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

GULISTON DAVLAT UNIVERSITETI

S.A.Tishlikov
A.N. Qudratov
J.D. Saidov
D.I. Doniyorov

AXBOROT XAVFSIZLIGI

Guliston-2023

UDK: 004
KBK: 73
A-93
S.A.Tishlikov, A.N. Qudratov., J.D.Saidov., D.I. Doniyorov. Axborot xavfsizligi. O‘quv-uslubiy qo‘llanma. Guliston, 2023. – 167 bet.

Mazkur o‘quv-uslubiy qo‘llanma amaldagi fan dasturi asosida tayyorlangan bo‘lib, unda axborot xavfsizlik tushunchalari va uning vazifalari, axborot xavfsizligiga bo‘ladigan taxdidlar, xujumlar va zaifliklar, axborot xavfsiligi sohasiga oid xalqaro va milliy me’yoriy-xuquqiy baza, xavfsizlik modellari, axborotni kriptografik himoyalash, identifikatsiya va autentifikatsiya, axborot sirqib chiqish ularni aniqlash, kanallari hamda ob’ektlarni texnik jixatdan himoyalash va extiyot chora-tadbirlarini ko‘rish jixatlari keltirib o‘tilgan.

O‘quv-uslubiy qo‘llanma Sirdariyo viloyati texnikumlari va kasb-hunar maktablariga ta’lim yo‘nalishlari o'uvchilari uchun mo‘ljallan va undan axborot texnologiyalari, kompyuter tizimlari xavfsizligi sohasida faoliyat ko‘rsatuvchilar foydalanishlari mumkin.

***

Этот учебно-методическая пособие основан на действующей научной программе, которая включает понятие информационной безопасности и ее задачи, угрозы информационной безопасности, атаки и уязвимости, международную и национальную правовую базу в области информационной безопасности, модели безопасности, криптографическую защиту информации, идентификация и аутентификация, каналы утечки информации и их обнаружение, а также инженерная защита и техническая защита объектов.

Учебное-методическая пособие предназначено для учащихся техникумов и профтехучилищ Сырдарьинской области и может быть использовано лицами, работающими в сфере информационных технологий, безопасности компьютерных систем.

***

This training manual is based on the current scientific program, which includes the concept of information security and its objectives, information security threats, attacks and vulnerabilities, international and national legal framework in the field of information security, security models, cryptographic information protection, identification and authentication, channels information leaks and their detection, as well as engineering protection and technical protection of objects.

The study guide is intended for students of technical schools and vocational schools of the Syrdarya region, and it can be used by those working in the field of information technologies, computer systems security.

Taqrizchilar: N.Z.Negmatulloev– GulDU Amaliy matematika va axborot texnologiyalari kafedrasi dots.phd.
M.B.Niyozov - GulDPI “Aniq va tabiiy fanlar” kafedra mudiri, p.f.b.f.d.(Phd)

Guliston davlat universiteti o'quv-uslubiy Kengashining 2023 yil 29 maydagi 10-sonli yig'ilish bayonnomasidan chop etishga ruxsat etilsin.

So‘z boshi

Ma’lumki, har qanday davlatning axborot resurslari uning iqtisodiy va harbiy salohiyatini belgilovchi omillaridan biri hisoblanadi. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirilishini ta’minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yigish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha ilg‘or axborot-kommunikatsiyalar texnologiyalarini qo‘llash keng ko‘lamda amalga oshiriladi. Axborotlashgan jamiyat tezlik bilan shakllanib bormoqda. Jahon kompyuter tarmog‘i davlat boshqaruvini tubdan o‘zgartirmoqda. Hududiy joylashishidan qat’iy nazar, kundalik hayotimizga turli xildagi axborotlar Internet xalqaro kompyuter tarmog‘i orqali kirib keldi. Shuning uchun ham mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborotni muhofaza qilish esa davlatning birlamchi masalalariga, davlat siyosati darajasiga aylanmoqda.

O‘quv- uslubiy qo‘llanma “Axborot xavfsizligi” fani bo‘yicha nazariy materiyallar, amaliy mashg‘ulotlar ishlanmalari, topshiriqlar, bilimlarni nazorat qilush uchun savollar majmuasi keltirilgan.

O‘quv- uslubiy qo‘llanma “Axborot xavfsizligi” fanining mazmuni, maqsadi va fazifalari, axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo‘ladigan taxdidlar, hujumlar va zaifliklar, axborot xavfsiligi sohasiga oid xalqaro va milliy me’yoriy-huquqiy baza, xavfsizlik modellari, axborotni kriptografik himoyalash, identifikatsiya va autentifikatsiya, masalalari keltirilgan.

Maskur o‘quv- uslubiy qo‘llanma ham kamchiliklardan holi emas. O‘quv-uslubiy qo‘llanma haqidagi fikr va mulohazalarini bildirgan hamkasblar va aziz o‘quvchilarga oldindan o‘z minnatdorchiligini bildiradi.

Manzilimiz: Guliston shahri,
Guliston davlat universiteti,
Axborot texnologiyalari
fakulteti, “Amaliy matematika va
. axborot texnologiyalari” kafedrasi.

I BOB. AXBOROT XAVFSIZLIGINING ASOSIY TUSHUNCHALARI VA UNING VAZIFALARI

1.1. Axborot xavfsizligining asosiy tushunchalari.

Tayanch ibora va tushunchalar: Xakerlar, krekerlar, tashkil qilingan ayg‘oqchilik, terroristik guruxlar, iqtisodiy ayroqchilik, "mantiqiy bomba", axborotlar urushi, axborotlarni himoyalash, siyosiy dissident.

Mavzuga oid asosiy muommalar:

Zamonaviy axborot texnologiyalarining taraqqiyoti sanoat shpionaji, kompyuter jinoyatchiligi, konfedensial ma’lumotlarga ruxsatsiz kirish, o‘zgartirish, yo‘qotish kabi salbiy hodisalar bilan birgalikda kuzatilishini izohlab bering.

Darsning maqsadi: Axborot xavfsizligi asoslari fani axborot texnologiyalari avtomatlashtirish va axborotni muhofaza qilish yo‘nalishlarida muntazam mukammallashib borish.

Har qanday taraqqiy etgan jamiyat hayotida axborotning ahamiyati uzluksiz ortib bormoqda. Uzoq o‘tmishdan davlatning harbiy-strategik ahamiyatiga molik bo‘lgan ma’lumotlar qat’iy sir tutilgan va himoyalangan. Hozirgi vaqtda ishlab chiqarish texnologiyalariga va mahsulotlarni sotishga tegishli axborot tovar ko‘rinishiga ega bo‘lib, ichki va tashqi bozorda unga bo‘lgan talab ortib bormoqda. Axborot texnologiyalari avtomatlashtirish va axborotni muhofaza qilish yo‘nalishlarida muntazam mukammallashib bormoqda. Zamonaviy axborot texnologiyalarining taraqqiyoti sanoat shpionaji, kompyuter jinoyatchiligi, konfedensial ma’lumotlarga ruxsatsiz kirish, o‘zgartirish, yo‘qotish kabi salbiy hodisalar bilan birgalikda kuzatilmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi hisoblanadi. O‘zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimi yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o‘z ifodasini topmoqda. «Axborotlashtirish to‘g‘risida», «Davlat sirlarini saqlash to‘g‘risida», «Elektron hisoblash mashinalari dasturlari va ma’lumotlar bazalarini huquqiy himoya qilish to‘g‘risida» va boshqa qonunlar hamda bir qator Hukumat qarorlari qabul qilindi va amalga tatbiq etildi.

Axborotni muhofaza qilish axborotni ixtiyoriy ko‘rinishda yo‘qotishda (o‘g‘irlash, buzish, qalbakilashtirish) ko‘riladigan zararning oldini olishni ta’minlashi lozim. Axborotni muhofaza qilish choralari axborot xavfsizligiga oid amaldagi qonun va me’yoriy hujjatlar asosida va axborotdan foydalanuvchilarning manfaatlariga ko‘ra tashkil etilishi zarur. Yuqori darajada axborotni muhofaza qilishni kafolatlash uchun muntazam ravishda murakkab ilmiy-texnik vazifalarni hal etish va himoya vositalarini takomillashtirish talab etiladi.

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonunida axborot va uning turlari to‘g‘risida quyidagi ta’riflar keltirilgan:

-axborot–manbalari va taqdim etilish shaklidan qat’iy nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to‘g‘risidagi ma’lumotlar;
-axborotni muhofaza etish – axborot borasidagi xavfsizlikka tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish chora-tadbirlari;
-ommaviy axborot–cheklanmagan doiradagi shaxslar uchun mo‘ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar;
-hujjatlashtirilgan axborot – identifikatsiya qilish imkonini beruvchi rekvizitlari qo‘yilgan holda moddiy jismda qayd etilgan axborot;
-maxfiy axborot–foydalanilishi qonun hujjatlariga muvofiq cheklab qo‘yiladigan hujjatlashtirilgan axborot. Ushbu ta’rif O‘zbekiston Respublikasi Vazirlar Mahkamasining “O‘zbekiston Respublikasi Prezidentining “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida” 2011-yil 8-iyuldagi PQ–1572-son qarorini amalga oshirish chora-tadbirlari haqida”gi 2011-yil 7-noyabr 296-sonli qarorida quyidagicha ifodalangan:

maxfiy axborot – O‘zbekiston Respublikasi qonun hujjatlariga muvofiq foydalanish cheklangan, davlat sirlariga mansub axborot mavjud bo‘lmagan hujjatlashtirilgan axborot.

Konfedensial axborot–hujjatlashtirilgan axborot, undan foydalanish qonun hujjatlariga muvofiq chegaralanadi. Saqlash, o‘zgartirish, uzatish va ma’lum maqsadlar uchun foydalanish ob’yekti bo‘lgan tevarak olam haqidagi ma’lumotlarni, keng ma’noda axborot deb tushunish mumkin. Bu tushunchaga ko‘ra inson, uning hayot tarziga va harakatlariga ta’sir etuvchi doimiy o‘zgaruvchi axborot maydoni ta’sirida bo‘ladi. Axborot o‘z tavsifiga ko‘ra siyosiy, harbiy, iqtisodiy.

Aloqa va axborotlashtirish sohasida axborot xavfsizligi: Atamalar va ta’riflar. Tarmoq standarti: TSt 45-010:2010. ilmiy-texnik, ishlab chiqarishga yoki tijoratga oid hamda maxfiy, konfedensial yoki nomaxfiy bo‘lishi mumkin.

O‘zbekiston Respublikasining 1993-yil 7-maydagi 848-XII-sonli “Davlat sirlarini saqlash to‘g‘risida”gi qonunning 1-moddasida davlat sirlari tushunchasi berilgan: “Davlat tomonidan qo‘riqlanadigan va maxsus ro‘yxatlar bilan chegaralab qo‘yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiy-texnikaviy va o‘zga xil ma’lumotlar O‘zbekiston Respublikasining davlat sirlari hisoblanadi”. Mazkur qonunning 3-moddasida davlat sirlarining toifalari keltirilgan:

O‘zbekiston Respublikasining davlat sirlari–davlat, harbiy va xizmat sirlarini qamrab oladi. Oshkor etilishi respublika harbiy-iqtisodiy imkoniyatlarining sifat holatiga salbiy ta’sir etishi yoki O‘zbekiston Respublikasining mudofaa qobiliyati, davlat xavfsizligi, iqtisodiy va siyosiy manfaatlari uchun boshqa og‘ir oqibatlar keltirib chiqarishi mumkin bo‘lgan ma’lumotlar davlat sirini tashkil etadi. Oshkor etilishi O‘zbekiston Respublikasining mudofaa qobiliyati, davlat xavfsizligi va Qurolli Kuchlari uchun og‘ir oqibatlar keltirib chiqarishi mumkin bo‘lgan harbiy xususiyatga ega ma’lumotlar harbiy sirni tashkil etadi. Oshkor etilishi O‘zbekiston Respublikasi

manfaatlariga zarar yetkazishi mumkin bo‘lgan fan, texnika, ishlab chiqarish va boshqaruv sohasiga doir ma’lumotlar xizmat sirini tashkil etadi.
Axborotlarga nisbatan xavf-xatarlar tasnifi.

Axborot xavfsizligi deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan qilingan ta’sirlardan axborot va uni qo‘llab-quvvatlab turuvchi infrastukturaning himoyalanganligi tushuniladi. Bunday ta’sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo‘llab quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin. O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi № 439-II-sonli “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonunida axborot xavfsizligi axborot borasidagi xavfsizlik deb belgilangan.

Axborot xavfsizligi – ko‘p qirrali faoliyat sohasi bo‘lib, unga faqat tizimli, kompleks yondashuv muvaffaqiyat keltirishi mumkin. Ushbu muammoni hal etishda huquqiy, ma’muriy, protsedurali va dasturiy-texnik choralarni qo‘llaniladi. Bugungi kunda axborot xavfsizligini ta’minlaydigan uchta asosiy tamoyil mavjud:
– ma’lumotlar butunligi – axborotni yo‘qotilishiga olib keluvchi buzilishlardan, shuningdek ma’lumotlarni mualliflik huquqi bo‘lmagan holda hosil qilish yoki yo‘q qilishdan himoya qilish;
– axborotning konfedensialligi. Axborot va uning tashuvchisining holatini belgilaydi va unda axborot bilan ruxsatsiz tanishishning yoki uni ruxsatsiz hujjatlashtirishning (nusxa ko‘chirishning) oldini olish ta’minlangan bo‘ladi;
–foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari.

Ta’kidlash joizki, ayrim faoliyat sohalari (bank va moliya institutlari, axborot tarmoqlari, davlat boshqaruv tizimlari, mudofaa va maxsus tuzulmalar) ularda ko‘riladigan masalalarning muhimligi va xarakteriga ko‘ra, ularning axborot tizimlari faoliyati ishonchliligiga nisbatan yuqori talablar va xavfsizlik bo‘yicha maxsus choralar ko‘rilishini talab etadi.

Axborot xavfsizligining milliy xavfsizlik tizimidagi o‘rni. XXI asrda shaxs, jamiyat va davlat taraqqiyotida axborot resurslari va texnologiyalarining rolini ortishi natijasida O‘zbekistonda fuqarolik jamiyatini axborotlashtirilgan jamiyat sifatida qurish masalasini hal etish bilan birga quyidagi omillar milliy xavfsizlikni ta’minlash tizimida axborot xavfsizligining yetakchi o‘rin egallashini belgilaydi:
– milliy manfaatlar, ularga tajovuz va ularni bu tajovuzlardan himoyalash axborot va axborot sohasi orqali ifodalanadi, amalga oshiriladi.
– inson va uning huquqlari, axborot va axborot tizimlari hamda ularga egalik qilish–bu nafaqat axborot xavfsizligining asosiy ob’yektlari, balki xavfsizlik sohasidagi barcha xavfsizlik ob’yektlarining asosiy elementlari hamdir;
– axborot yondashuvidan asosiy ilmiy-amaliy usul sifatida foydalanish orqali milliy xavfsizlik masalalarini hal etish mumkin;
– milliy xavfsizlik muammosi yaqqol ajralib turuvchi axborot tavsifiga ega.

Axborot xavfsizligi tizimi davlatning axborot sohasidagi siyosatini mamlakatda milliy xavfsizlikni ta’minlash davlat siyosati bilan chambarchas bog‘laydi. Bunda axborot xavfsizligi tizimi davlat siyosatining asosiy tashkil etuvchilarini yaxlit bir butunlikka biriktiradi.

Bu esa axborot xavfsizligining roli va uning mamlakat milliy xavfsizligi tizimidagi mavqeini belgilaydi. Axborot sohasidagi O‘zbekistonning milliy manfaatlarini, ularga erishishning strategik yo‘nalishlarini va ularni amalga oshirish tizimlarini o‘zida aks ettiruvchi maqsadlar yaxlitligi davlat axborot siyosatini anglatadi. Shu bilan birga davlat axborot siyosati mamlakatning tashqi va ichki siyosatining asosiy tashkil etuvchisi hisoblanadi hamda jamiyatning barcha jabhalarini qamrab oladi.

