 Mgs.da tugaydi.



8.7-rasm. Simsiz PAN tarmog‘i

Bluetooth texnolgiyasi asosan mobil telefonlar va dastlabki ishlab chiqilgan kompyuter qurilmalari uchun mo‘ljallangan bo‘lib, kichik hajmdagi ma’lumotni almashinishda keng foydalaniladi.

8.2-jadval

Bluetooth texnologiyasi versiyalari

Versiyasi	Uzatish tezligi
1.2 (Basic Rate, BR)	1 Mbit/s
2.0 (Enhanced Data Rate, EDR)	3 Mbit/s
3.0 (High Speed, HS)	24 Mbit/s
4.0 (Low Energy, LE)	24 Mbit/s
5.0	

Bluetooth standartining 1.1 va 1.2-versiyalari BR nomi bilan tanilib, ma’lumotning uzatishda amalga 720 Kbit/s tezlikga ega va

Gaussian Frequency-Shift Keying (GFSK) modulyasiyasidan foydalanadi.

Bluetooth standartining 2.0 versiyasi EDR texnologiyasi deb nomlanib, ma'lumotni uzutishda amalda 2.1 Mbit/s tezlikka ega. π/4 surishga asoslangan Differential Quaternary Phase Shift Keying (DQPSK) modulyasiyasidan foydalangan holda ma'lumot uzatish tezligi 2 Mbit/s ga teng bo‘lsa, 8 fazali Differential Phase Shift Keying (8DPSK) modulyasisidan foydalangan holda esa 3 Mbit/s tezlikka erishiladi. Ushbu texnologiya faqat Bluetooth 2.0 yoki undan yuqori versiyalarda mavjud.

Bluetooth 3.0 versiyasi HS texnologiyadan foydalanadi va Alternate MAC/PHYs (AMP) yordamida yuqori tezlikni ko‘rsatadi. AMR texnologiyasida Orthogonal Frequency-Division Multiplexing (OFDM) modulyasiyadan foydalangan holda 24 Mbit/s tezlikka erishiladi.

Bluetooth 4.0 versiyasida Bluetooth LE (Low Power Bluetooth) texnologiyasidan foydalanadi. Ushbu texnologiyaning qolgan versiyalarda foydalanilgan texnologiyalardan farqi uning kam quvvat talab etishi va resurslardan kam miqdorda foydalanilishini olish mumkin.

Simsiz lokal tarmoqlar ofislarning ichida va tashqarisida, ishlab chiqarish binolarida uzatishlarning yuqori xarakteristikalarini ta'minlaydi. Bunday tarmoqlardan foydalanuvchilar odatda noutbuklarni, shaxsiy kompyuterlarni va katta resurslarni talab etuvchi ilovalarni bajarishga qodir prosessorli va katta ekranli PDAlarni ishlatishadi. Xizmatchi tarmoq xizmatlaridan majlislar zalida yoki binoning boshqa xonalarida bo‘la turib foydalanashi mumkin. Bu xizmatchiga o‘z vazifalarini samarali bajarishga imkon beradi. Simsiz lokal tarmoqlar uzatishning 54Mbit/s.gacha tezligida barcha ofis yoki maishiy ilovalar talablarini qondirish imkoniga ega. Xarakteristikalari, komponentlari, narxi va bajaradigan amallari bo‘yicha bunday tarmoqlar Ethernet xilidagi an'anaviy simli lokal tarmoqlarga o‘xshash.

Ushbu turdagi simsiz aloqa turiga WI-FI texnologiyasi misol bo‘lib, 2.4 va 5,0 GGs chastotalarda ishlatiladi. Ushbu texnologiyani ko‘plab qurilmalar, shaxsiy kompyuterlar, video-o‘yin qurilmalari, smartfonlar, raqamli kameralar, raqamli audio qurilmalari qo‘llab quvvatlaydilar.

Simsiz regional tarmoqlar yuzasi bo‘yicha shaharga teng bo‘lgan xududga xizmat qiladi. Aksariyat xollarda ilovalarni bajarishda belgilangan ulanish talab etsa, ba’zida esa mobillik zarur bo‘ladi. Masalan, kasalxonada bunday tarmoq asosiy bino va masofadagi klinikalar orasida ma’lumotlarni uzatishni ta’minlaydi. Yoki, energetik kompaniya bunday tarmoqdan shahar masshtabida foydalanib, turli tumanlardan beriladigan ish naryadlaridan foydalanishini ta’minlaydi. Natijada, simsiz regional tarmoqlar mavjud tarmoq infratuzilmalarini bir joyga to‘playdi yoki mobil foydalanuvchilarga mavjud tarmoq infratuzilmalari bilan ulanishni o‘rnatishga imkon beradi.

Simsiz Internet xizmatlari bilan ta’minlovchilar (Wireless Internet Service Provider, WISP) uyda foydalanuvchilar va kompaniyalar uchun doimiy simsiz ulanishlarni ta’minlash maqsadida shaharlarda va qishloq joylarda simsiz regional tarmoqlarni mijozlar ixtiyoriga taqdim etadi. Bunday tarmoqlar, ko‘pincha simli ulanishlarni yotqizish bilan bog‘liq chegaralanishlarga ega bo‘lgan oddiy simli ulanishlarga nisbatan samarali xisoblanadi.

Simsiz regional tarmoqlarning xarakteristikalari turlicha. Ulanishlarda infraqizil texnologiyaning ishlatilishi ma’lumotlarni uzatish tezligining 100 Gbit/s va undan katta bo‘lishini ta’minlaydi.

Simsiz MAN tarmoqlari odatda WiMAX (Worldwide Interoperability for Microwave Access) texnologiyasi asosida quriladi. WiMAX texnologiyasi

Simsiz global tarmoqlar mobil ilovalarning, ulardan mamlakat yoki xatto kontinent masshtabida foydalanishni ta’minlash bilan ishlanishini ta’minlaydi. Iqtisodiy muloxazalarga tayangan xolda, telekommunikasiya kompaniyalari ko‘pgina foydalanuvchilar uchun uzoq masofadan ulanishni ta’minlovchi simsiz global tarmoqning nisbatan qimmat infratuzilmasini yaratadilar. Bunday yechimning xarajati barcha foydalanuvchilar o‘rtasida taqsimlanadi, natijada abonent to‘lovi unchalik yuqori bo‘lmaydi.

Ko‘pgina telekommunikasiya kompaniyalarining kooperasiyasi tufayli simsiz global tarmoqlarining ta’sir doirasi chegaralanmagan. Telekommunikasiya xizmatini ta’minlovchilarning biriga to‘lab, simsiz global tarmoq orqali dunyoning xar qanday nuqtasidan qator Internet xizmatidan foydalanish mumkin.

Simsiz global tarmoq xarakteristikalari nisbatan yuqori emas, ma’lumotlarni uzatishning tezligi 56 Kbit/s ni, ba’zida 170 Kbit/s ni tashkil etadi.

Simsiz global tarmoqlarga xos ilovalar Internetdan foydalanishni, elektron pochta xabarlarini uzatish va qabul qilishni, foydalanuvchi uydan yoki ofisdan tashqarida bo‘lganida korporativ ilovalardan foydalanishni ta’minlovchi ilovalardir. Abonentlar, masalan, taksida ketayotganlarida yoki shaxar bo‘yicha sayr qilinayotganlarida ulanishni o‘rnatishlari mumkin. Umuman, simsiz global tarmoqdan foydalanuvchilar xududiy chegaralanmaganlar.

Simsiz global tarmoqlar texnologiyasini tatbiq etishdagi muammolardan biri uning bino ichidagi foydalanuvchilar uchun bog‘lanishni ta’minlay olmasligi. Chunki bunday tarmoq infratuzilmalari bino tashqarisida joylashgan va radiosignallar binoda aytarlicha susayadi. Simsiz global tarmoqlarni bino ichiga o‘rnatilishi esa qimmatga tushadi va texnik nuqtai nazaridan asoslanmagan.

Simsiz shaxsiy, lokal, regional va global tarmoqlar bir-birini to‘ldiruvchi bo‘lib, turli talablarni qondiradi. Ammo, ba’zida bir tarmoqni ikkinchisidan farqlab bo‘lmaydi. Masalan, bino ichidagi simsiz lokal tarmoq foydalanuvchi PDAsi bilan shaxsiy kompyuterini simsiz shaxsiy tarmoq kabi ulashni ta’minlashi mumkin. Turli simsiz tarmoqlar orasidagi farqni aniqlashda ularda ishlatiladigan texnologiyalar va standartlardan foydalanishadi.

Agar foydalanuvchi nuqtai nazaridan istiqbol xususida so‘z yuritilsa, simsiz tarmoqlar orasida chegaraning yo‘qolishi shart. Turli xil simsiz tarmoq ishini madadlovchi kompyuter qurilmalari tarmogi interfeysining platalari paydo bo‘lmoqda. Masalan, sayyoxda yoki tijoratchida xam simsiz lokal xam simsiz global tarmoq bilan o‘zaro aloqa qiluvchi zamonaviy uyali telefon bo‘lishi mumkin.

8.4. Simsiz tarmoqlardagi mavjud zaifliklar

Xavfsiz simsiz ilovani yaratish uchun simsiz “xujumlar” o‘tuvchi bo‘lishi mumkin bo‘lgan barcha yo‘nalishlarni aniqlash lozim. Afsuski, ilovalar xech qachon butunlay xavfsiz bo‘lmaydi, ammo simsiz texnologiyalardagi xavf-xatarni sinchiklab o‘rganish xar xolda ximoyalanish darajasini oshishiga yordam beradi. Demak, mumkin bo‘lgan taxdidlarni taxlillab, tarmoqni shunday qurish lozimki, xujumlarga xalaqit berish va nostandart “xujumlar”dan ximoyalanishga tayyor turish imkoni bo‘lsin.

Nazoratlanmaydigan xudud. Simli va simsiz tarmoqlar orasidagi asosiy farq tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan zona bilan bog‘liq. Uyali tarmoqlarning yetarlicha keng makonida simsiz muhit aslo nazoratlanmaydi. Zamonaviy simsiz texnologiyalar tarmoq makonini boshqarish vositalarining chegaralangan to‘plamini taqdim etadi. Bu simsiz tuzilmalarning yaqinidagi xujum qiluvchilarga simli dunyoda mumkin bo‘lmagan xujumlarni amalga oshirishga imkon beradi.

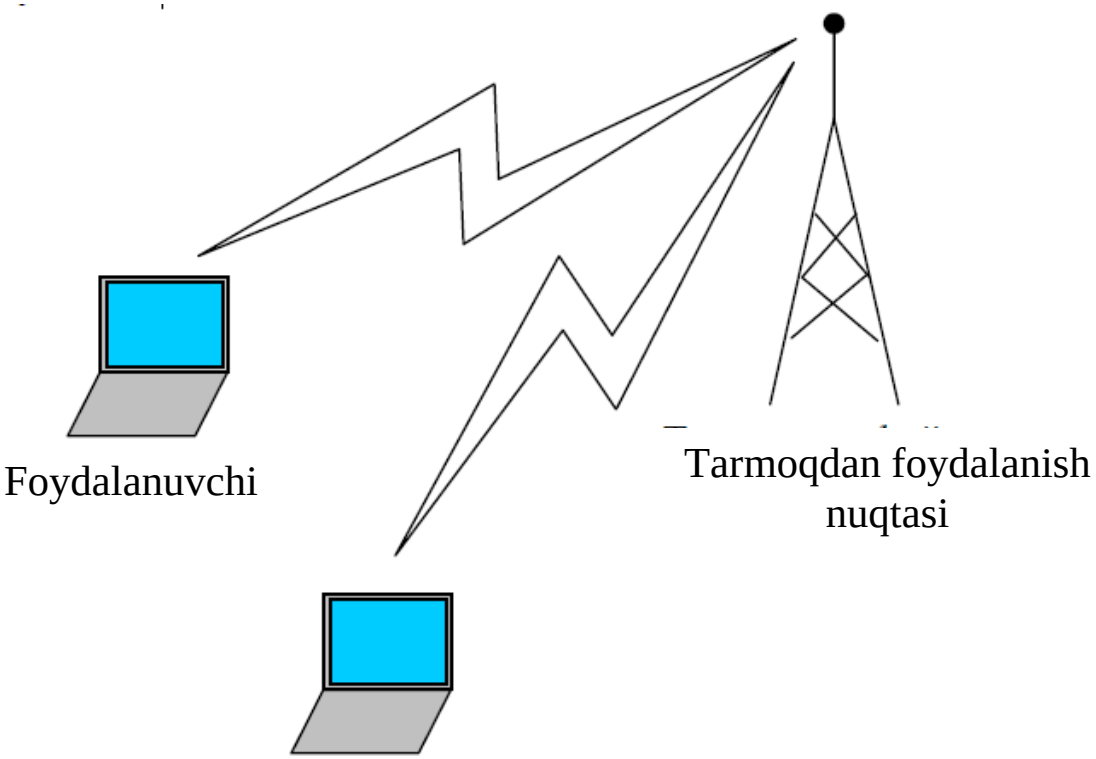
Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muxitda keng tarqalgan muammo - anonim xujumlarning mumkinligi. Anonim zararkunandalar 8.14-rasmda ko‘rsatilganidek radiosignallarni ushlab qolib, uzatiluvchi ma’lumotlarni deshifrlashi mumkin.

Uzatishni ushlab qolish uchun niyati buzuq odam uzatgich (peredatchik) oldida bo‘lishi lozim. Ushlab qolishning bunday turlarini umuman qaydlash mumkin emas va ularga xalaqit berish undan xam qiyin. Antennalar va kuchaytirgichlardan foydalanish, ushlab qolish jarayonida niyati buzuq odamlarga nishondan aytarlicha uzoq masofada bo‘lishlariga imkon beradi.

Yashirincha eshitishning yana bir usuli - simsiz tarmoqqa ulanish. Lokal simsiz tarmoqda yashirincha faol eshitish odatda Adress Resolution Protocol (ARP) protokolidan noto‘gri foydalanishga asoslangan. Boshida bu texnologiya tarmoqni “eshitish” maqsadida yaratilgan edi. Aslida, biz ma’lumotlar bolanishi satxida “man in the middle” (MITM – “o‘rtada odam”, pastroqqa qaralsin) xilidagi xujum bilan ish ko‘ramiz. Xujum qiluvchi lokal simsiz tarmoqning nishon stansiyasiga so‘ralmagan ARP-javoblarni yuboradi, nishon stansiyasi esa xujum qiluvchiga o‘zidan o‘tayotgan barcha trafikni jo‘natadi. So‘ngra niyati buzuq odam paketlarni ko‘rsatilgan adresatlarga yo‘llaydi. Shunday qilib, simsiz stansiya boshqa simsiz mijozning (yoki lokal tarmoqdagi simli mijozning) trafigini ushlab qolishi mumkin.

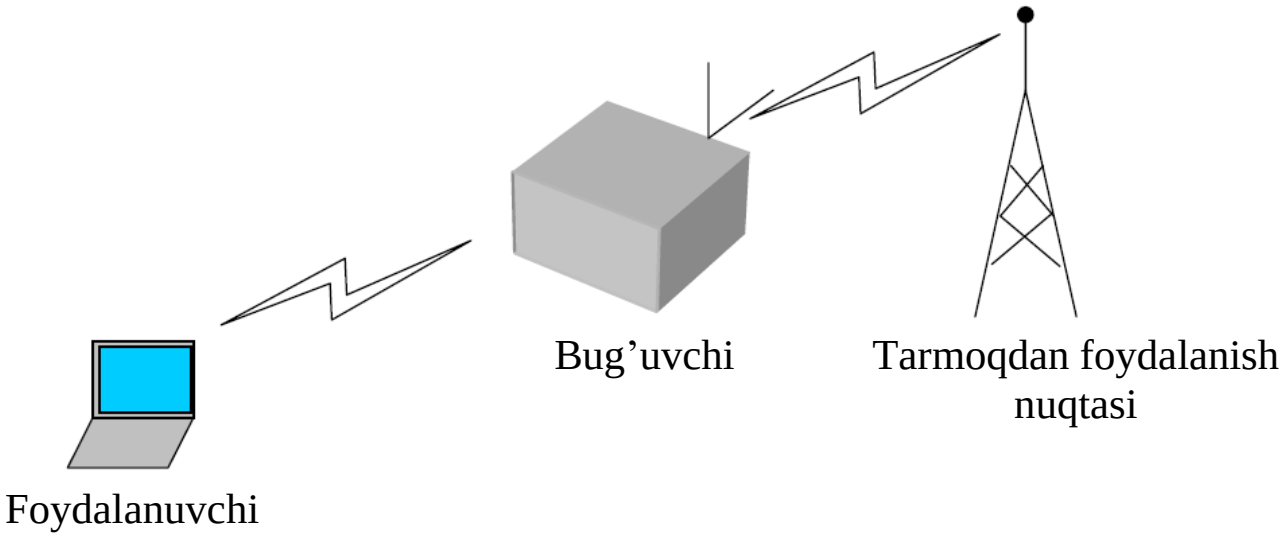
Xizmat ko‘rsatishdan voz kechish. DoS (Denial of Service - xizmat ko‘rsatishdan voz kechish) xilidagi xujum tarmoqni butunlay ishdan chiqarishi mumkin. Butun tarmoqda, jumladan bazaviy stansiyalarda va mi-joz terminallarida, shunday kuchli interferensiya paydo bo‘ladiki, stan-siyalar bir-birlari bilan bog‘lana olmaydilar. Bu xujum ma’lum doiradagi barcha kommunikasiyani o‘chiradi. Simsiz tarmoqqa bo‘ladigan DoS xujumni oldini olish yoki tuxtatish qiyin. Simsiz tarmoq texnologiyalarining aksariyati lisenziyalanmagan

chastotalardan foydalanadi, demak, bir qancha elektron qurilmalardan interferensiya bo‘lishi mumkin.



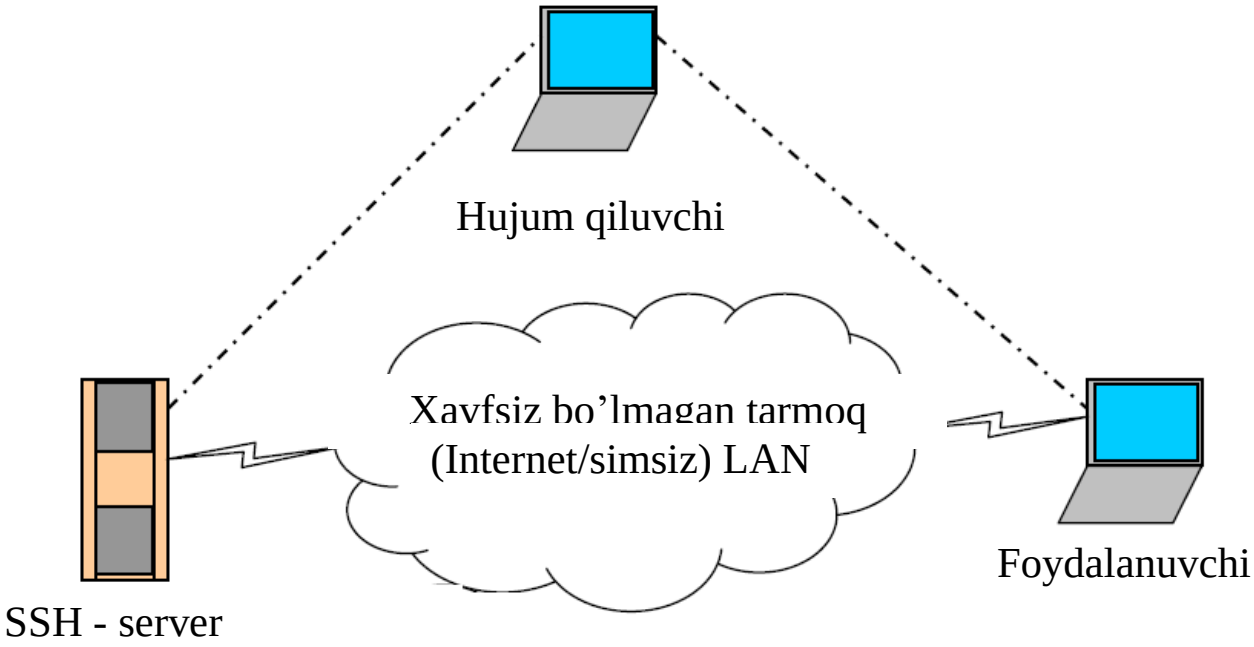
8.8-rasm. Simsiz aloqa tizimlarida yashirincha eshitish

Bo‘gish. Tarmoqlarda bo‘g‘ish atayin yoki atayin bo‘lmagan interferensiyaning aloqa kanalidagi jo‘natuvchi va qabul qiluvchi imkoniyatidan oshganida sodir bo‘ladi. Natijada bu kanal ishdan chiqariladi. Xujum qiluvchi bo‘g‘ishning turli usullaridan foydalanishi mumkin (8.15-rasm).



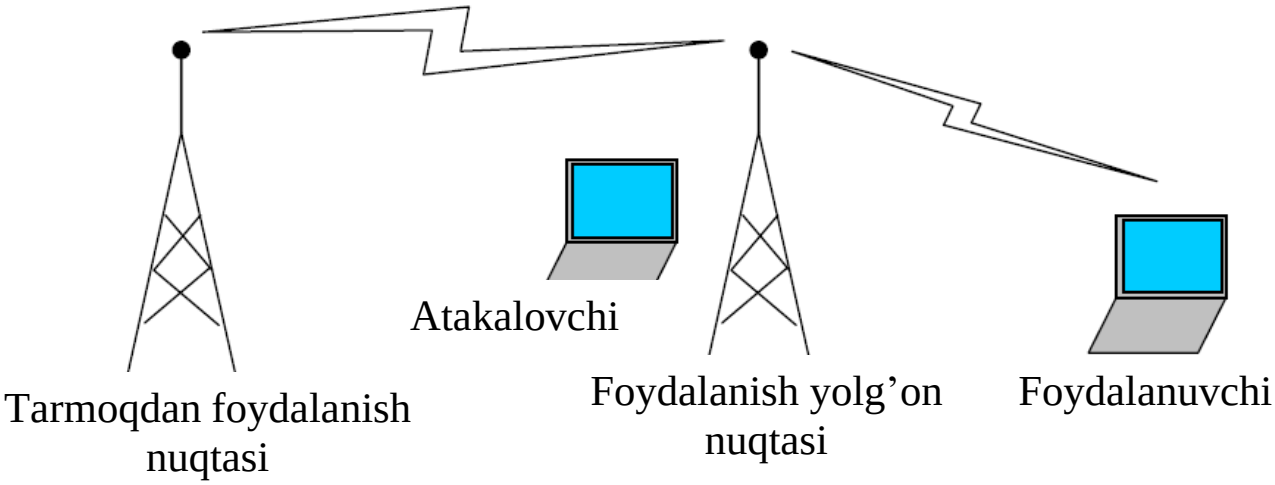
8.9-rasm. Simsiz aloqalarda bo‘g‘ish hujumlari

MITM(man in the middle) xujumi. MITM xujumi yuqorida tavsiflangan bostirib kirishlarga o‘xshash. Ular turli shakllarni olishlari mumkin va aloqa seansining konfidensialligini va yaxlitligini buzish uchun ishlatiladi. MITM xujumlar anchagina murakkab, chunki ularni amalga oshirish uchun tarmoq xususida batafsil axborot talab etiladi. Niyati buzuq odam, odatda, tarmoq resurslaridan birining identifikasiyasini bajaradi. Xujum qurboni ulanishni boshlaganida, firibgar uni ushlab qoladi va istalgan resurs bilan ulanishni tugallaydi, so‘ngra ushbu resurs bilan barcha ulanishlarni o‘zining stansiyasi orqali o‘tkazadi (8.16-rasm). Bunda xujum qiluvchi axborotni jo‘natishi, jo‘natilganini o‘zgartirishi yoki barcha muzokaralarni yashirincha eshitishi va so‘ngra rasshifrovka qilishi mumkin.



8.10-rasm. MITM xilidagi ataka

Tarmoqdan foydalanishning yolgon nuqtalari. Tajribali xujum qiluvchi tarmoq resurslarini imitasiya qilish bilan foydalanishning yolgon nuqtalarini tashkil etishi mumkin. Abonentlar, xech shubx,alanmasdan foydalanishning ushbu yolgon nuqtasiga murojaat etadilar va uni o‘zining muxim rekvizitlaridan, masalan, autentifikasiya axborotidan xabardor qiladilar. Xujumning 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 (8.17-rasm).



8.11-rasm. Foydalanishning yolg‘on nuqtasi

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. TCP/IPning ko‘pgina tarmoq ilovalari server va mijoz IP-adreslarining o‘zgarmasligini talab etadi, ammo tarmoqdagi rouming jarayonida abonent albatta uning bir joyini tark etib, boshqa joyiga qo‘shiladi. Simsiz tarmoqlarda mobil IP-adreslarning va boshqa rouming mexanizmlarining ishlatilishi ushbu talabga asoslangan.

8.5. Tarmoq orqali uzatiluvchi ma’lumotni shifrlash

Simsiz tarmoqlarda mavjud xavfsizlik protokollari

Bluetooth tizimida foydalanilgan kriptografik protokol

Bluetooth texnologiyasi haqidagi barcha ma’lumotlar Recommendations of the National Institute of Standards and Technology (NIST) universitetining 800-121 nashrida e’lon qilingan. Bluetooth standartida quyidagi xavfsizlik xizmatlari amalga oshirilgan:

- *Autentifikasiyalash.* Bluetooth qurilmalarining manzili orqali aloqa qurilmalarini tanib olish. Ushbu standartda haqiqiy foydalanuvchi autentifikasiyasi amalga oshirilmaydi.

- *Konfidensiyallik.* Ikki autentifikasiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo‘ladigan hujumlardan himoyalash uchun shifrlash amalga oshiriladi.

- *Avtorizasiyalash.* Ruxsat berilgan amallar bo‘yicha foydalanishga ruxsat berish.

Bluetooth standartda xavfsizlik amallari sanalgan auditlash, butunlik, rad eta olmaslik kabi amallarni qo‘llab quvvatlamaydi. Ushbu imkoniyatga ega bo‘lish uchun qo‘shimcha qurilma va jixoz kerak bo‘ladi.

Bluetooth standartda xavfsizlikning to‘rt xil rejimi amalga oshiriladi.

Birinchi rejimda ikki qurilma o‘zaro xavfsiz bo‘lmagan holda ulunadi. Aloqa ulanishda autentifikasiyalash va shifrlash amallaridan foydalanilmaydi.

Ikkinchi rejim kuchaytirilgan darajadagi xavfsizlik xizmatini ta’minlab, dastlab mantiqiy aloqa o‘rnatilib, shundan so‘ng kanal aloqasi o‘rnatiladi va xavfsizlik jarayonlari amalga oshiriladi. Ushbu rejimda autentifikasiyalash, shifrlash va avtorizasiyalash kabi xavfsizlik jarayonlari amalga oshiriladi.

Uchinchi rejim kuchaytirilgan kanal aloqasida xavfsizlikni ta’minlab, kanal aloqasi o‘rnatilmasdan oldin xavfsizlik ta’minlanadi. Ushbu rejimda mandatlangan autentifikasiya amalga oshiriladi va barcha ma’lumotlar shifrlangan holda yuboriladi.

To‘rtinchi rejimi ham ikkinchi rejim kabi, dastlab fizik va mantiqiy bog‘linishni talab etib, shundan so‘ng xavfsizlik amaliyotlarini amalga oshiradi. Ushbu rejimda Secure Simple Pairing (SSP) dan foydalaniladi. Oldingi rejimlarda esa “kanal kaliti” asosida kalitlarni taqsimlash amalga oshiriladi. Ya’ni, elliptik egri chiziqqa asoslangan Diffi-Xelman kalitlarni ochiq taqsimlash protokolidan foydalanadi.

WI-FI texnologiyasida foydalanilgan kriptografik protokollar

Simsiz lokal tarmoqlarda foydlanilgan WI-FI texnologiyasida quyidagi kriptografik protokollardan foydalanilgan:

- Wired Equivalent Privacy (WEP);
- Wi-Fi Protected Access (WPA) va uning ikkinchi varianti.

Wired Equivalent Privacy (WEP) xavfsizlik algoritmi IEEE 802.11 simsiz tarmoqlari uchun foydalanilib, IEEE 802.11 standarti 1999 yil sentyabr oyida qabud qilingan bo‘lib, simsiz tarmoqlarda (wireless LAN) ma’lumotni butunligini, autentifikasiya va to‘liqligini ta’minlashda foydalaniladi.

Ushbu protokolda 10 yoki 26 ta o‘n oltilik tizimdagi kalitdan foydalaniladi, va bu kalit dastlab routerni sozlashda foydalinilgan parol bilan bir xil bo‘ladi.

Ushbu protokolda quyidagi xavfsizlik amaliyotlaridan foydalanilgan:

- Autentifikasiyalash;
- Ma’lumotni butunligini ta’minlash;
- Ma’lumot maxfiylagini ta’minlash.

WEP da autentifikasiyalash. Ushbu protokolda ikki turdagi autentifikasiyalashdan foydalaniladi.

- Open System authentication;
- Shared Key authentication.

Birinchi usulda autentifikasiyalash amalga oshirilmay ixtiyoriy foydalanuvchi serverga bog‘lanishi mumkin. Ma’lumot WEP kaliti asosida shifrlanadi. foydalanuvchi serverga bog‘lanashi uchun kliyent to‘g‘ri kalitga ega bo‘lishi kerak.

Ikkinchi usulda WEP protokolida autentifikasiyalash uchun oddiy savol-javob tizimidan foydalanilgan. Jarayon ketma-ketligi quyidagicha:

1. Kliyent serverga (boshqaruv nuqtasiga) autentifikasiyalash so‘rovini yuboradi.
2. Server foydalanuvchiga tasodifiy sonni yuboradi (r, 128 bitdan katta bo‘lgan) .
3. Foydalanuvchi ushbu sonni umumiy kalit (boshqaruv nuqtasi paroli) bilan shifrlab yuboradi ($e_K(r)$).
4. Shifrmatnni ochish natijasiga qarab, autentifikasiyalashdan o‘tiladi yoki yo‘q.

WI-MAX texnologiyasida foydalanilgan protokollar

WI-MAX texnologiyasi haqidagi barcha ma’lumotlar Recommendations of the National Institute of Standards and Technology (NIST) universitetining 800-127 nashrida e’lon qilingan. IEEE 802.16 standartida xavfsizlikning ikkita masalasi autentifikasiyalash va maxfiylik ko‘rib chiqilgan bo‘lib, ushbu texnologiyada xavfsizlik uchta qadamda: autentifikasiyalash, kalitlarni boshqarish va ma’lumotni shifrlash amallari orqali taminlanadi.

Wi-MAX tarmoq arxitekturasi quyidagi beshta tashkil etuvchidan iborat:

Base Station (BS). Asos stansiya deb nomlanib, ikkita istemolchini operatorga ulash uchun xizmat qiladi.

Subscriber Station (SS). Ushbu foydalanuvchi stansiyalari asosan ko‘chmas bo‘lgan qurilmalarni o‘z ichiga oladi.