Axborot xavfsizligining zamonaviy konsepsiyasi axborot xavfsizligini ta’minlovchi maqsadlar, vazifalar, tamoyillar va asosiy yo‘nalishlar bo‘yicha rasmiy nuqtai nazarlar majmuini bildiradi. Quyida axborot xavfsizligining asosiy tashkil etuvchilari va jihatlari keltirilgan:

− axborotni muhofaza qilish (shaxsiy ma’lumotlarni, davlat va xizmat sirlarini va boshqa turdagi tarqatilishi chegaralangan ma’lumotlarni qo‘riqlash ma’nosida);

− kompyuter xavfsizligi yoki ma’lumotlar xavfsizligi – kompyuter tarmoqlarida ma’lumotlarning saqlanishini, foydalanishga ruxsat etilganligini va konfedensialligini ta’minlovchi apparat va dasturiy vositalar to‘plami, axborotdan ruxsatsiz foydalanishdan himoya qilish choralari;

− axborot egalariga yoki axborotdan foydalanuvchilarga hamda uni qo‘llab quvvatlovchi infratuzilmaga zarar yetkazishi mumkin bo‘lgan tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan ta’sir etishlardan axborot va uni qo‘llab quvvatlovchi infratuzilmaning himoyalanganligi;

− fuqarolar, alohida guruhlar va ijtimoiy qatlamlar, umuman olganda aholining yashash faoliyati, ta’lim olish va rivojlanishlari uchun zarur bo‘lgan sifatli axborotga bo‘lgan talablarining himoyalanganligi.

Ma’lumki, absolut xavfsiz tizimlar mavjud emas, lekin “ishonish mumkin bo‘lgan tizim” ma’nosidagi ishonchli tizimlardan foydalaniladi. Yetarlicha apparat va dasturiy vositalardan foydalanib, bir vaqtning o‘zida turli maxfiylik darajasidagi ma’lumotlarni foydalanuvchilar guruhi tomonidan foydalanish huquqlarini buzmagan holda qayta ishlash imkonini beruvchi tizim ishonchli hisoblanadi.

Ishonchlilikni baholovchi asosiy mezonlar–bu xavfsizlik siyosati va kafolatlanganlik.

Xavfsizlik siyosati–xavfsizlik ob’yektlari va subyektlarining berilgan ko‘pligining xavfsizligini ta’minlash protseduralari va mexanizmlarini belgilovchi qoidalar to‘plami. Tizim xavfsizligini ta’minlashning aniq mexanizmlarini tanlash qabul qilingan xavfsizlik siyosatiga muvofiq amalga oshiriladi. Kafolatlanganlik himoyaning passiv qismi bo‘lib, tizimdan foydalanishda unga bo‘lgan ishonch darajasini ifodalaydi. Ishonchli tizimda xavfsizlikka taalluqli barcha jarayonlar ro‘yxatga olib borilishi kerak.

Axborot xavfsizligi–bu uzatiluvchi, yig‘iluvchi va saqlanuvchi axborotning xususiyati (holati) bo‘lib, uning tashqi muhit (inson va tabiat) va ichki tahdidlardan himoyalanganlik darajasini xarakterlaydi. Axborotni muhofaza qilish keng ma’noda axborot xavfsizligiga tahdidni oldini olish va ularning asoratlarini yo‘q qilishga qaratilgan tashkiliy, huquqiy va texnik choralar kompleksini bildiradi. Axborotni muhofaza qilish axborotga bo‘lgan salbiy ta’sir manbalarini hamda sabab va sharoitlarni aniqlash va bartaraf etish ma’nosini anglatadi.

Bu manbalar axborot xavfsizligiga tahdidlarni tashkil etadi. Axborotni muhofaza qilish quyidagilarga yo‘naltirilgan:

– axborot xavfsizligini ta’minlash bo‘yicha tahdidlarning oldini olish;

– tizimli tahlil va nazorat orqali real va ehtimoli katta bo‘lgan tahdidlarni aniqlash va ularni o‘z vaqtida oldini olish choralari;

– aniq tahdidlar va jinoiy harakatlarni aniqlash maqsadida tahdidlarni topish;

– jinoiy harakatlarni bartaraf etish, shuningdek aniq jinoiy harakatlarni hamda tahdidlarni yo‘q qilish bo‘yicha choralar ko‘rish;

– tahdid va jinoiy harakatlarning oqibatlarini yo‘q qilish va mavqeini saqlash.

Ushbu barcha usullarning maqsadi axborot resurslarini noqonuniy tahdidlardan himoya qilish va quyidagilarni ta’minlashdan iborat:

– konfedensial axborotlarning tarqab ketishini oldini olish;

– konfedensial axborot manbalariga noqonuniy kirishni taqiqlash;

– axborotning butunligi, to‘liqligi va undan foydalana olishni saqlash;

– axborot konfedensialligiga rioya qilish;

– mualliflik huquqlarini ta’minlash.

Yuqoridagilarni e’tiborga olib, axborotni muhofaza qilish deganda davlat, jamiyat va shaxslarning axborot xavfsizligini ta’minlashga yo‘naltirilgan usul, vosita va choralar majmuini tushunish mumkin.

1.2. Axborot tizimlarida malumotlarga nisbatan xavflar.

Umuman olganda axborotni muhofaza qilishning maqsadini quyidagicha ifodalash mumkin:

– axborotni tarqab ketishi, og'irlanishi, buzilishi, qalbakilashtirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk ob’yekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfedensialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda subyektlarning huquqlarini ta’minlash. Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi.

Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan konsepsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

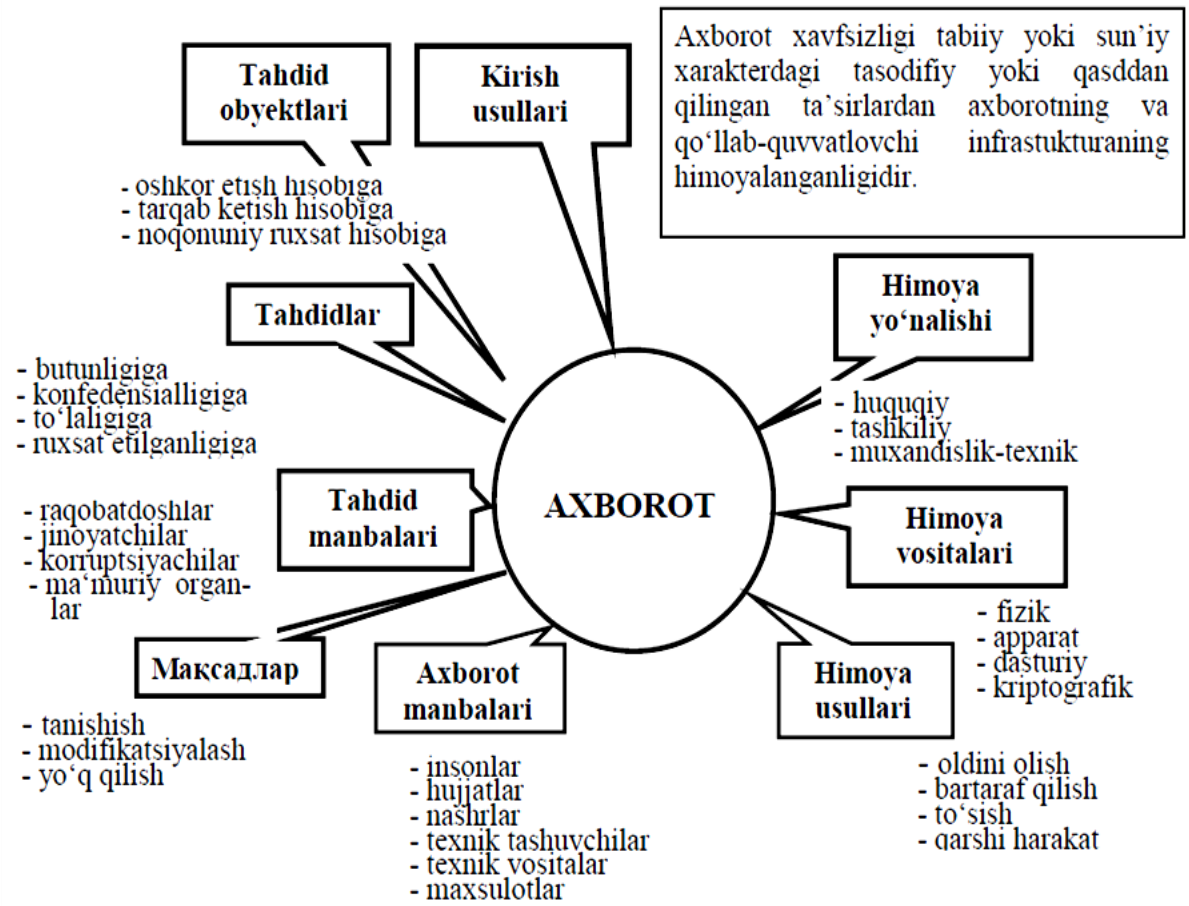
– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– axborotni muhofaza qilish masalalarini hal etishga ixtisoslashtirilgan tashkilotlarning mavjudligi;

– ushbu muammoga oid yetarlicha aniq ifodalangan qarashlar tizimi;

– yetarlicha amaliy tajriba va boshqalar.

Biroq, xorijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendensiyasiga ega bo‘lib bormoqda.



Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi.

Umumiy yo‘nalishga ko‘ra axborot xavfsizligiga tahdidlar quyidagilarga bo‘linadi:

– O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

– mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig‘ish, saqlash va samarali oydalanishni ta’minlashga nisbatan tahdidlar;

– Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining me’yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.

Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchini ko‘rib chiqish maqsadga muvofiq:

1) axborot;

2) texnik va dasturiy vositalar;

3) xizmat ko‘rsatuvchi personal va foydalanuvchilar.

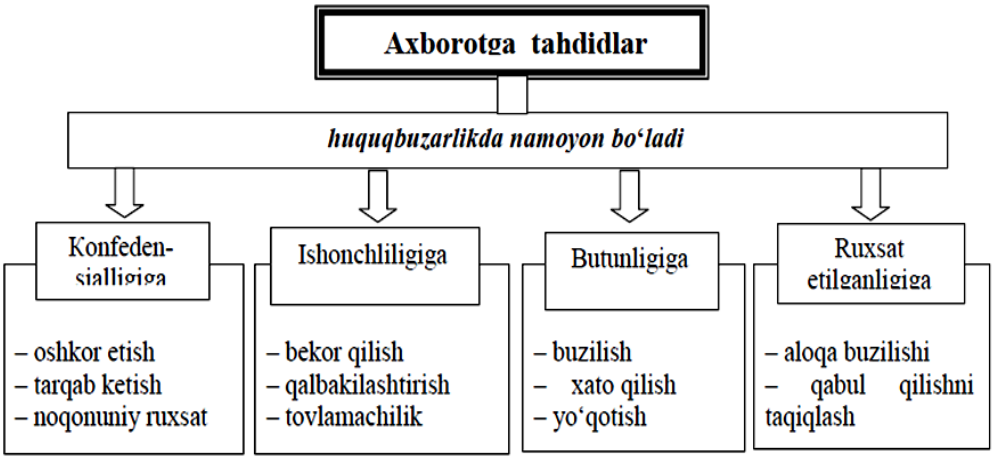
Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida hal etilishi zarur. Axborot tarqab ketishiga konfedensial ma’lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi.

Tahdidning uchta ko‘rinishi mavjud.

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgartirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgartirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqonuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisoblanadi. Axborot butunligi–axborotning buzilmagan holatda mavjudligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik– axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.



Axborot xavfsizligiga tahdidlarning toifalanishi. Axborot xavfsizligiga tahdidlar darajasiga ko‘ra quyidagicha toifalanishi mumkin:

a) shaxs uchun:

– axborotlarni qidirish, olish, uzatish, ishlab chiqish va tarqatish bo‘yicha fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini buzilishi;

– fuqarolarni shaxsiy hayot daxlsizligi huquqidan mahrum qilish;

– g‘ayri ixtiyoriy zararli axborotlardan fuqarolarning o‘z sog‘liqlarini himoya qilish huquqlari buzilishi;

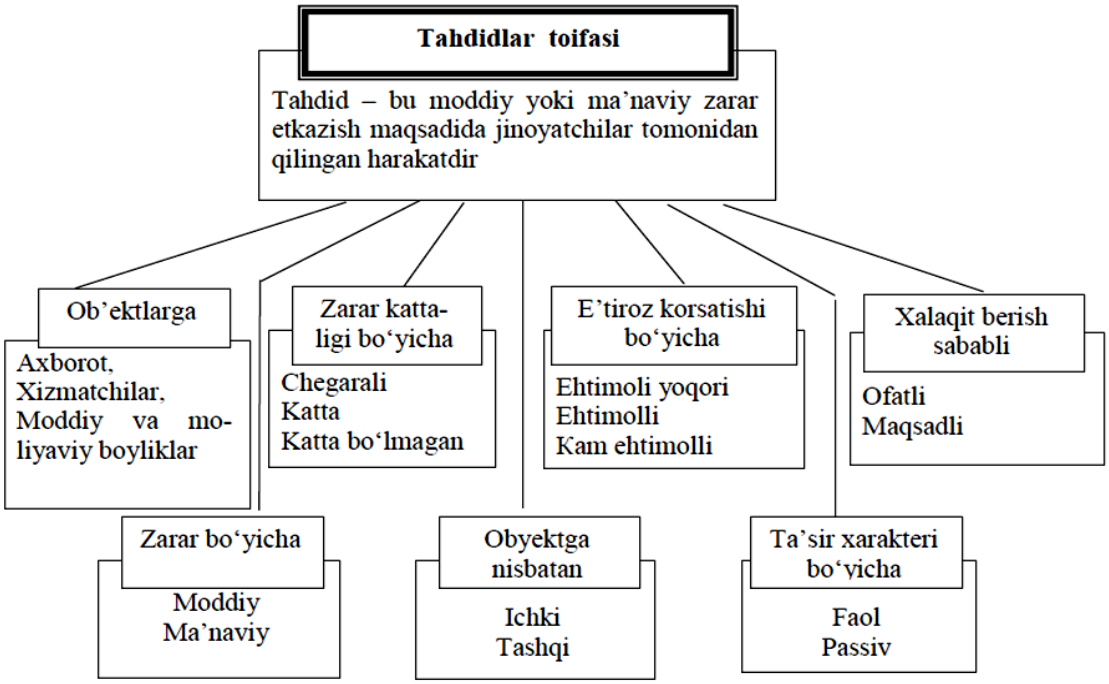
– intellektul mulk ob’yektlariga tahdid.

b) jamiyat uchun:

– axborotlashtirilgan jamiyatni qurishga to‘siqlar;

– jamiyatning ma’naviy yangilanish, uning ma’naviy boyliklarini saqlash, fidoyilik va xolislik, mamlakatning ko‘p asrlik ma’naviy an’analarini rivojlantirish, milliy, madaniy merosni targ‘ib qilish, axloq me’yorlari huquqlaridan mahrum qilish;

– zamonaviy telekommunikatsiya texnologiyalarini taraqqiy etishi, mamlakat ilmiy va ishlab chiqarish potensialini rivojlantirish va saqlab qolishga qarshilik qiluvchi muhitni yaratish.



Axborot himoyasiga metodologik yondashuv–bu konfedensial axborotlarni saqlash vazifasini turli bosqichlarda yechish bo‘yicha asos bo‘luvchi g‘oyalar, muhim tavsiyalardir. Ular axborotni me’yoriy himoya qilish bazalarini yaratishda inobatga olinadi. Shuningdek, qonun va qonunosti aktlarini qabul qilishda me’yor sifatida tatbiq qilinadi hamda ularni bajarish majburiy xarakterga ega bo‘ladi.

Tahdid – bu moddiy yoki ma’naviy zarar etkazish maqsadida jinoyatchilar tomonidan qilingan harakatdir.

1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat’iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma’naviy-etik. Ob’yektda qat’iy belgilangan o‘zini tutish qoidalarining buzilishi ko‘pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo‘llab quvvatlash.

3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to‘siqlar yaratish.

4. Ma’muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo‘llash.Fizik, apparatli, dasturli va hujjatli vositalarni o‘z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda himoya ob’yekti sifatida qaraladi.

Odatda, so‘nggi vaqtlarda axborotdan foydalanish, saqlash, uzatish va qayta ishlashda turli ko‘rinishdagi axborot tizimlarida amalga oshirilmoqda.

Axborot tizimi–bu odatda matnli yoki grafik axborotlarni yig‘ish, saqlash, qidirish va qayta ishlashga mo‘ljallangan amaliy dasturiy, ba’zan esa apparat-dasturiy nimtizimdir.

Axborotni muhofaza qilishning asosiy ob’yektlariga quyidagilar kiradi:

– davlat sirlari bilan bog‘liq va konfedensial ma’lumotlarni o‘zida saqlovchi axborot resurslari;

– vositalar va axborot tizimlari (hisoblash texnikasi vositalari, tarmoqlar va tizimlar), dasturiy vositalar (operatsion tizimlar, ma’lumotlar bazalarini boshqarish tizimlari, amaliy dasturiy ta’minot), avtomatlashtirilgan boshqaruv tizimlari, aloqa va ma’lumotlarni uzatish tizimlari, ruxsati chegaralangan axborotni qabul qilish, uzatish va qayta ishlash texnik vositalari (ovoz yozish, ovoz kuchaytirish, ovoz eshitish, so‘zlashuv va televizion qurilmalar, hujjatlarni tayyorlash, ko‘paytirish vositalari hamda boshqa grafik, matn va harfli-raqamli ma’lumotlarni qayta ishlash vositalari), konfedensial va davlat sirlari toifasiga oid bevosita qayta ishlovchi tizim va vositalar. Bunday tizim va vositalarni ko‘pincha axborotlarni qabul qilish, qayta ishlash va saqlash texnik vositalari (AQITV) deb atashadi. AQITV tarkibiga kirmaydigan, biroq konfedensial ma’lumotlar qayta ishlanuvchi hududga joylashgan texnik vosita va tizimlar ham mavjud. Bunday texnik vosita va tizimlar yordamchi texnik vosita va tizimlar (YOTVT) deb ataladi. Ularga quyidagilar kiradi: telefon, aloqa ovoz kuchaytirgich texnik vositalari, yong‘in va qo‘riqlash signalizatsiyasi tizimlari, radioaloqa tizimida ma’lumotlarni uzatish vositalari, nazorat o‘lchov qurilmalari, xo‘jalik elektr asboblari va boshqalar, shuningdek ular joylashgan bino. AQITVga statsionar jihozlar, periferiya qurilmalari, ulash liniyalari, taqsimlovchi va kommunikatsion qurilmalar, elektr manba tizimlarini o‘ziga biriktirgan tizim sifatida qarash mumkin. Konfedensial ma’lumotlarni qayta ishlashga mo‘ljallangan texnik vositalar, shuningdek ular joylashgan bino ham AQITV ob’yektini ifodalaydi.

Axborot himoyasi turlari ikki asosiy belgiga ko‘ra tasniflanadi:

birinchidan, axborot xususiyligi, aniqrog‘i qo‘riqlanadigan sirlar turiga ko‘ra;

ikkinchidan, axborot himoyasi uchun qo‘llaniluvchi kuchlar, vositalar va usullar guruhlari bo‘yicha.

Birinchi guruhga quyidagi asosiy yo‘nalishlar kiritilishi mumkin: davlat sirlarini himoya qilish, davlatlararo maxfiy ma’lumotlarni himoya qilish, tadbirkorlik sirlarini himoya qilish, xizmat sirlarini himoya qilish, mutaxassislik sirlarini himoya qilish va xususiy ma’lumotlarni himoya qilish. Ikkinchi guruhga quyidagi asosiy yo‘nalishlar kiradi: axborotlarni huquqiy himoyalash, axborotlarni tashkiliy himoyalash, axborotlarni muhandislik-texnik himoyalash.

Huquqiy himoyalash–bu huquqiy asosda axborot himoyasini ta’minlovchi maxsus qonunlar, boshqa me’yoriy hujjatlar, qoidalar, jarayonlar va tadbirlar.

Tashkiliy himoya–bu bajaruvchilarga yetkazilishi mumkin bo‘lgan ixtiyoriy zararni bartaraf etuvchi yoki yengillashtiruvchi, bajaruvchilarning me’yoriy-huquqiy asosdagi o‘zaro muomalasi va ishlab chiqarish faoliyatini qat’iy belgilash. Muhandislik-texnik himoya bu faoliyatga yetkaziluvchi zararlarga qarshilik qiluvchi turli texnik vositalardan foydalanishdir.

Axborot himoyasi vositalarini va usullarini tasniflash. Axborotni muhofaza qilishda foydalaniluvchi asosiy usullar quyidagilar hisoblanadi: yashirish, ranjirlash, noto‘g‘ri ma’lumot berish, bo‘laklash, sug‘urta qilish, hisobga olish, kodlash va shifrlash.

Yashirish–axborotni muhofaza qilish usuli sifatida amaliyotda ma’lumotlarni himoyalashning asosiy tashkiliy usullaridan biri hisoblanadi, maxfiy ma’lumotlarga ruxsat etilgan shaxslar sonini chegaralaydi. Yashirish axborotlarni himoya qilishda juda keng qo‘llaniluvchi usullardan biri hisoblanadi. Ranjirlash axborot himoya usuli sifatida, birinchidan, maxfiy ma’lumotlarni maxfiylik darajasi bo‘yicha taqsimlaydi, va ikkinchidan himoyalangan axborotga ruxsatni chegaralaydi.

Kodlash–himoyalanuvchi axborotni raqibdan yashirish maqsadida, axborotni kanal orqali uzatish jarayonida o‘zgalar tomonidan tutib olinishi xavfi mavjud bo‘lganda, uni kodlash usuli yordamida ochiq matnni shartli axborotga aylantirish usulidir. Kodlash uchun odatda belgilar to‘plami (belgilar, raqamlar va boshqalar), shuningdek axborotni tushunarsiz belgilar to‘plami ko‘rinishiga aylantirish imkonini beruvchi ma’lum qoidalar tizimi foydalaniladi. Bu axborotni o‘qish uchun esa uni yana o‘z xoliga keltirish, ya’ni kodni ochish (kalit) kerak bo‘ladi.

Axborotni kodlash texnik vositalar yordamida yoki qo‘lda amalga oshirilishi mumkin.

Shifrlash – axborotni muhofaza qilish usuli bo‘lib, ko‘pincha axborotlarni radioqurilmalar vositasida uzatishda, raqib tomonidan tutib olish xavfi bo‘lganda qo‘llaniladi. Axborotni shifrlash, uni o‘zgalar tomonidan tutib olinganda ham kalitsiz ma’nosini tushunib bo‘lmaydigan holatga o‘tkazishni anglatadi.

Axborot resurslari–bu tashkilot miqyosida axborotni muhofaza qilish bo‘yicha optimal boshqaruv yechimlari qabul qilinadigan axborot. Unga quyidagilar kiradi:

– huquqiy axborot (xavfsizlik muammolari bo‘yicha me’yoriy baza);

– tijorat axborotlari (ishlab chiqariladigan mahsulot va unda axborotni muhofaza qilish bo‘yicha ko‘rsatiladigan xizmatlar haqida axborot);

– ilmiy-texnik axborot (xavfsizlik bo‘yicha mamlakat va chet el davlatlari siyosati haqida axborot);

Axborotni muhofaza qilish tizimi deganda davlat axborotni muhofaza qilish tizimini hamda muayyan ob’yektlardagi himoya tizimlarini tushunish kerak. Davlat axborotni muhofaza qilish tizimiga quyidagilar kiradi:

– davlat me’yoriy hujjatlari, standartlar, boshqaruv hujjatlari va talablari;

– axborotni muhofaza qilish bo‘yicha konsepsiya, talablar, me’yoriy-texnik hujjatlar va ilmiy-uslubiy tavsiyalarni ishlab chiqish;

– davlat mulki bo‘lgan axborotni muhofaza qilishga yo‘naltirilgan chora-tadbirlarning tashkil etilishi, bajarilishi va amal qilinishi tartibi,shuningdek jismoniy va yuridik shaxslar ixtiyorida bo‘lgan axborotni muhofaza qilish bo‘yicha tavsiyalar;

– axborotni muhofaza qilish vositalarini sinash va sertifikatsiyalashni tashkillashtirish;
– axborotni muhofaza qilish uchun tashkilot va sohaviy koordinatsion tuzilmalarni tashkil etish;
– axborotni muhofaza qilishni tashkil etish bo‘yicha ishlarni nazorat qilish;
– chet el fuqarolari bo‘lgan yuridik va jismoniy shaxslarning davlat mulki bo‘lgan axborotdan yoki davlat tomonidan axborotni tarqatishga chegara qo‘yilgan yuridik va jismoniy shaxslar ma’lumotlaridan foydalana olish tartibini aniqlash.

Axborotlashtirishning muayyan ob’yektlarida axborotni muhofaza qilishning maqsadlari ehtimoli bo‘lgan tahdidlarning ro‘yxati bilan belgilanadi. Har qanday axborotni muhofaza qilish tizimi o‘zining xususiyatiga ega bo‘lish bilan birga umumiy talablarga javob berishi kerak. Axborotni muhofaza qilishga ko‘proq qo‘yiladigan umumiy talablar quyidagilardir:
– apparat ta’minoti (bunda axborotni muhofaza qilish hamda
muhofaza qilish tizimi faoliyatini ta’minlash uchun texnik vositalardan keng miqyosda foydalanish nazarda tutiladi);
– axborot ta’minoti (ushbu ta’minot tarkibiga tizimning faoliyatini ta’minlovchi vazifalarni hal yotuvchi ma’lumotlar, axborotlar, ko‘rsatkichlar, kattaliklar kiradi. Shuningdek, unga xavfsizlik ta’minoti xizmati faoliyati bilan bog‘liq bo‘lgan turli xarakterdagi ko‘rsatkichlar: ruxsat berish, ro‘yxatga olish, saqlash kabilar ham kiradi;
– dasturiy ta’minot (bunga konfedensial axborot manbalariga noqonuniy kirish yo‘llari hamda axborotni chiqib ketish kanallari mavjudligiga baho beruvchi turli axborot, hisobga olish, statistik va hisoblash dasturlari kiradi);
– matematik ta’minot (bu himoya uchun zarur bo‘lgan har xil hisoblarni amalga oshirishda, buzg‘unchilar texnik vositalarining xavfi tomonidan me’yorlar, hududlarga baho beruvchi matematik usullarni qo‘llashni nazarda tutadi);

AQSh Mudofaa Vazirligi (MV) kompyuter xavfsizligi Agentligi TSEC (Ishonchli Tizimlarning Himoyalanganligini Baholash Kriteriylari) nomli hisobotini chop etdi. U boshqacha aytganda Olov rang kitob (kitob rangiga ko‘ra) deb nomlandi. Unda ko‘p foydalanuvchili kompyuter tizimlarida maxfiy ma’lumotlarni himoyalash uchun xavfsizlikning 7 ta darajasi ajratilgan. Bular:

O‘zbekiston Respublikasi Adliya vazirligi me’yoriy-huquqiy hujjat loyihasini ishlab chiquvchi organ me’yoriy-huquqiy hujjatlarni Davlat ro‘yxatiga taqdim etish me’yoriy-huquqiy hujjat loyihasini qabul qiluvchi organga kiritish loyihani tayyorlovchi komissiya me’yoriy-huquqiy hujjatni tayyorlashda uning amaliyotda qo‘llanilishi va jamoatchilik fikrini o‘rganish me’yoriy-huquqiy hujjat loyihalarini ekspertiza qilish Me’yoriy-huquqiy hujjatning rasmiy matnini tasdiqlash me’yoriy-huquqiy hujjatni chop etish, kuchga kirishi va amal qilinishi bunga javob tariqasida GFR axborot xavfsizligi Agentligi Green Book (Yashil kitob)ni tayyorladi. Unda xususiy hamda davlat miqyosida axborot xavfsizligini ta’minlashda vujudga keluvchi talablar kompleks tarzda o‘z aksini topgan.

1990-yilda Yashil kitob GFR, Buyuk Britaniya, Fransiya va Gollandiya davlatlari tomonidan ma’qullandi va Yevropa Ittifoqiga yuborildi. Uning asosida Yevropa standartini ifodalovchi ITSEC (Axborot Texnologiyalarining Himoyalanganligini Baholash Kriteriyalari) yoki oq kitob tayyorlandi. Bu kitobda xavfsiz axborot tizimlarini tashkil etish kriteriyalari keltirilgan.

ITSEC Oq kitobda xavfsizlik kriteriyalarining quyidagi asosiy qismlari keltirilgan:
1. Axborot xavfsizligi.
2. Tizim xavfsizligi.
3. Mahsulot xavfsizligi.
4. Xavfsizlikka tahdid.
5. Xavfsizlik funksiyasi to‘plami.
6. Xavfsizlikning kafolatlanganligi.
7. Xavfsizlikning umumiy bahosi.
8. Xavfsizlik sinflari.
– identifikatsiya va autentifikatsiya (foydalanuvchining haqiqiyligini an’anaviy tekshirishgina emas, yangi foydalanuvchilarni ro‘yxatga olish, eskilarini o‘chirish, shuningdek autentifikasiya axborotlarini o‘zgartirish va tekshirish uchun funksiyalar, shu jumladan butunlikni nazorat qiluvchi vositalar ham tushuniladi);
– foydalanish huquqini boshqarish (shu jumladan, umumfoydalaniluvchi ob’yektlarning butunligini ta’minlash maqsadida ularga ruxsatni vaqtincha chegaralovchi xavfsizlik funksiyalari, ruxsat berish huquqini tarqatishni boshqarish kabilar);
– hisobot berishlilik (protokollashtirish);
– audit (mustaqil nazorat);
– ob’yektlardan qayta foydalanish;
– axborotning aniqligi (ma’lumot turli qismlarining o‘zaro mosligini ta’minlash (aloqa aniqligi) hamda axborotni uzatishda uni o‘zgarmasligini ta’minlash (kommunikatsiya aniqligi);
– xizmat ko‘rsatishning ishonchliligi (qisqa vaqt ichida vaqt bo‘yicha
kritik harakatlar bajarilishini ta’minlovchi funksiyalar; kritik bo‘lmagan, ya’ni kerakli vaqtda ma’lumotni olish imkonini berish; xatolarni topish va ularni bartaraf etish funksiyalari; kommunikatsiya xavfsizligini ta’minlovchi rejalovchi funksiyalar);
– ma’lumot almashish.
6. Xavfsizlik mexanizmlarini ifodalash.
Oq kitobda “tizim” va “mahsulot” o‘rtasida farq ifodalanadi.

“Tizim” deganda ma’lum bir maqsadda va ma’lum bir doirada qo‘llaniluvchi aniq apparat-dasturiy konfiguratsiya tushuniladi. “Mahsulot” deganda esa, o‘z xohishiga ko‘ra sotib olib ixtiyoriy “tizim”ga o‘rnatilishi mumkin bo‘lgan apparat-dasturiy paket tushuniladi. “Tizim” va “Mahsulot”ning kriteriyalarini umumlashtirish maqsadida ITSECda yagona – “ob’yekt” atamasi kiritilgan. “Ob’yekt”ni ishonchli deb qabul qilish uchun, xavfsizlikni

kafolatlovchi ma’lum bir darajadagi ishonch kerak bo‘ladi. U esa samaradorlik va aniqlikni o‘z ichiga oladi. Ba’zi manbalarda kafolatlanganlikni himoya vositalarining adekvatligi deb ham nomlanadi.

Har qanday tashkilot faoliyati axborot texnologiyalaridan foydalanish oqibatida ko‘plab tahdidlardan holi bo‘lmaganligi sababli tahdidlarni boshqarish nomli yangi funksiya paydo bo‘ldi. U o‘z ichiga ikki faoliyatni oladi: tahdidlarni baholash (o‘lchash) va samarali va tejamkor himoya boshqaruvchisini tashlash.
Tahdidlarni boshqarish jarayonini quyidagi bosqichlarga bo‘lish mumkin:
1. Tahlil qilinuvchi ob’yektlarni tanlash va ularni ko‘rib chiqishda batafsillik darajasi.
2. Tahdidlarni baholash metodologiyasini tanlash.
3. Aktivlarni identifikatsiyalash.
4. Tahdid va uning oqibatlari tahlili, himoyaning zaifliklarini aniqlash.
5. Tahdidlarni baholash.
6. Himoya choralarini tanlash.
7. Tanlangan choralarni qo‘llash va tekshirish.
8. Qoldiq tahdidni baholash.
Ushbu munosabatlarni huquqiy boshqarish avvalo, axborot tahdidlaridan sug‘urta qilish orqali amalga oshirilishi mumkin va zarur.

Mustaqil tayyorgarlik uchun savollar

1. Axborot xavfsizligi tushunchasi nimani anglatadi?
2. Axborot xavfsizligining qanday tashkil etuvchilari mavjud?

Nazorat savollari

1. Axborot xavfsizligi milliy xavfsizlik tizimida nima tushuniladi?
2. Axborot xavfsizligining zamonaviy konsepsiyasi nima?
3. Axborot xavfsizligiga tahdid deganda nima tushuniladi?
4. Axborotni ximoyalashda qanday usullari va turlari mavjud?
5. Axborotni muhofaza qilish qanday ob’yektlarga ega?
6. Axborotni muhofaza qilish vositalariga nimalar kiradi?

1.3. AXBOROT HIMOYASI VA UNING TURLARI

Tayanch ibora va tushunchalar: Axborot xavfsizligini ta’minlash, axborot himoyasi turlari, axborotni muhofaza qilish vositalari, yashirish, ranjirlash noto‘g‘ri ma’lumot berish, axborotni bo‘laklash, sug‘urta qilish.