Mobile Station (MS). Ushbu tashkil etuvchilar asosan harakatlanuvchi qurilmalarni o‘z ichiga oladi (mobil telefonlar, noutbuklar).

Relay Station (RS). Ushbu tashkil etuvchi bir nechta SS stansiyalarni o‘z ichiga oladi.

Operator Network. Butun tizimni birlashtirib turuvchi tarmoq.

GSM simsiz WAN tarmoq protokoli

GSM (Global System for Mobile Communications) standarti European Telecommunications Standards Institute (ETSI) tashkiloti tomonidan raqamli mobil telefonlarning ikkinchi avlodi (second-generation (2G)) uchun ishlab chiqilgan protokoldir. 2016 yilga kelib ushbu standart, mobil aloqa uchun eng ko‘p foydalanilgan global standart sanalib, butun dunyo bozorida 90 % ulushni tashkil etib, 219 ta davlat bo‘ylab xizmat ko‘rsatmoqda.

2G texnologiyasi 1G analog texnologiyaning o‘zgarishidan kelib chiqqan bo‘lib, hozirda uchunchi avlod (3G) UMTS standarti va to‘rtinchi avlod (4G) LTE Advanced standartlari ham amalda foydalanilmoqda.

SIM karta o‘zida IMSI (International Mobile Subscriber Identity) raqamini, autentifikasiyalash kalit K_i, foydalanuvchi ma’lumoti va xavfsizlik algoritmlarini saqlaydi.

GSM standartida quyidagi uchta xavfsizlik algoritmlari foydalanilgan:

- A3 – autentifikasiyalash algoritmi;
- A8 – kalit generatori algoritmi;
- A5/1 – ma’lumotni shifrlash algoritmi.

GSM standartida foydalanuvchi dastlab, identifikasiyadan, autentifikasiyadan o‘tkaziladi va so‘ngra unga xizmat ko‘rsatiladi. GSM autentifikasiyalash mexanizmi oddiy savol-javob tizimi asosida amalga oshiriladi. Foydalanuvchi SIM kartaga ega bo‘lish jarayonida mobil tarmoq operatori (HLR) ham ushbu sim kartadagi ma’lumotlarni, K_i, IMSI raqami va h. larni o‘zida ko‘chirib oladi va o‘zida saqlaydi.

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Tarmoqlararo ekranlash nima?
2. Virtual xususiy tarmoqlarni tushuntiring.
3. Suqilib kirishlarni aniqlash tizimlari (Intrusion Detection System, IDS) nima?
4. Ma’lumotlarning sirqib chiqishini oldini olish tizimlari (Data Leakage Prevention, DLP) qanday ishlaydi?
5. Simsiz tarmoq nima?
6. Qanday simsiz tarmoq turlarini bilasiz?
7. Simsiz tarmoqlarga bo‘luvchi hujumlar haqida gapirib bering.

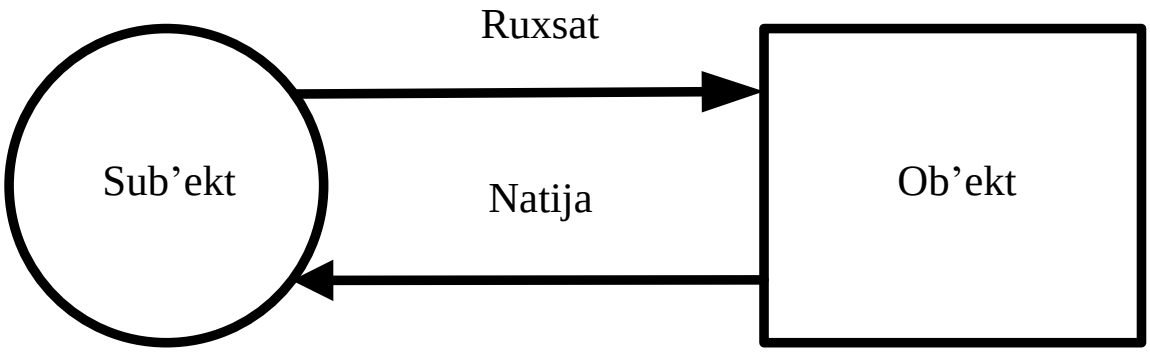
IX BOB. FOYDALANUVCHILIKNI TA’MINLASH USULLARI

9.1. Foydalanishni boshqarish

Foydalanishni boshqarish

Avtorizasiya ruxsatlarni nazoratlashning autentifikasiyadan o‘tgan foydalanuvchilar uchun harakatlarni cheklash bilan shug‘ullanuvchi qismi bo‘lib, aksariyat hollarda foydalanishni boshqarish modellari yordamida amalga oshiriladi. Ushbu ma’ruzada ma’lumotlarga nisbatan foydalanishni mantiqiy boshqarish tartibi bilan tanishib chiqiladi.

Foydalanishni boshqarish subyektni obyektga ishlash qobilyatini aniqlashdir. Umumiy holda foydalanishni boshqarish quyidagi diagramma bilan tavsiflanadi (9.1-rasm):



9.1-rasm. Foydalanishni boshqarish

Hozirda tizimlarda obyektlarni boshqarish uchun turlicha usullar mavjud bo‘lib, ularga quyidigalarni misol keltirish mumkin:

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

9.2. Foydalanishni diskresion boshqarish usuli (Discretionary access control, DAC)

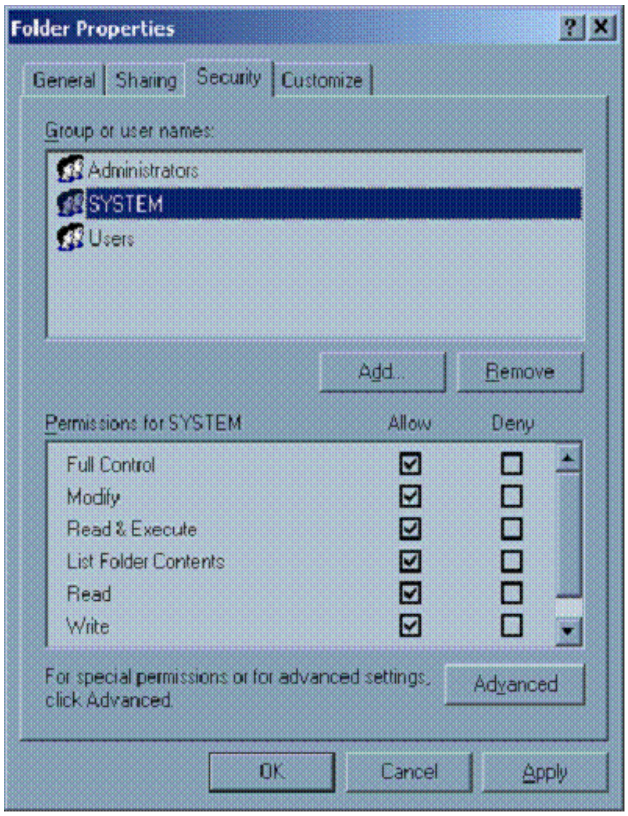
DAC usuli

Foydalanishni boshqarishning mazkur usuli tizimdagi shaxsiy obyektlarni himoyalash uchun qo‘llaniladi. Bunga ko‘ra obyekt

egasining o‘zi undan foydalanish huquqini va kirish turini o‘zi belgilaydi.

DAC da subyektlar tomonidan obyektlarni boshqarish subyektlarning identifikasiya axborotiga va asoslanadi. Masalan, UNIX operasion tizimida fayllarni himoyalashda, fayl egasi qolganlarga *o‘qish (r), yozish (w)* va *bajarish (x)* amallaridan bir yoki bir nechtasini berishi mumkin. Umumiy holda DAC usuli aksariyat operasion tizimlarda foydalanishlarni boshqarish uchun foydalaniladi. Masalan, quyidagi 9.3-rasmda DAC usulini Windows NT/2k/XP OTlarida foydalanish holati keltirilgan.

Biroq, DAC jiddiy kamchilikka ega. Bu holat ma’lumotlar undan foydalanish huquqiga ega bo‘lmagan subyektlar tomonidan foydalanilmasligini to‘liq kafolatlamaganidir. Bu holat ma’lumotni o‘qish huquqiga ega bo‘lgan bir foydalanuvchini ma’lumotni egasining ruxsatisiz huquqga ega bo‘lmagan foydalanuvchiga yuborish imkoniyati mavjudligida namayon bo‘ladi. Bundan tashqari, DACga tegishli yana bir kamchilik sifatida tizimdagi barcha obyektlar ulardan foydalanishni belgilaydigan suyektlarga tegishli. Amalda esa, tizimdagi barcha ma’lumotlar shaxslarga tegishli emas, balki butun tizimga tegishli bo‘ladi. Bularga yaqqol misol sifatida axborot tizimini keltirish mumkin.



9.2-rasm. Windows XP da DACdan foydalanish

DACning klassik tizimi dastlab obyekt hech kimga biriktirilmagan holatda “yopiq” deb ataladi. Agar obyekt foydalanuvchiga biriktirilsa va ulardan foydalanish bo‘yicha cheklovlar o‘rnatilgan bo‘lsa unda “ochiq” obyekt deb ataladi.

9.3. Foydalanishni mandatli boshqarish usuli (Mandatory access control, MAC)

Foydalanishning mazkur usulida foydalanish ruxsati obyektning egasi tomonidan amalga oshirilmaydi. Masalan, Alisa TOP SECRET ruxsatnomasiga ega bo‘lgan subyektlarga ruxsat bera olmaydi. Sababi u ushbu bosqichdagi hujjatlarni to‘liq nazorat qila olmaydi. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda xavfsizlik siyosati ma’muri tomonidan amalga oshiriladi. Bunda foydalanuvchi xavfsizlik siyosatini o‘zgartira olmaydi. DAC usulida esa obyektning egasi xavfsizlik siyosatini quradi va kimga foydalanish uchun ruxsat berilishini aniqlaydi.

MAS usuli o‘rnatilgan tizimlar xavfsizlik siyosati ma’muriga tashkilot bo‘ylab xavfsizlik siyosatini amalga oshirish imkoniyatini beradi. MAS usulida foydalanuvchilar tasodifan yoki qasddan ushbu siyosatni bekor qila olmaydilar. Bu esa xavfsizlik ma’muriga barcha foydalanuvchilar uchun bajarilishi kafolatlangan markaziy siyosatni belgilashga imkon beradi.

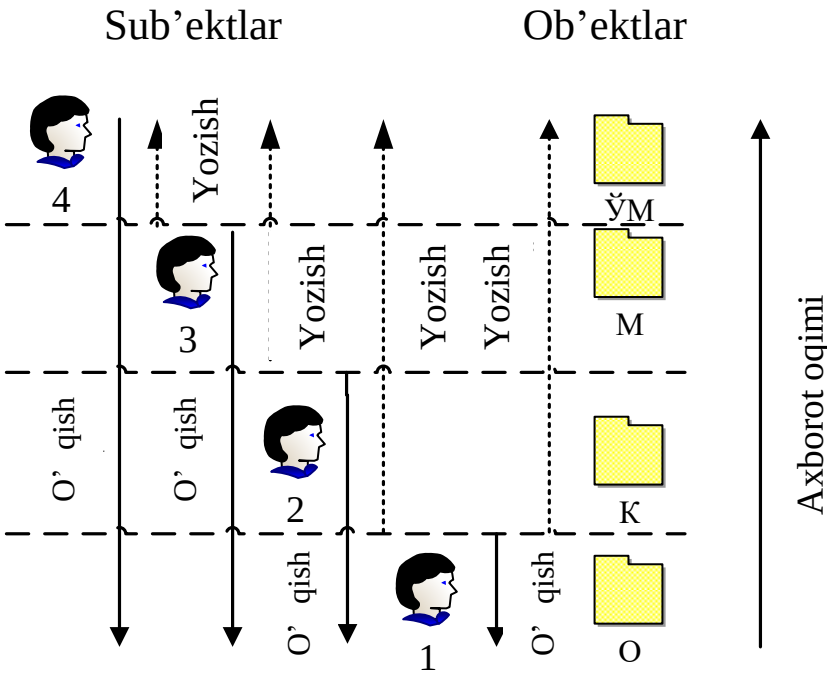
MAC usulida foydalanishlar subyektlar va obyektlar klassifikasiyalashga asosan boshqariladi. Tizimning har bir subyekti va obyekti bir nechta xavfsizlik darajasiga ega bo‘ladi. Obyektning xavfsizlik darajasi tashkilotda obyektning muhimlik darajasi bilan yoki yo‘qolgan taqdirda keltiradigan zarar miqdori bilanxarakterlanadi. Subyektning xavfsizlik darajasi esa unga ishonish darajasi bilan belgilanadi. Oddiy holda xavfsizlik darajasini: ЎТА МАХФИЙ (ЎМ), МАХФИЙ (М), КОНФИДЕНЦИАЛ (К) va ОЧИҚ (О) shaklida yoki: $ЎМ > М > К > О$.

MAS asosida axborot maxfiyligini ta’minlash

Agar obyekt va subyekning xavfsizlik darajalari orasidagi bir qancha bog‘liqliklar shartlari bajarilsa u holda subyekt obyektdan foydalanish huqiqiga ega bo‘ladi. Xususan, quyidagi shartlar bajarilish kerak:

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

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



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

Ushbu modelda foydalanuvchi va subyekt tushunchalri bir – biridan farq qiladi. Xavfsizlik darajasi subyektga beriladi. Foydalanuvchi esa u yoki bu vaqtda subyekt nomidan ish qilishi mumkin. Shuning uchun turli holatlarda bir foydalanuvchi turli subyekt nomidan ish ko‘rishi mumkin. Shu sababli, har bir aniq vaqtda foydalanuvchi faqat bitta subyekt nomidan ish qilishi muhim hisoblanadi. Bu axborotni yuqori sathdan quyi sathga uzatilmasligini ta’minlaydi.

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

1. Quyi sathli foydalanuvchi barcha yuqori sathli obyektlarga yozishi mumkin. Bu holda u o‘zining mavjud obyektini qayta yozishi mumkin va bu o‘chirishga tengdir. Ushbu kamchilikni yuqori darajadagi yozishni taqiqlash orqali yo‘q qilish mumkin. Ushbu sxemaning qoidalari quyidagicha bo‘ladi:

- agar subyektning xavfsizlik darajasi o‘zida obyektning xavfsizlik darajasini qamragan bo‘lsa, u holda o‘qish uchun ruxsat beriladi.

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

2. Diagrammadan ko‘rinib turgani kabi yuqori darajadagi ishonchga ega foydalanuvchilar xavfsizlik darajasi past bo‘lgan obyektlarni o‘zgartira olmaydilar. Ushbu muammoni hal qilishda foydalanuvchi turli hujjatlardan foydalanish uchun turli darajadagi ishonchga ega bo‘lgan subyektlar nomidan ish ko‘rishi mumkin. Ya’ni, “M” darajasiga ega foydalanuvchi “M”, “K” va “O” ishonch darajasidagi subyektlar nomidan ish ko‘rishi mumkin.

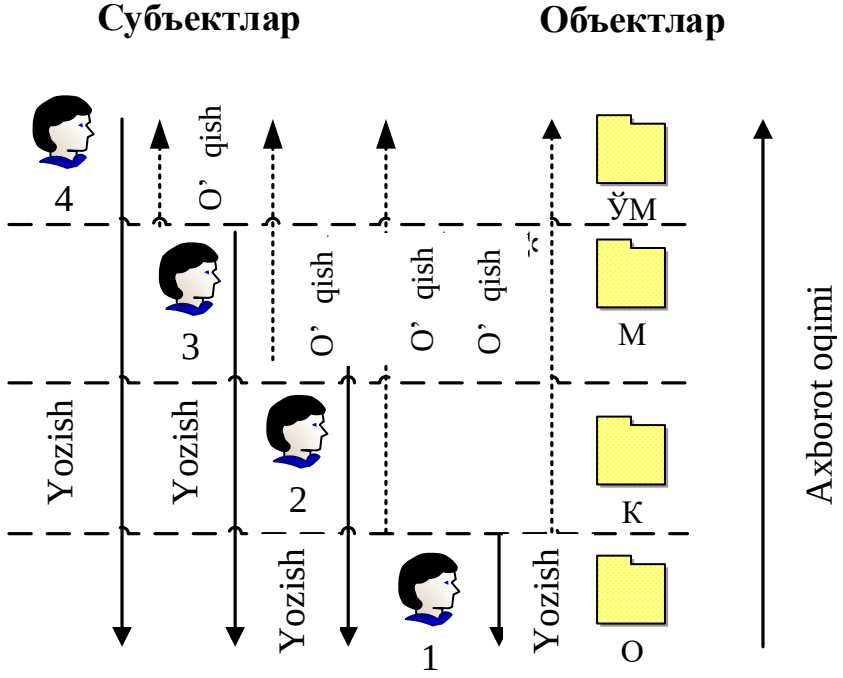
Axborot ishonchligini ta’minlash

Axborotni konfidensiyalligin ta’minlashdan tashqari, gohida axborot ishonchligini ta’minlash ham talab etiladi. Ya’ni, obyektning ishonchlik darajasi qanchalik yuqori bo‘lsa, uning ishonchligi shunchalik yuqori va subyektning xavfsizlik darajasi qanchalik yuqori bo‘lsa, u tizimga yanada ishonchli ma’lumotni kiritishi mumkin. Mazkur model uchun yuqorida keltirilgan qoidalarni quyidagicha o‘zgartirish kerak:

- agar subyektning xavfsizlik darajasida obyektning xavfsizlik darajasi mavjud bo‘lsa, u holda yozish uchun ruxsat beriladi.

- agar subyektning xavfsizlik darajasi obyektning xavfsizlik darajasida bo‘lsa, u holda o‘qishga ruxsat beriladi.

- Ko‘rinib turgani kabi ularning o‘rni almashgan (9.4-rasm).



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

MAC usulida xavfsizlik darajalaridan foydalanish bilan bir qatorda obyekt va subyektlarning kategoriyalaridan ham foydalanish mumkin. Bu holda xavfsizlik darajasidan tashqari har bir obyekt va subyektga tegishli bo‘lgan toifalar ro‘yxati berilishi mumkin. Obyektning kategoriyalari ushbu obyekt ishlatiladigan joylarni tavsiflash uchun ishlatilsa, subyektning kategoriyasi esa uning qaysi sohada ishlashini tavsiflaydi. Bundan tizim foydalanishlarni yanada batafsil boshqarish imkoniyatini beradi.

9.4. Foydalanishni rollarga asoslangan boshqarish usuli (Role-based access control, RBAC)

Foydalanishni boshqarishning rolli modeli (RBAC)

RBAC usulida foydalanishni boshqarishning asosiy g‘oyasi tizimning ishlash logikasini tashkilotda kadrlar vazifasini haqiqiy ajratilishiga maksimal darajada yaqinlashtirilgan.

RBAC usuli foydalanuvchini axborotga ruxsatini boshqarishda uning tizimdagi harakat xiliga asoslanadi. Ushbu usuldan foydalanish tizimdagi rollarni aniqlashni nazarda tutadi. Ro‘l tushunchasini muayyan faoliyat turi bilan bog‘liq harakatlar va majburiyatlar to‘plami sifatida belgilanishi mumkin. Shunday qilib, har bir obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o‘rniga, rol uchun obyektlardan foydalanish ruxsatini ko‘rsatish yetarli. Bunda foydalanuvchilar o‘z navbatida o‘zlarining rollarini ko‘rsatishadi. Biror rolni bajaruvchi foydalanuvchi rol uchun belgilangan foydalanish huquqiga ega bo‘ladi.

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

RBAC usulining asosiy afzalliklari quyidagilar:

1. Ma’murlashning osonligi

Foydalanishlarni boshqarishning klassik modellarida obyekt bo‘yicha muayan amallarni bajarish huquqlari har bir foydalanuvchi yoki foydalanuvchilar guruhi uchun ro‘yxatga olingan bo‘ladi. Rolli modelda rol va foydalanuvchi tushunchalarini ajratish vazifani ikki qismga ajratish imkonini beradi: foydalanuvchi rolini aniqlash va rol uchun obyektga ruxsatini aniqlash. Ushbu yondashuv boshqaruv

jarayonini sezilarli darajada osonlashtiradi. Chunki, foydalanuvchini javobgarlik sohasini o‘zgartirganda undan eski rolni olib tashlash va unga yangi vazifasiga mos kelidagan rolni berishning o‘zi kifoya qiladi. Agar foydalanish huquqi bevosita foydalanuvchi va obyektlar o‘rtasida aniqlansa, shu prosedura yangi foydalanuvchi huquqlarini qayta tayinlash uchun ko‘p harakatlarni talab qiladi.

2. Rollar iyerarxiyasi

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

3. Eng kam imtiyoz prinsipi

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

Eng kam imtiyoz prinsipi tizimdagi ma’lumotlarning ishonchligini ta’minlash uchun juda muhimdir. Bu foydalanuvchiga imkoniyatlari orasidan faqat muayan vazifani bajarishi uchun kerak bo‘lganini berilishini talab etadi. Buning uchun vazifa maqsadini aniqlash, uni bajarish uchun zarur bo‘lgan imtiyozlarni to‘plash va bu asosida foydalanuvchini imtiyozlari cheklash talab etiladi. Joriy vazifani bajarish uchun talab qilinmaydigan foydalanuvchi imtiyozlarini rad etish tizimning xavfsizlik siyosatini buzilishidan saqlaydi.

4. Majburiyatlarni ajratish

Tizimda foydalanishlarni boshqarishning yana bir muhim prinsiplaridan biri bu vazifalarni taqsimlashdir. Firibgarlikni oldini olish uchun bir shaxs tomonidan ko‘plab vazifalarni bajarib bo‘lmaydigan holatlar amalda yetarli mavjud. To‘lovni yaratish va uni tasdiqlash bunga misoldir. Shubhasiz bu amallarni bir shaxs bajara olmaydi. Rollarga asoslangan usul esa ushbu muammoni maksimal darajada osonlik bilan har qilishga yordam beradi.

9.5. Foydalanishni atributlarga asoslangan boshqarish usuli (Attribute-based access control, ABAC)

ABAC modeli

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

Attributga asoslangan siyosat normativ talablar murakkabligini kamaytirish orqali foydalanishni boshqarishni yanada samarali amalga oshiradi. Xuddi shu attributlarga asoslangan siyosat turli tizimlarda ishlatilishi mumkin. Bu bir tashkilotda yoki hamkorlikdagi tashkilotlarda resurslardan foydalanishda muvofiqlikni boshqarishga yordam beradi. Bunday markazlashgan foydalanishni boshqarish foydalanish ruxsati uchun yagona vakolatli manbani o‘z ichiga oladi. Bu esa har bir aniq tizim talablariga o‘z siyosati bilan moslikni tekshirishni talab etmaydi.

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

XACML standartida asosiy tushunchalar bular: qoida (rules), siyosat (policy), qoida va siyosatni mujassamlashtirgan algoritmlar (rule-combing algorithms), attributlar (attributes) (subyekt, obyekt, harakat va muhit shartlari), majburiyatlar (obligations) va maslahatlar (advices). Qoida markaziy element bo‘lib, o‘zida maqsad, ta’sir, shart, majburiyat va maslahatlarni o‘z ichiga oladi. Maqsad – bu subyekt obyekt ustida nima harakat qilishidir (o‘qish, yozish, o‘chirish va hak.). Ta’sir mantiqiy ifodalarga asoslangan bo‘ladi va tizim foydalanish uchun *ruxsat, taqiq, mumkin emas, aniqlanmagan* holatlaridan biri bo‘lgan ruxsatni berishi mumkin. *Mumkin emas* buyrug‘i mantiqiy shart noto‘g‘ri bo‘lganda qaytarilsa, ifodani hisoblash vaqtida yuzaga kelgan xatoliklar uchun *aniqlanmagan* ta’sirini ko‘rsatadi.

Qoidaga misol:

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 va hak.larda foydalanib kelinmoqda.

Foydalanishni boshqarish matrisasi

Avtorizasiyaning klassik ko‘rinishi Lampsonning foydalanishni boshqarish matrisasidan boshlanadi. Ushbu matrisa operasion tizimni barcha foydalanuvchilar uchun turli ma’lumotlarni boshqarishi xususisidagi qarorni qabul qilishi uchun zarur bo‘lgan barcha axborotni o‘z ichiga oladi.

Operasion tizimdagi foydalanuvchilar *subyekt* sifatida va tizim resurslari *obyekt* sifatida qaraladi. Avtorizasiya sohasidagi ikkita asosiy qurvchilar: *foydalanishni boshqarish ro‘yxati (Access control list, ACL)* va *imtiyozlar ro‘yxati (Capability list, C-list)* hisoblanib, har ikkalasi ham Lampsonning foydalanishni boshqarish matrisasidan olingan. Ya’ni, matrisaning satrlari subyektlarni va ustunlari obyektlarni ifodalaydi. Bundan ko‘rinib turibdiki, biror subyekt S ga va obyekt O uchun berilgan imtiyozlar ularning matrisadagi indekslari kesishgan nuqtada saqlanadi. Quyidagi 9.1-jadvalda foydalanishni boshqarish matrisasi keltirilgan bo‘lib, unda imtiyozlar UNIX operasion tizimidagi imtiyozlar shaklida, ya’ni, x, r ва w lar mos ravishda *bajarish, o‘qish* va *yozish* amalini anglatadi.

9.1-jadval

Foydalanishni boshqarish matrisasi

	OT	Buxgalteriyaga oid dastur	Buxgalteriyaga oid ma’lumot	Sug‘urta ma’lumoti	To‘lov qaydnomasi ma’lumoti
Bob	rx	rx	r	-	-
Alisa	rx	rx	r	rw	rw
Sem	rwx	rwx	r	rw	rw
Buxgal-teriyaga oid dastur	rx	rx	rw	rw	r

Yuqoridagi jadvalda aks ettirilgani kabi, buxgalteriyaga oid dastur ham subyekt ham obyekt sifatida olingan. Bu foydali tanlov bo‘lib, buxgalteriyaga oid ma’lumotlarni faqat buxgalteriyaga oid dastur tomonidan boshqarish imkonini beradi. Ya’ni, turli buxgalteriya tekshiruvlari va balans haqidagi ma’lumotlar faqat buxgalteriyaga oid dasturiy ta’minot tomonidan boshqarishilishi shart va yuqoridagi matrisada keltirilgan shakl buni ta’minlaydi. Biroq, bu matrisa bo‘lishi mumkin bo‘lgan barcha hujumlarni oldini olmaydi. Chunki, tizim ma’muri Sem buxgalteriga oid dasturni noto‘g‘ri versiya bilan almashtirish yoki soxta versiya bilan almashtirish orqali ushbu himoyani buzishi mukin. Ammo bu usul Alisa va Bobga buxgalteriya ma’lumotlariga qasddan yoki bexosdan buzilishiga yo‘l qo‘ymasdan kirish huquqini beradi.

ACL yoki S-list

Foydalanishni boshqarish jadvalida barcha subyektlar va barcha obyektlar mavjudligi tufayli, u avtorizasiya qarorlari asoslangan barcha ma’lumotlardan tashkil topgan. Biroq, katta foydalanishni boshqarish matrisasini boshqarish amaliy tomondan mushkul. Yuzlab (yoki undan ko‘p) subyektlar va minglab (yoki undan ko‘p) obyektlar mavjud bo‘lgan tizimda, millionlab (yoki undan ko‘p) yozuvlarga ega bo‘lgan foydalanishni boshqarish matrisasi har qanday obyektga har qanday subyekt tomonidan bajariladigan ishlar uchun tekshirishili shart. Buni hisoblash tizim uchun katta yuklamani keltirib chiqaradi.

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

$$(\text{Боб}, -), (\text{Алиса}, rw), (\text{Сем}, rw), (\text{бухгалтерияга оид дастур}, rw)$$

Alternativ holatda, foydalanishni boshqarish matrisasini satrlar bo‘yicha saqlash 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 matrisasining mazkur satriga qaraladi. Mazkur yondashuv imtiyozlar ro‘yxati kabi yoki C-list deb ataladi.

Ya’ni, ACL uchun ko‘rsatkich resurslardan foydalanuvchilarga qarab yo‘nalgan bo‘lsa, C-list uchun esa ko‘rsatkichlar foydalanuvchilardan resurslarga qarab yo‘nalgan. Bu ko‘ringan ahamiyatsiz farq muhim ahamiyatga ega. Xususan, imtiyozlar (C-list) bilan foydalanuvchilar va fayllar orasidagi aloqadorlik tizim ichida quriladi. ACLga asoslangan tizimda esa, foydalanuvchilarni faylga aloqadorligi uchun alohida usullar talab etiladi. Bundan kelib chiqadiki, C-list ACL ga nisbatan bir qancha xavfsizlik afzalliklariga ega va shuning uchun C-list akademik tadqiqot olamida ancha pastroqda.

Tartibsiz yordamchi

Tartibsiz yordamchi bu – ko‘p jabhalarda klassik xavfsizlik muammosi hisoblanadi. Ushbu muammoni yoritish uchun, ikkita resursga ega tizim olingan: birinchi resurs kompilyator bo‘lsa, ikkinchisi maxfiy to‘lov axborotidan iborat bo‘lgan BILL deb nomlangan fayl va bir foydalanuvchi, Alisadan iborat. Kompilyator ixtiyoriy faylga yozish imkoniyatiga ega. Alisa kompilyatorni ishga tushira oladi va buni uchun debaggerlash ma’lumoti yoziluvchi fayl nomini kiritishi talab etiladi. Biroq, Alisaga BILL nomli faylni zararlashi mumkinligi sababli, unga yozish ruxsati mavjud emas. Ushbu senariy uchun foydalanishni boshqarish matrisasi quyidagi 9.2-jadvalda keltirilgan.

9.2-jadval

Tartibsiz yordamchi holati uchun foydalanishni boshqarish matrisasi

	Kompilyator	BILL
Alisa	x	-
Kompilyator	rx	rw

Faraz qilinsin, Alisa kompilyatorni ishga tushirdi va fayl nomi sifatida BILL ni ko‘rsatdi. Alisa ushbu imtiyozga ega bo‘lmagani uchun, mazkur buyruq amalga oshirilmaydi. Biroq, Alisa nomidan ish ko‘ruvchi kompilyator BILL faylini qayta yozish imkoniyatiga ega.

ACL bilan mazkur holatini oldini olish juda ham murakkab (lekin imkonsiz emas). Boshqa tomondan, C-list bilan buni osonlikcha bartaraf etish mumkin. Imtiyozga asoslangan tizimlarda, Alisa kompilyatorga murojaatni amalga oshirganda, unga o‘zining C-listni beradi. Bu holda kompilyator Alisaning C-listini tekshiradi va agar

imtiyozi bo‘lgan taqdirda debag faylni yaratadi. Alisani BILL faylini qayta yozishga ruxsati bo‘lmagani sababli, 9.8-rasmdagi holat kuzatilmaydi.

ACL va C-listni foydali tomonlarini o‘zaro solishtirish juda ham foydali. ACL odatda foydalanuvchi o‘zining ma’lumotlarini boshqarsa va himoya ma’lumotga qaratilgan hollarda afzal ko‘riladi. Bundan tashqari ACL bilan biror resursga huquqlarni almashtirish oson. Boshqa tomondan, imkoniyatlar bilan (C-list) vakolatlar berish oson va foydalanuvchi qo‘shish yoki o‘chirish juda ham oson. Vakolat berish qobilyati tufayli tartibsiz yordamchi muammolaridan osonlik bilan qochish mumkin. Biroq, imkoniyatlarni amalga oshirish biroz murakkab va yuqori xarajatni talab etadi. Bu aniq bo‘lmasligin mumkin bo‘lsada, taqsimlangan tizimlarga xos bo‘lgan ko‘plab muammolar imkoniyatlar nuqtai nazaridan kelib chiqadi. Shu sababli, ACL hozirgi kunda amaliyotda C-listdan ko‘ra ko‘p foydalaniladi.

9.6. Ko‘p sathli xavfsizlik modellari

Ushbu bo‘limda ko‘p sathli xavfsizlik sohasida xavfsizlik modellarini qarab chiqamiz. Xavfsizlik modellari odatda xavfsizlik oid darsliklarda katta hajmda tushuntiriladi. Ammo, bu yerda biz ikkita aniq xavfsizlik modeliga to‘xtalib o‘tamiz.

Umuman olganda xavfsizlik modellari tavsif bo‘lib, taqiqlanadigan narsa emas. Ya’ni mazkur modellar himoyalanish uchun nima kerakligini aytadi. Biroq ular haqiqiy savolga javob bermaydi, ya’ni, bunday himoyani qanday ta’minlash kerakligini aytmaydi. Bu modellarning kamchiligi emas, sababi ular himoya uchun asos yaratishga mo‘ljallangan. Biroq, bu xavfsizlik modellashtirishining amaliy yordamiga xos bo‘lgan cheklovdir.

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

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

TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED (9.1)

Masalan, SECRET ruxsatnomasiga ega subyektga SECRET yoki undan kichik klassdagi ma’lumotlardan foydalanish imtiyozi mavjud. Biroq TOP SECRET klassidagi ma’lumotdan foydalanish imtiyoziga ega emas.

Faraz qilaylik O obyekt bo‘lsa, S unda subyekt bo‘lsin. U holda O klassifikasiyani va S ruxsatnomani anglatadi. O ning xavfsizlik sathi $L(O)$ sifatida va S ning xavfsizlik sathi $L(S)$ kabi belgilanadi. DOD tizimida (11.1) tengligida ko‘rsatilgan 4 ta sathli klassifikasiyalash va ruxsatnomalardan foydalaniladi. Shuningdek, SECRET ruxsatnomasini oluvchi shaxs uchun, ko‘p yoki kam muntazam orqavarotdan tekshiruvlar talab etiladi. TOP SECRET uchun esa keng qamrovli tekshiruv, poligraf tekshiruvi, psixologik holati va boshqalar talab etiladi.

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

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

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

9.7. Bell-LaPadula modeli

Birinchi ko‘rib o‘tiluvchi xavfsizlik modeli Bell-Lapadula (Bell-LaPadula, BLP) bo‘lib, bu nomlanish uning yaratuvchilari Bell va Lapadula nomlariga berilgan. BLPning asosiy maqsadi har qanday MLS tizimini qanoatlantirishi kerak bo‘lgan konfidensiallikka nisbatan

minimal talablarni to‘plashdir. BLP quyidagi ikki formulirovkadan tashkil topgan:

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

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

Xavfsizlikni oddiy shartiga ko‘ra Alisa tegishli ruxsatnomasi bo‘lmagan hujjatni o‘qiy olmaydi. Ushbu shart har qanday MLS tizimida aniq talab etiladi.

Bu yerda erkinlikni cheklash xususiyati unchalik yoritilmagan. Ushbu xususiyat masalan TOP SECRET axborotni SECRET hujjatda yozilishidan himoyalashni ta’minlaydi. Bu MLS xavfsizligini buzadi, chunki SECRET darajasiga ega foydalanuvchi TOP SECRET klassidagi ma’lumotni o‘qiy oladi. Yozish qasddan yoki masalan kompyuter virusi natijasida yuzaga kelishi mumkin.

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

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

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

9.8. Biba modeli

Ushbu bo‘limda Biba modeli bilan tanishib o‘tiladi. BLP modeli konfidensiallik bilan shug‘ullangan bo‘lsa, Biba modeli butunlik bilan shug‘ullanadi. Boshqa so‘z bilan aytganda, Biba modeli BLPning butunlikni ta’minlash versiyasi hisoblanadi.

Agar biz O_1 obyektning butunligiga ishonsak, biroq O_2 obyektning butunligiga ishonmasak, u holda obyekt O ikkita O_1 va O_2 obyektlardan yaratilgan bo‘lsa, u holda obyekt O ning butunligiga ishonmaymiz. Boshqa so‘z bilan aytilganda obyekt O ning butunligi uni tashkil etgan ixtiyoriy obyektning minimal butunlik darajasidan iborat. Boshqacha aytganda, butunlik uchun “past suv belgisi prinsipi” o‘rinli. Boshqa tomondan, konfidensiallik uchun “yuqori suv belgisi prinsipi” o‘rinli.

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

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

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

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

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

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

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

9.9. Mantiqiy va fizik foydalanishlarni boshqarish

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

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Foydalanishni boshqarish qanday amalga oshiriladi?
2. Foydalanishni diskresion boshqarish usuli (Discretionary access control, DAC)ni tushuntirib bering.
3. Foydalanishni mandatli boshqarish usuli (Mandatory access control, MAC)ni tushuntirib bering.
4. Foydalanishni rollarga asoslangan boshqarish usuli (Role-based access control, RBAC)ni tushuntirib bering.
5. Foydalanishni atributlarga asoslangan boshqarish usuli (Attribute-based access control, ABAC) ni tushuntirib bering.
6. Ko‘p sathli xavfsizlik modellari nima?
7. Bell-LaPadula modeli nima?
8. Biba modelini tushuntiring

X BOB. DASTURIY VOSITLAR XAVFSIZLIGI

10.1. Axborotlarga nisbatan mavjud xavfsizliklarning asosiy tushunchalari va uning tasnifi

Tez rivojlanib borayotgan kompyuter axborot texnologiyalari bizning kundalik hayotimizning barcha jabxalarida sezilarli uzgarishlarni olib kirmokda. Hozirda "axborot tushunchasi" sotib olish, sotish, biror boshka tovarga almashtirish mumkin bulgan maxsus tovar belgisi sifatida tez-tez ishlatilmokda. Shu bilan birga axborotning bahosi kup hollarda uning uzi joylashgan kompyuter tizimining bahosida bir necha yuz va ming barobarga oshib ketmoqda. Shuning uchun tamomila tabiiy holda axborotni unga ruxsat etilmagan holda kirishdan, qasddan o‘zgartirishdan, uni o‘girlashdan, yuqotishdan va boshqa jinoiy xarakterlardan himoya qilishga kuchli zarurat tug‘iladi. Ammo, jamiyatning avtomatlashtirishning yuqori darajasiga intilishi uni foydalaniladigan axborot texnologiyalarning xavfsizligi saviyasiga bog‘liq qilib qo‘yadi. Haqiqatan, kompyuter tizimlarining keng ko‘lamda ishlatilishi doimo o‘sib boruvchi axborot hajmini ishlash jarayonlarini avtomatlashtirishga imkon bersada, bu jarayonlarni agressiv ta’sirlarga nisbatan ojiz qilib qo‘yadi va, demak, axborot texnologiyalardan foydalanuvchilar oldida yangi muammo-axborot xavfsizlik muammosi kundalang bo‘ldi. Xavfsizlik muammosi, aslida, yangi muammo emas, chunki xavfsizligini ta’minlash har qanday tizim uchun, uning murakkabligi, tabiatidan qat’iy nazar, birlamchi vazifa hisoblanadi. Ammo, himoyalanuvchi obyekt axborot tizimi bo‘lsa, yoki agressiv ta’sir vositalari axborot shaklda bo‘lganda, himoyaning mutloq yangi texnologiyalarini va usullarini yaratishga tug‘ri keladi. Ma’lumotlarni himoyalovchi usullar hamda xakerlarga qarshi harakat vositalar majmuasini belgilash maqsadida kompyuter xavfsizligi atamasi ishlatila boshlandi.

Ma’lumotlarni ishlovchi taqsimlangan tizimlarning paydo bo‘lishi xavfsizlik masalasiga yangicha yondashishning shakllanishiga olib keldi. Ma’lumki, bunday tizimlarda tarmoqlar va kommunikatsion uskunalar foydalanuvchilarning terminallari bilan markaziy kompyuterlar o‘rtasida ma’lumotlar almashishga xizmat qiladi. Shu sababli ma’lumotlar uzatiluvchi tarmoqlarni himoyalash zaruriyati tug‘ildi va shuning bilan birga tarmoq xavfsizligi atamasi paydo bo‘ldi.

Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun xam qadimda axborotni himoyalash uchun turli xil

usullar qo‘llanilgan. Ulardan biri - sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o‘qiy olmagan. Asrlar davomida bu san’at - sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidensiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o‘n yil oldin hamma narsa tubdan uzgardi, ya’ni axborot o‘z qiymatiga ega bo‘ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o‘g‘irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug‘iladi.

Axborotni himoya qilish deganda:

Axborotning jismoniy butunligini ta’minlash, shu bilan birga axborot elementlarining buzilishi, yoki yo‘q qilinishiga yo‘l qo‘ymaslik;

Axborotning butunligini saqlab qolgan holda, uni elementlarini qalbakilashtirishga (uzgartirishga) yo‘l qo‘ymaslik;

Axborotni tegishli huquqularga ega bo‘lmagan shaxslar yoki jarayonlar orqali tarmoqdan ruxsat etilmagan holda olishga yo‘l qo‘ymaslik;

Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar faqat tomonlar o‘rtasida kelishilgan shartnomalar asosida qo‘llanilishiga ishonish kabilar tushuniladi.

Yuqorida ta’kidlab o‘tilganlarning barchasi asosida kompyuter tarmoqlari va tizimlarida axborot xavfsizligi muammosining dolzarbligi va muhimligi kelib chiqadi. Kompyuter tizimlari va tarmoqlarida axborotni himoya ostiga olish deganda, berilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta’minlash maqsadida turli vosita va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Ushbu axborot xavfsizligining vazifalari:

Kompyuter tarmoqlari va tizimlarida axborot xavfsizligi tug‘risidagi bilimlarni shakllantirish;

Axborotni himoya qilishning nazariy, amaliy va uslubiy asoslarini berish;

Kompyuter tarmoqlari va tizimlarida axborot xavfsizligini ta’minlashning zamonaviy usullari va vositalarini qo‘llashni amaliy jixatdan o‘rgatish;

Axborotni himoya qilish bo‘yicha ishlab chiqarilgan turli xil dasturiy mahsulotlardan erkin foydalana olish imkonini beradigan bilimlar bilan ta’minlash;

Axborotni uzatishda xavfsizlikni ta’minlashga qo‘yiladigan talablarni bevosita quyidagi atamalardan aniqlash mumkin: konfidenqiallik, autentifikatsiya, yaxlitlikni saqlash, yolg‘onning mumkin emasligi, foydalanuvchanlik, foydalanuvchanlikni boshqarish.

Ko‘p hollarda yaratuvchi e’tiboridan chetda qolgan himoya tizimining kamchiliklarini aniqlash maqsadida muammoga qarshi tomonning nuqtai nazaridan qarash lozim. Boshqacha aytganda, himoyaning u yoki bu mexanizmi yoki algoritmini yaratishda mumkin bo‘lgan qarshi choralarni ham ko‘rish lozim.

Himoya vositalaridan barcha qarshi choralar majmuasini hisobga olgan holda foydalanish lozim.

Xavfsizlikni ta’minlash choralari tizimi yaratilganidan so‘ng bu choralarni qachon va qayerda qo‘llash masalasini yechish lozim. Bu fizikaviy joy (ma’lum himoya vositasini qo‘llash uchun tarmoq nuqtasini tanlash) yoki xavfsizlikni ta’minlovchi mantiqiy zanjirdagi joy (masalan, axborot uzatuvchi protokol satxi yoki satxlarini tanlash) bo‘lishi mumkin.

Himoya vositalari, odatda, ma’lum algoritm va protokoldan farqlanadi. Ularga binoan barcha himoyadan manfaatdor axborotining qandaydir qismi maxfiy bo‘lib qolishi shart (masalan, shifr kaliti ko‘rinishida). Bu esa o‘z navbatida bunday maxfiy axborotni yaratish, taqsimlash va himoyalash usullarini ishlab chiqish zaruriyatini tug‘diradi.

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

Axborot xavfsizligi deb, ma’lumotlarni yo‘qotish va o‘zgartirishga yo‘naltirilgan tabiiy yoki sun’iy xossali tasodifiy va qasddan ta’sirlardan har qanday tashuvchilarda axborotning himoyalanganligiga aytiladi. Ilgarigi xavf faqatgina konfidensial (maxfiy) xabarlar va hujjatlarni o‘g‘irlash yoki nusxa olishdan iborat

bo‘lsa, hozirgi paytdagi xavf esa kompyuter ma’lumotlari to‘plami, elektron ma’lumotlar, elektron massivlardan ularning egasidan ruxsat so‘ramasdan foydalanishdir. Bulardan tashqari, bu harakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zahiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta’minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotni himoyalashning maqsadlari quyidagilardan iborat:

axborotning kelishuvsiz chiqib ketishi, o‘g‘irlanishi, yo‘qotilishi, o‘zgartirilishi, soxtalashtirilishlarning oldini olish;

shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf - xatarning oldini olish;

axborotni yo‘q qilish, uzgartirish, soxtalashtirish, nusxa ko‘chirish, to‘siqlash bo‘yicha ruxsat etilmagan harakatlarning oldini olish;

-hujjatlashtirilgan axborotning miqdori sifatida huquqiy tartibini ta’minlovchi, axborot zahirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko‘rinishlarining oldini olish;

axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning shaxsiy maxfiyligini va konfidensialligini saqlovchi fuqarolarning konstitusion huquqlarini himoyalash;

davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidensialligini saqlash;

-axborot tizimlari, texnologiyalari va ularni ta’minlovchi vositalarni yaratish, ishlab chiqish va qo‘llashda subyektlarning huquqlarini ta’minlash.

Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izoxlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikasiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng ko‘llanilmoqda (iqtisod, fan, ta’lim, harbiy ish, turli texnologiyalarni boshqarish va h.k.)

Milliy iqtisodda axborotlarni yaratish, tarqatish, qayta ishlash va foydalanish jarayoni hamda vositalarini qamrab olgan Yangi tarmoq vujudga keldi. «Milliy axborot resursi» tushunchasi Yangi iqtisodiy kategoriya bo‘lib xizmat qilmoqda. Davlatning axborot resurslariga

keltirilayotgan zarar axborot xavfsizligiga ham ta’sir kursatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakllantirish va uning asosida jahon yagona axborot maydoniga kirib borish natijasida milliy iqtisodimizga turli xildagi zararlar keltirish xavfi paydo bo‘lmoqda.

Mudofaa xavfsizligi. Mudofaa sohasida xavfsizlikning asosiy obyektlaridan bo‘lib, mamlakatning mudofaa potensialining axborot tarkibi va axborot resurslari hisoblanmoqda. Hozirgi kunda barcha zamonaviy qurollar va harbiy texnikalar juda ham kompyuterlashtirilib yuborildi. Shuning uchun ham ularga axborot qurollarini qo‘llash ehtimoli katta.

Zamonaviy axborot - kommunikasiyalar texnologiyalarining milliy iqtisod barcha tarmoqlarida keng qo‘llanishi inson psixologiyasi va jamoa ongiga «yashirin» ta’sir kursatish vositalarining samaradorligini yuksaltirib yubordi.

Ekologik xavfsizlik - global masshtabdagi muammodir. «Ekologik toza», energiya va resurs tejaydigan, chikindisiz texnologiyalarga o‘tish faqat milliy iqtisodni axborotlashtirish hisobiga qayta qurish asosidagina yo‘lga qo‘yish mumkin.

Axborotlarga nisbatan xavf-xatarlar tasnifi

Xavfsizlik siyosatining eng asosiy vazifalaridan biri himoya tizimida potensial xavfli joylarni qidirib topish va ularni bartaraf etish hisoblanadi. Tekshirishlar shuni kursatadiki, tarmoqdagi eng katta xavflar — bu ruxsatsiz kirishga mo‘ljallangan maxsus dasturlar, kompyuter viruslari va dasturning ichiga joylashtirilgan maxsus kodlar bo‘lib, ular kompyuter tarmoqlarining barcha obyektlari uchun katta xavf tug‘diradi.

Tashkilotning himoyalash tizimiga bo‘lgan haqiqiy ehtiyojini aniqlash va xavfsizlikning mavjud barcha xilma-xil choralaridan kerakligini tanlashda turli yondashishlardan foydalaniladi. Bunday yondashishlardan biri axborot himoyasining quyidagi uchta jiuatiga asoslangan.

Ximoyaning buzilishlari - bu korxonaga tegishli axborotni saqlash va ishlatish xavfsizligiga zarar keltiruvchi har qanday harakatlar.

Himoya mexanizmi deganda, himoyaning buzilishlarini aniqlash va bartaraf etish, hamda buzilishlar oqibatini yuqotish mexanizmlari tushuniladi.

Himoya xizmati - bu ma’lumotlarni ishlash tizimlari va korxonaga tegishli axborotni tashish xavfsizligi saviyasini k o‘tarishga mo‘ljallangan servis xizmati.

Himoyaning buzilishi. Kompyuter tizimi yoki tarmog‘i himoyasini buzishga urinishlarni kompyuter tizimini axborotni ta’minlovchi obyekt sifatida ko‘rish orqali klassifikasiyalash mumkin. Umumiy holda qandaydir manbadan(masalan, fayl yoki xotira qismi) axborot oqimining adresatga (masalan, boshqa fayl yoki bevosita foydalanuvchi) uzatilishi kuzatiladi. Shu nuqtai nazardan quyidagi hujumlarni farqlash mumkin:

Uzish (razyedineniye);

Ushlab qolish (perexvat);

Turlash (modifikasiya);

Soxtalashtirish (falsifikasiya).

Uzish (razyedineniye). Tizim resursi yo‘q qilinadi, axborotdan foydalanuvchanlik buziladi. Bunday buzilishlarga misol tariqasida uskunaning ishdan chiqishi, aloqa liniyasining uzilishi yoki fayllarni boshqaruvchi tizimning buzilishini ko‘rsatish mumkin.

Ushlab solish (perexvat). Resursdan ruxsat berilmagan foydalanishga yo‘l ochiladi. Natijada axborotning maxfiyligi (konfidensialligi) buziladi. Bunday foydalanuvchilar fizik shaxs, dastur yoki kompyuter bo‘lishi mumkin. Bunday buzilishlarga misol tariqasida ma’lumotlarni ushlab solish maqsadida aloqa kabeliga ulanish va fayllardan yoki dasturlardan noqonuniy nusxa ko‘chirishni ko‘rsatish mumkin.

Turlash (modifikasiya). Resursdan nafaqat noqonuniy foydalanishga yo‘l ochiladi, balki resurs buzg‘unchi tomonidan o o‘zgartiriladi. Natijada axborotning yaxlitligi buziladi. Bunday buzilishlarga misol tariqasida fayldagi ma’lumotlar mazmunini o‘zgartirilishini, dasturning vazifalari va xarakteristkalarini o‘zgartirish maqsadida uni modifikasiyalashni, tarmoq orqali uzatilayotgan axborotlar mazmunini uzgartirilishini va hokozolarni ko‘rsatish mumkin.

Soxtalashtirish (falsifikasiya). Tizimga soxta obyekt kiritiladi. Natijada axborotning asliga to‘g‘riligi (autenticnostligi) buziladi. Bunday buzilishlarga misol tariqasida tarmoq orqali yasama ma’lumotlarni uzatish yoki faylga yozuvlarni sushishni ko‘rsatish mumkin.

Yuqorida keltirilgan buzilishlar passiv va aktiv hujum atamalari bo‘yicha klassifikasiyalanganida passiv tahdidga ushlab solish(perexvat) mansub bo‘lsa, uzish(razyedineniye), turlash(modifikasiya) va soxtalashtirish(falsifikasiya) aktiv tahdidga mansub ekanligini ko‘rish qiyin emas.

Passiv xujumlar natijasida uzatilayotgan ma’lumotlar ushlab solinadi yoki monitoring amalga oshiriladi. Bunda buzgunchining massadi uzatilayotgan axborotni ushlab solishdir. Passiv buzilishlarni ikkita guruxga ajratish mumkin- axborotlar mazmunini fosh etish va ma’lumotlar osimini taxlil etish.

Axborotlar mazmunini fosh etish nima ekanligi ma’lum. Telefon orsali suxbatda, elektron pochta axborotida yoki uzatilayotgan faylda muxim yoki maxfiy axborot bulishi mumkin. Tabiiyki, bunday axborot bilan bu axborot muljallanmagan shaxslarning tanishishi masbul emas.

Ma’lumotlar oqimining tahlili mukammalroq hisoblanadi. Faraz qilaylik, biz axborot yoki boshqa uzatiluvchi ma’lumotlar mazmunini shunday maskirovka qilaylikki, buzg‘unchi axborotni o‘z ixtiyoriga kiritganida ham undagi axborotni chiqarib ololmasin. Ko‘pincha axborot mazmunini maskirovka qilishda shifrlash qo‘llaniladi. Ammo, axborot mazmuni shifrlash yordamida ishonchli tarzda berkitilgan b maskirovka bo‘lsada, buzg‘unchida uzatiluvchi ma’lumotlarning o‘ziga xos alotomatlarini kuzatish imkoniyati qoladi. Masalan, uzatuvchini va axborotlarni uzatishga ishlatiluvchi uzellarni, axborotlar uzunligini va ularning almashinuv chastotasini aniqlash mumkin. Bunday axborot ma’lumotlar almashinuvidan ko‘zlangan maqsadni aniqlashda juda ham qo‘l kelishi mumkin.

Himoyaning passiv buzilishlarini aniqlash juda qiyin, chunki ularda ma’lumotlarga qandaydir uzgartirishlar kiritish ko‘zda tutilmaydi. Ammo, bunday xil buzilishlarni oldini olishni amalga oshirsa bo‘ladi. Shu sababli passiv buzilishlar holida e’tiborni ularni aniqlashga emas, balki ularni oldini olishga qaratish lozim.

Aktiv hujumlar natijasida ma’lumotlar oqimi o‘zgartiriladi yoki soxta oqimlar hosil qilinadi. Bunday buzilishlarni to‘rtta guruhga ajratish mumkin: imitasiya, tiklash, axborotni turlash (modifikasiyalash), xizmat ko‘rsatishdagi xalallar.

Imitasiya deganda obyektning o‘zini boshqa obyekt qilib ko‘rsatishi tushuniladi. Odatda imitasiya aktiv buzilishlarning boshqa bir xilining urinishi bilan birgalikda bajariladi. Masalan, buzg‘unchi tizimlar almashinayotgan autentifikasiya ma’lumotlarining oqimini

ushlab qolib so‘ngra autentifikasiya axborotlarining haqiqiy ketma-ketligini tiklashi mumkin. Bu esa vakolati chegaralangan obyektning o‘zini vakolati kengroq obyekt qilib ko‘rsatishi (imitasiya) orqali vakolatini kengaytirishiga imkon beradi.

Tiklash deganda ma’lumotlar blokini passiv ushlab qolib, keyin uni ruxsat berilmagan natijani hosil qilish maqsadida retranslyasiya qilish tushuniladi.

Ma’lumotlarni modifikasiyalash deganda ruxsat berilmagan natijani hosil qilish maqsadida qonuniy axborot qismini o‘zgartirish, yoki axborot kelishi ketma-ketligini uzgartirish tushuniladi.

Xizmat kursatishdagi xalallar aloqa yoki ularni boshqaruvchi vositalarning normal ishlashiga to‘sqinlik qiladi. Bunday buzilishlarda muayyan maqsad ko‘zlanadi: masalan, obyekt ma’lum adresatga yo‘naltirilgan barcha axborotlarni to‘xtatib solishi mumkin. Yana bir misol, tarmoqni atayin axborotlar oqimi bilan ortiqcha yuklash orqali yoki tarmoqni ishdan chiqarish yo‘li bilan barcha tarmoq ishini blokirovka qilish.

Himoyaning aktiv buzilishlarini butunlay oldini olish juda murakkab, chunki bunga faqat barcha aloqa vositalarini uzluksiz fizik himoyalash orqali erishish mumkin. Shu sababli himoyaning aktiv buzilishlarida asosiy maqsad ularni operativ tarzda aniqlash va tezda tizimning ishga layoqatliligini tiklash bo‘lishi shart. Buzilishlarning o‘z vaqtida aniqlanishi buzg‘unchini to‘xtatish vazifasini ham o‘taydi, va bu vazifani buzilishlardan ogohlantirish tizimining qismi deb ko‘rish mumkin.

Himoya mexanizmlari

Amaliyotda ishlatiladigan himoya mexanizmlarining aksariyati kriptografiya usullariga asoslangan. Shifrlash yoki shifrlashga yaqin axborotni o‘zgartirishlar ma‘lumotlarni himoyalash usullari hisoblanadi.

Himoya xizmati

Amaliyotda qo‘llaniladigan himoya vazifalari to‘plamlaridan biriga quyidagilar kiradi: konfidensiallik, autentifikasiyalash, yaxlitlik, yolg‘onning mumkin emasligi, foydalanuvchanlik, foydalanuvchanlikni boshqarish.

Konfidensiallik. Konfidensiallik ma’lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. Axborotlar mazmunining muhimliligiga qarab himoyaning bir necha sathlari o‘rnatilishi mumkin. Keng manodagi himoya xizmati ixtiyoriy ikkita foydalanuvchi o‘rtasida

uzatiluvchi barcha ma’lumotlarni ma’lum vaqt mobaynida himoyasini ta’minlashi lozim. Masalan, agar ikki tizim o‘rtasida virtual aloqa o‘rnatilgan bo‘lsa bunday keng ma’nodagi himoya foydalanuvchilar malumotlari uzatilgandagi har qanday yo‘qolishlarga to‘siq bo‘la oladi. Tor ma’nodagi himoya xizmati alohida axborotni yoki hatto axborotning alohida qismining himoyasini taminlay oladi. Ammo bunday choralarning samarasi keng manodagi himoya xizmatiga nisbatan kam, ularni amalga oshirish esa ba’zida murakkab va qimmat bo‘lishi mumkin.

Konfidensiallikning yana bir jihati malumotlar oqimini uning analitik tadqiq qilinishidan himoyalashdir. Analitik tadqiq deganda aloqa tizimidagi axborotlar tavsifiga taalluqli axborot manbaini, adresatni, axborotlar uzatiladigan chastotani, axborotlar o‘lchamini v.h.k. buzg‘unchi tomonidan bilishga urinish tushuniladi.

Autentifikasiya. Autentifikasiya xizmati axborot manbaini ishonchli identifikasiyalashga mo‘ljallangan. Masalan, biror xavf to‘g‘risida signal berilganida autentifikasiya xizmatining vazifasi bu signalning manbai haqiqatan ham signal uzatuvchi ekanligini tekshirishdan iborat bo‘ladi. Tashqi interaktiv aloqada, masalan, terminal yordamida bosh uzelga ulanishdagi servis xizmatining ikki jihatini ajratish mumkin. Birinchidan, bog‘lanish o‘rnatilishida autentifikasiya vositalari aloqada ishtirok etuvchilarning haqiqiy (ekanliklariga) kafolat berishi lozim. Ikkinchidan, keyingi ma’lumot almashinuvida bu vositalar malumotlar oqimiga qandaydir uchinchi tomonning aralashishiga yo‘l qo‘ymasligi lozim.

Yaxlitlik. Yaxlitlik konfidensiallik kabi axborotlar oqimiga, alohida axborotga yoki hatto axborot qismiga taalluqli bo‘lishi mumkin. Bu holda ham jami oqimni himoyalash maqsadga muvofiq hisoblanadi. Axborot yaxlitligini bog‘lanishlar asosidagi himoyalovchi vositalar axborot oqimi bilan ish ko‘radi va qabul qilingan axborotlarning uzatilganiga kamaymasdan, qo‘shilmasdan dastlabki uzatish ketma-ketligi buzilmasdan, qaytarishlarsiz aniq mos kelishi kafolatini ta’minlaydi. Bu vositalar ma’lumotlar buzilishi himoyasini ham ta’minlaydi. Shunday qilib, axborot yaxlitligini bog‘lanishlar asosidagi himoyalovchi vositalar axborot oqimini modifikaqilashdan hamda xizmat ko‘rsatishdagi xalallardan himoyalovchi vositalarni o‘z ichiga oladi.

Axborot yaxlitligini bog‘lanishlar o‘rnatilmagandagi himoyalovchi vositalar alohida axborotlar bilan ish ko‘radi va axborotlarni faqat modifikaqiyalashdan himoyalashni ta’minlaydi.

Yaxlitlikni himoyalovchi vositalarning aktiv hujumga qarshi turishi hisobga olinsa buzilishlarni oldini olish emas, balki buzilishlarni aniqlash muhim hisoblanadi. Yaxlitlikning buzilishi aniqlanganidan so‘ng bunday xizmat faqat buzilish sodir bo‘lganligini xabarlashi mumkin, buzilgan yoki yo‘qolgan axborotni tiklash esa boshqa dastur vositalari yoki operator tomonidan amalga oshiriladi. Umuman, avtomatik tiklash vositalaridan foydalanish afzal hisoblanadi.

Yolg‘onning mumkin emasligi. Yolg‘onning mumkin emasligini kafolatlovchi vositalar uzatuvchi va qabul qiluvchining axborotlar uzatilganligi haqiqat ekanligidan tonishlariga imkon bermasligi kerak. Shunday qilib, agar axborot ishonch qozonmagan uzatuvchi tomonidan yuborilgan bo‘lsa, qabul qiluvchi axborot xuddi shu uzatuvchi tomonidan yuborilganligini isbot qilish imkoniyatiga ega bo‘lishi zarur.

Resurslardan foydalanuvchanlik. Buzilishlarning ko‘pgina xillari resurslardan foydalanuvchanlikni yo‘qolishiga yoki ulardan foydalanishning qiyinlashishiga olib keladi. Bunda ba’zi hollarda autentifikasiya va shifrlash kabi avtomatlashtirilgan qarshi choralar samara bersa, bazi hollarda buzilishlarni oldini olish yoki tizim foydalanuvchanligini tiklash uchun ma’lum fizikaviy harakatlar talab qilinadi.

Foydalanuvchanlikni boshqarish. Foydalanuvchanlikni boshqarish deganda aloqa kanallari orqali tarmoq uzellaridan, ilovalardan foydalanishni chegaralash va nazorat qilish imkoniyati tushuniladi. Bunday nazoratda har bir obyekt o‘zining vakolat doirasiga ega bo‘lganligi sababli obyektlarning resurslardan foydalanishga urinishlarining har birida obyektlarni identifikasiyalash imkoniyati mavjud bo‘lishi kerak.