Mavzuga oid asosiy muommalar: Axborot ximoyasi va uning turkumlari, tarmoq xavfsizligini nazorat qilishni texnik vositalari, avtomatlashtirilgan axborot tizimlarida ma’lumotlarga nisbatan xavflar, avtomatlashtirilgan axborot tizimlarida ximoyalash zaruratlarini izohlab bering.

Darsning maqsadi: Talabalarga axborot xavfsizligini ta’minlashga yo‘naltirilgan himoya harakatlari qator kattaliklar bilan tavsiflanishi mumkin: tahdid xarakteri, harakat usullari, uning tarqalganligi, o‘rab olish masshtabi kabilar

Axborot xavfsizligini ta’minlashga yo‘naltirilgan himoya harakatlari qator kattaliklar bilan tavsiflanishi mumkin: tahdid xarakteri, harakat usullari, uning tarqalganligi, o‘rab olish masshtabi kabilar.

Tahdid xarakteriga ko‘ra himoya harakatlari ma’lumotlarni oshkor bo‘lishi, chiqib ketishi va noqonuniy kirishdan himoya qilishga yo‘naltiriladi. Harakat usullariga ko‘ra ularni kamomad yoki boshqa zararlarni: ogohlantirish, aniqlash, oldini olish va tiklash kabilarga taqsimlash mumkin. O‘rab olish bo‘yicha himoya harakatlari hududga, binoga, inshoatga, qurilmalarga yoki ularning alohida elementlariga yo‘naltirilgan bo‘lishi mumkin. Himoya tadbirlarining masshtabi esa obyekt, guruh yoki individual himoya bo‘yicha tavsiflanadi.

Axborot himoyasi turlari ikki asosiy belgiga ko‘ra tasniflanadi: birinchidan, axborot xususiyligi, aniqrog‘i qo‘riqlanadigan sirlar turiga ko‘ra; ikkinchidan, axborot himoyasi uchun qo‘llaniluvchi kuchlar, vositalar va usullar guruhlari bo‘yicha.

Birinchi guruhga quyidagi asosiy yo‘nalishlar kiritilishi mumkin: davlat sirlarini himoya qilish, davlatlararo maxfiy ma’lumotlarni himoya qilish, tadbirkorlik sirlarini himoya qilish, xizmat sirlarini himoya qilish, mutaxassislik sirlarini himoya qilish va xususiy ma’lumotlarni himoya qilish. Ikkinchi guruhga quyidagi asosiy yo‘nalishlar kiradi: axborotlarni huquqiy himoyalash, axborotlarni tashkiliy himoyalash, axborotlarni muhandislik-texnik himoyalash.

Huquqiy himoyalash–bu huquqiy asosda axborot himoyasini ta’minlovchi maxsus qonunlar, boshqa me’yoriy hujjatlar, qoidalar, jarayonlar va tadbirlar.

Tashkiliy himoya–bu bajaruvchilarga yetkazilishi mumkin bo‘lgan ixtiyoriy zararni bartaraf etuvchi yoki yengillashtiruvchi, bajaruvchilarning me’yoriy-huquqiy asosdagi o‘zaro muomalasi va ishlab chiqarish faoliyatini qat’iy belgilash.

Muhandislik-texnik himoya–bu faoliyatga yetkaziluvchi zararlarga qarshilik qiluvchi turli texnik vositalardan foydalanishdir.

Axborot himoyasi vositalarini va usullarini tasniflash. Axborotni muhofaza qilishda foydalaniluvchi asosiy usullar quyidagilar hisoblanadi: yashirish, ranjirlash, noto‘g‘ri ma’lumot berish, bo‘laklash, sug‘urta qilish, hisobga olish, kodlash va shifrlash.

Yashirish –axborotni muhofaza qilish usuli sifatida amaliyotda ma’lumotlarni himoyalashning asosiy tashkiliy usullaridan biri hisoblanadi, maxfiy ma’lumotlarga ruxsat etilgan shaxslar sonini chegaralaydi. Yashirish axborotlarni himoya qilishda juda keng qo‘llaniluvchi usullardan biri hisoblanadi.

Ranjirlash axborot himoya usuli sifatida, birinchidan, maxfiy ma’lumotlarni maxfiylik darajasi bo‘yicha taqsimlaydi, va ikkinchidan himoyalangan axborotga ruxsatni chegaralaydi.

Noto‘g‘ri ma’lumot berish – axborot himoya usullaridan biri bo‘lib, biror obyekt haqidagi haqiqiy ma’lumot o‘rniga atayin yolg‘on ma’lumot tarqatishni anglatadi.

Sug‘urta qilish–axborotni muhofaza qilish usuli sifatida endigina tan olinmoqda. Uning ma’nosi axborot egasi huquqlari va manfaatlarini yoki axborot vositalarini an’anaviy tahdidlar va axborot xavfsizligi tahdidlaridan himoya qilishni bildiradi. Ushbu usul tijorat sirlarini saqlashda ko‘proq qo‘llanilishi ehtimoli mavjud. Axborotni sug‘urta qilishda u dastlab, auditorlik tekshiruvidan o‘tishi va xulosaga ega bo‘lishi talab etiladi.

Axborotlarni ma’naviy-ma’rifiy himoyalash usuli axborotni muhofaza qilishda juda muhim rol o‘ynaydi. Aynan inson, u korxona yoki tashkilot xodimi, maxfiy ma’lumotlardan voqif bo‘lib, o‘z xotirasida ko‘plab ma’lumotlarni jamlaydi va ba’zi hollarda axborot chiqib ketishi manbaiga aylanishi mumkin hamda uning aybi bilan o‘zgalar ushbu axborotga noqonuniy ega bo‘ladilar. Axborotlarni ma’naviy-ma’rifiy himoyalash usuli quyidagilarni nazarda tutadi:

-xodimni tarbiyalash, u bilan ma’lum sifatlarni, qarashlarni shakllantirishga yo‘naltirilgan maxsus ishlarni olib borish (vatanparvarlik, axborotni muhofaza qilish uning shaxsan o‘zi uchun ham qanday ahamiyat kasb etishini tushuntirish);

-xodimni axborotni muhofaza qilish qoidalari va usullariga o‘rgatish, konfedensial axborot tashuvchilar bilan amaliy ishlash ko‘nikmalarini shakllantirish.

Hisobga olish axborotni muhofaza qilishning muhim usullaridan biri bo‘lib, konfedensial ma’lumotlar tashuvchilarning hamda undan foydalanuvchilarning ixtiyoriy vaqtda qayerda joylashganligi haqida ma’lumot olish imkonini beradi. Ushbu usulsiz himoya muammosini hal etish juda qiyin. Sir saqlanuvchi axborotlarni hisobga olish tamoyillari:

- ✓ himoyalanuvchi axborotlarni tashuvchilarning barchasini ro‘yxatga olish majburiyligi;
- ✓ muayyan axborot tashuvchini ro‘yxatga olish bir marta bo‘lishligini (takrorlanmasligini) ta’minlash;
  ro‘yxatda konfedensial ma’lumot tashuvchining ayni vaqtda qaysi manzildaligini ko‘rsatish;
- ✓ har bir himoyalangan axborot tashuvchining saqlanishiga yagona javobgarlik va hisobda ushbu axborotni ishlatgan foydalanuvchi haqida ma’lumotni aks ettirish.

Kodlash–himoyalanuvchi axborotni raqibdan yashirish maqsadida, axborotni kanal orqali uzatish jarayonida o‘zgalar tomonidan tutib olinishi xavfi mavjud bo‘lganda, uni kodlash usuli yordamida ochiq matnni shartli axborotga aylantirish usulidir. Kodlash uchun odatda belgilar to‘plami (belgilar, raqamlar va boshqalar), shuningdek axborotni tushunarsiz belgilar to‘plami ko‘rinishiga aylantirish imkonini beruvchi ma’lum qoidalar tizimi foydalaniladi. Bu axborotni o‘qish uchun esa uni yana o‘z xoliga keltirish, ya’ni kodni ochish (kalit) kerak bo‘ladi. Axborotni kodlash texnik vositalar yordamida yoki qo‘lda amalga oshirilishi mumkin.

Shifrlash– axborotni muhofaza qilish usuli bo‘lib, ko‘pincha axborotlarni

radioqurilmalar vositasida uzatishda, raqib tomonidan tutib olish xavfi bo‘lganda qo‘llaniladi. Axborotni shifrlash, uni o‘zgalar tomonidan tutib olinganda ham kalitsiz ma’nosini tushunib bo‘lmaydigan holatga o‘tkazishni anglatadi.

Axborotni muhofaza qilish vositalari–bu axborotni muhofaza qilish masalalarini hal etish uchun foydalaniluvchi muhandislik-texnik, elektr, elektron, optik va boshqa qurilma vositalar to‘plamidir.

Moddiy resurslar axborotni muhofaza qilishda maxsus ahamiyatga ega. Unga maxsus ajratilgan bino, maxsus qurilmalar, qabul qilingan me’yorlar asosida attestatsiya qilingan kompyuter va orgtexnika, apparat vositalari, dastur vositalari, axborotni muhofaza qilish vositalari va boshqalar.

Axborot resurslari – bu tashkilot miqyosida axborotni muhofaza qilish bo‘yicha optimal boshqaruv yechimlari qabul qilinadigan axborot. Unga

- ✓ huquqiy axborot (xavfsizlik muammolari bo‘yicha me’yoriy baza);
- ✓ tijorat axborotlari (ishlab chiqariladigan mahsulot va unda axborotni muhofaza qilish bo‘yicha ko‘rsatiladigan xizmatlar haqida axborot);
- ✓ ilmiy-texnik axborot (xavfsizlik bo‘yicha mamlakat va chet el davlatlari siyosati haqida axborot);
- ✓ ishlab chiqarish texnologiyasi jarayonlari bo‘yicha axborot;
- ✓ tashkilotning axborot xavfsizligi holati, unga tahdidlar bo‘yicha axborot-tahliliy faoliyat natijasida olingan tahliliy axborot.

Moddiy resurslar. Axborotni muhofaza qilishni loyihalashtirishni, uni ishga tushirishni moddiy ta’minotsiz amalga oshirib bo‘lmaydi. Bu ish murakkab sharoitlarda amalga oshiriladi: xavfsizlik sohasida raqobatchilik, xizmat ko‘rsatuvchining kam xarajat qilib ko‘p foyda olish istagi, xavfsizlik bo‘yicha sifatsiz ishlarni amalga oshirishi va hokazo.

Axborot xavfsizligi uning egalari tomonidan himoyalanuvchi axborotning tarqab ketish, buzilish, yo‘q qilish va modifikatsiya qilishni oldini olish maqsadiga yo‘naltirilgan kompleks chora-tadbirlarni ifodalaydi.

Axborotni muhofaza qilish tizimi deganda davlat axborotni muhofaza qilish tizimini hamda muayyan obyektlardagi himoya tizimlarini tushunish kerak.

Davlat axborotni muhofaza qilish tizimiga quyidagilar kiradi:
-davlat me’yoriy hujjatlari, standartlar, boshqaruv hujjatlari va talablari;
- axborotni muhofaza qilish bo‘yicha konsepsiya, talablar, me’yoriy-texnik hujjatlar va ilmiy-uslubiy tavsiyalarni ishlab chiqish;
-davlat mulki bo‘lgan axborotni muhofaza qilishga yo‘naltirilgan chora-tadbirlarning tashkil etilishi, bajarilishi va amal qilinishi tartibi, shuningdek jismoniy va yuridik shaxslar ixtiyorida bo‘lgan axborotni muhofaza qilish bo‘yicha tavsiyalar;
-axborotni muhofaza qilish vositalarini sinash va sertifikatsiyalashni tashkillashtirish;

-axborotni muhofaza qilish uchun tashkilot va sohaviy koordinatsion tuzilmalarni tashkil etish;
-axborotni muhofaza qilishni tashkil etish bo‘yicha ishlarni nazorat qilish;

Axborotlashtirishning muayyan obyektlarida axborotni muhofaza qilishning maqsadlari ehtimoli bo‘lgan tahdidlarning ro‘yxati bilan belgilanadi. Har qanday axborotni muhofaza qilish tizimi o‘zining xususiyatiga ega bo‘lish bilan birga umumiy talablarga javob berishi kerak. Axborotni muhofaza qilishga ko‘proq qo‘yiladigan umumiy talablar quyidagilardir: Axborotni muhofaza qilish tizimi

- bir butunlikda bo‘lishi;
- axborotning, axborot vositalarining xavfsizligini va axborot munosabatidagilar manfaatlarining himoyasini ta’minlashi;
- tizimning ichida uning elementlari orasida axborot aloqasini ta’minlashi;
- axborot faoliyatining texnologik kompleksini o‘ziga qamrab olishi;
- foydalanish vositalari bo‘yicha turli, axborotdan foydalana olishlilik bo‘yicha ko‘p darajali iyerarxik ko‘rinishda bo‘lishi;
- axborot xavfsizligi choralarini o‘zgartirish va to‘ldirishga ochiq bo‘lishi;
- nostandart bo‘lishi (himoya vositalarini tanlashda buzg‘unchining himoya imkoniyatlari bilan tanish emasligiga ishonishmaslik);
- texnik xizmat ko‘rsatishga oddiy va foydalanish uchun qulay bo‘lishi;
- ishonchli bo‘lishi, kerak (texnik vositalardagi ixtiyoriy buzilish axborotning tarqab ketish kanali bo‘lib qolishi mumkin).

Boshqa tizimlar kabi axborotni muhofaza qilish tizimi o‘z ta’minotining ma’lum turlariga ega bo‘lishi kerak. Shu sababli bu tizim quyidagilarga ega bo‘lishi mumkin:
huquqiy ta’minot (bunga bajarilishi majburiy bo‘lgan me’yoriy hujjatlar, ko‘rsatmalar, yo‘riqnomalar, talablar kiradi);
tashkiliy ta’minot (bunda axborotni muhofaza qilish ma’lum bir tuzilmaviy birliklar orqali qo‘llanilishi nazarda tutiladi: hujjatlar himoyasi xizmati; qo‘riqlash, kirishga ruxsat berish xizmati; texnik vositalar yordamida axborotni muhofaza qilish xizmati; axborot-tahliliy faoliyat va boshqalar);
apparat ta’minoti (bunda axborotni muhofaza qilish hamda muhofaza qilish tizimi faoliyatini ta’minlash uchun texnik vositalardan keng miqyosda foydalanish nazarda tutiladi);
axborot ta’minoti (ushbu ta’minot tarkibiga tizimning faoliyatini ta’minlovchi vazifalarni hal yotuvchi ma’lumotlar, axborotlar, ko‘rsatkichlar, kattaliklar kiradi. Shuningdek, unga xavfsizlik ta’minoti xizmati faoliyati bilan bog‘liq bo‘lgan turli xarakterdagi ko‘rsatkichlar: ruxsat berish, ro‘yxatga olish, saqlash kabilar ham kiradi);
dasturiy ta’minot (bunga konfedensial axborot manbalariga noqonuniy kirish yo‘llari hamda axborotni chiqib ketish kanallari mavjudligiga baho beruvchi turli axborot, hisobga olish, statistik va hisoblash dasturlari kiradi);
matematik ta’minot (bu himoya uchun zarur bo‘lgan har xil hisoblarni

amalga oshirishda, buzg‘unchilar texnik vositalarining xavfi tomonidan me’yorlar, hududlarga baho beruvchi matematik usullarni qo‘llashni nazarda tutadi);

lingvistik ta’minot (axborotni muhofaza qilish sohasida mutaxassislar va foydalanuvchilar tomonidan qo‘llaniluvchi maxsus til vositalarining to‘plami);

me’yoriy-uslubiy ta’minot (bunga axborotni muhofaza qilishni ta’minlovchi organlar, xizmatlar, vositalar faoliyati me’yorlari va reglamentlari, axborotni muhofaza qilish qattiq talab etiladigan sharoitlarda foydalanuvchilar tomonidan o‘z vazifalarini bajarishda faoliyatni ta’minlovchi turli uslublar kiradi).

Mustaqil uchun savollar

1. Axborotlarni muhofaza qilishning texnik vositalari tushunchasi nimani anglatadi?
2. Ma’lumotlarni ruxsatsiz olishning ob’yektlari, usullari va vositalari nimalardan iborat?
3. Maskirovkalovchi belgilarning ochilishi tushunchasini nimani bildiradi?
4. Demaskirovka belgilari nimalar bilan farq qiladi?

Nazorat savollari.

1. Axborot xavfsizligi milliy xavfsizlik tizimida nima tushuniladi?
2. Axborot xavfsizligining zamonaviy konsepsiyasi nima?
3. Axborot xavfsizligiga tahdid deganda nima tushuniladi?
4. Axborotni ximoyalashda qanday usullari va turlari mavjud?
5. Axborotni muhofaza qilish qanday ob’yektlarga ega?
6. Axborotni muhofaza qilish vositalariga nimalar kiradi?