10.2. Axborot xavfsizligining tashkiliy-ma’muriy ta’minoti

Axborotni ishonchli himoya mexanizmini yaratishda tashkiliy tadbirlar muhim rol o‘ynaydi, chunki konfidensial axborotlardan ruxsatsiz foydalanish asosan, texnik jihatlar bilan emas, balki himoyaning elementar qoidalarini e’tiborga olmaydigan foydalanuvchilar va xodimlarning jinoyatkorona harakatlari, beparvoligi, sovuqqonligi va ma’suliyatsizligi bilan bog‘liq.

Tashkiliy ta’minot konfidenisal axborotdan foydalanishga imkon bermaydigan yoki jiddiy qiyinchilik tug‘diruvchi ijrochilarning ishlab-chiqarish va o‘zaro munosabatlarini me’yoriy-huquqiy asosida reglamentlashdir.

Tashkiliy tadbirlarga quyidagilar kiradi:

Xizmatchi va ishlab chiqarish bino va xonalarni loyihalashda, qurishda va jihozlashda amalga oshiriladigan tadbirlar. Bu tadbirlarning asosiy maqsadi hududga va xonalarga yashirincha kirish imkonini yo‘qotish; odamlarning va transportning yurishi nazoratining qulayligini ta’minlash; foydalanishning alohida tizimiga ega b o‘lgan ishlab-chiqarish zonalarini yaratish v.h.k.;

xodimlarni tanlashda amalga oshiriladigan tadbirlar. Bu tadbirlarga xodimlar bilan tanishish, konfidensial axborot bilan ishlash qoidalarini o‘rgatish, axborot himoyasi qoidasini buzganligi uchun javobgarlik darajasi v.h.k. bilan tanishtirish kiradi;

-ishonchli propusk rejimini va tashrif buyuruvchilarning nazoratini tashkil qilish;

-xona va hududlarni ishonchli qo‘riqlash;

hujjatlar va konfidensial axborot eltuvchilarini saqlash va ishlatish, shu jumladan qayd etish, berish, bajarish va qaytarish tartiblariga rioya qilish;

axborot himoyasini tashkil etish, ya’ni muayyan ishlab chiqarish jamoalarida axborot xavfsizligiga javobgar shaxsni tayinlash, konfidensial axborot bilan ishlovchi xodimlar ishini muntazam tekshirib turish.

Bunday tadbirlar har bir muayyan tashkilot uchun o‘ziga xos xususiyatga ega bo‘ladi.

Axborotni hujjatlashtirish qat’iy belgilangan qoidalar yordamida amalga oshiriladi. Bu qoidalarning asosiylari GOST 6.38-90

"Tashkiliy-boshqaruvchi hujjatlar tizimi.Hujjatlarni rasmiylashtirishga talablar", GOST 6.10.4-84 "Unifikasiyalangan hujjatlar tizimi. Hisoblash texnika vositalari orqali yaratiluvchi mashina eltuvchilaridagi va mashina dasturlardagi hujjatlarga huquqiy kuch berish" kabilar bayon etilgan. Bu GOSTlarda axborotga hujjat huquqini beruvchi 31 ta rekvizitlar ko‘zda tutilgan, ammo bu rekvizitlarning barchasining hujjatda mavjudligi shart emas. Asosiy rekvizit - matn. Shu sababli, har qanday ravon bayon etilgan matn hujjat hisoblanadi va unga huquqiy kuch berish uchun sana va imzo kabi muhim rekvizitlarning mavjudligi kifoya.

Avtomatlashtirilgan axborot tizimlaridan olingan hujjatlar uchun alohida tartib qo‘llaniladi. Bunda, ma’lum hollarda, masofadan olingan axborot elektron imzo bilan tasdiqlanadi. Axborotni himoyalash uchun barcha tashkiliy tadbirlarni ta’minlovchi maxsus ma’muriy xizmatni yaratish talab qilinadi. Uning shtat strukturasi, soni va tarkibi firmaning real ehtiyojlari, axborotning konfidensiallik darajasi va xavfsizligining umumiy holati orqali aniqlanadi. Ma’muriy tadbirlarga quyidagilar kiradi:

operasion tizimning to‘g‘ri konfigurasiyasini madadlash;

ish jurnallarining nazorati;

parollar almashishining nazorati;

himoya tizimida "raxna"larni aniqlash;

axborotni himoyalovchi vositalarni testlash.

Tarmoq operasion tizimining to‘g‘ri konfigurasiyalashni odatda, tizim ma’muri hal etadi. Ma’mur operasion tizim (odamlar emas) rioya qilishi lozim bo‘lgan ma’lum qoidalarni yaratadi. Tizimni ma’murlash - konfigurasiya fayllarini to‘g‘ri tuzishdir. Bu fayllarda (ular bir nechta bo‘lishi mumkin, masalan tizimning har bir qismiga bittadan fayl) tizim ishlashi qoidalarining tavsifi bo‘ladi.

Xavfsizlik ma’muri kompyuter tarmog‘i holatini operativ tarzda (tarmoq kompyuterlari himoyalanishi holatini kuzatish orqali) va operativ bo‘lmagan tarzda (axborot himoyasi tizimidagi voqealarni qaydlovchi jurnallarni tahlillash orqali) nazoratlash lozim. Ishchi stansiyalar sonining oshishi va turli-tuman komponentlari bo‘lgan dasturiy vositalarning ishlatilishi axborot himoyasi tizimidagi hodisalarni qaydlash jurnallar hajmini jiddiy oshishiga olib keladi. Jurnallardagi ma’lumotlar hajmi shunchalik oshib ketishi mumkinki, ma’mur ular tarkibini joiz vaqt mobaynida tahlillay olmaydi.

Tizim zaifligining sababi shundaki, birinchidan, foydalanuvchini autentifikasiyalash tizimi foydalanuvchi ismiga va uning paroliga (ko‘z turidan foydalanish kabi ekzotik holllar bundan mustasno), ikkinchidan, foydalanuvchi tizimida tizimni ma’murlash huquqi berilgan supervizorning (nazoratchi) mavjudligiga asoslanadi. Supervizor parolini saqlash rejimining buzilishi butun tizimdan ruxsatsiz foydalanish imkonini yaratadi.

Undan tashqari bunday koidalarga asoslangan tizim-statik, qotib qolgan tizim. U faqat qat’iy ma’lum hujumlarga qarshi tura olishi mumkin. Oldindan ko‘zda tutilmagan qandaydir yangi taxdidning paydo bulishida tarmoq hujumi nafaqat muvaffaqiyatli, balki tizim

uchun ko‘rinmaydigan bo‘lishi mumkin. Shuning uchun, muassasada ishlatiluvchi axborotning qaysisi himoyaga muhtoj ekanligini aniq tasavvur qilish muhim hisoblanadi. Mavjud axborotni taxlillashdan boshlash lozim. Bu muolajalar axborot himoyasini ta’minlash bo‘yicha tadbirlarni differensiallash imkonini beradi va natijada, sarf-xarajatlarning qisqarishiga sabab bo‘ladi.

Axborot himoyasi tizimini ekspluatasiya qilish bosqichida xavfsizlik ma’murining faoliyati foydalanuvchilar vakolatlarini o‘z vaqtida o‘zgartirishdan hamda tarmoq kompyuterlaridagi himoya mexanizmlarini sozlashdan iborat bo‘ladi. Foydalanuvchilar vakolatlarini va kompyuter tarmoqlarida axborotni himoyalash tizimini sozlashni boshqarish muammosi, masalan, tarmoqdan markazlashtirilgan foydalanish tizimidan foydalanish asosida hal etilishi mumkin. Bunday tizimni amalga oshirishda tarmoq asosiy serverida ishlovchi maxsus foydalanishni boshqaruvchi serverdan foydalaniladi. Bu server markaziy himoya ma’lumotlari bazasini lokal himoya ma’lumotlari bazasi bilan avtomatik tarzda sinxronlaydi. Foydalanishni boshqarishning bu tizimida foydalanuvchi vakolati vaqti-vaqti bilan o‘zgartiriladi va markaziy himoya ma’lumotlari bazasiga kiritiladi, ularning muayyan kompyuterlarda o‘zgarishi navbatdagi sinxronlash seansida vaqtida amalga oshiriladi.

Undan tashqari foydalanuvchi parolini ishchi stansiyalarining birida o‘zgartirsa, uning yangi paroli markaziy himoya ma’lumotlari bazasida avtomatik tarzda akslanadi, hamda bu foydalanuvchi ishlashiga ruxsat berilgan ishchi stansiyalarga uzatiladi.

10.3. Kompyuter viruslari, ularning klassifikasiyasi va ular bilan kurashish mexanizmlari

Kompyuter viruslari va ularning klassifikasiyasi;

Zararkunanda dasturlar va avvalo, viruslar kompyuter tizimi uchun jiddiy xavf hisoblanadi. Bu xavfni nazar pisand qilmaslik foydalanuvchilar axboroti uchun jiddiy oqibatlarga sabab bo‘lishi mumkin. Viruslarning xavfini haddan tashqari oshirib yuborish ham kompyuter tizimlarining barcha imkoniyatlaridan foydalanishga salbiy ta’sir ko‘rsatadi. Viruslar ta’siri mexanizmini, ular bilan kurashish metodlarini bilish viruslarga qarshi samarali kurashishni tashkil etishga, ular ta’siri natijasida zararlanish ehtimolini va yuqotishlarni minimumga keltirishga imkon beradi.

«Kompyuter virusi» atamasi 80-yillarning o‘rtalarida kiritilgan. Biologik viruslarga tegishli o‘lchamlarining kichikligi, o‘z-o‘zidan ko‘payib va obyektlarga singib(ularni zaharlab) tez tarqalish qobiliyati, tizimga salbiy tasiri kabi alomatlar zararkunanda dasturlarga ham taalluqlidir. Kompyuter viruslari bilan ish ko‘rilganda «virus» atamasi bilan bir qatorda «zaharlanish», «yashash muhiti», «profilaktika», kabi tibbiyot atamalaridan ham foydalaniladi. «Kompyuter viruslari» - kompyuter tizimlarida tarqalish va o‘z-o‘zidan qaytadan tiklanish (replikasiya) xususiyatlariga ega bo‘lgan bajariluvchi yoki sharxlanuvchi kichik dasturlardir. Viruslar kompyuter tizimlarida saqlanuvchi dastur taminotini o‘zgartirishi yoki yo‘qotishi mumkin.

Hozirda dunyoda faqat Ro‘yxatga olingan 65 mingdan ortiq kompyuter viruslari mavjud. Zamonaviy zarakunanda dasturlarning aksariyati o‘z-o‘zidan ko‘payish qobiliyatiga ega bo‘lganliklari sababli ularni ham kompyuter viruslariga taalluqli deb hisoblaydilar. Barcha kompyuter viruslari quyidagi alomatlari bo‘yicha klassifikasiyalanishi mumkin:

yashash muhiti bo‘yicha;

yashash muhitining zaharlanishi bo‘yicha;

zararkunandalik tasirning xavfi darajasi bo‘yicha;

ishlash algoritmi bo‘yicha.

Yashash muhiti bo‘yicha kompyuter viruslari quyidagilarga bo‘linadi: tarmoq viruslari; fayl viruslari; yuklama viruslar; kombinasiyalangan viruslar.

Tarmoq viruslarning yashash muhiti kompyuter tarmoqlarining elementlaridir. Fayl viruslar bajariluvchi fayllarda joylashadi. Fayl viruslar ichida makroviruslar alohida o‘rin tutadi. Makroviruslar-makrotillarda yozilgan zararkunanda dasturlar, elektron jadvallar v.h.k. Yuklama viruslar tashqi xotira qurilmalarining yuklama sektorlarida (boot-sektorlarda) bo‘ladi. Kombinasiyalangan viruslar bir necha yashash muhitida joylashgan bo‘ladi. Misol tariqasida yuklama fayl viruslarni ko‘rsatish mumkin.

Yashash muhitining zaharlanishi usuli bo‘yicha kompyuter viruslari quyidagilarga bo‘linadi:

rezident;

rezident bo‘lmagan;

Rezident viruslar faollashganlaridan so‘ng to‘laligicha yoki qisman yashash muhitidan (tarmoq, yuklama sektori, fayl) hisoblash mashinasining asosiy xotirasiga ko‘chadi. Bu viruslar, odatda, faqat

operasion tizimga ruxsat etilgan imtiyozli rejimlardan foydalanib yashash muxitini zaharlaydi va ma’lum sharoitlarda zararkunandalik vazifasini bajaradi.

Rezident bo‘lmagan viruslar faqat faollashgan vaqtlarida hisoblash mashinasining asosiy xotirasiga tushib, zaharlash va zararkunandalik vazifalarini bajaradi. Keyin bu viruslar asosiy xotirani butunlay tark etib yashash muhitida qoladi. Agar virus yashash muhitini zaharlamaydigan dasturni asosiy xotiraga joylashtirsa bunday virus rezident bo‘lmagan virus deb hisoblanadi.

Virusning zararkunandalik imkoniyatlari ularni yaratuvchisining maqsadi va malakasiga hamda kompyuter tizimlarining xususiyatlariga bog‘liq.

Foydalanuvchining informatsion resurslari uchun xavf darajasi bo‘yicha kompyuter viruslarini quyidagilarga ajratish mumkin: beziyon viruslar; xavfli viruslar; juda xavfli viruslar;

Beziyon kompyuter viruslari kompyuter tizimi resurslariga qandaydir shikast yetkazishni uziga maqsad qilmagan mualliflar tomonidan yaratiladi. Ularning maqsadi, odatda, uzlarini dasturchilik imkoniyatlarini ko‘z-ko‘z qilishdir. Bunday viruslarning zararkunandaligi monotoringda aybsiz matnlarni va rasmlarni, musiqiy parchalarning ijro etilishiga olib keladi v.h.k.

Ammo bezarar bo‘lib ko‘ringan bunday viruslar kompyuter tizimlariga ma’lum shikast yetkazadi. Birinchidan bunday viruslar kompyuter tizimlarining resurslarini sarflaydi, natijada uning ishlash samaradorligi pasayadi. Ikkinchidan, kompyuter viruslarida kompyuter tizimlarining informatsion resurslariga shikast keltiruvchi xatoliklar bo‘lishi mumkin.

Xavfli viruslarga kompyuter tizimlarining samaradorligini jiddiy pasayishiga olib keluvchi, ammo xotirlovchi qurilmalarda saqlanuvchi axborotning yaxlitligini va maxfiyligini buzmaydigan viruslar kiradi. Bunday viruslar tasiri oqibatlarini unchalik katta bo‘lmagan moddiy va vaqtiy resurslar sarfi evaziga yo‘qotish mumkin. Bunday viruslarga misol tariqasida hisoblash mashinasi xotirasini egallovchi, ammo tarmoq ishiga ta’sir qilmaydigan viruslarni, dasturni qaytadan ishlanish, operasion tizimining qaytadan yuklanish yoki ma’lumotlarni aloqa kanallari orqali qaytadan uzatilish v.h.k. zaruriyatini tug‘diruvchi viruslarni ko‘rsatish mumkin.

Juda xavfli viruslarga axborotning maxfiyligining buzilishiga, yo‘q qilinishiga, qaytarilmaydigan turlanishga (shifrlash ham shu

qatorda) hamda axborotdan foydalanishga to‘sqinlik qiluvchi va natijada apparat vositalarning ishdan chiqishiga va foydalanuvchilar sog‘ligiga shikast yetishiga sabab bo‘luvchi viruslar kiradi.

Ishlash algoritmining xususiyatlari bo‘yicha viruslarni ikkita sinfga ajratish mumkin:

tarqalishida yashash makonini o‘zgartirmaydigan, tarqalishida yashash makonini o‘zgartiradigan.

Yashash makonini o‘zgartirmaydigan viruslar o‘z navbatida ikkita guruhga ajratilishi mumkin.

viruslar-«yo‘ldoshlar», yoki «hamroh» (companion),

viruslar-«qurtlar» (worm).

Viruslar-«yuldoshlar» fayllarni o‘zgartirmaydi. Uning ta’sir mexanizmi bajariluvchi fayllarning nusxalarini yaratishdan iboratdir.

Viruslar-«qurtlar» tarmoq orqali ishchi stansiyaga tushadi, tarmoqning boshqa abonentlari bo‘yicha virusni jo‘natish adreslarini hisoblaydi va virusni uzatishni bajaradi. Virus fayllarni o‘zgartirmaydi va disklarning yuklama sektorlariga yozilmaydi. Bazi bir viruslar-«qurtlar» diskda virusning ishchi nusxasini yaratadi, boshqalari faqat hisoblash mashinasining asosiy xotirasida joylashadi.

Algoritmlarning murakkabligi, mukammalik darajasi va yashirinish xususiyatlari bo‘yicha yashash makonini o‘zgartiradigan viruslar quyidagilarga bo‘linadi:

talaba viruslar;

«stels»(Yashirin:.Yashirin texnologiya) viruslar (ko‘rinmaydigan viruslar);

Polimorf (poli... va yun. morphe — shakl) viruslar.

Talaba-viruslar malakasi past yaratuvchilar tomonidan yaratiladi. Bunday viruslar, odatda, rezident bo‘lmagan viruslar qatoriga kiradi, ularda ko‘pincha xatoliklar mavjud bo‘ladi, osongina taniladi va yo‘qotiladi.

«Stels» viruslar malakali mutaxasislar tomonidan yaratiladi. «Stels»-viruslar operasion tizimning shikastlangan fayllarga murojaatlarini ushlab qolish yo‘li bilan o‘zini yashash makonidaligini yashiradi va operasion tizimni axborotning shikastlanmagan qismiga yo‘naltiradi. Virus rezident hisoblanadi, operasion tizim dasturlari ostida yashirinadi, xotirada joyini o‘zgartirishi mumkin. «Stels» - viruslar rezident antivirus vositalariga qarshi ta’sir ko‘rsata olish qobiliyatiga ega.

Polimorf viruslar ham malakali mutaxasislar tomonidan yaratiladi va doimiy tanituvchi guruhlar-signaturalarga ega bo‘lmaydi. Oddiy viruslar yashash makonining zaharlanganligini aniqlash uchun zaharlangan obyektga maxsus tanituvchi ikkilik ketma-ketlikni yoki simvollar ketma-ketligini (signaturani) joylashtiradi. Bu ketma-ketlik fayl yoki sektorning zaharlanganligini aniqlaydi. Polimorf viruslar virus tanasini shifrlashdan va shifrlash dasturini turlantirishdan foydalanadi. Bunday o‘zgartirish evaziga polimorf viruslarda kodlarning muvofiqligi bo‘lmaydi.

Ma’lum viruslar bilan ishlashda qulaylikni ta’minlash maqsadida viruslar katalogidan foydalaniladi. Katalogda viruslarning quyidagi standart xususiyatlari tug‘risidagi ma’lumot joylashtiriladi: nomi, uzunligi, zaxarlanuvchi fayllar, fayldagi o‘rni, zaxarlash usuli, rezident viruslar uchun asosiy xotiraga joylashtirish usuli, kelib chiqaradigan natijalari, zarakunandalik vazifalarining borligi (yuq-ligi) va xatoliklar. Kataloglarning mavjudligi viruslarni tavsiflashda ularning standart xususiyatlari va ta’sirlarini tushirib qoldirib, faqat o‘ziga xos xususiyatlarini ko‘rsatishga imkon beradi.

Viruslar bilan kurashish metodlari va vositalari.

Viruslar tarqalishining ommalashuvi, ular ta’siri oqibatlarining jiddiyligi virusga qarshi maxsus vositalarni va ularni qo‘llash metodlarini yaratish zaruriyatini tug‘dirdi. Virusga qarshi vositalar yordamida quyidagi masalalar yechiladi:

kompyuter tizimlarida viruslarni aniqlash;

viruslar ta’siri oqibatlarini yo‘qotish.

Viruslarni aniqlashni ularning ta’siri boshlanishi bilanoq yoki, loaqal, zararkunandalik vazifalari boshlanmasdanoq amalga oshirish maqsadga muvofiq hisoblanadi. Ta’kidlash lozimki, barcha xil viruslarning aniqlanishini kafolatlovchi virusga qarshi vositalar mavjud emas.

Kompyuter tizimlarida viruslarni aniqlashning quyidagi metodlari mavjud:

skanerlash;

o‘zgarishlarni bilib qolish; evristik tahlil;

rezident qorovullardan foydalanish;

dasturni vaksinasiyalash;

viruslardan apparat-programm himoyalanish.

Skanerlash - viruslarni aniqlashning eng oddiy metodlaridan hisoblanadi. Skanerlash programma-skaner tomonidan amalga

oshiriladi. Bu programma-skaner viruslarning tanituvchi qismini-signaturani (lot. signo — belgilayman, ko‘rsataman) qidirish maqsadida fayllarni ko‘rib chiqadi. Ko‘pincha programma-skanerlar aniqlangan viruslarni yo‘qotishi mumkin. Bunday programmalar polifaglar ((poli... va ... fagiya)) deb ataladi. Skanerlash usuli signaturalari ajratilgan va doimiy bo‘lgan viruslarni aniqlashda qo‘llaniladi.

O‘zgarishlarni bilib qolish usuli programm-taf-tishchidan foydalanishga asoslangan. Bunday dasturlar odatda virus joylashadigan diskning barcha qismlari xarakteristikalarini aniqlaydi va eslab qoladi. Programma-taf-tishchining davriy bajarilishi jarayonida saqlanuvchi xarakteristikalari bilan disk qismlarini nazoratlash natijasidagi xarakteristikalar taqqoslanadi. Taftish natijasida dastur viruslar borligi xususida taxminga asoslangan axborotni beradi.

Metodning eng asosiy afzalligi- viruslarning barcha xilini hamda noma’lum viruslarni aniqlashi imkoniyatidir.

Evristik tahlil usuli ham o‘zgarishlarni bilib olish metodlari kabi noma’lum viruslarni aniqlash imkonini beradi. Ammo bu metod fayl tizimi xususidagi axborotni oldindan yozosh, ishlash va saqlashni talab etmaydi. Evristik tahlilning moxiyati-viruslarning mumkin bo‘lgan yashash makonlarini tekshirish va ulardagi viruslarga xarakterli komandalarni (komandalar guruhini) aniqlashdan iboratdir.

Rezident qorovullaridan foydalanuvchi usuli hisoblash mashinasining asosiy xotirasida doimo saqlanuvchi va boshqa programmalar harakatini kuzatuvchi programmalarga asoslangan. Bu metodning, jiddiy kamchiligi sifatida yolg‘ondakam trevogalar foizining ko‘pligidir.

Dasturni vaksinasiyalash deganda uning yaxlitligini nazorat qilish maqsadida maxsus modulning yaratilishi tushuniladi. Fayl yaxlitligining xarakteristikasi sifatida odatda nazorat yig‘indisidan foydalaniladi. Vaksinasiyalangan faylning zaharlanishi sodir bo‘lsa nazorat moduli nazorat yigindisining o‘zgarishini aniqlaydi va bu xususida foydalanuvchini ogoxlantiradi.

Viruslarga qarshi apparat-programm vositalardan foydalanish usuli viruslardan ximoyalanishning eng ishonchli usuli hisoblanadi. Hozirda shaxsiy kompyuterlarni himoyalashda maxsus kontrollerlar va ularning **dasturiy ta’minotidan** foydalaniladi. Kontroller umumiy shinadan foydalana oladi va shu sababli disk tizimiga bo‘lgan barcha murojaatlarni nazorat qila oladi. Kontrollerning dasturiy ta’minotida

ishlashning oddiy rejimida diskning o‘zgartirilishi mumkin bo‘lmagan qismlari xotirlanadi.

Viruslarga qarshi apparat-dasturiy vositalar quyidagi afzalliklarga ega:

- doimo ishlaydi;
- ta’sir mexanizmidan qat’iy nazar barcha viruslarni aniqlaydi;
- virus ta’siri yoki malakasiz foydalanuvchi ishi natijasidagi ruxsatsiz harakatlarni to‘xtadi.

Bu vositalarning kamchiligi sifatida ularning shaxsiy kompyuter apparat vositalariga bog‘liqligini ko‘rsatish mumkin.

Viruslar ta’siri oqibatlarini yo‘qotish jarayonida viruslarni yo‘qotish, hamda virus bo‘lgan fayllar va xotira qismlarini tiklash amalga oshiriladi. Viruslarga qarshi dasturlar yordamida viruslar ta’siri oqibatlarini yo‘qotishning ikki usuli mavjud:

Birinchi metodga binoan tizim ma’lum viruslar ta’siridan so‘ng tiklanadi. Virusni yo‘qotuvchi dasturni yaratuvchi virusning stukturasini va uning yashash makonida joylashish xarakteristkalarini bilishi shart.

Ikkinchi metod noma’lum viruslar bilan zaharlangan fayllarni va yo‘qlama sektorini tiklashga imkon beradi. Fayllarni tiklash uchun tiklovchi dastur fayllar xususidagi viruslar yo‘qligidagi axborotni oldindan saqlashi lozim. Zaharlanmagan fayl xususidagi axborot va viruslar ishlashining umumiy prinsiplari xususidagi axborotlar fayllarni tiklashga imkon beradi.

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Kompyuter viruslari qanday alomatlari bo‘yicha klassifikasiyalanadi?
2. Fayl virusi va uning ta’siri algoritmini tushuntiring.
3. Makrovirus va yuklama viruslar ta’siri algoritmi qanday?
4. Viruslarni aniqlash metodlari.
5. Viruslar ta’siri oqibatlarini yo‘qotish metodlari.
6. Kompyuter tizimlarining viruslar bilan zaharlanishining oldini oluvchi profilaktik choralar ketma-ketligini sanab o‘ting.

XI BOB. AXBOROT XAVFSIZLIGI SIYOSATI VA RISKLARNI BOSHQARISH

11.1. Risk darajasi, risk chastotasi, risk matritsasi

Risklarni boshqarish

Risk bu – belgilangan sharoitlarda tahdidning manbalarga potensial zarar yetkazilishini kutish. Bundan tashqari, riskni quyidagicha tushunish mumkin:

- Risk bu – ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo‘qotilishi yoki boshqa salbiy ta’sir ko‘rsatishi mumkin bo‘lgan voqyea.

- Risk bu – manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta’sirida tahdid bo‘lishi ehtimoli.

- Risk bu – voqyea sodir bo‘lishi ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta’siri.

Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish mavjud bo‘lib, ularni quyidagicha tasvirlash mumkin: RISK = Tahdid × Zaiflik × Ta’sir.

Boshqa tomondan, hodisaning axborot aktiviga ta’siri bu – aktivdagi yoki manfaatdor tomonlar uchun aktivning qiymatidagi zaiflikning natijasi ekanligini inobatga olgan holda, riskni quyidagicha ifodalash mumkin: RISK = Tahdid × Zaiflik × Aktiv qiymati.

Risk o‘zida quyidagi ikkita faktorni mujassamlashtiradi:

- zararli hodisani yuzaga kelish ehtimoli;

- va zararli hodisaning oqibatlari.

Riskning ta’siri. Risk normal amalga oshirish jarayoniga va loyiha narxiga yoki kutilgan qiymatga ta’sir yetadi. Risk ta’siri tashkilot, jarayon yoki tizimga zararli muhit sababli yuzaga keladi. Ta’sir riskni kuzatilish ehtimoli jiddiyligini ko‘rsatadi.

Riskning chastotasi. Riskni aniqlash va baholashga bog‘liq holda, risklarni tasniflashda ularning takrorlanish chastotatasiga va ko‘p sonli ketma-ketliklarga asoslanadi. Chastota va ko‘p sonlilik risklarni monitoring qilishda muhim hususiyat hisoblanib, shu nuqtai nazaridan risklar ikki guruhga: minor risklar – e’tibor talab qilmaydigan va major risklar – alohida e’tibor va kuzatuv talab qiluvchilarga ajratiladi. Risklar chastotasi va ko‘p sonligiga asoslangan holda ularni ikki o‘lchamli matrisa usuli yordamida guruhlarga ajratish mumkin.

Riskning darajalari. Risk darajasi tarmoqda (yoki tizimga) natijaviy ta’sirning bahosi bo‘lib, risk chastotasi va uning ko‘p

sonligiga ko‘ra risklarni darajaga ajratishning ko‘plab usullari mavjud. Ulardan eng keng tarqalgan usullaridan biri bu – ikki o‘lchamli matrisa usulidir.

Risklarni tahlil qilishda, chastota yoki mojaro kuzatilishi va natijasining ehtimoli bilan ishlash talab etiladi. Bu esa risk darajasini ifodalaydi. Risk quyidagi tenglik bilan ifodalanadi: Risk darajasi=natija ×ehtimollik.

Risk darajalari 4 ta: ekstirmal yuqori, yuqori, o‘rta va past, bo‘lishi mumkin.

Ekstrimal yuqori yoki yuqori risk paydo bo‘lishini va salbiy ta’sirini kamaytirish uchun maxsus yo‘naltirilgan qarshi choralarni talab etadi. Bu darajadagi risklar yuqori yoki o‘rtacha ta’sirning yuqori ehtimolligiga ega bo‘ladi. Mazkur darajadagi risklar jiddiy xavfni olib keladi va shuning uchun, zudlik bilan aniqlash hamda qarshi chora ko‘rishni talab qiladi.

O’rta darajali risklar yuqori ehtimollikka ega past natijali hodisa yoki past ehtimollikka ega yuqori natijali hodisa bo‘lishi mumkin. Alohida qaralganda yuqori ehtimollikka ega past natijali hodisalar loyiha narxiga yoki kutilgan natijaga kam ta’sir qiladi. Past ehtimollikka ega yuqori natijali hodisalar doimiy monitoringni talab etadi. O’rta darajali risklarga zudlik bilan chora ko‘rish talab etilmasada, himoyani dastlabki vaqtda o‘rnatish talab etiladi.

Past darajali risklar odatda e’tibor bermasa bo‘ladigan yoki keyingi baholashlarda e’tibor bersa bo‘ladigan risklar toifasi bo‘lib, ularni bartaraf etish qisqa muddatda amalga oshirilishni talab qilmaydi yoki ortiqcha sarf xarajatni keltirib chiqarmaydi.

Risk matrisasi risklarni paydo bo‘lish ehtimolini ularning natijasi va ta’siri orqali aniqlaydi hamda risk jiddiyligini va unga qarshi himoya chorasi sathini grafik taqdim etadi. Risk matrisasi riskning ortib boruvchi ko‘rinishi uchun foydalaniluvchi sodda jarayon bo‘lib, qarshi choralarni ko‘rishda yordam beradi. Risk matrisasi risklarni turli darajalarda aniqlash va jiddiylik nuqtai nazaridan guruhlash imkonini beradi. Bundan tashqari, har bir tashkilot tomonidan amalga oshiriladigan risklarni o‘lchash usullari ham mavjud (11.1-rasm).

Ehtimollik (ravshan)		Oqibat/ ta’sir					
			Muhim emas	Kam	O’rta	Ko’p	Jiddiy
81-100%	Ehtimollik (noravshan)	Juda yuqori	Past	O’rta	Yuqori	O’ta yuqori	O’ta yuqori
61-80%		Yuqori	Past	O’rta	Yuqori	Yuqori	O’ta yuqori
41-60%		Teng	Past	O’rta	O’rta	Yuqori	Yuqori
21-40%		Past	Past	Past	O’rta	O’rta	Yuqori
1-20%		Juda past	Past	Past	O’rta	O’rta	Yuqori

11.1-rasm. Risk matrisasi

Yuqorida taqdim etilgan risk matrisasi risklarni vizual taqdim etish va o‘zaro taqqoslash imkonini berib, undagi har bir yacheyka ehtimollik va oqibat kattaliklarining kombinasiyasidan iborat bo‘ladi. Riskning jiddiyligi uning ehtimoli va ta’sir darajasiga bog‘liq bo‘ladi. Keltirilgan risk matrisasida paydo bo‘lish ehtimoli bo‘yicha ular 5 ta guruhga ajratilgan. Shunga mos ravishda, risk oqibati ham 5 ta darajaga ajratilgan.

11.2. Risklarni boshqarish

Risklarni boshqarish. Risklarni boshqarish bu – risklarni aniqlash, baholash, javob berish va potensial ta’sirga tashkilot tomonidan qanday javob berilishini amalga oshirish jarayoni. Risklarni boshqarish xavfsizlikning hayotiy siklida o‘zining muhim o‘rniga ega bo‘lib, u davomiy va hattoki murakkablashib boruvchi jarayon hisoblanadi. Risklar turli tashkilotlar uchun turlicha bo‘lsada, risklarni boshqarishga tayyorgarlik ko‘rish barcha tashkilotlar uchun umumiy bo‘ladi. Risklarni boshqarishdan asosiy maqsad quyidagilar:

- potensial risklarni aniqlash;
- risk ta’sirini aniqlash va tashkilotlarga yaxshiroq risklarni boshqarish strategiyasi va rejasini ishlab chiqishga yordam berish;
- jiddiylik darajasiga asoslangan holda risklarni tasniflash va yordam berish uchun risklarni boshqarish usullari, vositalari va texnologiyalaridan foydalanish;
- risklarni tushunish, tahlil qilish va aniqlangan risk hodisalarini qayd etish;
- risklarni nazorat qilish va risk ta’siriga qarshi kurashish;

- xavfsizlik xodimlarini ogohlantirish va risklarni boshqarish strategiyasini ishlab chiqish.

Risklarni boshqarish risklarni aniqlashda tizimlashgan yondashuvni ta’minlaydi va quyidagi afzalliklarga ega:

- potensial risk ta’siri sohasiga e’tibor qaratadi;
- risklarni darajalari bo‘yicha manzillaydi;
- risklarni tutish jarayonini yaxshilaydi;
- kutilmagan holatlarda xavfsizlik xodimini samarali harakat qilishiga ko‘mak beradi;
- resurslardan samarali foydalanish imkonini beradi.

Risklarni boshqarishda muhim rollar va javobgarliklar. Risklarni boshqarishda rollar va javobgarliklar bajaruvchilar o‘rtasida quyidagicha taqsimlangan:

− Bosh boshqaruvchi. Bosh boshqaruvchi tashkilotda risklarni boshqarish jarayonini olib borishga rahbar hisoblanib, u risk paydo bo‘lganga ularni aniqlash uchun talab qilinadigan siyosat va usullarni ishlab chiqadi. Bundan tashqari, kelajakda bo‘lishi mumkin bo‘lgan risklarni tutib olish uchun zarur bo‘lgan ishlarni amalga oshirish ham uning vazifasi hisoblanadi.

− Axborot texnologiyalari bo‘yicha direktor. Mazkur lavozim egasi tashkilot axborot va kompyuter texnologiyalarini madadlash uchun zarur bo‘lgan siyosat va rejalarni amalga oshirishga javobgar bo‘lib, risklarni boshqarishdagi asosiy reja va siyosatlarda muhim rol o‘ynaydi. Ushbu lavozim egasi uchun asosiy javobgarliklar bu – xodimlarni xavfsizlik bo‘yicha o‘qitish hamda axborot texnologiyalarida bo‘lishi mumkin bo‘lgan risklarni va ularni biznes jarayonlariga ta’sirini boshqarishdan iborat.

− Tizim va axborot egalari. Tizim va axborot egalarining vazifasi asosan axborot tizimlari uchun ishlab chiqilgan rejalar va siyosatlarni monitoring qilib borish bo‘lib, quyidagi javobgarliklarni o‘z ichiga oladi:

sozlanishlarni boshqarish jarayoniga bog‘liq barcha muzokaralarda ishtirok etish;

axborot texnologiyalari komponentlari qaydlarini saqlash;

axborot tizimlarida barcha o‘zgarishlarni va ularni ta’sirlarini tadqiq qilish;

barcha tizimlar uchun xavfsizlik holati bo‘yicha hisobotlarni tayyorlash;

axborot tizimlarini himoyalash uchun zarur bo‘lgan xavfsizlik nazoratlarini yangilab borish;

doimiy ravishda xavfsizlikka oid hujjatlarni yangilab borish;

mavjud xavfsizlik nazoratini o‘zining samaradorligini ta’minlashi bo‘yicha tekshirish va baholash.

− Biznes va funksional menedjerlar. Mazkur lavozim egalari tashkilotdagi barcha boshqaruv jarayonlarini madadlash uchun javobgar bo‘lib, bu vazifani bajarishida tashkilot rahbariyati tomonidan qo‘llab quvvatlanadi. Funksional menedjeri quyidagilarni anglatadi:

rivojlantirish jamoasi menedjeri;

savdo menedjeri;

mijozlarga xizmat ko‘rsatuvchi menedjer.

− AT xavfsizlik dasturi menedjerlari va kompyuter xavfsizligi bo‘limi direktori. Ushbu lavozim egalari tizimni himoyalashda xavfsizlik nazoratlarini tanlash orqali axborot tizimi egalarini qo‘llab quvvatlaydi. Ushbu lavozim egalari tashkilotda xavfsizlik nazoratini tanlashda va tuzatishda muhim ro‘l o‘ynaydi.

− AT xavfsizlik amaliyotchilari. AT xavfsizlik amaliyotchilari tashkilotda shaxsiy, fizik va axborot xavfsizligini amalga oshiradilar va ular quyidagilarga javobgar:

tashkilotda yaxshiroq xavfsizlik usullarini yaratish;

tashkilot standartlariga to‘liq mos keluvchi usullarni ishlab chiqish;

risklarni boshqarish va biznesni rejalashtirish uchun tashkilot xavfsizlik yondashuvlarini tekshirish;

xavfsizlik insidentlarini tutish va qayd qilish;

tashkilotda xavfsizlik uchun rol va javobgarliklarni belgilash;

tashkilotdagi barcha xavfsizlik o‘lchovlarini nazorat qilish.

− Xavfsizlik bo‘yicha murabbiy. Xavfsizlik bo‘yicha murabbiy tashkilotdagi tayyorgarlik va o‘quv kurslarini amalga oshiradi. Bu vazifani odatda soha mutaxassislari tomonidan bajarilishi tavsiya etiladi.

Muhim risk ko‘rsatkichlari. Muhim risk ko‘rsatkichlari risklarni samarali boshqarish jarayonida muhim tashkil etuvchi bo‘lib, dastlabki bosqichlarda harakatlarning xavflilik darajasini ko‘rsatadi. Muhim risk ko‘rsatkichlarini to‘g‘ri aniqlash tashkilot maqsadini tushunishni talab etadi. U tashkilotdagi risk ehtimolini ko‘rsatuvchi o‘lchov bo‘lib, quyidagilarni amalga oshirishda yordam beradi:

- hodisa ta’sirini aniqlash;

- chegara qiymatda ogohlantirish;
- risk hodisalarini qayta ko‘rish.

Muhim risk ko‘rsatkichi aniqlik bilan hisoblanishi va tashkilotning muhim amalga oshirish ko‘rsatkichlariga salbiy ta’sirlarni aks ettirishi kerak. Bu yerda, tashkilotning muhim amalga oshirish ko‘rsatkichi tashkilotni o‘zining maqsadalariga erishish jarayonini baholash ko‘rsatkichi hisoblanadi.

11.3. Risklarni boshqarish bosqichlari

Risklarni boshqarish bosqichlari. Risklarni boshqarish uzluksiz jarayon bo‘lib, har bir bosqichda muvaffaqqiyatli amalga oshirilishni talab etadi. U aniqlangan va faol ishlaydigan xavfsizlik dasturidan foydalangan holda xavfni maqbul darajada oldini oladi. Risklarni boshqarish quyidagi asosiy to‘rtta bosqichga bo‘linadi:

1. Risklarni aniqlash.
2. Risklarni baholash.
3. Risklarni bartaraf etish.
4. Risk monitoringi va qayta ko‘rib chiqish.

Har bir tashkilot risklarni boshqarish jarayonida yuqorida keltirilgan bosqichlarni bosib o‘tadi. Quyida ushbu bosqichlar bilan yaqindan tanishib chiqiladi.

Risklarni aniqlash. Risklarni boshqarishdagi dastlabki qadam bo‘lib, uning asosiy maqsadi riskni tashkilotga zarar yetkazmasdan oldin aniqlash hisoblanadi. Risklarni aniqlash jarayoni mas’ul mutaxassislar qobiliyatiga bog‘liq bo‘lganligi sabab, ular turli tashkilotlar uchun farq qiladi. Risklarni aniqlash o‘zida tashkilot xavfsizligiga ta’sir qiluvchi ichki va tashqi risklarning manbasini, sabablarini, natijasini va boshqalarni aniqlashni mujassamlashtirgan. Risklar odatda quyidagi 4 ta muhim sohalardan kelib chiqadi:

- Muhit.Muhitga aloqador bo‘lgan risklar o‘zida ish joyidagi kamchiliklar, turli xalaqitlar, issiq/ sovuq muhit, tutun, past yoritilganlik va elektr xavflari kabilarni birlashtiradi.
- Jixoz. Jixozga aloqador risklar sifatida jixozlarning past ta’mirlash muhiti, ishlamaslik, mavjud bo‘lmaslik va vazifaga nomutanosibligini keltirish mumkin.
- Mijoz. Mijozlar bilan bog‘liq risklar odatda muhim o‘zgarishlar, kutilmagan ko‘chishlar va zaif aloqa natijasida yuzaga keladi.
- Vazifalar. Vazifalarga aloqador bo‘lgan risklarga yetarli bo‘lmagan bajarish vaqti, takroriy vazifalar, ishni loyihalash va

xodimlar sonini yetarli bo‘lmasiligi orqali paydo bo‘luvchi risklar misol bo‘ladi.

Risklarni aniqlash jarayoni ikki bosqichda amalga oshiriladi:

- kontekstni belgilash: xodim ichki va tashqi muhitni va tashkilot faoliyatidagi joriy holatni aniqlaydi;

- risklarni sanash: bo‘lishi mumkin bo‘lgan risklarni va ular sababli kutilayotgan natijalar aniqlanadi.

Riskni aniqlash risklarni boshqarish jarayonidagi turli og‘ishlarni kamaytiradi va bu o‘z navbatida kelajakda ta’sir qiluvchi omillar ehtimolini kamaytiradi. Risklarni aniqlashning ko‘plab usullari mavjud bo‘lib, ular asosida turli dasturiy vositalar ishlab chiqilgan. Ko‘plab risklarni aniqlash jarayonlari maxsus shakllantirilgan jamoa tomonidan amalga oshiriladi. Risklarni aniqlash jarayoni bir qancha faktorlarga, masalan, tarmoqning holati va jamoa a’zolarini risklarni boshqarishdagi qobiliyatlariga asoslanadi.

Riskni baholash. Risklarni baholash bosqichida tashkilotdagi risklarga baho beriladi va bu risklarning ta’siri yoki yuzaga kelish ehtimoli hisoblanadi. Risklarni baholash uzluksiz davom etuvchi jarayon bo‘lib, riskka qarshi kurashish va rejalarni amalga oshirish uchun imtiyozlarni belgilaydi. Risklarni baholash ularning miqdor va sifat qiymatini aniqlaydi. Har bir tashkilot risklarni aniqlash, darajalarga ajratish va yo‘q qilish uchun o‘zida riskni baholash jarayonini qabul qilishi kerak.

Riskni baholash taqdim etilgan risk turini, riskning ehtimoli va miqdorini, uning darajasini hamda uni nazoratlash uchun rejani aniqlaydi. Tashkilotlar risklarni baholash jarayonini odatda xavf aniqlanganda va uni zudlik bilan nazoratlay olmaganlarida amalga oshiradilar. Riskni baholashdan so‘ng ma’lum vaqt oralig‘i bilan barcha axborot vositalarini yangilash talab etiladi.

Risklar baholangandan so‘ng, ular miqdor va tashkilotga keltiradigan zarariga ko‘ra darajalanadi. Darajalarga ajratish risklarga qarshi kurashishga va resurslarni joylashtirishga yordam beradi. Taqdim etilgan risklarning darajalari ularning miqdoriga bog‘liq bo‘ladi:

1-2: darajasi 1-2 ga teng bo‘lgan risklarni zudlik bilan bartaraf etish talab etiladi yoki bartaraf etish imkoni bo‘lmasa, nazorat harakatlari orqali uning xavflilik darajasini tushirish talab etiladi.

3-4: darajasi 3-4 ga teng bo‘lgan risklarni o‘ylangan biror vaqt oralig‘ida bartaraf etish yoki xavfni nazoratga olish zarur hisoblanadi.

5-6: mazkur darajaga ega risklarni imkoni bor bo‘lgan vaqtda bartaraf etish yoki imkoni bo‘lsa xavfni nazoratga olish zarur.

Risklarni baholash quyidagi ikki bosqichdan iborat:

Riskni tahlil qilish: risk tabiatini aniqlash va uni paydo bo‘lish darajasini hisoblash bosqichi bo‘lib, u risklarni nazoratlashga yordam beradi.

Riskni darajalarga ajratish: risklarni tahlil qilish jarayonida ularning miqdoriy jixatdan reytingini aniqlash va qarshi choralarni loyihalash bosqichi hisoblanadi.

Risklarni bartaraf etish. Risklarni bartaraf etish jarayoni aniqlangan risklarni modifikasiyalash maqsadida mos nazoratni tanlash va amalga oshirishni ta’minlab, bunda miqdoriy darajasi yuqori bo‘lganlariga birinchi murojaat qilinadi. Ushbu bosqichda qaror qabul qilish riskni baholash natijasiga asoslanadi. Ushbu bosqichning asosiy vazifasi jiddiy hisoblangan risklarni nazoratlash uchun qarshi choralarni aniqlash bo‘lib, bunda risklarni individual ravishda yo‘q qilish, monitoring qilish va qayta ko‘rib chiqish uchun ularni darajalarga ajratish amalga oshiriladi. Risklarni yo‘q qilishdan oldin quyidagi axborotni to‘plash talab etiladi:

- mos himoya usulini tanlash;
- himoya usuli uchun javobgar shaxsni tayinlash;
- himoya narxini inobatga olish;
- himoya usulini afzalligini asoslash;
- muvaffaqqiyatga erishish ehtimolini aniqlash;
- himoya usulini o‘lchash va baholash usulini aniqlash.

Agar aniqlangan risklarni bartaraf etish talab etilsa, risklarni boshqarish rejasini doimiy qayta ko‘rib chiqish va ishlab chiqish zarur bo‘ladi. Turli himoya usullaridan foydalanish riskdan qochish, ularni kamaytirish va ular uchun javobgarliklarni boshqaga o‘tkazish kabi imkoniyatlar taqdim qiladi.

Xodimlar risklarni kamaytirish yoki minimallashtirish uchun quyidagilarni amalga oshirishi talab etiladi:

- riskni nazoratlash rejasini ishlab chiqish;
- ko‘rsatilayotgan xizmatga riskni ta’sirini aniqlash;
- riskni nazoratlash rejasini tamomlash uchun qat’iy cheklovlarni qo‘yish;
- risklarni nazoratlash strategiyasini amalga oshirish;
- risklarni nazoratlashda mijoz harakatini aniqlash;

- risklarni nazoratlash daravomida madadlovchi xodimlar/ ishchilar bilan aloqani o‘rnatish;

- risklarni nazoratlash jarayonining bir qismi sifatida risklarni nazoratlash rejasini to‘liq hujjatlashtirish.

Tashkilotda risklarni boshqarish freymvorki (Enterprise Risk Management Framework, ERM Framework). Risklarni boshqarish freymvorki tashkilotning risklarni boshqarish usuliga xos bo‘lgan amalga oshirish tadbirlarini belgilaydi va tashkilotda axborot xavfsizligi va risklarni boshqarish bo‘yicha faoliyatni birlashtiruvchi tarkibiy jarayonni ta’minlaydi. Tashkilotda risklarni boshqarish freymvorki quyidagi harakatlarni aniqlaydi, tahlil qiladi va amalga oshiradi:

- riskka olib keluvchi harakatlarni bekor qilish orqali riskdan qochish;

- risk ta’siri yoki ehtimolini minimallashtirish orqali riskni kamaytirish;

- risklarni boshqarish jarayoni standartlarini taqdim qilish.

Tashkilotda risklarni boshqarish freymvorkining asosiy maqsadlari quyidagilardan iborat:

- tashkilotda risklarni boshqarishni tashkilot faoliyatini boshqarish bilan birlashtirish;

- risklarni boshqarishning afzalliklarini o‘zaro bog‘lash;

- risklarni boshqarish uchun tashkilotda rollarni va vazifalarni aniqlash;

- risklar to‘g‘risida hisobot berish va rivojlanish jarayonini standartlashtirish;

- tashkilotda risklarni boshqarish uchun standart yondashuvlarni o‘rnatish;

- risklarni boshqarishda resurslarga ko‘maklashish;

- tashkilotda risklarni boshqarishning doirasi va ilovalarini o‘rnatish;

- tashkilotda risklarni boshqarishni takomillashtirish uchun vaqti-vaqti bilan tekshirishni amalga oshirish.

Amalda tashkilotda risklarni boshqarish freymvorklari sifatida NIST ERM, COSO ERM va COBIT ERM kabilardan keng qo‘llaniladi.

11.4. Risklarni boshqarishning axborot tizimlari

Risklarni boshqarishning axborot tizimlari (Risk Management Information Systems, RMIS). RMIS bu – boshqaruv axborot tizimi bo‘lib, axborotni saqlashni boshqarish, tahlil qilish va tashkilot

tarmog‘i uchun risk to‘g‘risida ma’lumot olish imkoniyatini taqdim qiladi. Tashkilotlar risklarni boshqarish jarayonini optimallashtirish uchun RMIS bilan risklarni boshqarish freymvorkini birlashtiradi. RMIS tizimlari quyidagi afzalliklarga ega:

- ma’lumot ortiqchaligi va xatoligini kamaytirish orqali ma’lumot ishonchligini yaxshilaydi;
- RMIS orqali xabarlar boshqaruvining yaxshilanishi natijasida tashkilotdagi xarajatlarni kamaytiradi;
- RMIS tashkilotning standartlariga muvofiq ravishda, ularga risklarni boshqarish siyosatidan samarali foydalanishda yordam beradi.

RMIS turli omillar bo‘yicha hisobotlarni hosil qiladi va ushbu hisobotlar tashkilotda tarmoq risklari to‘g‘risida yaxlit tasavvurga ega bo‘lishga hamda ularni boshqarishga imkon beradi. Hosil qilingan RMIS hisoboti turlari unga yuborilgan so‘rov turiga bog‘liq bo‘ladi. RMIS quyidagi turdagi hisobotlarni hosil qiladi:

- Standart hisobotlar: yuborilgan umumiy so‘rovlarga javob sifatida RMIS standart hisobotlarni hosil qiladi. Ushbu hisobot guruhga ajratilgan ma’lumotlardan tashkil topmaydi.
- Maxsus hisobotlar: bundan tashqari RMIS tizimi maxsus so‘rovlarga nisbatan maxsus javoblarni generasiya qiladi va ular turli guruhga tegishli ma’lumotlardan tashkil topgan bo‘ladi.

Amalda RMIS tizimining turli ko‘rishdagi vositalaridan keng foydalaniladi. Ularga misol sifatida, Aon Enterprise Risk Management, Stars RMIS, RiskEnvision, RiskonnectRMIS, INFORM, Traveler’s e-CARMA vositalarini keltirish mumkin.

11.5. Foydalanuvchanlik tushunchasi

Parol va kriptografik kalit

Axborot texnologiyalari sohasida faoliyat yuritayotgan mutaxasislar orasida ko‘p hollarda parol va kriptografik kalit tushunchalarini chalkashtirish holatlari kuzatiladi. Biroq ushbu ikki tushuncha bir-biridan farq qiladi. Keling ushdu ikki tushunchalarni tahlil qilsak.

Kriptografik kalitlarning o‘lchovi bitlarda ifodalanadi. Masalan, hujumchi T 64-bitli kalitni barcha variantlarini hisoblash talab etilsin. Mazkur holatda 264 ta variant mavjud bo‘lib, hujumchi T kalitni to‘g‘ri topishi uchun agar kalit tasodifiy tanlangan bo‘lsa o‘rta hisobda 263 ta kalitni tekshirib ko‘rishi talab etiladi.

Parolning o‘lchov birligi esa odatda parol tarkibidagi belgilar soni bilan o‘lchanadi. Masalan, parol uzunligi 8 ga teng bo‘lsa va foydalanilgan alifbo uzunligi 256 ga teng bo‘lsa, u holda bo‘lishi mumkin bo‘lgan barcha parollar variatni 2568=264 ga teng. Bir qarashda shuncha sondagi parollarni topish kriptogarfik kalitni topish murakkabligi bilan bir xildek ko‘rinadi. Biroq, parollarni tanlashda foydalanuvchilar tasodifiy bo‘lishiga e’tibor berishmaydi. Natijada esa, foydalanuvchi 8 ta belgidan iborat bo‘lgan parol sifatida kf&Yw!a[dan emas, balki password ko‘rinishidagi parollardan foydalanishga olib kelmoqda.

Bu esa, 263 dan kichik hisoblashga va katta ehtimol bilan parolni topish imkoniyatini keltirib chiqaradi. Masalan, $2^{20} \approx 1\,000\,000$ ta eng keng tarqalgan parollardan iborat bo‘lgan parollar lug‘ati, parolni topish uchun buzg‘unchiga juda qo‘l kelishi mumkin. Kriptografik kalitni topishda esa, 264 ta kalitni 220 ta bo‘lishi mumkin bo‘lgan kalitdan biriga mos kelish ehtimoli $\frac{2^{20}}{2^{64}} = 1/2^{44}$ ga yoki kamida 17 triliondan birga to‘g‘ri keladi. Bu esa parollarni tasodifiy tanlanmasligi ulardagi eng jiddiy muammo ekanligini anglatadi.

11.6. Zaxira nusxalash

Parollarni tanlash tartibi

Barcha parollar bir xil uzunlikda bo‘lsa ham bir xil murakkablik darajasiga ega emas. Masalan quyidagi parollar aksariyat foydalanuvchilar tomonidan zaif deb topilishi mumkin, ayniqsa ismi Frank yoki Austin Stamp bo‘lganlar yoki tug‘ulgan kuni 10/25/1960 bo‘lganlar:

Frank;

Pikachu;

10251960;

AustinStamp.

Biror narsani bilishga asoslangan autentifikasiyada xavfsizlik parolga bog‘liq bo‘ladi va foydalanuvchidan murakkab paroldan foydalanish zaruriyatini qo‘yadi. Biroq, foydalanuvchidan mazkur murakkab parollarni esda saqlash ham talab etiladi. Bu tomondan qaralganda, quyidagi parollar yuqorida keltirilgan zaif parollarga qaraganda yaxshiroqmi???

jfIej(43j-EmmL+y;

09864376537263;

PokemON;

FSa7Yago.

Masalan, jfIej(43j-EmmL+y parolni buzish buzg‘unchi uchun qanchalik murakkab bo‘lsa, uni eslash foydalanuvchi uchun ham shunchalik murakkab. Bunday parolni, ehtimol foydalanuvchi kompyuteri oldidagi eslatmada saqlash mumkin. Bu esa, foydalanuvchi osonroq parolni tanlangan holatga ko‘ra buzg‘unchi uchun ancha oson hisoblanadi.

Yuqorida keltirilgan ikkinchi parol ham faqat raqamlardan tashkil topgan bo‘lsada, uni esda saqlash murakkab vazifa. Hattoki, yadroviy raketani uchirish uchun javobgar bo‘lgan AQShning malakaviy hodimidan ham 12 raqamdan iborat bo‘lgan otish kodini eslab qolishi talab etiladi. Mazkur muammolarni keltirilgan qolgan parollarga nisbatan ham aytish mumkin.

Biroq parollarni oson esda saqlashga imkon beruvchi xiylalar mavjud bo‘lib, ular – iboralarga asoslanadi. Masalan, keltirilgan FSa7Yago parol “four score and seven years ago” iborasidan olingan. Natijada esa, foydalanuvchini esida qolishi oson bo‘lgan biroq hujumchini aniqlashi murakkab bo‘lgan parol yaratildi.

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

Gruppa A. Parol kamida 6 ta belgidan iborat bo‘lishi va ulardan kamida biri harf bo‘lmasligi. Bu holat odatiy parolni tanlash kabi.

Gruppa B. Iboralarga asoslangan holda parollarni yaratish.

Gruppa S. Parol tasodifiy tanlangan 8 ta belgidan iborat bo‘lishi.

Tajribada qatnashgan foydalanuvchilarni parollarini buzishga harakat qilingan va quyidagi natijalar olingan:

Gruppa A. 30% ga yaqin parol osonlik bilan buzilgan. Bunda foydalanuvchilar tomonidan parollarni esda saqlash oson deb topilgan.

Gruppa B. 10% ga yaqin parol buzilgan. Bunda foydalanuvchilar tomonidan parollarni esda saqlash oson deb topilgan.

Gruppa S. 10% ga yaqin parol buzilgan. Bunda foydalanuvchilar tomonidan parollarni esda saqlash juda ham murakkab bo‘lgani aytilgan.

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

11.7. Ma’lumotlarni qayta tiklash

Parolga qarshi hujum tizimlari

Faraz qilaylik buzg‘unchi tashqarida joylashgan (begona) va biror bir tizimga kirish huquqiga ega emas. Bu holda buzg‘unchining umumiy hujum yo‘li quyidagicha bo‘ladi: begona→normal foydalanuvchi→ administrator.

Boshqacha aytganda buzg‘unchi dastlab ixtiyoriy akkauntga kirish usulini qidiradi va keyin o‘z imtiyoz darajasini oshirishga harakat qiladi. Mazkur senariyda, tizimdagi bitta zaif parol yoki butun tarmoqdagi bitta zaif parol hujumning birinchi bosqichini muvaffaqqiyatli amalga oshirilishi uchun yetarli bo‘lishi mumkin. Bundanda xavflirog‘i esa, zaif parollar juda ham ko‘p bo‘lishi mumkin.

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

11.8. Hodisalarni qaydlash

Parollarni saqlash va o‘zaro solishtirish

Parolga asoslangan autentifikasiyalashda kiritilgan parolni to‘g‘riligini tekshirish muhim ahamiyatga ega. Kompyuter uchun, parolni to‘g‘riligini tekshirish uchun, parol taqqoslanuvchi biror bir narsa bo‘lishi kerak. Ya’ni, kompyuter kiritilgan parolni to‘g‘riligini tekshirish uchun biror ko‘rinishda boshqarishi kerak. Biroq, parolni haqiqiy holatda faylda saqlash juda ham yomon g‘oya. Sababi, mazkur holda bu parollar fayli buzg‘unchining asosiy maqsadiga aylanadi. Bu

yerda ham, axborot xavfsizligini ko‘plab sohalarida bo‘lgani kabi, bu muammoni kriptografiya yecha oladi.

Parolni faylda simmetrik kriptotizim yordamida shifrlangan holatga saqlash maqbul ishdek ko‘rinishi mumkin. Biroq, parolni tekshirish uchun ushbu fayl deshifrlanishi shart va deshifrlash kaliti boshqa bir faylda saqlanishi zarur. Bu esa, ushbu kalitlar faylini buzg‘unchi tomonidan o‘g‘irlanishi mumkinligi ehtimolini yaratadi. Ya’ni, parollarni shifrlangan holatda saqlash eng muhim usul sanalmas ekan.

Parolni faylda shifrlangan ko‘rinishda saqlash o‘rniga parolni xeshlangan qiymatini saqlash ancha xavfsiz usul. Masalan, A tomonning paroli FSa7Yago ga teng bo‘lsa, biz faylda $y = h(FSa7Yago)$ ni saqlaymiz. Bu yerda h - kriptografik xesh funksiya. Shundan so‘ng, tizim Alisadan parol x ni kiritishni talab etsa, parol dastlab xeshlanadi va y bilan taqqoslanadi. Ya’ni, agar $y = h(x)$ bo‘lsa, kiritilgan parol to‘g‘ri deb topiladi va foydalanuvchi A autentifikasiyadan o‘tkaziladi.

Parolni xeshda saqlashdan asosiy maqsad, buzg‘unchi parollar saqlangan faylni qo‘lga kiritgan taqdirda ham, haqiqiy parolni o‘rniga uning xesh qiymatini qo‘lga kiritadi. Xesh funksiyalarga qo‘yilgan bir tomonlamalik xususiyatiga ko‘ra, xesh qiymatdan haqiqiy parolni topishning imkoni mavjud emas. Albatta, buzg‘unchi ixtiyoriy parol olib uni xeshlashdan olingan qiymatini solishitirish orqali uni aniqlashi mumkin (faraz bo‘yicha hujum yoki parolni barcha variantlarini ko‘rib chiqish hujumi). Biroq, buzg‘unchi zarur bo‘lgan parolni aniqlashi uchun yetarlicha vaqt va zarur amallarni bajarishi talab etiladi.

Faraz qilaylik, buzg‘unchida N ta eng keng foydalanilgan parollar, $d_0, d_1, d_2, \dots, d_{N-1}$, saqlangan lug‘at mavjud. Shundan so‘ng lug‘atdagi har bir parolni xeshlaydi: $y_0 = h(d_0), y_1 = h(d_1), \dots, y_{N-1} = h(d_{N-1})$ va (d_0, y_0) juftlik ko‘rinishidagi yangi lug‘atni hosil qiladi.

Shundan so‘ng, agar buzg‘unchi biror xesh qiymat ko‘rinishidagi parolni “orqaga qaytarish” uchun uni N ta xesh qiymat bilan solishtirib ko‘radi. Agar moslik aniqlansa, u holda parolni haqiqiy qiymati topiladi. Bundan tashqari, buzg‘unchi hosil qilgan yangi lug‘ati asosida ixtiyoriy parollar faylligini buzish uchun foydalanishi mumkin. Bundan tashqari, (d_0, y_0) ko‘rinishdagi ko‘plab lug‘atlarni Internet tarmog‘i orqali bepul yoki pullik ko‘rinishlarda topish mumkin. Bu esa, mavjud bo‘lgan (d_0, y_0) ko‘rinishdagi lug‘atni bir marta yaratib, so‘ng undan

barcha parollar faylini buzish uchun foydalanish mumkinligini anglatadi.