1.4. Axborotlarni stenografik himoyalash.

Tayanch ibora va tushunchalar: Uzish (raz’edinenie), ushlab qolish (perexvat), turlash(modefikatsiya), soxtalashtirish(falsifikatsiya), passiv xujumlar, aktiv xujumlar, imitatsiya, tiklash, ma’lumotlarni modefikatsiyalash.

Mavzuga oid asosiy muommalar: Axborotni muhofaza qilishning apparat-dasturiy vositalari, kompyuter tizimlarida axborot xavfsizligi, kompleks xavfsizlik, kompleks yondashuv bo‘lgan uzluksiz jarayonini nazarda tutadi.

Darsning maqsadi: Axborotlarni stenografik himoyalash, axborotlarni stenografik himoyalash usullari, zamonafiy kompyter stenografiyasi.

Axborotni muhofaza qilishning apparat-dasturiy vositalari – axborotni muhofaza qilish funksiyalarini (foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish, resurslardan foydalana olishni cheklash, voqealarni qayd qilish, axborotni kriptografik himoyalash va shu kabilar) bajaradigan (mustaqil yoki boshqa vositalar bilan birgalikda) turli elektron qurilmalar va maxsus dasturlardir. Axborotni muhofaza qilishning apparat vositasi – bu, maxsus

himoya qurilmasi yoki axborotni qayta ishlash texnik vositasining komplektiga kiruvchi moslama.

Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlanadi. Buzg‘unchi tarmoqning birorbir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin. Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun “tarmoqlararo ekran” (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

Axborotlarni himoyalashning apparat vositalariga, kompyuterning texnik vositalariga taalluqli bo‘lgan, axborot xavfsizligini ta’minlashning ayrim funksiyalarini mustaqil ravishda yoki dasturiy vositalar bilan bir majmua tarkibida bajaradigan elektron va elektron-mexanik moslamalari kiritiladi. Bunday qurilmalarni ma’lumotlarni himoyalashning injenertexnik vositalariga emas, balki apparat vositalariga kiritishning asosiy sharti, ularni kompyuterning texnik vositalari tarkibida kiritilishi bilan belgilanadi. Axborotlarni muhofaza qilishning asosiy apparat vositalariga quyidagilarni kiritish mumkin:

– foydalanuvchini identifikatsiyalovchi ma’lumotlarni kiritish qurilmalari (magnit va plastik kartalar, barmoq izlari va boshqalar);

– ma’lumotlarni shifrlovchi qurilmalar;

– ish stansiyalari va serverlarga noqonuniy ulanib olishga xalaqit beruvchi qurilmalar (elektron qulflar va blokiratorlar).

Ma’lumotlarni muhofaza qilishning yordamchi apparat vositalariga quyidagilar misol bo‘la oladi:

– magnitli tashuvchilardagi ma’lumotlarni yo‘q qiluvchi qurilmalar;

– kompyuter vositalaridan foydalanuvchilarining noqonuniy harakatlari bo‘yicha xabardor qiluvchi (signalizatsiya beruvchi) qurilmalar va boshqalar.

Axborotlarni muhofaza qilishning dasturiy vositalari deganda, faqatgina axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlar tushuniladi. Axborotlarni muhofaza qilishning asosiy dasturiy vositalariga quyidagilarni kiritish mumkin:

–kompyuter tizimlarida foydalanuvchilarni identifikatsiyalovchi va autentifikatsiyalovchi dasturlar;

–kompyuter tizimlari resurslaridan foydalanuvchilarning huquqlarini cheklovchi dasturlar;

– axborotlarni shifrlovchi dasturlar;

–axborot resurslarini (tizimli va amaliy dasturiy ta’minotni, ma’lumotlar bazalarini, ta’limning kompyuter tizimlarini va hokazo) noqonuniy o‘zgartirishlardan, foydalanishlardan va ko‘paytirishlardan himoyalovchi dasturlar.

Kompyuter tizimlarida axborot xavfsizligini ta’minlashga taalluqli ma’noda identifikatsiyalash atamasi kompyuter tizimlari subyektining unikal nomini bir qiymatli tanib olishni bildiradi. Autentifikatsiyalash esa taqdim etilgan nomni ushbu subyektga mosligini tasdiqlashni anglatadi (subyektning aslligini tasdiqlash). Axborotlarni muhofaza qilishning yordamchi dasturiy vositalariga misol qilib quyidagilarni keltirish mumkin:

– qoldiq axborotlarni (tezkor xotira blokidagi, vaqtinchalik fayllardagi va hokazo) yo‘q qiluvchi dasturlar;
– kompyuter tizimlarining xavfsizligi tizimiga bog‘liq bo‘lgan turli voqea va hodisalarni tiklash hamda shunday voqea va hodisalar ro‘y berganini isbotlash uchun foydalaniladigan audit dasturlari (qayd qilish jurnallarini yuritish);
– qoidabuzar bilan ishlashni imitatsiyalovchi dasturlar (qoidabuzarni go‘yoki yopiq axborotlarni olgan deb chalg‘itish);
– kompyuter tizimlarining himoyalanganligini sinovdan o‘tkazuvchi nazorat dasturlar va boshqalar.
Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklariga quyidagilar kiradi:
– ko‘paytirishning osonligi;
– moslanuvchanlik (turli sharoitlarda qo‘llaniladigan muayyan kompyuter tizimlarini, axborot xavfsizligiga tahdidning o‘ziga xosligini hisobga olib, sozlash imkoniyati);
– qo‘llashning qulayligi–bir xil dasturlar, masalan shifrlovchi dasturlar “shaffof” (foydalanuvchiga ko‘rinmaydigan) rejimda ishlaydi, boshqalari foydalanuvchidan hech qanday qo‘shimcha yangi (boshqa dasturlari bilan taqqoslaganda) ko‘nikmalar talab qilmaydi;
– ularni axborot xavfsizligiga yangi tahdidlar hisobini yuritish uchun o‘zgartirishlar kiritish yo‘li bilan takomillashuvining amaldagi chegarasiz imkoniyatlari mavjudligi.

Kompyuter tizimlaridan foydalanish huquqini cheklashning usul va vositalari. Axborot xavfsizligini ta’minlashning asosiy konsepsiyasini turli aloqa va xavfsizlikni ta’minlash nimtizimlari, umumiy texnik vositalar, aloqa kanallari, dasturiy ta’minot va ma’lumotlar bazalariga ega yagona tizimga integrasiyasiga asoslangan kompleks yondashuv tashkil etadi.

Kompleks xavfsizlik–vujudga kelishi mumkin bo‘lgan barcha turdagi tahdidlar (noqonuniy foydalanish, ma’lumotlarni tutib olish, terrorizm, yong‘in, tabiiy ofatlar va hokazolar)ni majburiy hisobga olib, zamon va makon (faoliyatning barcha texnologik sikllari) bo‘yicha xavfsizlikni ta’minlashning majburiy bo‘lgan uzluksiz jarayonini nazarda tutadi.

Kompleks yondashuv qanday shaklda qo‘llanilishidan qat’iy nazar, u murakkab va turli yo‘nalishdagi xususiy masalalarni, ularning o‘zaro chambarchas bog‘liqlikdagi yechimi bilan hal etiladi. Bunday masalalarning eng dolzarblari bo‘lib, axborotlardan foydalanishni cheklash, axborotlarni texnik va kriptografik himoyalash, texnik vositalarning yondosh nurlanishlari darajasini kamaytirish, obiyektlarning texnik mustahkamlanganligi, ularning qo‘riqlash va tahlikadan xabardor qilish (signalizatsiya) qurilmalari bilan jihozlanganligi hisoblanadi.

Obiektning axborot xavfsizligini ta’minlash tizimining samaradorligi muhim ahamiyat kasb etadi. Kompyuter tizimlari uchun ushbu samaradorlikni, hisoblash tizimida qo‘llanilayotgan apparat-dasturiy vositalarni tanlanganligi bilan baholash mumkin. Bunday samaradorlikni baholash, xavfsizlikni ta’minlash darajasi foydalanish huquqiga bo‘lgan nazoratni kuchaytirilishiga

bog‘liqlikni ko‘rsatuvchi o‘suvchi egri chiziq orqali amalga oshirilishi mumkin. Axborotlarni muhofaza qilishning dasturiy vositalari himoyalanayotgan tizim. Axborotlarni muhofaza qilishning dasturiy vositalari qurilmadan, jumladan kompyuterdan foydalana olish deganda, subyektga ushbu qurilmadan foydalanib, unga muayyan ruxsat etilgan harakatlarni bajara olish imkonini berish tushuniladi. Masalan, kompyuter foydalanuvchisiga kompyuterni ishga tushirish va o‘chirish, dasturlar bilan ishlash, ma’lumotlarni kiritish va chiqarishga ruxsat etiladi. Xizmat ko‘rsatuvchi shaxs esa o‘rnatilgan tartibda kompyuterni tekshiradi, ishdan chiqqan bloklarni almashtiradi va tiklaydi.

Ruxsat etilgan subyektni identifikatsiyalash uchun kompyuter tizimlarida ko‘p hollarda atributivli identifikatorlardan foydalaniladi. Biometrik identifikatsiyalashning oson yo‘li – klaviaturada ishlash ritmi orqali aniqlashdir. Atributivli indentifikatorlar ichidan, odatda, quyidagilaridan foydalaniladi:

– parollar;
– yechib olinadigan axborot tashuvchilar;
– elektron jetonlar;
– plastik kartochkalar;
– mexanik kalitlar.

Konfedensial ma’lumotlar bilan ishlaydigan deyarli barcha kompyuterlarda foydalanuvchilarni autentifikatsiyalash parollar yordamida amalga oshiriladi. Parol–bu simvollar (harflar, raqamlar, maxsus belgilar) kombinatsiyasi bo‘lib, uni faqat parol egasi bilishi kerak. Ayrim hollarda xavfsizlik tizimi ma’muriga ham ma’lum bo‘ladi. Kompyuterning zamonaviy operatsion tizimlarida paroldan foydalanish o‘rnatilgan. Parol xeshlangan holatda kompyuterning qattiq diskida saqlanadi. Parollarni taqqoslash operatsion tizim (OT) tomonidan foydalanuvchi huquqiga mos imkoniyatlar yuklangunga qadar amalga oshiriladi. Lekin, kompyuterning OTdan foydalanishda kiritiladigan foydalanuvchi parolidan tashqari, Internetda ro‘yxati keltirilgan ayrim «texnologik» parollardan ham foydalanish mumkin. Ko‘pgina kompyuter tizimlarida identifikator sifatida, foydalanishga ruxsat etilgan subyektni identifikatsiyalovchi kod yozilgan yechib olinuvchi axborot tashuvchilardan foydalaniladi.

Autentifikatsiyalash jarayonida kompyuter tizimi foydalanuvchi monitoriga raqamli ketma-ketlikdan iborat so‘rov chiqaradi, foydalanuvchi ushbu so‘rovni jeton tugmalari orqali kiritadi. Bunda jeton o‘z indikatorida akslanadigan javob ketma-ketligini ishlab chiqadi va foydalanuvchi ushbu ketma-ketlikni kompyuter tizimiga kiritadi. Natijada, yana bir bor bir martalik qaytarilmaydigan parol olinadi. Jetonsiz tizimga kirishning imkoni bo‘lmaydi. Jetondan foylanishdan avval unga foydalanuvchi o‘zining shaxsiy parolini kiritishi lozim. Atrubutivli identifikatorlardan (parollardan tashqari) ruxsat berilish va qayd qilish chog‘ida foydalanilish mumkin yoki ular ish vaqti tugagunga qadar ishlatilayotgan qurilmaga doimiy ulangan holda bo‘lishi shart. Qisqa vaqtga biror joyga chiqilganda ham identifikator olib qo‘yiladi va qurilmadan foydalanish blokirovka qilinadi. Bunday apparat-dasturiy vositalar nafaqat qurilmalardan foydalanishni cheklash masalalarini hal qila oladi, shu

bilan birga axborotlardan noqonuniy foydalanishdan himoyalashni ta’minlaydi. Bunday qurilmalarning ishlash prinsipi qurilmaga o‘rnatilgan OT funksiyalarini kengaytirishga asoslangan. Autentifikatsiyalash jarayoni kompyuter tizimlari bilan ruxsat etilgan subyekt orasida amalga oshiriladigan dialogni ham o‘z ichiga olishi mumkin. Ruxsat etilgan subyektga bir qator savollar beriladi, olingan javoblar tahlil qilinadi va ruxsat etilgan subyektning aslligi bo‘yicha yakuniy xulosa qilinadi.

Ko‘pincha sodda identifikator sifatida mexanik kalitlardan foydalaniladi. Mexanik qulf qurilmaga tok yetkazib beruvchi qurilmaga o‘rnatilgan bo‘lishi mumkin. Qurilmaning asosiy boshqaruv organlari joylashgan joyni berkituvchi qopqog‘i qulflangan holda bo‘lishi mumkin.

Xizmat ko‘rsatuvchi xodimning qurilmadan foydalanishiga ruxsat etishni tashkil etish foydalanuvchiga berilgan ruxsatdan farqlanadi. Eng avvalo, qurilma konfedensial ma’lumotlardan tozalanadi hamda axborot almashinish imkonini beruvchi aloqalar uziladi. Qurilmaga texnik xizmat ko‘rsatish va uning ish qobiliyatini tiklash mansabdor shaxs nazorati ostida amalga oshiriladi. Bunda ichki montaj va bloklarni almashtirishga bog‘liq ishlarni amalga oshirilishiga jiddiy e’tibor beriladi. Himoyalovchi apparat-dasturiy komplekslarning ko‘pchiligi maksimal sondagi himoyalash mexanizmlaridan foydalaniladi. Bu mexanizmlarga quyidagilar kiradi:

– foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;
– fayllar, papkalar, disklardan foydalanishga ruxsatni cheklash;
– dasturiy vositalar va axborotlar butunligini nazorat qilish;
– foydalanuvchi uchun funksional yopiq muhitni yaratish imkoniyati;
– OTni yuklanish jarayonini himoyalash;
– foydalanuvchi yo‘qligida kompyuterni blokirovka qilish;
– ma’lumotlarni kriptografik o‘zgartirish;
– hodisalarni qayd qilish;
– xotirani tozalash.

Foydalanishni cheklash vositalari yordamida noqonuniy foydalanishdan himoyalash (NFH)ning usul va vositalaridan tashqari kompyuterni himoyalash uchun quyidagi uslub va vositalar qo‘llaniladi:

– qurilmalarni noqonuniy ulab olishga qarshi harakatlar;
– boshqaruv va ulanishlarni, ichki montajni noqonuniy aralashuvlardan himoyalash;
– foydalanish jarayonida dastur tuzilishining butunligini va himoyasini nazorat qilish.

Kompyuter tizimlariga (KT) qurilmalarni noqonuniy ulab olishga qarshi harakatlarni tashkil etishda, bu ulanish KTning texnik tuzilishininoqonuniy o‘zgartirish imkonini beruvchi yo‘llardan bir ekanligini nazarda tutish lozim. Ushbu o‘zgartirishlar ro‘yxatdan o‘tkazilmagan qurilmalarni ulash yoki kompyuter tizimlarining tarkibiy vositalarini almashtirish orqali amalga oshiriladi.

Axborotlarni stenografik himoyalash usullari.

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga yetarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Viruslarning ta’sir mexanizmlarini, ularga qarshi kurash usullari va vositalarini bilish viruslanishga qarshi harakatlarni samarali tashkil etish, ularning ta’siridan zararlanish ehtimolligini va talafatlarni minimumga keltirish imkonini beradi. Kompyuter viruslari–bu KTda tarqalish va o‘zini o‘zi ishlab chiqish xususiyatiga ega bo‘lgan kichik hajmdagi bajariluvchi dasturlar. Viruslar KTda saqlanayotgan dasturiy vositalar yoki ma’lumotlarni yo‘q qilishi yoki o‘chirib yuborishi mumkin. Tarqalish jarayonida viruslar o‘zini modifikatsiyalashi mumkin. Viruslarning ommaviy tarqalib ketishi va ularning KT resurslariga ta’siri oqibatlarining jiddiyligi, maxsus antivirus vositalarini va ularni qo‘llash usullarini yaratish va foydalanish zaruriyatini keltirib chiqardi.

Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:
– KTda viruslarni topish;
– virus – dasturlar ishini blokirovka qilish;
– viruslar ta’sirining oqibatlarini bartaraf qilish.