Xo‘sh, ushbu hujumni oldini olish yoki buzg‘unchi ishini yanada murakkablashtirishning biror usuli bormi? Albatta bor. Buning uchun parolni xeshlab saqlashda unga maxfiy bo‘lgan kattalikni (“tuz”, salt – deb ataladi) qo‘shib, keyin xeshlash tavsiya etiladi. Ya’ni, $y = h(p,s)$ ko‘rinishida. Bu yerda, p – parol bo‘lsa, s – “tuz”. Bu kattalik, simmetrik blokli shifrlashning CBC rejimidagi IV kattalik hisoblanadi. IV kattalik bir xil ochiq matnni turlicha shifrmatnlar ko‘rinishida shifrlash uchun foydalanilgan bo‘lsa, $salt$ ham bir parolni turli xesh qiymatlar ko‘rinishida ifodalash uchun ishlatiladi. “tuz” parollar faylidagi har bir fayl uchun turlicha bo‘ladi. Xo‘sh, mazkur usul qanday qilib buzg‘unchining ishiga salbiy ta’sir ko‘rsatadi.

Faraz qilinsin, p yangi kiritilgan parol bo‘lsin. Biz tasodifiy $salt$, s ni generasiya qilamiz va $y = h(p,s)$ hisoblaymiz va parollar faylida (s,y) shaklida saqlaymiz. Bu o‘rinda foydalanilgan s qiymat maxfiy emas, ya’ni, parollar faylida ochiq ko‘rinishda saqlanadi. Kiritilgan parol x ni tekshirish uchun, parollar faylidan (s,y) olinadi va $h(x,s)$ ni hisoblaydi va uni y bilan taqqoslaydi. Bu holda taqqoslash $salt$ ishlatilmagani kabi, bir xil amalga oshiriladi. Biroq, buzg‘unchiga murakkablik tug‘iladi. Ya’ni, u kerakli parolni olish uchun juda ko‘p hisoblashlarni amalga oshirishi talab etiladi. Faraz qilaylik, A tomonning paroli “tuz” s_a bilan birgalikda xeshlangan va B tomonning paroli esa s_b bilan birgalikda xeshlangan. Mazkur holda, buzg‘unchi A tomonning parolini o‘zidagi parollar lug‘ati asosida tekshirishi uchun lug‘atidagi barcha parollarga s_a ni biriktirib, keyin xeshlashi talab etiladi. Biroq, B tomonning parolini tekshirish uchun esa o‘zidagi barcha parollarga s_b ni biriktirib, xeshlashi talab etiladi. N ta foydalanuvchidan iborat parollar fayli uchun, buzg‘unchining ishi N faktorga ko‘payadi. Bundan tashqari, buzg‘unchi o‘zi uchun yaratgan (d_0,y_0) shaklidagi parollar lug‘ati ham foydasiz bo‘ladi.

Parolni buzushning matematik hisobi

Keling endi parolni buzish matematik tomondan qancha hisob kitobni talab etishini ko‘rib chiqaylik. Faraz qilaylik, olingan parol uzunligi 8 ga teng va foydalanilgan alifbo 128 ta belgidan iborat. Bu holda jami parollarning soni $128^8 = 2^{56}$ ga teng bo‘ladi. Faraz qilaylik foydalanuvchi parollari saqlanuvchi fayl 210 ta paroldan iborat va buzg‘unchi eng keng tarqalgan 220 ta paroldan iborat lug‘atga ega.

Bundan tashqari, ixtiyoriy berilgan parolni buzg‘unchining parollar lug‘atidan topilish ehtimoli ¼ ga teng bo‘lsin. Mazkur holda, buzg‘unchining bajaradigan ishi xeshlashlar soni bilan o‘lchanadi.

Yuqorida keltirilgan farazlar asosida, quyidagi holatlar uchun parolni muvaffaqqiyatli buzishning ehtimolini aniqlaymiz:

Buzg‘unchi A tomonning parolini aniqlashni xoxlaydi (bu holda A tomon balki tizim yoki tarmoq administratoridir). Buzg‘unchi parolni aniqlashda o‘zining parollar lug‘atidan foydalanmaydi.

Buzg‘unchi A tomonning parolini aniqlashni xoxlaydi. Buzg‘unchi o‘zining parollar lug‘atidan foydalanadi.

Buzg‘unchini parollar faylidagi ixtiyoriy parolni o‘zining lug‘atidan foydalanmasdan turib buzish qanoatlantiradi.

Buzg‘unchini parollar faylidagi ixtiyoriy parolni o‘zining lug‘atidan foydalanib turib buzish qanoatlantiradi.

Har bir holatni biz “tuz” bilan yoki “tuz” siz holatlar uchun ko‘rib o‘tamiz.

Holat 1. Agar buzg‘unchi A tomonni parolini aniqlashni istasa va u o‘zining parollar lug‘atidan foydalana olmasa, u holda parolni bo‘lishi mumkin bo‘lgan barcha variantlarini ko‘rib chiqishdan boshqa imkoni yo‘q. Parolni bo‘lishi mumkin bo‘lgan barcha variantlarini hisoblashda esa, buzg‘unchi o‘rtacha $\frac{2^{56}}{2} = 2^{55}$ hisoblashni amalga oshirishi talab etiladi.

Mazkur holdagi natija parol “tuz” bilanmi yoki “tuz”siz xeshlangan holati uchun ham juda ko‘p hisoblashni talab etadi. Masalan, agar parol “tuz”siz holatda xeshlangan bo‘lganda, buzg‘unchidan 2^{55} ta kombinasiyani hisoblash talab etilsa, “tuz” bilan xeshlangan holatda esa parolni xeshlashdan umuman foyda bo‘lmaydi. Ixtiyoriy holatda ham, buzg‘unchi uchun juda katta hisoblash talab etilishi aniq. Shuning uchun bundan keyin mazkur holat ortiq qarab chiqilmaydi va mazmunga ega emas deb qaraladi.

Holat 2. Mazkur holatda ham, buzg‘unchi A foydalanuvchini parolini buzishni istaydi va buning uchun o‘zining eng keng tarqalgan parollar lug‘atidan foydalanadi. Bunda olingan farazga binoan, A tomonning paroli ¼ ehtimollik bilan buzg‘unchining lug‘atidan topilishi mumkin. Faraz qilaylik, A tomonning paroli “tuz” yordamida xeshlangan. Bundan tashqari, A tomonning paroli buzg‘unchining parol lug‘atida bo‘lsin. U holda buzg‘unchi o‘zidagi parol lug‘atini yarmini, 219, hisoblagandan keyin uni aniqlagan bo‘lsin. A tomon paroli ¾

ehtimollik bilan buzg‘unchining lug‘atida mavjud emasligi orqali parolni aniqlash uchun o‘rtacha 255 hisoblash talab etiladi. Mazkur holatlarni birlashtirgan holda buzg‘unchidan kutilayotgan amallar soni quyidagiga teng bo‘ladi:

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

Mazkur holda buzg‘unchining amalga oshiradigan ishlar hajmi birinchi holat bilan (ya’ni, lug‘at foydalanilmagan holat) bir xil.

Agar parol “tuz” siz xeshlangan holatida, buzg‘unchi o‘zining barcha 220 parolini xeshlab oladi va shundan so‘ng kichik vaqt ichida buzg‘unchi hujumni amalga oshiradi.

Holat 3. Mazkur holda, buzg‘unchi parollar faylida saqlangan 1024 ta parolni birini buzsa ham yetarli bo‘ladi. Bunda ham buzg‘unchi o‘zining parollar lug‘atidan foydalana olmaydi.

Faraz qilaylik, $y_0, y_1, \cdots, y_{1023}$ parolning xeshlangan qiymatlari bo‘lsin. Faraz qilaylik, parollar lug‘atidagi barcha 210 parol unikal. $p_0, p_1, \cdots, p_{2^{56}-1}$ parollar 256 ta barcha variantlar bo‘lsin. Parolni topishning barcha variantlarini topish hujumi kabi, buzg‘unchi zarur bo‘lgan parolni topish uchun 255 tekshirishni amalga oshirishi talab etiladi.

Agar parol “tuz”siz xeshlangan bo‘lsa, buzg‘unchi $h(p_0)$ hisoblaydi va uni har bir y_i ($i = 0,1,2,\ldots,1023$ uchun) bilan solishtiradi. Keyin $h(p_1)$ ni hisoblaydi va barcha y_i lar bilan solishtirib chiqadi va qolganlari uchun ham xuddi shu ketma-ketlik takrorlanadi. Mazkur holda buzg‘unchining har bir xeshni hisoblashi 210 ta tekshirishni ta’minlaydi. Buzg‘unchi amalga oshiradigan ish hajmi xeshlashlar soni bilan o‘lchanishi (taqqoslashlar soni bilan emas) sababli va 255 ta taqqoslash talab etilgani bois, buzg‘unchi tomonidan bajarishi kutiladigan ish hajmi $\frac{2^{55}}{2^{10}} = 2^{45}$ ga teng bo‘ladi.

Boshqa holat, parolni “tuz” yordamida xeshlangan bo‘lsin. Bunda, s_i xeshlangan parol y_i ni hisoblashda foydalanilgan bo‘lsin. U holda, buzg‘unchi $h(p_0, s_0)$ ni hisoblaydi va y_0 bilan taqqoslaydi. Keyin, u $h(p_0, s_1)$ ni hisoblaydi va y_1 bilan taqqoslaydi va $h(p_0, s_2)$ ni hisoblaydi va y_2 bilan taqqoslaydi. Shu tarzda davom etib, hisoblash $h(p_0, s_{1023})$ gacha davom etadi. Shundan so‘ng, ushbu jarayon p_1 uchun, p_2 uchun v.h.k. davom ettirilishi shart. Umumiy holda esa buzg‘unchi tomonidan bajariladigan ishlar hajmi birinchi holatdagi kabi 255 ga teng bo‘ladi.

Ushbu holat parolni xeshlashda “tuz” dan foydalanishning afzalligini ko‘rsatadi. Biroq, bu holda amalda uchramasa ham buzg‘unchini eng keng tarqalgan parollar lug‘atidan foydalanmaganini ham hisobga olish zarur.

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

Agar parollarni xeshlashda “tuz”dan foydalanilmagan bo‘lsa, buzg‘unchi osonlik bilan o‘zining lug‘atidagi parollarni xeshlaydi va fayldagi 1024 parolni xesh qiymati bilan taqqoslaydi. 1024 ta paroldan kamida bittasini lug‘atda mavjudligini aniqlashning o‘zi yetarli bo‘lgani uchun, buzg‘unchi tomonidan bajariladigan ish 220 ga teng. Biroq, buzg‘unchi yanada tajribali bo‘lsa, ushbu bajariladigan ishni kamaytirishi mumkin. Shunga qaramay, buzg‘unchining lug‘atida parollar faylidagi kamida bitta parol bo‘lishi mumkin deb faraz qilaylik. Natijada, buzg‘unchi o‘zi kutgan parollar faylidagi bitta parolni aniqlashi uchun o‘zining lug‘atidagi parollarning yarmini, 219 xeshlashi talab etiladi. Uchinchi holatda bo‘lgani kabi, har bir xeshlash amali 210 ta taqqoslashni talab etadi va shuning uchun buzg‘unchidan bajarishi kutilidagan ish hajmi $2^{19}/_{2^{10}}=2^9$ ga teng.

Agar parolni xeshlashda “tuz”dan foydalanilmagan bo‘lsin. Agar lug‘atdagi parollarni xeshlash oldindan amalga oshirilgan bo‘lsa, parollar faylidagi ixtiyoriy parolni topish uchun qo‘shimcha ish talab etilmaydi. Ya’ni, buzg‘unchi parollar faylidagi parollarni o‘zining parollar lug‘atining oldingan hisoblangan qiymatlari bilan solishtiradi va natijada o‘zining lug‘atida mavjud bo‘lgan parol aniqlanadi.

Keling endi amalda bo‘lish ehimoli yuqori bo‘lgan holatni: parollar faylidagi xesh qiymatlar “tuz”dan foydalangan va buzg‘unchi eng keng tarqalgan parollar lug‘atidan foydalangan bo‘lsin. Mazkur holatda, $y_0, y_1, \cdots, y_{1023}$ – fayldagi xeshlangan parollar bo‘lsin va $s_0, s_1, \ldots, s_{1023}$ – ushbu parollarga mos foydalanilgan “tuz” bo‘lsin. Shuningdek, buzg‘unchi tomonidan foydalanilayotgan parollar lug‘ati $d_0, d_1, \ldots, d_{2^{20}-1}$ bo‘lsin. U holda buzg‘unchi $h(d_0, s_0)$ hisoblaydi va y_0

bilan taqqoslaydi. Shunga o‘xshash $h(d_1, s_0)$ hisoblaydi va y_0 bilan taqqoslaydi, $h(d_2, s_0)$ hisoblaydi va y_0 bilan taqqoslaydi v.h.k. Ya’ni, buzg‘unchi dastlab y_0 ni o‘zidagi parollar lug‘atidagi barcha parollar uchun tekshiradi. Bu holat har bir y_i uchun amalga oshiriladi.

Agar y_0 parol lug‘atda mavjud bo‘lsa (1/4 ehtimollik bilan), u holda buzg‘unchi uni 219 ta hisoblashdan so‘ng aniqlaydi. Aks holda (3/4 ehtimollik bilan), buzg‘unchidan 220 ta hisoblash talab etiladi. Agar buzg‘unchi y_0 parol lug‘atdan topsa, u holda o‘zining ishini bajargan hisoblanadi. Aks holda, u y_1 ni hisoblashdan oldin 220 ta hisoblashni bajarishi talab etiladi. Mazkur holatni davom ettirsak, buzg‘unchi tomonidan bajarilishi mumkin bo‘lgan ishni taxminiy hisobi quyidagiga teng bo‘ladi:

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

Albatta bu, kichik bir vazifani bajarish uchun talab etilayotgan ishni yuqori hajmda ekanligini anglatadi.

Umumiy holda aytganda agar foydalanilgan parol zaif bo‘lgan taqdirda, uni aniqlash juda ham oson va ixtiyoriy bir parolni aniqlash butun tizim xavfsizligini yo‘qolishiga olib keladi.

Parol bilan bog‘liq boshqa muammolar

Hozirgi kunda ko‘plab foydalanuvchilarda qator qayd yozuvlari mavjud. Biroq, foydalanuvchilar ko‘p sonli parollarni esda saqlash qobiliyatiga ega emas va shuning uchun ko‘plab hollarda bir xil paroldan foydalanish holatlari kuzatiladi. Bu esa, foydalanuvchining bir parolini buzg‘unchi tomonidan aniqlanishi, ko‘plab qayd yozuvlarini ham buzulishiga olib keladi.

Bundan tashqari, sosial injineriya ham parollarni aniqlashda katta ta’sir qiladi. Masalan, tizim ma’muri tomonidan qayd yozuv bilan bog‘liq muammoni bartaraf etish uchun foydalanuvchi paroli so‘ralganda, aksariyat hollarda uni berish holatlari kuzatilgan. Yaqinda olib borilgan tadqiqotlarga ko‘ra, 34% holatda foydalanuvchilardan parollari so‘ralganda, ular tomonidan so‘rov ma’qullangan.

Bundan tashqari, parollarni qo‘lga kiritishda “keylogger” deb nomlangan zararli dasturiy vositalardan keng foydalaniladi. Mazkur zararli dasturiy vositalar klaviatura orqali kiritiluvchi barcha ma’lumotlarni o‘zida saqlaydi va o‘z serveriga yuborib turadi.

Shuningdek, xeshlangan parollarni aniqlash uchun maxsus dasturiy vositalar mavjud bo‘lib, ularga misol tariqasida LophtCrack (Windows OT uchun) va John the Ripper (Unix OT uchun). Ushbu dasturiy vositalarnnig o‘zida keng tarqalgan parollar lug‘ati mavjud bo‘lib, sodda parollarni topishni osonlik bilan amalga oshirishda qo‘l keladi.

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Risk tushunchasiga izoh bering?
2. Risk darajasi tushunchasiga izoh bering?
3. Risk matrisasi va uning asosiy vazifasini tushuntiring?
4. Risklarni boshqarish nima va uning asosiy bosqichlarini ayting?
5. Tashkilotda risklarni boshqarish freymvorki nima va uning asosiy vazifasini ayting?
6. Risklarni boshqarishning axborot tizimlari nima va ularga misollar keltiring.

XII BOB. KIBERJINOYATLARNING INSON XVFSIZLIGIGA TA’SIRI

12.1. Ijtimoiy injeneriya

“Sotsial injineriya” bu - turli xil psixologik usullar va firibgarlik amaliyotining to‘plami bo‘lib, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olishdir. Maxfiy ma’lumotlar - bu foydalanuvchi ismlari / parollari, shaxsiy muhim ma’lumotlari, ayblov dalillari, bank kartalari raqamlari va moliyaviy yoki obro‘sini yo‘qotadigan har qanday narsa.

Ushbu atama xakerlik sohasidan kirib kelgan. Xaker - bu kompyuter tizimidagi zaifliklarni qidiradigan odam, boshqacha aytganda – “buzg‘unchi”. Ushbu holda sosial injineriya qanday aloqador bo‘lishi mumkin. Hammasi juda oddiy. Hozirgi vaqtda xakerlar har qanday tizimdagi asosiy zaiflik - bu mashina yemas, balki shaxs yekanligini yaxshi tushunishadi. Inson, xuddi kompyuter singari, muayyan qonunlarga muvofiq ishlaydi. Psixologiya, hiyla-nayranglar va ta’sir mexanizmlari doirasida insoniyat tomonidan to‘plangan tajribadan foydalangan holda, xakerlar “odamlarga hujum qilishni” boshladilar. Gohida ular “aql xakerligi” deb ham ataladi.

Misol. Xaker sizdan pul olmoqchi deb faraz qilaylik. Aytaylik u sizning telefon raqamingiz va ijtimoiy tarmoqdagi akkauntingiz haqida ma’lumotga ega. Bundan tashqari u izlanish natijasida sizning akangiz borligini ham aniqladi va akangiz haqida ham yetarlicha ma’lumot to‘pladi. U shuningdek, akangizni telefon raqamini ham qo‘shimcha ishonch uchun bilib qo‘ydi. Shundan so‘ng ushbu ma’lumotlar asosida o‘z rejasini tuza boshladi.

Reja: Xaker sizga kechki vaqtda telefon qilib, sizga (sizni simingiz o‘rniga faqat u atydigan biror lichka ham bo‘lishi mumkin) men akangman deb tanishtiradi va o‘zini ko‘chada bezorilarga duch kelganini va ular barcha narsalarini (telefon, pul, plastik kartochka va boshqalar) olib qo‘yganini aytadi. Bundan tashqari u o‘ziga bir qiz yordam berganini, biroq uning yonida puli yo‘qligini aytadi. Biroq, ushbu qizni yonida plastik kartasi borligini va sizdan ushbu plastik kartaga kasalxonaga yetib borish uchun zarur bo‘lgan 20000 pulni ko‘chirib berishni talab qiladi. Mazkur holatlarning 8/10 da xakerlar muvaffaqqiyatga erishganlar va bu ishlarni amalga oshirish malakali xaker uchun qiyinchilik tug‘dirmaydi.

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

Ushbu holatda xaker tomonidan foydalanilgan fikrlarni ko‘rib chiqaylik:

1. Shaxsni yaxshi yashirdi va real misollarga asoslangan (masalan, sizning rasmlaringiz, faqat sizning yaqinlaringiz biladigan joylar va hak.) yaxshi afsona o‘ylab topdi.

2. Bularning barchasi yetarlicha tez va ishonchli tarzda aytilgan.

3. Ta’sirning juda katta mexanizmidan foydalanilgan – achinishga ta’sir qilingan (hissiyotlarga murojaat qilish).

12.2. Fishing ataka

Sotsial injineriya yo‘nalishlari

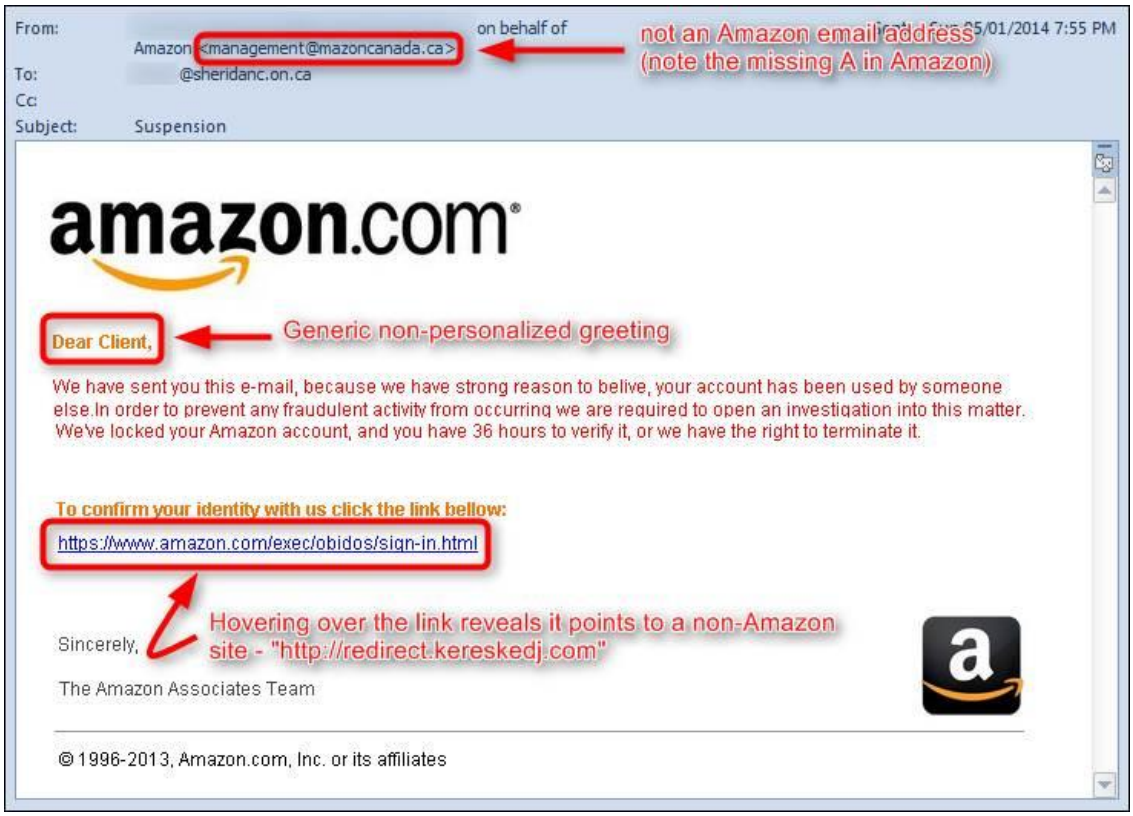
Fishing

Fishing (ing. Phishing – balik ovlash) bu – Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo‘lishdir. Bu hozirda keng tarqalgan sosial injineriya sxemalaridan biri hisoblanadi. Katta hajmdagi shaxsiy ma’lumotlarni keng tarqalishi, fishing “shamolisiz” amalga oshirilmaydi. Fishingning eng keng tarqalgan na’manasi sifatida jabrlanuvchi elektron pochtasiga yuborilgan rasmiy ma’lumot ko‘rinishidagi bank yoki to‘lov tizimidan soxtalashtirilgan xabar hisoblanadi. Bunday elektron pochta xabarlari odatda rasmiy rasmiy veb-saytga o‘xshash va shaxsiy ma’lumotlarni talab qiladigan shaklda bo‘lgan qalbaki veb sahifaga havolani o‘z ichiga oladi.

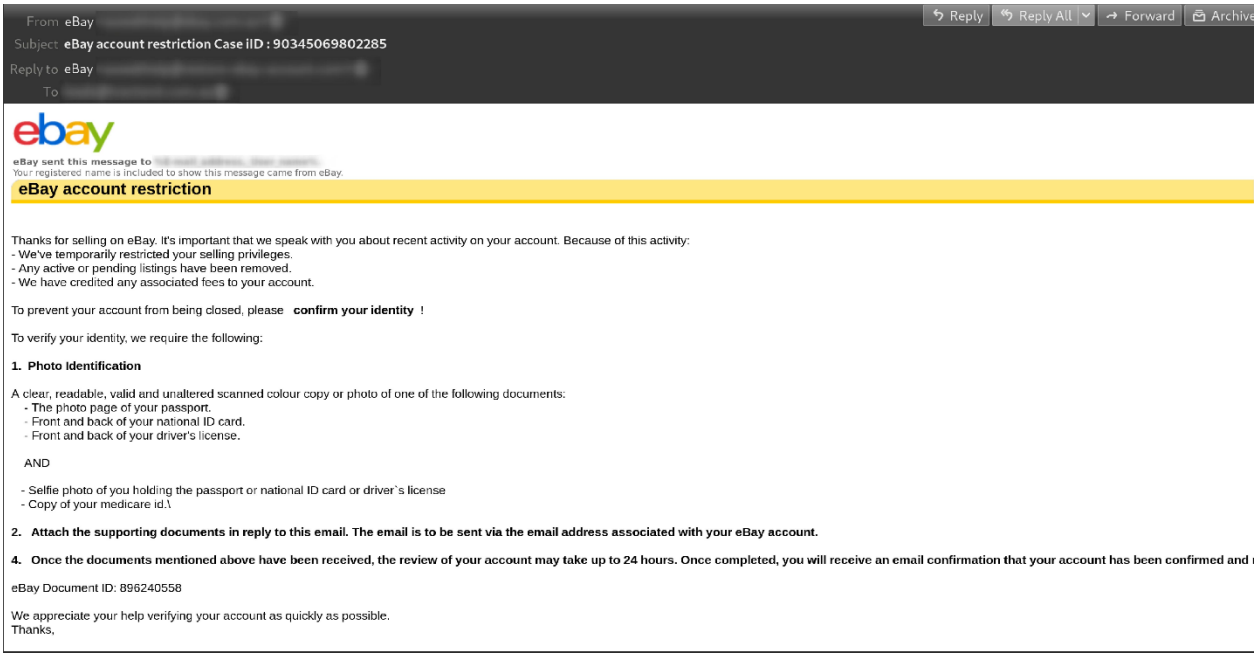
Quyida keng tarqalgan fishing sxemalariga misollar keltirilgan.

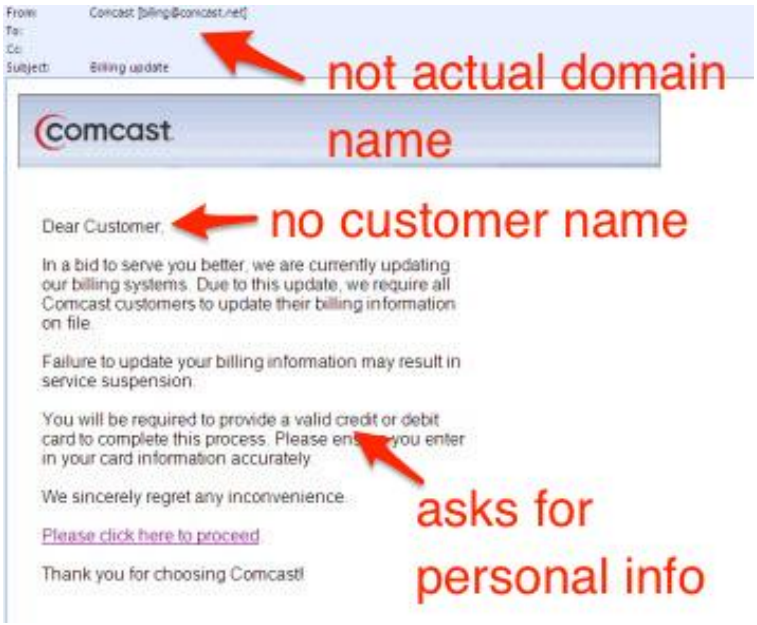
Mavjud bo‘lmagan havola

Fishing hujumining mazkur ko‘rinishida kutilayotgan veb saytga o‘xshash saytni o‘z ichiga olgan havolaga murojaat amalga oshirilishiga jalb qilinadi. Masalan, www.PayPai.com manzili www.PayPal.com manzili sifatida yuborish mumkin. Bu holda kamdan-kam holda foydalanuvchilar “l” harfini o‘riniga “i” harfi borligiga e’tibor berishadi. Havolaga murojat qilinganda esa www.PayPal.com veb saytga o‘xshash, biroq soxtalashtirilgan saytga tashrif buyuriladi va talab kiritilgan to‘lov kartasi ma’lumotlari kiritiladi. Natijada kiritilgan ma’lumotlar tezda xaker qo‘lida bo‘ladi.



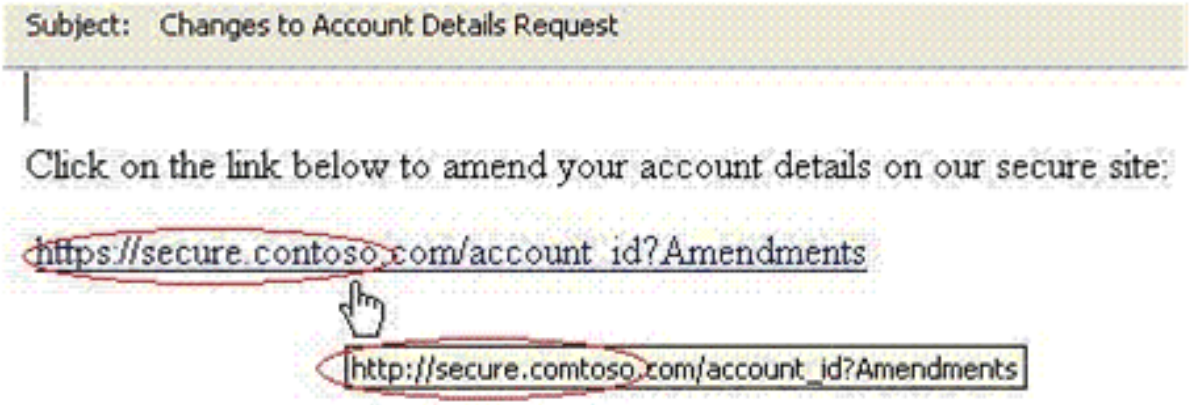
Bunga yaqqol misol sifatida, 2003 yilda eBay foydalanuvchilariga tarqalgan fishing xabarni olish mumkin. Bunga ko‘ra foydalanuvchilarning akkauntlari bloklangani va kredit karta ma’lumotlari blokdan chiqarilishi kerakligi to‘g‘risidani ma’lumot tarqalgan. Ushbu elektron pochtalarda rasmiy veb-saytga o‘xshash soxta veb sahifaga olib boruvchi havola mavjud bo‘lgan. Ushbu fishing hujumini keltirgan zarari bir necha yuz ming dollarga teng bo‘lgan.





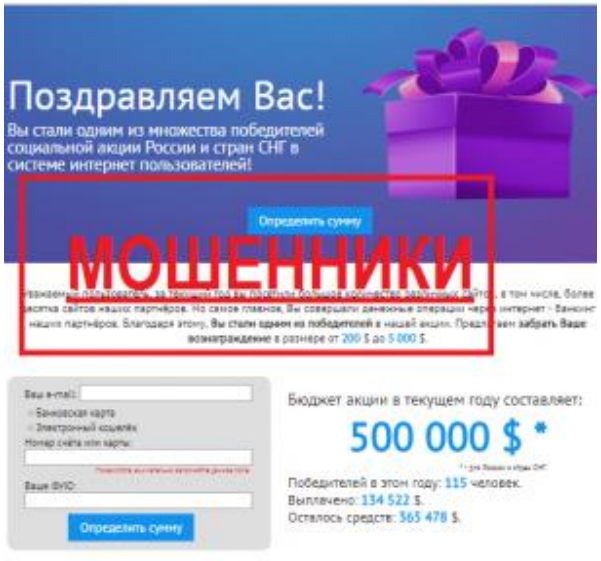
Taniqli korporativ brendidan foydalishga asoslangan firibgarlik

Firibgarlikning mazkur ko‘rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchi elektron pochtalariga xabarlar yuboriladi. Xabarlarda kompaniya tomonidan o‘tkazilgan biror tanlovda g‘alaba qozinilganligi haqidagi tabriklar bo‘lishi mumkin. Unda shuningdek zudlik bilan qayd yozuvi ma’lumotlari va parolni o‘zgartirish kerakligi so‘raladi. Shunga o‘xshash sxemalar texnik ko‘maklashish xizmati nomidan ham amalga oshiririlishi mumkin.



Soxta lotareyalar

Mazkur fishing sxemasiga ko‘ra foydalanuvchi har qanday taniqli kompaniya tomonidan o‘tkazilgan lotareyada yutgani to‘g‘risidagi xabarlarni olishi mumkin. Tashqi tomondan bu elektron xabarlar kompaniyaning yuqori lavozimli xodimlaridan biri nomidan yuborilganga o‘xshaydi.

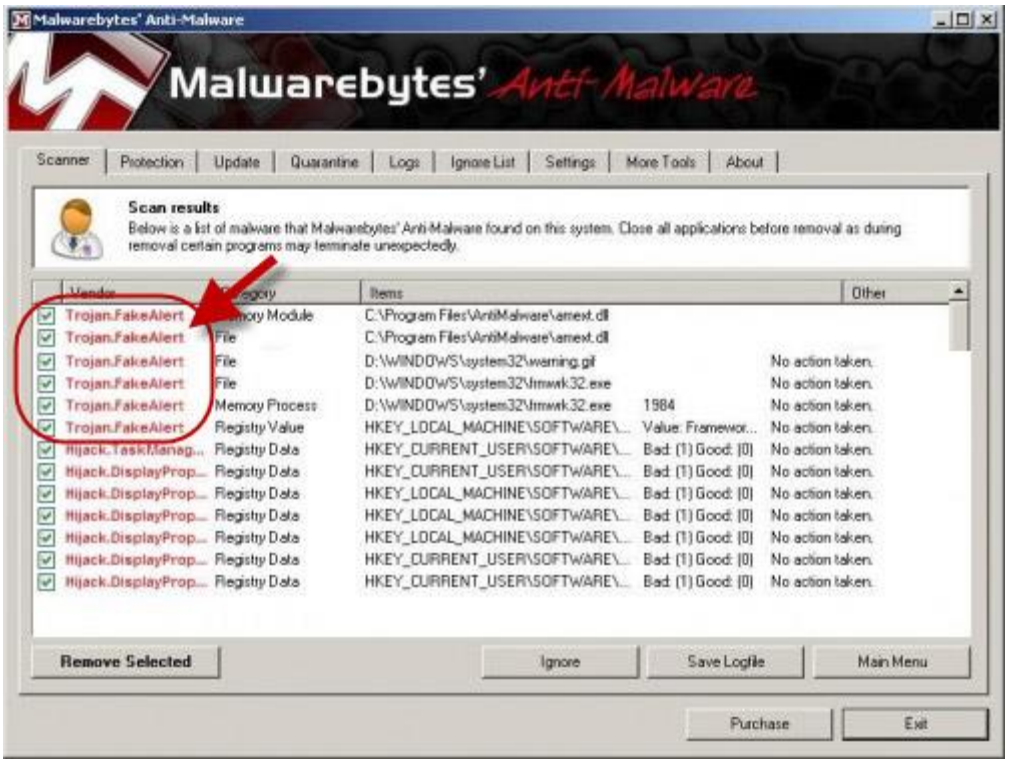


Soxta antivirus va xavfsizlik dasturi

Shunga o‘xshash firibgar dasturiy ta’minot, shuningdek “chaqqon dastur” deb nomlanuvchi mazkur dasturlar antivirus dasturlariga o‘xshasada, ammo vaziyat aksincha bo‘ladi. Bu dasturiy ta’minot turli tahdidlar to‘g‘risida yolg‘on xabarnomalarni keltirib chiqaradi va foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ular bilan elektron pochta, onlayn e’lonlar, ijtimoiy tarmoqlarda, qidiruv tizimlardagi natijalarida va hatto tizim xabarlarini taqlid qiluvchi kompyuterlagi qalqib chiquvchi oynalarda duch kelishi mumkin. Quyida keltirilgan misolda aslida Microsoft Security Essentials bo‘lishi kerak bo‘lgan biroq, o‘ziga Security Essentials 2010 nomini bergan soxta antivirus dasturining ko‘rinishi keltirilgan.

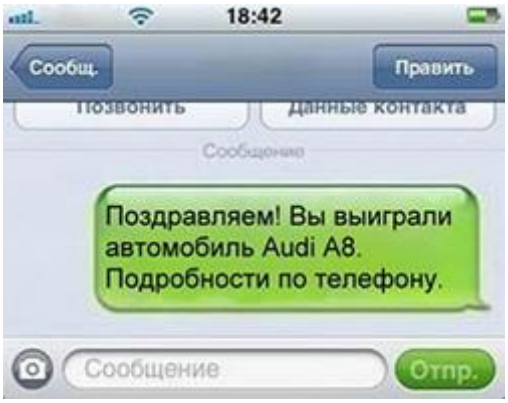


Bundan tashqari Rogue Anti-Spyware (yoki rogueware) deb nomlangan soxta dasturiy vosita mavjud bo‘lib, boshqa antivirus dasturlari tomonidan quyidagi troyan dastur sifatida topiladi.



IVR (Interactive Voice Response) yoki telefon orqali fishing

Fishing sxemasining mazkur usuli oldindan yozib olingan xabarlar tizimidan foydalanishga asoslangan bo‘lib, ular bank va boshqa IVR tizimlarining “rasmiy qo‘nqiroqlari”ni qayta tiklash uchun ishlatiladi. Odatda jabrlanuvchi bakn bilan bog‘lanish va har qanday ma’lumotlarni tasdiqlash yoki yangilash haqidagi so‘rov oladi. Tizim PIN yoki parolni kiritish orqali foydalanuvchini tasdiqlashni talab qiladi. Shuning uchun, oldin kalit iboralarni yozib olgani sababli jabrlanuvchi barcha ma’lumotlarni kiritishi mumkin bo‘ladi. Masalan, parolni almashtirish uchun “1” ni bosing va operator javobini olish uchun “2” ni bosing va hak.



Preteksting

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

Kvid pro kvo (lotinchadan: Quid pro quo)

Ushbu ibora ingliz tilida “xizmat uchun xizmat” degan ma’noni anglatib, sosial injineriyaning mazkur turida xaker korporativ tarmoq yoki elektron pochta orqali kompaniyaga murojaat qiladi. Ko‘pincha xaker o‘zini texnik xizmat ko‘rsatuvchi yordamchi sifatida taqdim qilib, texnik xodimning ij joyidagi muammolarni hal qilishda “yordam beraman” deb tanishtiradi. Texnik muammoni “xal qilishda” nishondagi shaxsni buyruqlarni bajarishga yoki jabrlanuvchining kompyuteriga turli xil dasturlarni o‘rnatishga imkon beradigan harakatlarni bajarishga majbur qiladi.

2003 yilda Axborot xavfsizligi dasturi doirasida o‘tkazilgan tadqiqot shuni ko‘rsatdiki, ofis xodimlarining 90% har qanday xizmat yoki to‘lov uchun maxfiy ma’lumotlarni, masalan, o‘zlarining parollarini, berishga tayyor ekanlar.

“Yo‘l-yo‘lakay olma”

sotsial injineriyaning mazkur usulida xaker maxsus yozilgan zararli dastur yozilgan ma’lumot saqlagichlardan foydalanadi. Buning uchun u zararli dasturlar yozilgan saqlagichlarni qurbon ish muhiti yaqinida, jamoat joylarida va hakazo joylarda qoldiradi. Ma’lumot saqlovchilar tashkilotga tegishli shaklda rasmiylashtiriladi. Masalan, ushbu hujum turiga xaker tomonidan korporasiya logotipi va rasmiy veb-say manzili tushurilgan kompakt diskni qoldirib ketadi. Ushbu disk sirtida “Rahbarlar uchun ish haqlari” dib yozilishi mumkin. Ushbu saqlagichni qo‘lga kiritgan qurbon uni o‘z kompyuteriga qo‘yib ko‘radi.

Ochiq ma’lumot to‘plash

sotsial injineriya texnikasi nafaqat psixologik bilimlarni, balki inson haqida kerakli ma’lumotlarni to‘plash qobilyatini ham talab qiladi. Bundan ma’lumotlarni olishning nisbatan yangi usuli uni ochiq manbalardan, asosan ijtimoiy tarmoqlardan to‘plashdir. Masalan, «Odnoklassniki», «VKontakte», «Facebook», «Instagram» kabi

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

Bunga yaqqol misol sifatida Yevgeniy Kasperskiyning o‘g‘lini o‘g‘irlab ketilganini misol qilib olish mumkin. Ya’ni, tergov davomida jinoyatchilar o‘smirning kun tartibini va marshrutini ijtimoiy tarmoqdagi sahifalardagi yozuvlardan bilib olishgani aniqlangan.

Ijtimoiy tarmoqdagi o‘z sahifasidagi ma’lumotlarga kirishni cheklab qo‘ygan taqdirda ham, foydalanuvchi hyech qachon firibgarlik qurboni bo‘lmasligiga ishonch yo‘q. Masalan, Brazilyaning kompyuter xavfsizligi bo‘yicha tadiqiqotchisi 24 soat ichida sosial injereniya usullaridan foydalangan holda har qanday Facebook foydalanuvchisi bilan do‘st bo‘lishi mumkinligini ko‘rsatdi. Tajriba davomida Nelson Novayes Neto dastlab tanlab olingan maqsadi uchun uning atrofidagi odam – uning xo‘jayni uchun soxta qayd yozuvini yaratadi. Avval Neto jabrlanuvchining xo‘jaynining do‘stlariga va undan keyin to‘g‘ridan-to‘g‘ri qurbonning do‘stiga do‘stlik so‘rovini yubordi. 7.5 soatdan so‘ng esa tadjqiqotchi jarblanuvchi bilan do‘stlashdi. Shunday qilib, tadqiqotchi foydalanuvchining shaxsiy ma’lumotlarini olish ikoniyatiga ega bo‘ldi.

“Elka orqali qarash” hujumi

Ushbu hujumga ko‘ra buzg‘unchi jabrlanuvchiga tegishli ma’lumotlarini uning elkasi orqali qarab qo‘lga kiritadi. Ushbu turdagi hujum jamoat joylarida, masalan, kafe, avtobus, savdo markazlari, ayeroport, temir yo‘l stansiyalarida keng tarqalgan.

Olib borilgan so‘rovnomalar shuni ko‘rsatdiki:

85% ishtirokchilar o‘zlari bilishlari kerak bo‘lmagan maxfiy ma’lumotlarni ko‘rganliklarini tan olishdi;

82% ishtirokchilar ularning ekranidagi ma’lumotlarini ruxsatsiz shaxslar ko‘rishi mumkinligini tan olishdi;

82% ishtirokchilar tashkilotdagi hodimlar o‘z ekranini ruxsatsiz odamlardan himoya qilishiga ishonishmaydi.

Teskari sosial injineriya

Jabrlanuvchining o‘z tajovuzkorga o‘z ma’lumotlarini taqdim qilishi teskari sosial injineriyaga tegishli holat hisoblanadi. Bu bir qarashda ma’noga ega bo‘lmagan fikr hisoblansada, aksariyat hollarda jarblanuvchilarning o‘zi muammolarini hal qilish uchun tajovuzkorni

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

Mashhur sosial injinerlar

Kevin Mitnik. Kevin tarixdagi eng mashhur sosial injnerlardan biri bo‘lib, u dunyodagi mashhur kompyuter xakeri va xavfsizlik bo‘yicha mutaxassisi bo‘lib qolmasdan, u sosial injineriyaga asoslangan kompyuter xavfsizligiga asoslangan ko‘plab kitoblarning ham muallifidir. Uning fikriga ko‘ra xavfsizlik tizimini buzishdan ko‘ra, aldash yo‘li orqali parolni olish osonroq.

Aka-uka Badirlar. Ko‘r bo‘lishiga qaramasdan aka-uka Mushid va Shadi Badirlar 1990 yillarda Isroilda sosial injineriya va ovozni soxtalashtirish usullaridan foydalangan holda bir nechta yirik firibgarlik sxemalarini amalga oshirishga muvaffaq bo‘lgan. Televideniyaga bergan intervyusida ular: “faqat telefon, elektr va noutbuklardan foydalanmaydiganlar faqat tarmoqda xavfsizdir” dedi.

12.3. Ijtimoiy injeneriyadan himoyalanish chora-tadbirlari

O’zlarining hujumlarini amalga oshirishda sosial injineriya texnikasidan foydalangan tajovuzkorlar tez-tez muloyimlik, dangasalik, xushmomilalik hamda foydalanuvchi va tashkilotlar xodimlarining qiziqishlaridan foydalanadilar. Ushbu hujumlarni oldini olish ular 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 etkazib beruvchi, hamkor kompaniyaning xodimi, qonun vakili sifatida tanishtirish;

o‘zini biror rahbar sifatida tanishtirish;

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

muammo yuzaga kelganda yordam beruvchi va keyinchalik muammo tug‘ilganda yordam beruvchi sifatida tanishtirish;

ishonchli hosil qilish uchun ichki jarangdorlik va terminologiyadan foydalanish;

maktubga turli zararli dasturlarni qo‘shib yuborish;

soxta ochilgan oynada login/parolni qayta kiritishni so‘rash;

foydalanuvchi nomi va paroli bilan saytdan o‘tish uchun biror sovg‘a taklif etish;

jabrlanuvchi kompyuteriga yoki dasturiga kiritilgan kalitlarni yozib olish (keylogger dasturlari);

turli xil ma’lumot saqlovchilarni zararli dasturiy vosita bilan bilan foydalanuvchi stoliga tashlash;

turli ovozli qo‘ng‘iroqlardagi ovozli xabarlar va hak.

sotsial injineriya bilan bog‘liq tahdidlarni quyidagicha klassifikasiyalash mumkin:

Telefon bilan bog‘liq tahdidlar. Telefon hanuzgacha tashkilotlar ichida va ular o‘rtasidagi aloqaning eng mashhur usullaridan biri hisoblanadi. Shuning uchun u sosial injineriya uchun samarali vosita bo‘lib qolmoqda. Telefonda gaplashayotganda, suhbatdoshning shaxsini tasdiqlashning iloji yo‘q. Bu hujumchilarga xodimga, xo‘jayinga yoki maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonish mumkin bo‘lgan har qanday boshqa shaxsni o‘rniga bo‘lish imkonini beradi. Zo‘ravonlik qurboni yordam berishdan boshqa imkoni yo‘q. Ayniqsa uyushtiriladigan suhbat so‘rov ahamiyatsiz bo‘lib ko‘rinsa.

Uyali telefondan foydalanuvchilarni pul o‘g‘irlashga qaratilgan firibgarlikning turli usullari ham mashhur. Bu qo‘ng‘iroqlar yoki lotereyalardagi yutuqlar, SMS-xabarlar, xatolar orqali pulni qaytarish to‘g‘risida so‘rovlar yoki jabrlanuvchining yaqin qarindoshlari muammoga duch kelganligi hamda ma’lum miqdordagi pulni zudlik bilan o‘tkazish kerakligi haqidagi xabarlar bo‘lishi mumkin.

Mazkur hollarda quyidagi xavfsizlik choralarini amalga oshirish talab etiladi:

telefon qiluvchining shaxsini aniqlash;

raqamni aniqlash xizmatidan foydalanish;

SMS – xabardagi nomalum havolalarga e’tibor bermaslik.

Elektron pochta bilan bog‘liq tahdidlar. Ko‘pgina xodimlar har kuni korporativ va shaxsiy pochta tizimlari orqali o‘nlab yoki hatto yuzlab elektron pochta xabarlarini olishadi. Albatta, bunday

yozishmalar oqimi bilan har bir harfga etarlicha e’tibor berishning imkoni yo‘q. Bu hujumlarni o‘tkazishni sezilarli darajada osonlashtiradi. Elektron pochta tizimlarining ko‘plab foydalanuvchilari bunday ishlarni bir papkadan ikkinchisiga qog‘ozlarni o‘tkazishni elektron analogi sifatida qabul qilib, bunday xabarlarni qabul qilishda xotirjam bo‘lishadi. Tajovuzkor pochta orqali oddiy so‘rov yuborganda, uning qurboni ko‘pincha uning xatti-harakatlari haqida o‘ylamasdan ular so‘ragan narsani bajaradi. Elektron pochtalarda xodimlarni korporativ atrof-muhit muhofazasini buzishga undaydigan giperhavolalar bo‘lishi mumkin. Bunday havolalar har doim ham da’vo qilingan sahifalarga olib kelmaydi.

Xavfsizlik choralarining aksariyati ruxsatsiz foydalanuvchilarning korporativ resurslarga kirishini oldini olish uchun ishlab chiqilgan. Agar buzg‘unchi tomonidan yuborilgan giperhavolani bosish orqali foydalanuvchi troyan yoki virusni korporativ tarmoqqa yuklasa, bu ko‘plab himoya turlarini chetlab o‘tishga imkon beradi. Giperhavola, shuningdek, ma’lumot yoki yordamni talab qiladigan qalqib chiquvchi ilovalar bilan xostga ishora qilishi mumkin. Firibgarlikning boshqa turlari singari, zararli hujumlardan himoya qilishning eng samarali usuli bu kutilmagan kiruvchi elektron pochta xabarlariga shubha bilan qarashdir. Ushbu yondashuvni butun tashkilotda tarqatish uchun quyidagi elementlarni o‘z ichiga olgan xavfsizlik siyosatiga elektron pochtadan foydalanishning aniq prinsiplari kiritilishi kerak:

hujjatlarga qo‘shimchalar;

hujjatdagi giperhavolalar;

shaxsiy yoki korporativ ma’lumotlarni kompaniya ichiga so‘rash;

shaxsiy yoiki korportiv ma’lumotlarga kopmaniya tashqarisidan keladigan so‘rovlar.

Tezkor xabarlardan foydalanishga asoslangan tahdidlar. Tezkor xabar almashish bu - ma’lumotlarni uzatishning nisbatan yangi usuli. Ammo u korporativ foydalanuvchilar orasida allaqachon mashhurlikka erishgan. Foydalanishning tezligi va qulayligi tufayli ushbu aloqa usuli turli xil hujumlar uchun keng imkoniyatlarni ochib beradi. Foydalanuvchilar unga telefon kabi qarashadi va uni potensial dasturiy tahdidlar bilan bog‘lashmaydi. Tezkor xabarlar xizmatidan foydalanishga asoslangan hujumlarning ikkita asosiy turi bu zararli dasturga havola va dasturning o‘zi haqida xabarning ko‘rsatilishidir. Albatta, tezkor xabar almashish ham ma’lumot so‘rash usullaridan biridir. Tezkor xabarlar xizmatlarining xususiyatlaridan biri bu

aloqaning norasmiy xususiyati. Har qanday nomlarni moslashtirish qobiliyati bilan bir qatorda, bu omil tajovuzkorni boshqa odam bo‘lib ko‘rsatishga imkon beradi va muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada oshiradi. Agar kompaniya tezkor xabarlar orqali taqdim etiladigan xarajatlarni kamaytirish va boshqa afzalliklardan foydalanmoqchi bo‘lsa, korporativ xavfsizlik siyosatida tegishli tahdidlardan himoya qilish mexanizmlarini ta’minlash kerak. Korporativ muhitda tezkor xabar almashish ustidan ishonchli boshqaruvga ega bo‘lish uchun siz bir nechta talablarga javob berishingiz kerak:

tezkor xabarlar uchun bitta platformani tanlash;

tezkor xabar yuborish xizmatini o‘rnatishda xavfsizlik sozlamalarini aniqlash;

yangi aloqalarni o‘rnatish tamoyillarini aniqlash;

parol tanlash standartlarini o‘rnatish;

tezkor xabarlardan foydalanish bo‘yicha tavsiyalar berish.

sotsial injineriyaning mutaxassislari tashkilotlar uchun quyidagi asosiy himoya usullarini qo‘llashni tavsiya etadilar:

muhim ma’lumotlar ko‘rinishida bo‘lishi mumkin bo‘lgan zararsiz ko‘rinadigan ma’lumotlar turlarini hisobga oladigan ishonchli ma’lumotlarni tasniflash siyosatini ishlab chiqish;

ma’lumotlarni shifrlash yoki foydalanishni boshqarish yordamida mijoz ma’lumotlari xavfsizligini ta’minlash;

xodimlarni sosial injinerni tanib olish ko‘nikmalariga o‘rgatish, ular shaxsan tanimaydigan odamlar bilan muloqotdagi shubhani paydo bo‘lishiga o‘rgatish;

xodimlarga parollarni almashishni yoki umumiy foydalanishni taqiqlash;

shaxsan tanish bo‘lmagan yoki biron-bir tarzda tasdiqlanmagan shaxsga bo‘limga tegishli ma’lumotni berishni taqiqlash;

maxfiy ma’lumotlarga kirishni so‘raganlar uchun maxsus tasdiqlash proseduralaridan foydalanish.

sotsial injineriya texnikasidan foydalangan holda yirik kompaniyalar va ularning xodimlarini firibgarlardan himoya qilish uchun ko‘pincha murakkab ko‘p darajali xavfsizlik tizimlari qo‘llaniladi. Bunday tizimlarning ba’zi xususiyatlari va majburiyatlari quyida keltirilgan:

Fizik xavfsizlik. Kompaniya binolari va korporativ resurslarga kirishni cheklaydigan to‘siqlar. Shuni unutmangki, kompaniyaning

resurslari, masalan, kompaniya hududidan tashqarida joylashgan axlat konteynerlari fizik himoyalanmagan.

Ma’lumotlar. Biznes ma’lumotlari: qayd yozuvlari, pochta va boshqalar. Tahdidlarni tahlil qilish va ma’lumotlarni himoya qilish choralarini rejalashtirishda qog‘oz va elektron ma’lumotlar tashuvchilar bilan ishlash tamoyillarini aniqlash kerak.

Ilovalar. Foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofingizni himoya qilish uchun tajovuzkorlar elektron pochta dasturlari, tezkor xabarlar xizmati va boshqa dasturlardan qanday foydalanishlari mumkinligini ko‘rib chiqishingiz kerak.

Komp’yuterlar. Tashkilotda ishlatiladigan serverlar va mijoz tizimlari. Korporativ komp’yuterlarda qaysi dasturlardan foydalanish mumkinligini ko‘rsatadigan qat’iy tamoyillarni belgilab, foydalanuvchilarni o‘zlarining komp’yuterlariga to‘g‘ridan-to‘g‘ri hujumlardan himoya qilish.

Ichki tarmoq. Korxona tizimlari o‘zaro ta’sir qiladigan tarmoq. Bu mahalliy, global yoki simsiz bo‘lishi mumkin. So‘nggi yillarda masofadan ishlaydigan usullarning mashhurligi oshib borishi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o‘zboshimchalik asosida kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilish uchun nima qilish kerakligini tushunishlari kerak.

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

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

daromadning oshishi;

o‘zgaruvchi vaziyatlarga reaksiya tezligining oshishi: harajat va chiqimlarning pasayishi;

innovatsiyaning tezlashishi;

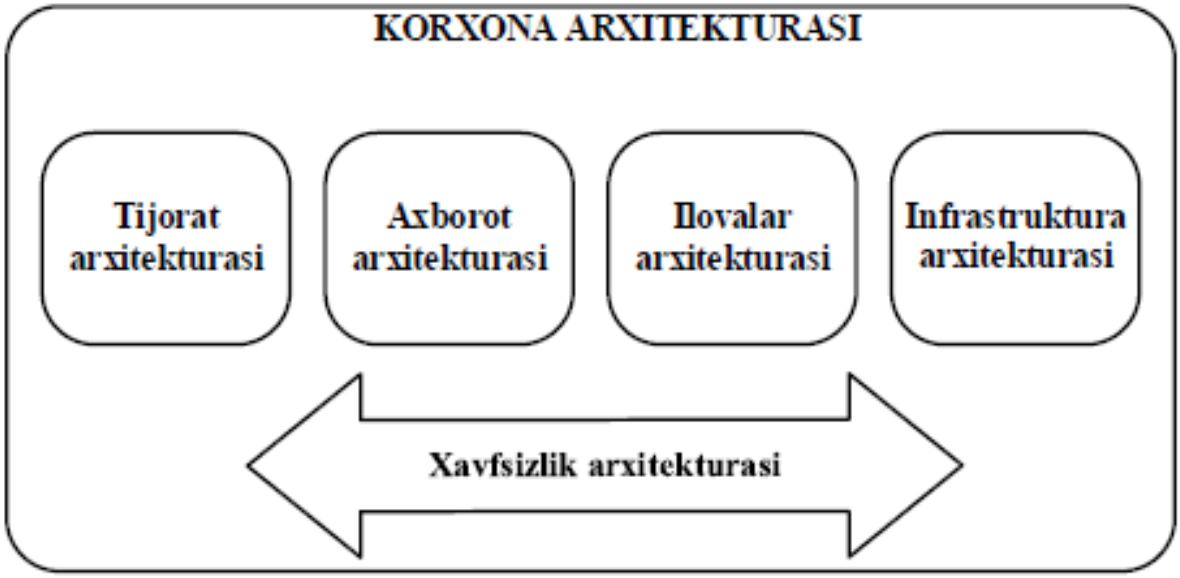
bozorga mahsulot va xizmatlarni taqdim etish vaqtining qisqarishi;

buyurtmachilar va sheriklar xolisligining oshishi: raqobatlik qobiliyatining oshishi;

me'yoriy talablarga moslikni ta'minlash.

Yuqorida keltirilgan barcha masalalarni yechishda korxona arxitekturasidan foydalaniladi (4.1-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.



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.

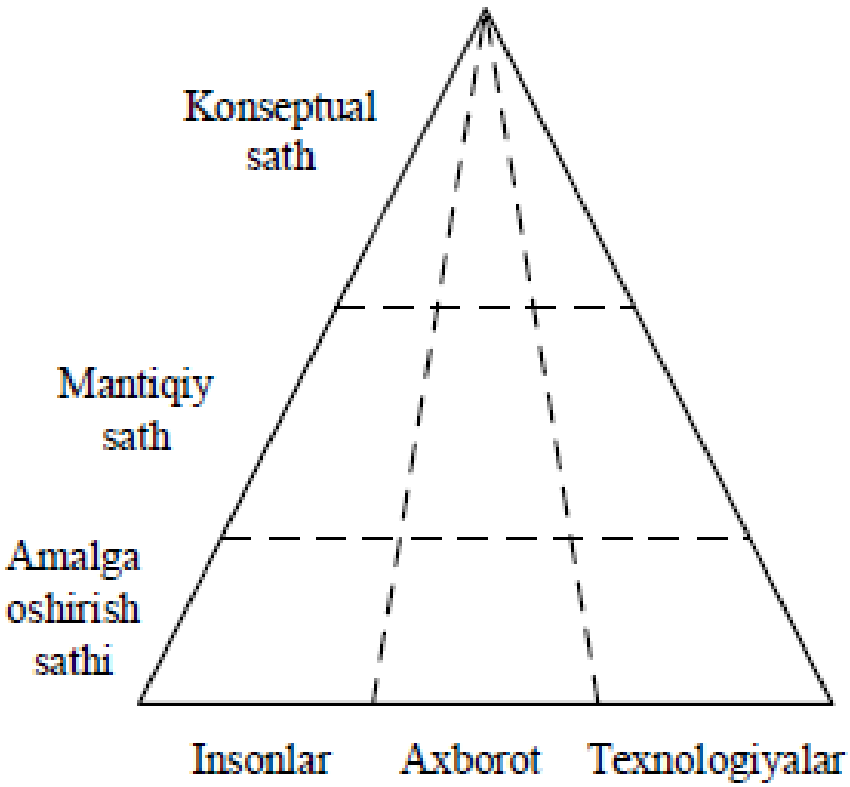
Axborot va axborot tizimlari nafaqat tijoratdagi har qanday o‘zgarishlarni madadlaydi, balki ularni oldindan sezadi, ularga oldindan tayyorlanadi. ba'zi xollarda esa yangi tijorat-imkoniyatlarining paydo bo‘lishiga yordam beradi. Biroq tijorat doimo istalgancha rivojlanmaydi. Bunda ma`lumotlarning sirqib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

12.4. Kiberxavfsizlik arxitekturasi

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 holatini 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). 12.1-rasmda bunday arxitektura keltirilgan bo‘lib, odatda texnologiyalar jihatidagi qismi xavfsizlik xizmati nazoratidan chetda qoladi.

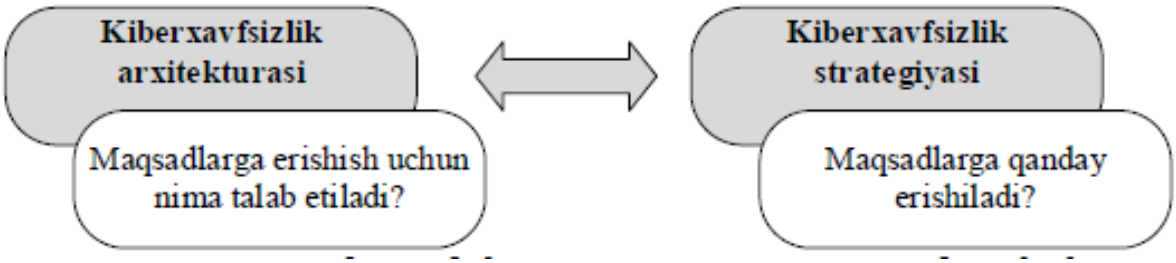


12.1-rasm. Kiberxavfsizlik arxitekturasi

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

12.5. Kiberxavfsizlik strategiyasi

Strategiya korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta'minlashga mo‘ljallangan strukturalangan va o‘zaro bog‘langan harakatlar to‘plami. 12.2-rasmda arxitektura bilan strategiyaning o‘zaro bog‘liqligi keltirilgan. Strategiya kiberxavfsizlik arxitekturasi ko‘rinishidagi maqsadga ega bo‘lgan holda erishishning optimal yo‘lini belgilaydi.