Viruslarni topishni, ularni joylashib olish bosqichida yoki hech bo‘lmaganda virusning buzg‘unchilik funksiyalarini boshlagunga qadar amalga oshirgan maqsadga muvofiq. Shuni ta’kidlash joizki, barcha turdagi viruslarni topishni kafolatlovchi antivirus vositalar mavjud emas. Virus topilgan holatda, uning tizimga keltirishi mumkin bo‘lgan zararli ta’sirini minimallashtirish maqsadida darhol virus-dasturning ishini to‘xtatilish lozim. Virusning ta’sir oqibatlarini bartaraf qilish ikki yo‘nalishda olib boriladi:
– virusni o‘chirish;
– fayllarni, xotira sohalarini tiklash.

KTning xavfsiz ishlashining asosiy shartlaridan biri, amalda sinovdan o‘tkazilgan va o‘zining yuqori samara berishini ko‘rsatgan bir qator qoidalarga1 rioya qilish hisoblanadi.

Birinchi qoida–qonuniy rasmiy yo‘l bilan olingan dasturiy mahsulotlardan foydalanish. Dasturiy ta’minotning qaroqchilik yo‘li bilan ko‘paytirilgan nusxalarida, rasmiy yo‘l bilan olinganlariga nisbatan viruslarning mavjudlik ehtimoli juda yuqori.

Ikkinchi qoida–axborotlar zaxirasini hosil qilish. Avvalo dasturiy ta’minotning distributivlari yozilgan tashuvchilarni saqlash zarur. Bunda tashuvchilarga ma’lumotlarni yozish imkoni berilgan bo‘lsa, imkon qadar uni blokirovka qilish zarur. Ishga taalluqli ma’lumotlarni saqlanishiga jiddiy yondashishi zarur. Muntazam ishga taalluqli fayllarning zaxira nusxalarini yaratib borish va ularni yozishdan himoyalangan yechib olinuvchi tashuvchilarda saqlash kerak. Agar bunday nusxalar yechib olinmaydigan tashuvchilarda yaratilayotgan bo‘lsa, ularni butunlay boshqa kompyuterning doimiy xotirasida yaratish maqsadga muvofiq. Bunda yoki faylning to‘liq nusxasi yoki kiritilayotgan o‘zgarishlarning nusxalari saqlanadi.

Uchinchi qoida– antivirus vositalaridan muntazam foydalanish. Antivirus vositalari muntazam yangilanib turilishi lozim.

To‘rtinchi qoida–yangi yechib olinadigan axborot tashuvchilardan va yangi fayllardan foydalanilganda ehtiyotkorlikka rioya qilish. Yangi yechib olinadigan tashuvchilar olinganda, albatta, yuklanuvchi va fayl viruslari mavjudligiga, olingan fayllar esa fayl viruslari mavjudligiga tekshirilishi lozim. Tekshiruv, skanerlovchi–dasturlar va evristik tahlilni amalga oshiruvchi dasturlar yordamida amalga oshirilishi kerak. Olingan hujjatlar va jadvallar bilan ishlashda, ushbu fayllar to‘liq tekshirilgunga qadar, matn va jadval muharrirlariga o‘rnatilgan makrokomandalarning bajarilishini taqiqlash zarur.

Beshinchi qoida–tizimga, ayniqsa taqsimlangan tizimlarga yoki jamoa bo‘lib foydalaniladigan tizimlarga, kiritilayotgan fayllarni va yechiladigan axborot tashuvchilarni maxsus ajratilgan kompyuterlarda tekshirish. Uni tizim administratori yoki ma’lumotlar xavfsizligiga mas’ul bo‘lgan shaxsning avtomatlashtirilgan ish joyidan amalga oshirilishi maqsadga muvofiq. Disk va fayllarni har tomonlama antivirus tekshiruvidan o‘tkaziluvidan so‘ng ularni tizimdan foydalanuvchilarga taqdim etish mumkin.

Oltinchi qoida–agar axborotlarni tashuvchilarga yozish nazarda tutilmagan bo‘lsa, bunday amallarni bajarilishini blokirovka qilish. Yuqorida keltirilgan tavsiyalarga doimiy rioya qilinishi virus dasturlar bilan zararlanish ehtimolini ancha kamaytiradi va foydalanuvchini axborotlarni qaytib tiklab bo‘lmaydigan yo‘qotishlardan saqlaydi. KTdan foydalanish bosqichlarida tizimdagi axborotlarning butunligi va ulardan foydalanish huquqi quyidagilar orqali ta’minlanadi:

– KTda mavjud axborotlarning butunligi;
– KTning rad etishga barqarorligini oshirish;
– tizimning qayta yuklanishi va “osilib qolishi”ni bartaraf etish;
– axborot zaxiralarini yaratish;
– qat’iy belgilangan dasturlar majmuidan foydalanish;
– texnik xizmat ko‘rsatish va kam-ko‘stini to‘ldirish jarayonlarining o‘ziga xos tartibiga rioya qilish;
– antivirus tadbirlari kompleksini o‘tkazish.

KTda axborotlarning butunligi va foydalanishga qulayligini ta’minlashning asosiy shartlaridan biri ularning zaxiralarini hosil qilishdan iborat. Axborotlar zaxirasini yaratish strategiyasi axborotning muhimligini, KTning uzluksiz ishlashiga bo‘lgan talablarni, ma’lumotlarni tiklashdagi qiyinchiliklarni hisobga olgan holda tanlanadi. Himoyalangan KTda faqatgina ruxsat etilgan dasturiy ta’minotdan foydalanilishi lozim. Foydalanishiga rasman ruxsat etilgan asturlarning ro‘yxati, ularning butunligini nazorat qilishning usullari va davriyligi KTni ekspluatatsiya qilinishidan oldin aniqlanishi kerak. Dasturlar butunligini nazorat qilishning sodda usullaridan biri nazorat yig‘indilari usuli hisoblanadi.

Nazorat yig‘indisi–ma’lumotlar blokining oxiriga yoziladigan bitlar ketma-ketligi. Nazoratdagi faylga kiritilgan o‘zgartirishni, nazorat yig‘indini tuzatib qo‘yish bilan, berkitishni istisno qilish maqsadida nazorat yig‘indini

shifrlangan holda saqlash yoki nazorat yig'indini hisoblashning maxfiy algoritmidan foydalanish zarur. Axborot butunligini nazorat qilishning ko'proq maqbul bo'lgan metodlarida bir xesh-funksiyadan foydalanish hisoblanadi. Xesh funksiyaning qiymatini uning kalitini bilmasdan turib qalbakilashtirib bo'lmaydi, shu sababli xeshlash kalitini shifrlangan ko'rinishda yoki jinoyatchining "qo'li yetmaydigan" joydagi xotirada saqlash kerak. Axborot xavfsizligini ta'minlashning dasturiy va apparat-dasturiy vositalardan foydalanishga qo'yiladigan asosiy talablar.

Xavfsizlik modelini to'g'ri tanlash OT mutaxassislarinigina emas, xavfsizlik bo'yicha mutaxassislarning asosiy vazifasi hisoblanadi. Hozirda mavjud standartlar modellarning majburiy ro'yxatini faqat ikki model, ya'ni foydanish huquqini boshqarishning diskret va mandatli turlari bilan cheklaydi. Ko'p hollarda ushbu ikki modelning qo'llanilishi yetarli hisoblanadi.

OTda axborot xavfsizligini samarali ta'minlash uchun quyidagi tavsiyalarni bajarish lozim:

1. Xavfsizlik modelini to'g'ri joriy etish.

2.Obiektlar va subyektlarning ishonchli identifikatsiyalash va autentifikatsiyalashdan o'tkazish. Ushbu muammo texnik xarakterga ega.

Hozirda, ishonchli identifikatsiyalashni va berilgan aniqlikda autentifiksiyalashni ta'minlashlaydigan tizimlar mavjud. Identifikatsiyalashning ishonchliligi foydalanilayotgan belgilarning noyobligi (unikalligi) bilan, autentifikatsiyalashniki esa–qalbakilashtirishning qiyinligi bilan ta'minlanadi.

Foydalanuvchilarni identifikatsiyalash va autentifikatsiyalashni ishonchli algoritmlarini qo'llash uchun maxsus apparat vositalar–magnit kartalar, foydalanuvchining fiziologik kattaliklari (barmoq izlari, ko'z to'r pardasi va hokazo)ni o'quvchi qurilmalar zarur. Ushbu usullarni dasturiy jihatdan ixtiyoriy mavjud tizimlarga joriy etish mumkin. Subyektlar va obiektlarning dasturiy (inson ishtirokisiz) identifikatsiyalash va autenfikatsiyalash uchun keyingi paytlar keng qo'llanilayotgan elektron imzodan foydalanilmoqda.

Identifikatsiyalash va autenfikatsiyalashning muayyan bir mexanizmi, qurilmasi va vositasini tanlash muayyan tizimga qo'yiladigan talablardan kelib chiqadi va axborot xavfsizligini ta'minlashda qo'llanilayotgan boshqa qarorlarga bog'liq bo'lmagan holda amalga oshirilishi mumkin.

3. Xavfsizlikni ta'minlash tizimini dasturiy amalga oshirishdagi xatoliklarni kamaytirish yoki to'liq bartaraf etilishiga erishish. Boshqa dasturiy ta'minotlar singari himoyalashning usul va vositalari ham joriy etish xatoliklaridan holi emas. Himoya tizimining ixtiyoriy tashkil etuvchisidagi biror xatolik butun tizimning xavfsizligini shubha ostida qoldirishi tabiiydir. Shu sababli xavfsizlikka javobgar bo'lgan dasturiy ta'minotdagi xatoliklar nafaqat o'z vazifani bajara olmay qoladi, balki butun tizimni izdan chiqaradi. Ushbu muammoni hal etilishiga qaratilgan chora-tadbirlar dasturlash texnologiyasi va OTning ishonchlik sohasiga taalluqli bo'ladi.

4. Xavfsizlikni ta'minlash vositalarining butunligini tegishli nazoratini tashkil etish. Ushbu muammo sof texnologik xarakterga ega bo'lib, hozirda butunlikni nazorat qilish usullari yetarlicha rivojlangan va ushbu masalaning ishonchli

yechimlari topilgan (masalan, elektron raqamli imzo orqali). Ammo, amaliyotda, odatda ushbu metodlar faqatgina ma’lumotlar butunligini nazorat qilish uchungina (masalan, aloqa kanali orqali ma’lumotlarni uzatishda) qo‘llaniladi. Ushbu muammoni hal etish uchun birinchi navbatda, xavfsizlikni ta’minlovchi mexanizmlar butunligini nazorat qilish lozim.

5. Dasturiy va qurilmaviy mahsulotlarni ishlab chiqishning yakuniy bosqichida sozlash va testdan o‘tkazish vositalarini mavjudligini ta’minlash. Ushbu muammoni hal etilishi uchun tashkiliy tadbirlardan foydalanish mumkin. Xavfsizlik hal qiluvchi ahamiyatga ega bo‘lgan barcha tizimlar, o‘zida shunga o‘xshash imkoniyatlar mavjud emasligini tasdiqlovchi sertifikatlarga ega bo‘lishi lozim. Tabiiyki, ushbu talabni bajarilishi uchun to‘liq javobgarlikni ishlab chiqaruvchi o‘z zimmasiga oladi.

6. Administratsiyalashdagi xatoliklarni minimumga keltirish. Ushbu muammo inson faktori bilan bog‘liqligi sababli sof texnik vositalar yordamida hal etila olmaydi. Shu kabi xatoliklarni vujudga kelish ehtimolligini kamaytirish uchun xavfsizlikni boshqarish va foydalanishga ruxsat berishni nazorat qilish vositalarini qulay va ishlashga oson bo‘lgan interfeys bilan ta’minlash lozim hamda imkoniyatga qarab boshqaruvning avtomatlashtirilgan tizimidan foydalangan ma’qul. Bundan tashqari, hisoblash tizimi konfiguratsiyasini administrasiyalashning adekvat emasligini tekshiradigan tarifikatsiyalovchi vositalarning qo‘llanilishi ham nazarda tutilishi mumkin. Ma’lumotlarni bazasini boshqarish tizimi (MBBT)da ma’lumotlarni qayta ishlash jarayonini himoyalash.

Ma’lumotlar bazasida ma’lumotlarni qayta ishlash jarayonini himoyalash vositalarini yaratishda, ushbu vositalarning nafaqat OT bilan, balki MBBT bilan birgalikda ishlay olishini hisobga olish kerak. Zamonaviy ma’lumotlar bazasida ma’lumotlardan foydalanishga ruxsat berishni cheklash, ma’lumotlarning fizik butunligini va mantiqiy saqlanganlik masalasi yetarli darajada muvaffaqiyatli hal etilgan. Hozirda foydalanuvchi tomonidan ma’lumotlar bazasi yozuvlaridan va yozuv maydonlaridan foydalanishga ruxsatni cheklash algoritmlaridan unumli foydalanilmoqda, ushbu himoyani jinoyatchi zararlovchi dasturlarni joriy etish yoki foydalanuvchi huquqlarini qalbakilashtirish yordamida yengib o‘tishi mumkin. Ma’lumotlar bazasi faylidan va bazaning qismlaridan foydalanishga ruxsat berish MBBT tomonidan, foydalanuvchining huquqlarini belgilab berish va ruxsat berilishi kerak bo‘lgan obiektlardan foydalanishga ruxsat berish huquqlarini nazorat qilish yo‘li bilan amalga oshiriladi. Foydalanuvchi huquqlari MBBT administratori tomonidan belgilanadi. Odatda, foydalanuvchining standart identifikatori bo‘lib, shifrlangan ko‘rinishda uzatiladigan parol hisoblanadi. Taqsimlangan KTda foydalanuvchining haqiqiyligini tasdiqlash jarayoni, masofaviy jarayonlarni o‘zaro autentifikatsiyalash kabi maxsus protsedura bilan to‘ldiriladi.

Zamonafiy kompyter stenografiyasi.

Tarmoq texnologiyasining keng ko‘lamda qo‘llanishi natijasida umumiy resurslardan foydalanish imkonini beruvchi lokal tarmoqqa kompyuterlar

birlashtirildi. Kliyent-server texnologiyasining tatbiq etilishi esa bu tarmoqni taqsimlangan hisoblash muhitiga aylantirdi. Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlanadi. Buzg‘unchi tarmoqning biror-bir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin. Zamonaviy telekommunikatsiya texnologiyalari lokal tarmoqlarni global tarmoqqa – Internetga ulash imkonini berdi. Internetning rivojlanishi xavfsizlikni ta’minlashni dolzarb masalaga aylantirdi va Internetga ulangan tarmoq va tizimlarda, qanday ma’lumotlarga ishlov berilishidan qat’iy nazar, xavfsizlik vositalari bo‘lishini taqozo etadi. Chunki, Internetning imkoniyatlaridan foydalanib, buzg‘unchi xavfsizlikni buzishni global masshtabda olib borishi mumkin. Internetga ulangan kompyuter tajovuz obiekti bo‘lsa, hujumni amalga oshirayotgan shaxsga uning qayerda (qo‘shni xonada yoki boshqa kontinentda) joylashgani katta ahamiyatga ega emas. Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun “tarmoqlararo ekran” (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi. Odatda, alohida ajratilgan va himoyalangan KT “tarmoqlararo ekran” orqali hamma foydalanadigan tarmoqqa ulanadi. Tarmoqlararo ekran himoyalangan KTga kelib tushayotgan va undan chiqib ketayotgan axborotlarni nazorat qilish uchun qo‘llaniladi.

Tarmoqlararo ekran quyidagi to‘rtta funksiyani bajaradi:

– ma’lumotlarni filtrlash;
– ekranlovchi agentlardan foydalanish;
– manzillarni translatsiyalash;
– hodisalarni qayd qilish.

Tarmoqlararo ekranning asosiy vazifasi (kirayotgan yoki chiqayotgan) trafikni filtrlashdan iborat. Korporativ tarmoqning himoyalanganlik darajasiga qarab filtrlashning turli qoidalari o‘rnatilishi mumkin. Filtrlash qoidalari filtrlar ketma-ketligini tanlash orqali amalga oshiriladi. Ushbu filtrlar o‘zidan keyingi filtrga yoki protokol sathiga ma’lumotlarni uzatilishiga ruxsat beradi yoki taqiqlaydi.