12.2-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.

12.6. Kiberxavfsizlik siyosati

Kiberxavfsizlik siyosati va uni amalga oshirish

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

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

Inventarizatsiya apparat va dasturiy vositalardan tashqari dasturiy va apparatura hujjatlari, texnologik hujjat va h. kabi kompyuterga taalluqli bo‘lmagan resurslarni ham qamrab olishi shart. Ushbu hujjatlar

tarkibida tijoratni tashkil etish xususiyatlari to‘g‘risidagi axborot bo‘lishi mumkin va bu hujjatlar buzg‘unchilar foydalanishi mumkin bo‘lgan joylarni ko‘rsatadi.

Xavfsizlik siyosatining zaruriyati:

Tashkilot bo‘ylab foydalanilayotgan qurilmalar soni ortib borishi tarmoqda uzatilayotgan va saqlanadigan axborot hajmini ortishiga olib kelmoqda. Bu holat esa o‘z navbatida turli zaifliklar natijasida hosil bo‘lgan xavfsizlik tahdidlarini ortishiga ham sababchi bo‘ladi. Xavfsizlik siyosati tashkilotga ushbu tahdidlarga qarshi kurashish va unga axborotning yo‘qolishidan himoyalash imkonini beradi.

Xavfsizlik siyosati tashkilotning barcha funksiyalarini xavfsiz tarzda amalga oshirish orqali xavfsizlik prinsiplarining kelishilgan vazifalarini ta'minlaydi. Xavfsizlik siyosati mijozlar bilan ishonchga asoslangan aloqani qurishda axborot xavfsizligi standartlarining mosligini ta'minlaydi. Xavfsizlik siyosati tashqi axborot tahdidlariga kompaniyaning duchor bo‘lishi xavfini pasaytirishga yordam beradi.

Xavfsizlik siyosati tarmoqda qanday qoidalar foydalanishi kerakligini. konfidensial axborot qanday saqlanishi va tashkilot ma'lumotlarini oshkor bo‘lishi va majburiyatlari kamaytirish uchun qanday shifrlash algoritmlari kerakligini aniqlash orqali qonuniy himoyani ta'minlaydi.

Xavfsizlik siyosati tahdidlarning sodir bo‘lishidan oldin ularni bashoratlash va zaifliklarni aniqlash orqali xavfsizlik buzilishlari holatining ehtimolini kamaytiradi.

U shuningdek, zaxira nusxalash va qayta tiklash amallarini joriy qilish orqali tashkilot ma'lumotlarining yo‘qolishi va sirqib chiqishi xavfini minimallashtiradi.

Xavfsizlik siyosatining afzalliklari:

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

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

Qurilmalardan foydalanish va ma'lumotlar transferining monitoringlanishi va nazoratlanishi: xavfsizlik siyosati xodimlar tomonidan amalga oshirilgani bois, ma'murlar tashkilotdagi trafikni va

foydalanilgan tashqi qurilmalarni doimiy tarzda monitoringlashi zarur. Kiruvchi va chiquvchi trafikning monitoringi va auditi doimiy ravishda amalga oshirilishi shart.

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

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

Boshqaruvdagi hayajon darajasining kamayishi: xavfsizlik siyosati amalga oshirilganida boshqaruvchi kam hayajonga ega bo‘ladi. Xavfsizlik siyosatidagi bir vazifa tashkilotning biror xodimiga biriktirilishi shart. Agar ushbu holat amalga oshirilsa, tarmoqda biror nojo‘ya holat kuzatilsa ham, boshqaruvda hech qanday xavotir bo‘lmaydi.

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

Xavfsizlik siyosatining iyerarxiyasi:

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

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

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

Siyosatlar. Siyosatlar yordamida tashkilot shaxsiy tarmoq xavfsizligi uchun qonuniy ichki tarmoq talablarini yaratadi. Siyosat turli muolajalardan iborat bo‘lib, ular tashkilot uchun xavfsizlik arxitekturasini 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‘riqnomalari 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 risklari 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. Bundan tashqari, xavfsizlik siyosati tashkilotdagi dasturiy ta'minot va jihozlar vazifasini tavsiflaydi.

Axborot texnologiyalari sohasidagi korxonalarda quyidagi xavfsizlik siyosatlari qo‘llaniladi:

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

Muammoga qaratilgan xavfsizlik siyosatlari (Issue-Specific Security Policies, ISSP): bu siyosatlar tashkilotdagi aynan xavfsizlik muammosiga qaratilgan bo‘lib, ushbu xavfsizlik siyosatlarining qamrovi va qo‘llanilish sohasi muammo turi va unda foydalanilgan usullarga bog‘liq bo‘ladi. Unda profilaktik choralar, masalan, foydalanuvchilarning foydalanish huquqini avtorizasiyalash uchun zarur bo‘lgan texnologiyalar ko‘rsatiladi.

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

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

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

Internetdan foydalanish siyosatini quyidagi to‘rtta kategoriyaga ajratish mumkin:

1. Tartibsiz siyosat (Promiscuous Policy): ushbu siyosat tizim resurslaridan foydalanishda hech qanday cheklovlarni amalga oshirmaydi. Masalan, bu siyosatga ko‘ra foydalanuvchi istalgan saytga kirishi, istalgan dasturni yuklab olishi, masofadagi kompyuterdan yoki tarmoqdan foydalanishi mumkin. Bu siyosat korporativ tashkilotlarning ofislarida ishlovchi yoki tashkilotga kelgan mehmonlar uchun foydali hisoblansada, kompyuterni zararli dasturlar asosidagi tahdidlarga zaif qilib qo‘yishi mumkin. Ya’ni, Internetdan foydalanishda cheklanishlar mavjud bo‘lmagani bois, foydalanuvchilar bilimsizligi natijasida zararli dasturlar kirib kelishi mumkin.

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

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

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

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

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

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

O‘z-o‘zini nazorat va muhokama qilish uchun savollar

1. Ijtimoiy injeneriya deganda nimani tushunasiz?
2. Fishing atakalar qanday amalga oshirilari?
3. Ijtimoiy injeneriyadan qanday himoyalanish mumkin?
4. Axborot xavfsizligi arxitekturasi va uning sathlari mohiyati.
5. Axborot xavfsizligi strategiyasi tushunchasi.
6. Korxona arxitekturasini tuzishda xavfsizlik strategiyasi va
7. arxitekturasining o‘rni.
8. Axborot xavfsizligi siyosati va uning asosiy vazifasi nimadan iborat?
9. Xavfsizlik siyosati nima uchun zarur?

GLOSSARIY

Termin	O’zbek tilidagi sharhi	Ingliz tilidagi sharhi
Axborot	muayyan obyekt xususidagi bilimlarimizning noaniqlik darajasini pasaytirishga imkon beruvchi har qanday ma’lumot.	data that reduces the uncertainty degree of knowledge about certain object.
Avtomatlashtirilgan axborot tizimi	ma’lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo‘ljallangan dasturiy va apparat vositalar.	a set of software and hardware designed for the creation, transmission, processing, distribution, storage and/or data and information management and production calculations.
Xavf-xatarni agregirlash	birlashgan xavf-xatarni teranrok tushunishga mo‘ljallangan bir necha xavf-xatarni bitta xavf-xatarga birlashtirish.	sombine multiple risks in a risk, aimed at a better understanding of the overall risk.
Xavf - xatar tahlili	nomuvofik hodisalar paydo bo‘lish holida kutiladigan zararni aniqlash maqsadida, ehtimollik hisoblashlardan foydalanib, tizim xarakteristikalarini va salbiy tomonlarini o‘rganish jarayoni. Xavf – xatarni tahlillash masalasi u yoki bu xavf – xatarning maqbullik darajasini aniqlashdan iborat.	the process of studying the characteristics and weaknesses of the system, conducted using a probabilistic calculations in order to determine the expected damage in case of adverse events. The task of risk analysis is to determine the acceptability of a risk to the system.
Xavfsizlik xizmati ma’muri	xavfsizlikni ta’minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to‘liq tasavvurga ega shaxs (yoki shaxslar guruhi).	person (or group of people) having (s) complete understanding of one or more security systems and controls (s) design and use.
Faol tahdid	tizim holatiga atayin ruxsatsiz o‘zgartirish kiritish tahdidi.	the threat of a deliberate unauthorized system state changes.
Trafik tahlili	1. Trafik oqimini kuzatish (borligi, yukligi xajmi, yunalishi va chastotasi) asosida	1 . Report on the state information based on observation of traffic

	axborat xolati xususida xulosa qilish. 2. Deshifrlanishga sabab bo‘lmaydigan, ammo g‘animga yoki buzg‘unchiga uzatilayotgan ochik matn va, umuman, kuzatilayotgan aloqa tizimining ishlashi xususidagi bilvosita axborotni olishiga imkon beruvchi aloqa tizimi orqali uzatiluvchi shifrlangan xabarlar majmuining tahlili. Trafik tahlili shifrlangan xabarlarning rasmiylashtirish xususiyatlaridan, ularning uzunligi, uzatilish vaqti, uzatuvchi va qabul qiluvchi xususidagi malumotlardan foydalanadi.	flows (presence , absence, amount , direction and frequency . 2 . Analysis of all encrypted messages sent over the communication system does not lead to decrypt , but allowing the opponent and / or the offender obtain indirect information about the transmitted Post and generally observed on the functioning of the communication system. A. that uses features of registration messages encrypted , and their length , the transmission time , the data sender and recipient , etc.
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.	programs, asking for “listening” network traffic and automatically selects the network traffic of user names, passwords, credit card numbers, other similar information.
Apparat himoya	kompyuterda ma’lumotlarni himoyalashda apparat vositalardan, masalan, chegara registrlaridan yoki qulflardan va kalitlardan foydalanish.	the use of hardware, for example, registers boundaries or locks and keys to protect data in computers.
Faol hujum	kriptotizimga yoki kriptografik protokolga hujum bo‘lib, unga binoan dushman va/yoki buzg‘unchi qonuniy foydalanuvchi xarakatiga ta’sir etishi, masalan, qonuniy foydalanuvchi xabarini almashtirishi yoki yo‘q qilishi va xabarni yaratib uning nomidan uzatishi va h. mumkin.	attack on a cryptosystem or cryptographic protocol in which the offender or the enemy and can affect the legitimate user actions, for example, replace or remove legitimate posts, create and send messages on his behalf, etc.

Xizmat qilishdan voz kechishga undaydigan atayin qilinmaydigan hujum	tasodifiy yuz bergan holat natijasida (reklama natijasida qiziqishning keskin oshishi, to‘satdan va kutilmagan kamdan – kam bo‘ladigan mashhurlik va h.) DOS hujumning mavaffaqiyatli o‘tkazilgani xususida taassurot tug‘diruvchi qandaydir servis uchun xizmat qilishdan voz kechish. Ko‘pincha faollikning avj onlarida yangilik saytlariga qiziqarli axborotni joylashtirish natijasida, xamda qidiruv tizimlari yordamida ommabop URL – havolalarni o‘tkazish qobiliyati cheklangan foydalanish kanallariga ega media – resurslariga indekslash natijasida paydo bo‘ladi.	denial of service for any service which has come as a result of chance (sharply increased interest in the result of the promotion , the sudden and unexpected exception pop, etc.) , giving the impression of a successful DoS attack . Often occurs in times of peak activity as a result of placement of interesting information on news sites , as well as from popular search engines indexing URL-links to various media resources with limited bandwidth channel access.
Xavfsizlik auditi	kompyuter tizimi xavfsizligiga ta’sir etuvchi bo‘lishi mumkin bo‘lgan xavfli harakatlarni xarakterlovchi, oldindan aniqlangan hodisalar to‘plamini ro‘yxatga olish(audit faylida qaydlash) yo‘li bilan himoyalanishni nazoratlash.	maintain security control by registering (fixation in the audit file) a predetermined set of events that characterize the potentially dangerous actions in the computer affecting its security.
Axborot tarmog‘i xavfsizligi	axborot tarmog‘ini ruxsatsiz foydalanishdan, me’yoriy harakatiga tasodifan aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.	measures designed to protect network information from unauthorized access, accidental or intentional interference with normal activities or attempts to destroy its components.
Kompyuter tizimi xavfsizligi	destruktiv harakatlarga va yolg‘on axborotni zo‘rlab qabul qilinishiga olib keluvchi ishlanadigan va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga kompyuter tizimining qarshi tura olish hususiyati.	property computer systems to resist attempts of unauthorized access to information processed and stored, the input of information, leading to destructive actions, and the imposition of false information.

Xodim xavfsizligi	qandaydir jiddiy axborotdan foydalanish imkoniyatiga ega barcha xodimlarning kerakli avtorizasiyaga va barcha kerakli ruxsatnomalarga egalik kafolatini ta’minlovchi usul.	method of ensuring that all personnel having access to some sensitive information has the necessary authorization, as well as all the necessary permissions.
Korxona xavfsizligi	korxona o‘z faoliyatini buzilishsiz va to‘xtalishsiz yurgiza oladigan vaqt bo‘yicha barqaror bashoratlanuvchi atrof-muhit holati.	stable condition projected time environment in which the company can carry out their activities without disturbances and interruptions.
Axborotning blokirovka qilinishi	axborotning texnik vositalar yordamida ishlanishida uning foydalanuvchanlik xususiyatining yo‘qolishi. Natijada tanishish, xujjatlash, modifikasiyalash yoki yo‘q qilish bo‘yicha vakolatli amallarni bajarish qiyinlashadi yoki to‘xtatiladi.	the loss of information when it is processed by technical means accessibility property, expressed in difficulty or termination of authorized access to it for authorized operations familiarization, documentation, modification, or destruction.
Xavf-xatarga ta’sir	havf-xatarni modifikasiyalash (o‘zgartirish) jarayoni. Havf-xatarga ta’sir quyidagilarni o‘z ichiga olishi mumkin: faoliyatini boshlamaslik yoki davom ettirmaslik qarori orqali xavf-xatarni oldini olish natijasida xavf-xatar paydo bo‘ladi; qulay imkoniyatdan foydalanish uchun xavf-xatarni qabul qilish yoki ko‘paytirish; xavf-xatar manbaini yo‘q qilish; imkoniyatini o‘zgartirish; oqibatlarni o‘zgartirish; xavf-xatarni boshqa taraf yoki taraflar bilan bo‘lishish (jumladan, shartnomalar va xavf-xatarni moliyalash); xavf-xatarni tushungan holda ushlab qolish.	the modification (changing) risk. Effects on risk may include: - avoid the risk by decision not to commence or to continue, resulting in the risk; - Adoption or increase the risk for a favorable opportunity; - Eliminate the source of the risk; - Changing opportunities; - Change impacts; - Sharing the risk with another party or parties (including contracts and risk financing); - Conscious retention risk.

Konfidensial axborotdan foydalanish	muayyan shaxsga tarkibida konfidensial xarakterli ma’lumot bo‘lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati.	authorized authorized official introduction of a particular person with the information containing confidential information.
Axborotdan ruxsatsiz foydalanish	manfaatdor subyektning huquqiy hujjatlarni yoki mulkdor, axborot egasi tomonidan o‘rnatilgan himoyalanuvchi axborotdan foydalanish huquqlari yoki qoidalarini buzib himoyalanuvchi axborotga ega bo‘lishi.	preparation of protected information interested entity in violation of the legal instruments or by the owner, the owner of the information or rights of access to protected information.
Tizimning osilib qolishi	yangi topshiriqlar kiritilishini bostirish yo‘li bilan multidastur tizimini to‘xtatish (“yaxlatish”).	system hang - stop ("freezing") multiprogramming system by inhibiting the entry of new jobs.
Axborotni fosh qilinishdan himoyalash	himoyalanuvchi axborotni, ushbu axborotdan foydalanish xuquqiga ega bo‘lmagan manfaatdor subyektlarga (iste’molchilarga) ruxsatsiz yetkazishni bartaraf etishga yo‘naltirilgan axborot himoyasi.	the information security directed on prevention of unauthorized finishing of protected information to interested subjects (consumers), not having right of access to this information.
Ijtimoiy injeneriya	xizmatchi xodimlar va foydalanuvchilar bilan, turli nayrang, aldash va h. orqali chalg‘itish asosidagi muloqotdan olinadigan axborot yordamida axborot tizimining xavfsizlik tizimini chetlab o‘tish.	round of system of safety of system information by means of information received from contacts with the service personnel and users on the basis of their introduction in delusion at the expense of various tricks, deception and so forth.
Insayder	guruxga tegishli yashirin axborotdan foydalanish xuquqiga ega gurux a’zosi. Odatda, axborot	the member of group of the people having access to the classified

	sirqib chiqish bilan bog‘liq mojoroda muhim shaxs hisoblanadi. Shu nuqtai nazaridan, insayderlarning quyidagi xillari farqlanadi: beparvolar, manipulyasiyalanuvchilar, ranjiganlar, qo‘shimcha pul ishlovchilar va h.	information, belonging this group. As a rule, is the key character in the incident, connected with information leakage. From this point of view distinguish the following types of insiders: negligent, manipulated, offended, disloyal, earning additionally, introduced, etc.
Insident	ruxsatsiz foydalanish xuquqiga ega bo‘lishga yoki kompyuter tizimiga xujum o‘tkazishga urinishning qayd etilgan xoli.	the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.
Tashqi insident	manba jabrlanuvchi tomon bilan bevosita bog‘lanmagan buzg‘unchi bo‘lgan mojoro.	the incident which source is the violator who hasn't been connected with an affected party directly.
Ichki insident	manba jabrlanuvchi tomon bilan bevosita bog‘langan (mehnat shartnomasi yoki boshqa usullar bilan) buzg‘unchi bo‘lgan mojoro.	the incident which source is the violator connected with an affected party directly (the employment contract or other ways).
Axborotdan noqonuniy foydalanish	qonuniy yo‘l bilan olingan ma’lumotlarni, ushbu ma’lumotlarga va bunday harakatlarga qo‘l uruvchi subyektlarga o‘rnatilgan qoidalarni va vakolatlarni (sanksiyalarni) buzgan holda, uzatish, tarqatish (chop etish) va qo‘llash.	transmission, distribution(publishing), the use of information obtained through legal means in violation of the rules and powers(sanctions) established forthis information and subject,to take such action.
Suqilib kirishga sinash	tizimni uning himoyalash vositasini (xususan, ruxsatsiz foydalanishdan himoyalash	system test for the purpose of check of means of its protection (in

	vositasini) tekshirish maqsadida sinash.	particular from illegally go access).
Yashirin kanal	xavfsizlik siyosatini buzish uchun ishlatilishi mumkin bo‘lgan, axborot texnologiyasi tizimini va avtomatlashtirilgan tizimlarni ishlab chiqaruvchilar ko‘zda tutmagan kommunikasiya kanali. Axborot uzatish mexanizmi bo‘yicha yashirin kanallar xotira bo‘yicha yashirin kanalga, vaqt bo‘yicha yashirin kanalga va statistik yashirin kanalga bo‘linadi.	unforeseen the developer of system of technologies information and systems automated the communication channel which can be applied to security policy violation. On the information transfer mechanism c.s subdivide on: c.s. on memory c.s. on time; hidden statistical channels.
Axborot sirqib chiquvchi kanal	ko‘riklanuvchi ma’lumotlardan (tijorat siri, fizik muhit va sanoat ayg‘oqchilik vositalari majmui) ruxsatsiz foydalanishga imkon beruvchi konfidensial axborot manbaidan to niyati buzuqgacha bo‘lgan fizik yo‘l.	actual path from a source of confidential information to the malefactor, on which probably unauthorized obtaining protected data (set of a source of a trade secret, the physical environment and means of industrial espionage).
Keylogger	klaviaturali kiritishni ushlab qolishga mo‘ljallangan dastur yoki apparat vosita. Bosilgan klavishlar skan-kodlarini aniqlashni va ularni yashirincha saqlashni va/yoki yashirincha qandaydir kanal orqali uzatishni amalga oshiradi.	the program or the hardware device intended for interception of keyboard input. Carries out recognition of scan-codes of the pressed keys and the hidden preservation and/or their hidden transfer on any channel.
Kompyuter jinoyatchiligi	o‘zi yoki uchinchi shaxs uchun mulkiy foyda olish hamda raqibiga mulkiy ziyon yetkazish maqsadida axborot resursidan ruxsatsiz foydalanishni, uni modifikasiyalashni yoki yo‘qotishni amalga oshirish.	implementation of unauthorized access to information resource, its modification (fake) or destruction for the purpose of obtaining property benefits for itself or for the third party, and also for causing property damage to the competitor.

Mantiqiy “bomba”	axborotdan ruxsatsiz foydalanish uchun ma’lum vaqtiy va axborot sharoitlarida ishga tushiriluvchi dastur.	the program which is started under certain temporary or information conditions for implementation of unauthorized access to information.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

Асосий адабиётлар

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.
2. С.К. Ганиев, З.Т. Худойкулов, Н.Б. Насруллаев. Основы кибербезопасности: Учебное пособие, – Т. “Mahalla oila nashriyoti”, 2021. – 224 b.
3. S.K. Ganiyev, M.M. Karimov, K.A. Tashev; Axborot xavfsizligi: darslik; O‘zb. aloqa va axborotlashtirish agentligi. - T. Alooqachi, 2008. - 383 b.
4. S.K.Ganiev, D.Y.Irgasheva, Z.T.Xudoykulov., Kiberxavfsizlik asoslari: Darslik.TOSHKENT 2022.-258bet.
5. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari:
6. o‘quv qo‘llanma. – T.: «Aloqachi», 2020, 303 bet.
7. S.K.Ganiyev, M.M.Karimov, K.A.Tashev., Axborot xavfsizligi: Darslik. “Fan va texnologiyalar” nashriyoti, Toshkent-2016.-366 bet.
8. J.I.Samandarov., Axborot xavfsizligi: O’quv qullanma. Toshkent-2022.-133 bet.
9. Sh.U. Eshonqulov.,N.A.Qarshiboyev ―Axborot xavfsizligi‖ fanidan o‘quv qo‘llanma, JizPI, 148 b., Jizzax- 2022.
10. S.K. Ganiyev, M.M. Karimov, K.A. Tashev; Axborot xavfsizligi: darslik/ O‘z R Oliy va o‘rta maxsus ta’lim vazirligi, TATU. - Qayta nashr. - T. Fan va Texnologiya, 2017. - 372 b.
11. В.Ф.Шаньгин, Информационная безопасность компьютерных систем и сетей: учебное пособие - М. ФОРУМ : ИНФРА-М, 2019. - 416 с.

Qo‘shimcha adabiyotlar

12. Asylbekov U.B., Ismailova A.A. A 89 Cybersecurity: Protection in the Digital World / Кибербезопасность: защита в цифровом мире: textbook (part 1) / U.B. Asylbekov, A.A. Ismailova. – Almaty: «Bastau», 2021. – 344 p
13. 4.Диогенес Ю., Озкайя Э. Д44 Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Белико ва. – М.: ДМК Пресс, 2020. – 326 с.: ил.
14. Mirziyoyev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta’minlash-yurt taraqqiyoti va xalq farovonligining garovi. 2017.

15.Mirziyoyev Sh.M. Erkin va farovon, demokratik O’zbekiston davlatini birgalikda barpo etamiz. 2017.

16.Mirziyoyev Sh.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. 2017.

17.“Axborot texnologiyasi. Axborotlarni kriptografik muxofazasi. Ma’lumotlarni shifrlash algoritmi” O’zbekiston Davlat standarti. O’zDSt 1105:2009.

18.Хилл Б. «Полный справочник по Сиссо» Пер. с англ. М.: Изд. дом Вилямс. 2008г.

19.Шнаер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издателство ТРИУМФ, 2003 – 816

Internet saytlari

20.https://csec.uz/uz/

21.https://unicon.uz/

22.https://lex.uz/ru/docs/-5960604 - O‘zbekiston Respublikasining KIBERXAVFSIZLIK TO‘G‘RISIDA Qonuni, 15.04.2022 yildagi O‘RQ-764-son.

23.https://www.youtube.com/watch?v=_HcACxBsBLg

24.http://www.ziyonet.uz

25.http://uz.denemetr.com/download/docs-229149/768-229149.doc

26.http://www.nasa.gov\statistics\

27.http://www.security.uz

28.http://www.cert.uz

29.http://www.uzinfocom.uz.

MUNDARIJA

KIRISH 3
I BOB. KIRISH. KIBER XAVSIZLIKNING ASOSIY TUSHUNCHALARI VA TARIXI 7
1.1. Asosiy tushunchalar 7
1.2. Axborotning xavfsizlikka oid xususiyatlari 7
1.3. Kiberxavfsizlikning bilim sohalari.....9
1.4. Kiberjinoyatchilik. 14
1.5. Kiberqonunlar 15
1.6. Kiberetika.....16
II BOB. AXBOROTNING KRIPTOGRAFIK HIMOYASI.....25
2.1.Kriptografiya bo‘limlari.....25
2.2. Kriptografiya tarixi.....26
2.3. Kriptografik akslantiishlar.....30
III BOB. SIMMETRIK SHIFRLAR. ASSIMMETRIK SHIFRLAR 34
3.1. Simmetrik kriptografik algoritmlar 34
3.2. Oqimli simmetrik shifrlash algoritmlari.....34
3.3. Blokli simmetrik shifrlash algoritmlari 37
IV БОБ. FOYDALANISHNI NAZORATLASH 38
4.1. Bir tomonlama funksiya.....38
4.2. RSA algoritmi 42
4.3. Ochiq kalitli kriptotizimlardan foydalanish 44
4.4. Simmetrik shifrlash algoritmlaridan ma’lumot butunligini tekshirish 46
4.5. Xesh – funksiyalar asosida ma’lumot yaxlitligini tekshirish 48
4.6. Elektron raqamli imzo.....49
4.7. Apparat-dasturiy shifrlash.....54
4.8. Disk va fayl tizim sathida shifrlash.....58
4.9. Hujjatlarni yo‘q qilish usullari 62
V BOB. AUTENTIFIKASIYA.....67
5.1. Identifikasiya.....67
5.2. Autentifikasiya 68
5.3. Ko‘p omilli autentifikasiya.....73
VI BOB. MA’LUMOTLARNING FIZIK XAVFSIZLIGI. MA’LUMOTLARDAN FOYDALANISHNING MANTIQIY NAZORATI. FORMAL MODELLAR. 77
6.1. Fizik xavfsizlik, uning zaruriyati 77
6.2. Fizik xavfsizlikka ta’sir qiluvchi omillar 79

6.3. Fizik xavfsizlikni nazoratlash.....81
VII BOB. PAROLLARGA HUJUMLAR VA PAROLLARNI SAQLASH. MA'LUMOTLAR BUTUNLIGI. 99
7.1. Tarmoq topologiyalari.....99
7.2. Tarmoqqa qo'yiladigan talablar 99
7.3. TCP/IP modeli.....101
7.4. Zaiflik, tahdid, hujum.....122
VIII BOB. TARMOQ XAVFSIZLIGI 127
8.1. Tarmoqlararo ekranlash.....127
8.2. Virtual xususiy tarmoqlar.....131
8.3. Simsiz tarmoq turlari.....133
8.4. Simsiz tarmoqlardagi mavjud zaifliklar 139
8.5. Tarmoq orqali uzatiluvchi ma'lumotni shifrlash.....143
IX BOB. FOYDALANUVCHILIKNI TA'MINLASH USULLARI 148
9.1. Foydalanishni boshqarish.....148
9.2. Foydalanishni diskresion boshqarish usuli (Discretionary access control, DAC).....148
9.3. Foydalanishni mandatli boshqarish usuli (Mandatory access control, MAC) 150
9.4. Foydalanishni rollarga asoslangan boshqarish usuli (Role-based access control, RBAC) 153
9.5. Foydalanishni atributlarga asoslangan boshqarish usuli (Attribute-based access control, ABAC).....155
9.6. Ko'p sathli xavfsizlik modellari.....159
9.7. Bell-LaPadula modeli.....160
9.8. Biba modeli 162
9.9. Mantiqiy va fizik foydalanishlarni boshqarish.....163
O'z-o'zini nazorat va muhokama qilish uchun savollar.....163
X BOB. DASTURIY VOSITLAR XAVFSIZLIGI.....164
10.1. Axborotlarga nisbatan mavjud xavfsizliklarning asosiy tushunchalari va uning tasnifi 164
10.2. Axborot xavfsizligining tashkiliy-ma'muriy ta'minoti 173
10.3. Kompyuter viruslari, ularning klassifikasiyasi va ular bilan kurashish mexanizmlari.....176
XI BOB. AXBOROT XAVFSIZLIGI SIYOSATI VA RISKLARNI BOSHQARISH 183
11.1. Risk darajasi, risk chastotasi, risk matritsasi.....183
11.2. Risklarni boshqarish.....185

11.3. Risklarni boshqarish bosqichlari 188
11.4. Risklarni boshqarishning axborot tizimlari 191
11.5. Foydalanuvchanlik tushunchasi 192
11.6. Zaxira nusxalash.....193
11.7. Ma’lumotlarni qayta tiklash 195
11.8. Hodisalarni qaydlash.....195
XII BOB. KIBERJINOYATLARNING INSON XVFSIZLIGIGA TA’SIRI.....203
12.1. Ijtimoiy injeneriya.....203
12.2. Fishing ataka 204
12.3. Ijtimoiy injeneriyadan himoyalanish chora-tadbirlari.....211
12.4. Kiberxavfsizlik arxitekturasi.....216
12.5. Kiberxavfsizlik strategiyasi.....217
12.6. Kiberxavfsizlik siyosati.....218
GLOSSARIY 225
FOYDALANILGAN ADABIYOTLAR RO‘YXATI.....233

JOMONQULOVA FAZILAT ESIRGAPOVNA

KIBER XAVFSIZLIK

DARSLIK

Muharrir: Z.N. Bobodustov
Musahhih: M.O. Mardiyeva
Texnik muharrir: D. Hamrayev

Darslik institut Kengashining 2024 - yil 30 - yanvardagi majlisda muhokama qilingan va nashrga tavsiya etilgan. (6-sonli majlis bayoni).

“STAP-SEL” MChJ nashriyoti, Samarqand - 2024

7523 **ISBN:** 978-9910-753-76-3

Tasdiqnona № 033337 (27.07.2022)
Nashrga ruxsat etildi: 19.07. 2024 y.
© “STAP-SEL” MChJ nashriyoti.

11.11.2024 yilda chop etildi.
Qog‘oz bichimi A5, 60x84 1/16, Ofset qog‘ozi.
“Times New Roman” garniturasi.
Nashr bosma tabog`i 14.87
Buyurtma № 0125A/24. Adadi 100 nusxa

Samarqand iqtisodiyot va servis institutining matbaa bo`limida chop etildi.
LICENSE № 025316.
REESTR № X-119112.
Manzil: Samarqand shahar, Shoxrux ko`chasi 60-uy.