Tarmoqlararo ekran filtrlashni kanallar, tarmoqlar, transport va amaliy sathlarda amalga oshiradi. Ekran qancha ko‘p sathni o‘z ichiga olsa, shuncha takomillashgan hisoblanadi. Tarmoqlararo ekranda, dasturiy vositachi vazifani bajaruvchi va subyekt va obiekt orasida ulanishni ta’minlovchi, so‘ngra axborotni qayd qilish va nazoratini amalga oshirib jo‘natuvchi, ekranlovchi agentlardan (proxy-serverlar) foydalaniladi. Ekranlovchi agentlarning qo‘shimcha vazifasi foydalanishga ruxsat berilgan subyektdan haqiqiy obiektni yashirishdan iborat. Ekranlovchi agentlarning o‘zaro aloqa ishtirokchilariga ta’siri yo‘q. Tarmoqlararo ekranning manzillarni translatsiyalash funksiyasi haqiqiy ichki manzillarni tashqi abonentlardan yashirish uchun mo‘ljallangan. Bu tarmoq topologiyasini yashirish va agar himoyalangan tarmoq uchun yetarli miqdorda manzillar ajratilmagan bo‘lsa, yanada ko‘proq sondagi manzillardan foydalanishga imkon yaratadi.

Tarmoqlararo ekran maxsus jurnallarda hodisalarni qayd qilib boradi. Biror aniq talab bo‘yicha ekranni sozlash orqali jurnallarni yuritish imkoniyati

nazarda tutilgan. Yozuvlar tahlili o‘rnatilgan qoidalarni buzishga bo‘lgan buzg‘unchilarning urinishlarini qayd qilish va ularni aniqlash imkonini beradi. Ekran simmetrik emas. U “tashqi” va “ichki” tushunchalarini farqlay oladi. Ekran ichki sohani nazoratsiz va adovatli bo‘lgan tashqi muhitdan himoyasini ta’minlab beradi. Shu bilan birga ekran himoyalangan tarmoq subyektlari tomonidan ommaviy tarmoq obiektlaridan foydalanishni cheklashni ham ta’minlaydi. Foydalanishga ruxsat berilgan subyektning vakolatlari buzilgan Tarmoqlararo ekranlarga quyidagi zamonaviy talablar qo‘yiladi:

holatda uning ish faoliyati blokirovka qilinadi va barcha kerakli ma’lumotlar jurnalga yozib qo‘yiladi.

1. Asosiy talablar – bu ichki tarmoqning xavfsizlikni ta’minlash va tashqaridan ulanishlar va aloqa seanslarini to‘liq nazorat qilish.
2. Ekranlovchi tizim tashkilotning xavfsizlik siyosatini oddiy va to‘liq yuritish uchun quvvatli va moslanuvchan boshqarish vositalariga ega bo‘lmog‘i darkor.
3. Tarmoqlararo ekran lokal tarmoq foydalanuvchilariga sezdirmasdan ishlashi va ular tomonidan ruxsat etilgan amallarni bajarishlariga xalaqit bermasligi lozim.
4. Tarmoqlararo ekran ko‘p miqdordagi murojaatlar bilan blokirovka qilib qo‘yishni va ishdan chiqishining oldini olish uchun, uning protsessori tez ishlay olish, pik rejimlarida kiruvchi va chiquvchi oqimlarni yetarli darajada samarali qayta ishlay olishga ulgurishi lozim.
5. Xavfsizlikni ta’minlash tizimi har qanday tashqi noqonuniy ta’sirlardan himoyalangan bo‘lishi lozim, chunki bu ta’sirlar tashkilotning konfedensial ma’lumotlarini ochish kaliti bo‘lishi mumkin.
6. Ekranni boshqaruv tizimi olisdagi filiallar uchun ham yagona xavfsizlik siyosatini yuritishni markazlashgan holda ta’minlash imkoniyatiga ega bo‘lmog‘i lozim.
7. Tarmoqlararo ekran foydalanuvchilarning tashqi ulanishlari orqali foydalanishga ruxsat berishning ualliflashtirish vositalariga ega bo‘lmog‘i kerak. Bu tashkilot xodimlarini xizmat safarida ham tarmoqdan foydalanishlariga imkon yaratadi.

Mustaqil uchun savollar

1. Axborotlarni muhofaza qilishning asosiy va yordamchi apparat vositalariga nimalar kiradi?
2. Axborotlarni muhofaza qilishning dasturiy vositalari qanday dasturlardan iborat?
3. Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklari va kamchiliklari nimalardan iborat?

Nazorat uchun savollar:

1. Ximoyaning buzilishlariga sabab bo‘luvchi xujumlar qanday klassifikatsiyalanadi?
2. Passiv taxdidga qanday xujumlar taalluqli?
3. Aktiv taxdidga qanday xujumlar taalluqli?

II BOB. AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH.

2.1. Axborotlarni kriptografik himoyalash tamoillari.

Tayanch tushuncha va iboralar: Ochiq tekst, shifr tekst, autentifikatsiya, butunlik, inkor qilmaslik, simmetrik shifrlashtirish, ochiq kalitli shifrlashtirish, kriptotizim, kriptotaxlilchi, almashtirish va o‘rin almashtirish shifrlari.

Mavzuga oid asosiy muammolar: Kriptografiya tushunchi va kriptografiyaning maqsad va vazifalari, kriptografiya himoyalash. Axborotlarni kriptografik himoyalash usullari va axborotlarni kriptografik himoyalash tamoillari.

Darsning maqsadi: Kriptografiya axborotni himoyalash vositasi, axborot xavfsizligini ta’minlashning afzalliklari haqida ma’lumot berish.

Insoniyat axborotni himoya qilish muammosi bilan yozuv paydo bo‘lgandan beri shug‘ullanadi. Bu muammo harbiy va diplomatik ma’lumotlarni yashirincha uzatish zaruratidan kelib chiqqan. Masalan, antik spartalilar harbiy ma’lumotlarni shifrlashgan. Xitoyliklar tomonidan oddiy yozuvni iyerogriflar ko‘rinishida tasvirlashlari uni xorijiylardan yashirish imkonini bergan.

“Kriptografiya” atamasi grek tilidan tarjima qilinganda “yashirish, yozuvni berkitib qo‘ymoq” ma’nosini bildiradi. Atamaning ma’nosi kriptografiya kerakli ma’lumotni yashirin saqlash va himoyalash maqsadida qo‘llanishini anglatadi. Kriptografiya axborotni himoyalash vositasi, shuning uchun u axborot xavfsizligini ta’minlashning bir tarmog‘i hisoblanadi.

Kriptologiyaning (kripto–yashirin, logiya–fan, bilim) rivojlanishini uchta bosqichga ajratish mumkin. Birinchi bosqich– kriptologiyani fan sifatidan e’tirof etilmagan davri, tor doiradagi qiziquvchilarga xos faoliyat turi bo‘lgan. Ikkinchi bosqich 1949-yildan boshlanib, K.Shenonning “Maxfiy tizimlarda aloqa nazariyasi” nomli risolaning chop etilishi bilan bog‘lanadi. Bu risolada shifrlashning fundamental ilmiy tadqiqoti va uning mustahkamligi yoritib berilgan. Bu kitobning chop etilishi kriptologiya amaliy matematikaning tarkibiy qismi sifatida shakllanishiga asos bo‘ldi. Va, nihoyat 3-bosqich 1976-yilda U.Diffi va M.Xellman tomonidan «Kriptografiyaning yangi yo‘nalishlari» nomli asarning chop etilishi bilan belgilanadi. Unda maxfiy aloqa, yopiq kalitni avvaldan bermasdan ham, amalga oshirish mumkinligi bayon etilgan. Ushbu sanadan boshlab to hozirgi kungacha an’anaviy klassik kriptografiya bilan bir qatorda ochiq kalitli kriptografiyaning intensiv rivojlanishi davom etmoqda. Bir necha asrlar davomida yozuvning paydo bo‘lishini o‘zi axborotni himoyalash sifatida e’tirof etilar edi, chunki yozuvni hamma ham tushunmas edi.

Eramizdan oldingi XX asr. Mesopatamiyada o‘tkazilgan qazilmalar vaqtida eng qadimiy shifrlangan matnlar topilgan. Loydan yasalgan taxtachaga qoziqchalar bilan yozilgan matn hunarmandlarning sopol buyumlarini qoplash uchun tayyorlanadigan bo‘yoqning retsepti bo‘lib, u tijorat siri hisoblangan. Qadimgi misrliklarning diniy yozuvlari va tibbiyot retseptlari ham ma’lum.

Eramizdan oldingi IX asrning o‘rtalari. Plutarx bergan ma’lumotlariga ko‘ra, ana shu davrda shifrlovchi qurilma–skital, qo‘llanilgan bo‘lib, u o‘rin almashtirishlar orqali matnni shifrlash imkonini bergan. Matnni shifrlashda

so‘zlar biror diametrli silindrga (skitalga) o‘ralgan ensiz lentaga yozilgan. Lenta yoyilganda unda ochiq matn harflarining o‘rinlari almashtirilgan holati hosil bo‘lgan. Bunda kalit sifatida silindrning diametri xizmat qilgan. Bunday matnni shifrdan yechish usulini Aristotel taklif etgan. U lentani konusga o‘ragan va o‘qilishi mumkin bo‘lgan so‘z yoki so‘zning bir qismini ko‘rsatuvchi joy silindrning diametri deb hisoblagan.

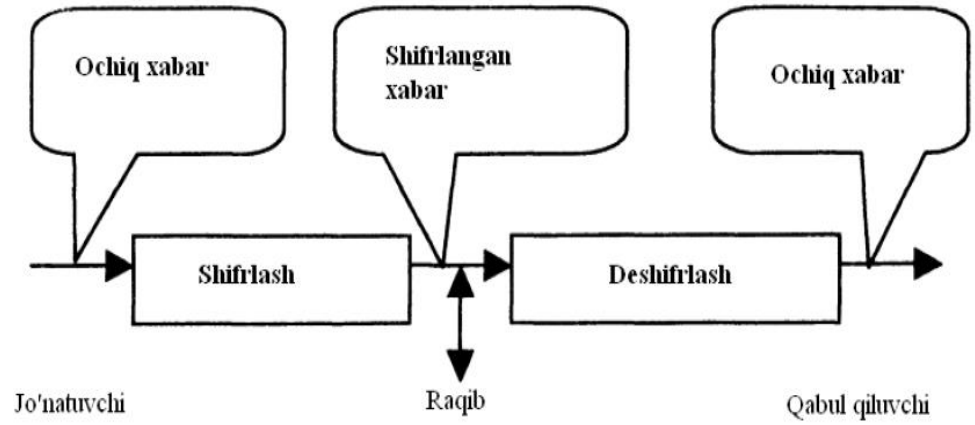
Eramizning 56-yili. Y.Sezar gallar bilan urush vaqtida shirflashning almashtirish turini qo‘llagan. Ochiq matn alfaviti ostiga sikl bo‘yicha (Sezarda uchta pozitsiyaga) siljitish orqali shu alfavit yozilgan. Shifrlashda ochiq matndagi alfavitlar, ya’ni yuqori qismda joylashgan harflar quyi qismdagi mos harflar bilan almashtirilgan. Bu turdagi shifrlash Y.Sezargacha ma’lum bo‘lgan bo‘lsada, lekin bunday shifrlash usuli uning nomi bilan yuritiladi.

Germaniyalik Iogann Tritemiy (1462–1516) kriptografiya bo‘yicha birinchi darsliklardan birini yozgan. “Ave Maria” deb nomlangan ko‘p qiymatli almashtirishli original shifrlashni taklif etgan. Ochiq matnning har bir harfi shifrlovchining tanlovi bo‘yicha bir emas, bir nechta harflarga almashtirilishi mumkin bo‘lgan. Bunda harflar harf yoki so‘zlar bilan shunday almashtirilganki, natijada psevdomatn hosil bo‘lgan. ko‘p qiymatli almashtirish usulidan hozirgi kunda ham foydalaniladi (masalan, ARJ arxivatorida). Italiyalik matematik, mexanik, vrach Djirolamo Kardano (1506–1576) Kardano panjarasi deb nomlangan shifrlash tizimini ixtiro qilgan. Ikkinchi jahon urushi vaqtida Buyuk Britaniya harbiy-dengiz qo‘shinlarining mustahkam shifrlaridan biri shu tizim asosida yaratilgan. Panjaralar chizilgan karton bo‘lagida ixtiyoriy tartibda nomerlangan teshikchalar qilingan. Shifrlangan matnni hosil qilish uchun, karton bo‘lagini qog‘ozni ustiga qo‘yib, kartonning teshiklari bo‘lgan joylariga tanlangan tartibda harflar yozib chiqilgan. Karton olib tashlangandan so‘ng, yozilgan harflarning oralari psevdomazmunli jumlalar bilan to‘ldirilgan, shu orqali shifrlangan xabar yaratilgan. Agar harflar orasidagi masofalar katta bo‘lib, so‘zlar uzunligi kichik bo‘lsa (masalan ingliz tilidagi so‘zlar), yashirish oson amalga oshirilgan. XVI asr. Almashtirish shifrlari matematik Djovanni Batista Port va diplomat Bleza de Vijiner ishlarida o‘z rivojini topdi. Vijiner tizimi u yoki bu ko‘rinishda hozirgi paytda ham qo‘llanilmoqda.

XVII asr. Fransiya qiroli Lyudovik XIII huzuridagi vazir kardinal Rishelye dunyoda birinchi bo‘lib shifrlash xizmatini tashkil etgan. Lord Frensis Bekon (1562–1626) birinchi bo‘lib harflarni 5 qiymatli ikkilik kod bilan belgilagan: A= 00001, V =00010, .. va hokazo. Bekon bu kodlarga qayta ishlov bermagan, shuning uchun bunday yashirish usuli mustahkam bo‘lmagan. Uch asrdan so‘ng, bu kodlash tamoyili elektr va elektron aloqada asos qilib olindi. Bunda Morze va Bodo kodlarini, 2-sonli xalqaro telegraf kodini, ASCII kodini, eslash ham o‘rinli, chunki ular ham oddiy almashtirish asosida yaratilgan. XVII asrda lug‘atli shifrlar ixtiro etilgan. Shifrlashda ochiq matn harflari ikkita son bilan belgilangan. Bunda keng tarqalgan kitoblardan biri olinib, shifrlanuvchi harf kitobning ma’lum betidagi qator nomeri va harf nomeriga almashtirilgan. Bu tizim mustahkam shifrlash usuli hisoblanadi, lekin undan foydalanish qulay emas. Shu bilan birga, kitob raqib qo‘liga tushib qolishi ehtimolidan holi emas.

Zamonaviy kriptografiya axborot xavfsizligining konfedensiallik, butunlik, autentifikatsiya va tomonlarning mualliflikni inkor etolmasliklari muammolarini hal etuvchi bilim sohasi hisoblanadi.

Konfedensiallikni ta’minlash deganda axborot bilan tanishish huquqi bo‘lmagan shaxslardan bu axborotni himoyalash tushuniladi.



Raqib tomonidan nazoratda bo‘lgan aloqa kanali orqali uzatiladigan xabarning konfedensialligini ta’minlash muammosi kriptografiyaning an’anaviy masalalaridan hisoblanadi. Oddiy holda bu muammo uchta subyekt (tomonlar)ning o‘zaro munosabati sifatida bayon etiladi. Axborot egasi (jo‘natuvchi), raqibdan himoya qilish maqsadida, ochiq kanal orqali qabul qiluvchiga yuborilayotgan ochiq ma’lumotni o‘zgartiradi, ya’ni shifrlaydi. Uzatilayotgan xabar ma’nosi bilan tanishish huquqi yo‘q subyekt raqibni anglatadi. Deshifrlash bilan shug‘ullanuvchi kriptotahlilchi ham raqib sifatida qaralishi mumkin. Olingan xabarni haqiqiy qabul qiluvchi deshifrlaydi. Raqib esa himoyalangan xabarga egalik qilmoqchi bo‘ladi, uning harakati hujum hisoblanadi. Hujum faol yoki sust bo‘lishi mumkin. Sust hujum yashirin eshitish, trafikni tahlil qilish, shifrlangan xabarni qo‘lga kiritish, deshifrovka qilish, ya’ni himoyani “sindirish”ga qaratilgan harakatlar hisoblanadi. Faol hujumda raqib xabarni uzatish jarayonini to‘xtatib qo‘yishi, qalbaki xabarlar yuborishi yoki shifrlab uzatilayotgan xabarni modifikatsiya qilishi mumkin. Bu faol harakatlar mos ravishda imitatsiya qilishga va almashtirib qo‘yishga urinish hisoblanadi.

Kalit shifrlashning asosiy elementi bo‘lib, berilgan xabarni shifrlashdagi almashtirishlar u orqali amalga oshiriladi. Odatda, kalit harf va sonlarning biror-bir ketma-ketligidan iborat bo‘ladi. Har bir almashtirish kalit bilan bir qiymatli aniqlanadi va biror kriptografik algoritm orqali amalga oshiriladi. Shifrlashda bir kriptografik algoritm har xil rejimlarda qo‘llanishi mumkin. Shu tarzda har xil shifrlash usullari (oddiy almashtirish, gammalash va boshqalar) amalga oshiriladi. Har bir rejimning afzallik va kamchilik tomonlari mavjud. Shuning uchun rejimni tanlash konkret holatga bog‘liq. Deshifrlashdagi kriptografik algoritm, umumiy holda, shifrlashdagi algoritmdan farq qilishi mumkin. Bu holatda shifrlashdagi va deshifrovka qilishdagi kalitlar ham mos tushmasligi mumkin. Shifrlovchi va deshifrovka qiluvchi algoritmlar juftligini kriptotizim, bu algoritmlarni amalga oshiruvchi qurilmani shifrovchi texnika deyiladi. Himoyalanadigan axborot turli-tuman shakllarga (matnli, tovushli, rasmli va

boshqalar) ega bo‘lishi mumkin. Har bir shaklning o‘ziga xos xususiyatlari mavjud bo‘lib, shifrlash usulini tanlashda uni inobatga olish kerak. Shifrlangan axborotning hajmi, uni talab etilgan tezlikda uzatish hamda aloqa kanalining har xil xalaqit beruvchi shovqinlardan himoyalanganligi katta ahamiyatga ega. Bularning barchasi kriptografik algoritmni tanlashda va himoyalangan aloqani tashkil etishda muhim rol o‘ynaydi. Butunlikni ta’minlash deganda axborotni ruxsatsiz o‘zgartirib bo‘lmasligining kafolati tushuniladi. Butunlikni kafolatlash uchun ma’lumotlar bo‘yicha biron-bir o‘zgartirishlarni amalga oshirishni aniqlaydigan sodda va ishonchli mezon bo‘lishi kerak. Bu o‘zgartirishlar matnni o‘chirish, almashtirish, yangisini qo‘yish orqali amalga oshirilishi mumkin.

Kriptotahlil kriptografiyaga teskari bo‘lib, unda kalitni bilmasdan turib axborotni deshifrlash amalga oshiriladi.

Kriptografiya himoyalash. Axborotlarni kriptografik himoyalash usullari.

An’anaviy (klassik) shifrlash usullariga o‘rinlarini almashtirish shifrlari, oddiy va murakkab almashtirish shifrlari va ularning kombinatsiyalari va modifikatsiyalari kiradi. Ta’kidlash joizki, o‘rinlarini almashtirish shifrlari va almashtirish shifrlarining kombinatsiyalari amaliyotda qo‘llanilayotgan har xil turdagi simmetrik shifrlarni tashkil etadi.

O‘rinlarini almashtirish shifrlarida shifrlanadigan matnning harflari shu matn bloki ichida ma’lum qoidalar bo‘yicha o‘rin almashtiriladi. O‘rinlarini almashtirish shifrlari eng sodda va eng qadimiy hisoblanadi.

Shifrlovchi jadvallar. Tiklanish (XIV asr oxirlari) davrining boshlarida o‘rinlarini almashtirish shifrlarida shifrlovchi jadvallardan foydalanilgan. Shifrlovchi jadvallarning kaliti sifatida: jadvalning o‘lchami; o‘rin almashtirishni belgilovchi so‘z yoki jumla; jadval tuzilishining xususiyati bo‘lgan. Kalit sifatida jadvalning o‘lchami berilishi eng sodda jadvalli shifrlash hisoblanadi. Quyidagi matn berilgan bo‘lsin:

OBIEKT BELGILANGAN JOYGA BORADI

Ushbu axborot ustun bo‘yicha ketma – ket jadvalga kiritiladi:

O	K	L	A	N	G	R
B	T	G	N	J	A	A
Y	B	I	G	O	B	D
E	E	L	A	Y	O	I

Natijada, 4x7 o‘lchovli jadval tashkil qilinadi.

Endi shifrlangan matn qatorlar bo‘yicha aniqlanadi, ya’ni o‘zimiz uchun 4 tadan belgilarni ajratib yozamiz.

OKLA NGRB TGNJ AAYB IGOB DEEL AYOI

Bu yerda kalit sifatida jadval o‘lchovlari xizmat qiladi. Tabiiyki, uzatuvchi va qabul qiluvchi kalit jadval o‘lchami bo‘lishligini o‘zaro kelishib olishlari kerak. Deshifrlashda teskari amal bajariladi. Endi, kalit bo‘yicha oddiy o‘rnini almashtirish shifrini Ko‘rib chiqaylik. Bu usul oldingisiga nisbatan deshifrovka

qilish uchun ancha murakkabdir. Bu usulda jadval ustunlari kalit bo‘luvchi so‘z, ibora, jumla orqali o‘rin almashtiriladi.

Misol tariqasida UCHRASHUV INDINGA XIVA KINOTEATRIDA matnini TEGIRMON so‘zini kalit sifatida qabul qilib, O‘rnini almashtirish shifrini qo‘lla b shifrlaylik. Matnda 32 ta va kalitda 8 ta harflar borligi uchun 8x4 jadval tuzamiz.

U	A	V	I	X	K	T	R
C	S	I	N	I	I	E	I
H	H	N	G	V	N	A	D
R	U	D	A	A	O	T	A

Endi kalit orqali 8x6 jadval tuzib kalitdagi harflarni alfavit bo‘yicha raqamlab chiqamiz.

T	e	g	i	r	m	o	n
8	2	1	3	7	4	6	5

U	A	V	I	X	K	T	R
C	S	I	N	I	I	E	I
H	H	N	G	V	N	A	D
R	U	D	A	A	O	T	A

Raqam bo‘yicha ustunlar o‘zgartiriladi.

g	e	i	m	n	o	r	T
1	2	3	4	5	6	7	8
V	A	I	K	R	T	X	U
I	S	N	I	I	E	I	C
N	H	G	N	D	A	V	H
D	U	A	O	A	T	A	R

Qator bo‘yicha 4 tadan bloklarga bo‘lib, simvollar ketma-ketligidagi shifrlangan matnni olamiz. Shuni e’tiborga olish kerakki, agar qatorda ketma-ket ikkita bir xil harf kelsa, chap tarafdan kelayotgan harf birinchi raqamlanadi, keyin esa ikkinchisi raqamlanadi va shifrlangan matn hosil qilinadi. Natijada quyidagi shifrlangan matn hosil bo‘ladi:

VAIK RTXU ISNI IEIC NHGN DAVN DUAO ATAR

Shifrni ochishda teskari jarayon amalga oshiriladi. Shifrlangan matnning ochilishini yanada murakkablashtirish uchun u qaytadan shifrlanishi mumkin. Bu usul ikki tomonlama o‘rin almashtirish shifri deyiladi. Bu usulda kalit sifatida ustun va qatordagi harflar tartibidagi sonlardan foydalaniladi. Avvalam bor kalit simvollariga qarab jadval tuziladi va ochiq matn joylashtirilib chiqiladi. so‘ngra raqamlar navbatma-navbat tartiblanib, avval ustun, keyin qatorlar o‘rni almashtiriladi va jadvaldagi ma’lumot qator bo‘yicha o‘qilib, shifrlangan matnga ega bo‘linadi.

Masalan: «OBIEKT BUGUN KASAL» ochiq matni shifrlash talab etilsin. Bu yerda kalit bo‘lib 1342 va 2341 xizmat qiladi.

4x4 jadval yaratib, ochiq matn qator bo‘yicha yoziladi:

	2	3	4	1
1	O	B	Y	E
3	K	T	B	U
4	G	U	N	K
2	A	S	A	L

K_1

Endi qator va ustunlar tartib bo‘yicha o‘rinlari almashtiriladi.

	2	3	4	1
1	O	B	Y	E
2	A	S	A	L
3	K	T	B	U
4	G	U	N	K

	1	2	3	4
1	E	O	B	Y
2	L	A	S	A
3	U	K	T	B
4	K	G	U	N

Oxirgi jadvalga asosan shifrlangan matnni yozamiz va bloklarga bo‘lib chiqamiz.

EOBY LASA UKTB KGUN

Ikki tomonlama almashtirishda jadval kattaligiga qarab variantlar ham ortib boradi. Jadval o‘lchamining kattaligi shifr chidamliligini oshiradi: 3x3 jadvalda 36 ta variant, 4x4 jadvalda 576 ta variant, 5x5 jadvalda 14400 variant.

Sehrli kvadrat deb, katakchalariga 1 dan boshlab natural sonlar yozilgan, undagi har bir ustun, satr va diagonal bo‘yicha sonlar yig‘indisi bitta songa teng bo‘lgan kvadrat shaklidagi jadvalga aytiladi. Sehrli kvadratga sonlar tartibi bo‘yicha belgilar kiritiladi va bu belgilar satrlar bo‘yicha o‘qilganda matn hosil bo‘ladi.

Misol tariqasida 4x4 o‘lchovli sehrli kvadratni olamiz, bunda sonlarning 880 ta har xil kombinatsiyasi mavjud. Kvadratni quyidagicha to‘ldiramiz:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Boshlang‘ich matn sifatida quyidagi **TOVAR OLTIDA KELDI** matnini olamiz va jadvalga joylashtiramiz:

I	V	O	E
R	D	A	T
I	O	L	K
A	D	L	T

Shifrlangan matn jadval elementlarini satrlar bo‘yicha o‘qish natijasida tashkil topadi:

IVOE RDAT IOLK ADLT

O‘rta va katta o‘lchamdagi sehrli kvadratlar yordamida, u davrlarda mustahkam shifrlashni amalga oshirish mumkin bo‘lgan. Chunki deshifrovka qilishda barcha variantlarni qo‘lda amalga oshirib bo‘lmas edi. Oddiy almashtirish orqali shifrlash shifrlanadigan matnning harflari berilgan qoida bo‘yicha shu yoki boshqa alfavitdagi harflarga almashtiriladi. Oddiy almashtirish shifrida berilgan matnning har bir harfi shu alfavitdagi unga mos qo‘yilgan boshqa harfga almashtiriladi. Odatda, bu shifrlash usuli bir alfavitli almashtirish shifri deb ataladi.

Sezarning shifrlash tizimi. Sezarning shifrlash usuli oddiy almashtirish shifrining xususiy holidir. Bu usulda alfavitning har bir harfi K songa surilgan harfga almashtirilgan. Surilish alfavit oxiriga yetganda, uning boshidan boshlangan. Sezar K=3 bo‘lgan siljitishni qo‘llagan. Quyidagi jadvalda bu siljitishdagi lotin grafikasidagi harflarining mosligi keltirilgan:

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

Sezarning “keldim, ko‘rdim, yutdim” mazmundagi xabari VENI VIDI VICI, u taklif etgan usulda shifrlanganda YHQL YLGL YLFL ko‘rinishni oladi. Sezar usulining kamchiligi bu bir xil harflarning o‘z navbatida, bir xil harflarga almashishidir. Kriptotahlilda harflarning takrorlanish chastotasi yordamida bu usulda shifrlangan matn tezgina rasshifrovka qilinishi mumkin. Kalit so‘zli Sezar tizimi. Sezarning kalit so‘zli shifrlash tizimi bitta alfavitli almashtirish tizimi hisoblanadi. Bu usulda kalit so‘zi orqali harflarning surishda va tartibini o‘zgartirishda foydalanadi. Misol tariqasida kalit so‘zi sifatida DIPLOMAT so‘zi va surish 5 ga teng qilib olingan bo‘lsin. Kalit so‘zi alfavit ostiga 5 ta harfga surilgan holda yoziladi:

0	1	2	3	4	5					10					15					20					25
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
					D	**I**	**P**	**L**	**O**	**M**	**A**	**T**													

Alfavitning qolgan alfavit ketma-ketligida kalit so‘zdan keyin yoziladi.

0	1	2	3	4	5					10					15					20					25
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
V	W	X	Y	Z	**D**	**I**	**P**	**L**	**O**	**M**	**A**	**T**	B	C	E	F	G	H	J	K	N	Q	R	S	U

Natijada, berilgan matnning harflariga mos almashtiruvchi harflar aniqlanadi. Agar ochiq matn TOVAR KELDI bo‘lsa, shifrlashdan so‘ng JCNVG MZAYL matniga aylanadi.

Vijinerning shifrlash tizimi. XVI asrda fransuz diplomati Vijiner tomonidan yaratilgan shifrlash tizimi 1586-yilda chop etilgan. U mashhur ko‘p alfavitli tizim hisoblanadi. Vijiner tizimi Sezar shifrlash tizimiga qaraganda mukammalroq hisoblanib, unda kalit harfdan harfga almashtiriladi. Bunday ko‘p alfavitli almashtirish shifrini shifrlash jadvali orqali ifodalash mumkin. Quyidagi jadvallarda rus va lotin alfavitlari uchun mos keluvchi jadvallar ko‘rsatilgan. Bu jadvallardan matnni shifrlash va uni ochish uchun foydalaniladi. Jadvalning ikkita kirishi bo‘lib:

– yuqori qatordagi harflardan kiruvchi ochiq yozuv uchun foydalaniladi.

– chap ustunda esa kalit so‘zi joylashadi.

Ochiq matnni shifrlashda bu matn bir satrga yoziladi. Uning ostidagi satrga kalit so‘z joylashtiriladi. Agar kalit so‘zning uzunligi qisqa bo‘lsa, bu so‘z ochiq matnning oxirgi harfigacha takrorlab yoziladi. Shifrlash jarayonida jadvalning yuqori qismida joylashgan ochiq matnning harfi topiladi va chap qismdan kalit so‘zning harfi tanlanadi. Satr va ustun kesishgan katakdagi harf berilgan harfni almashtiradi.

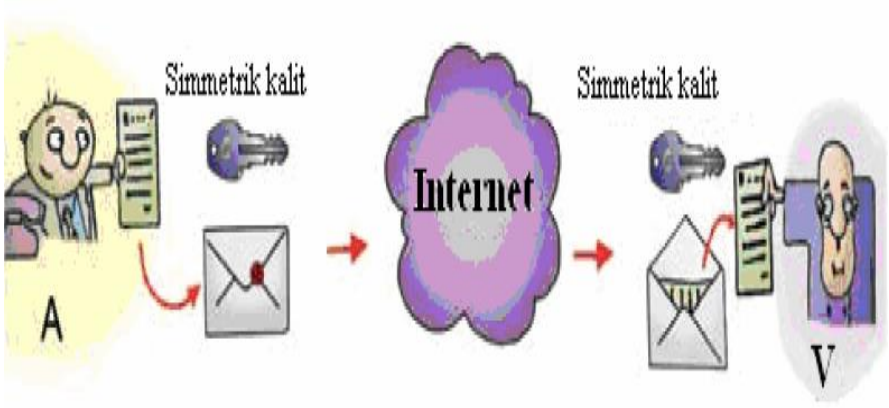
Xabar	B	A	Y	R	A	M	K	U	N	I
Kalit	V	A	Z	A	V	A	Z	A	V	A
Shifrmatn	G	A	R	R	V	M	S	U	P	I

Kalitdan foydalanib shifrlash algoritmining ikki xil ko‘rinishi mavjud: simmetrik va asimmetrik (ochiq kalitli).

Xabarlarni shifrlash uchun foydalanilgan kalit shifrni ochish kalitidan olingan va aksi o‘rinli bo‘lsa, bunday kriptografik algoritmlar simmetrik deb nomlanadi.

Ko‘pgina simmetrik algoritmlarda yagona kalitdan foydalaniladi. Bunday algoritmlar bir kalitli yoki maxfiy kalitli algoritmlar deb ataladi hamda xabarni yuboruvchi va uni qabul qiluvchi qanday kalitdan foydalanishni kelishib olishlarini talab etadi. Bir kalitli algoritmlarning ishonchliligi kalitni tanlash bilan aniqlanadi. Agar jinoyatchiga kalit ma’lum bo‘lsa, hech qanday qarshiliksiz barcha tutib olingan ma’lumotlar shifrini ochish imkoni yaratiladi. Demak tanlangan kalitni begonalardan sir saqlash zarur. Shifrlashning simmetrik algoritmlari ikki turda bo‘ladi. Ulardan biri ochiq matnga bitlar bo‘yicha ishlov beradi. Ular potokli algoritmlar yoki potokli shifrlar deb nomlanadi. Ikkinchisida esa, ochiq matn bir necha bitdan iborat bo‘lgan bloklarga bo‘linadi. Bunday algoritmlar blokli algoritmlar yoki blokli shifrlar deb nomlanadi. Blokli shifrlashning zamonaviy kompyuter algoritmlarida, odatda, blok uzunligi 64 bitni tashkil etadi. Simmetriyali tizimlarda quyidagi ikkita muammo mavjud: 1) Axborot almashuvida ishtirok etuvchilar qanday yo‘l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin? 2) Jo‘natilgan xabarning haqiqiyligini qanday aniqlasa bo‘ladi? Simmetrik kalit bilan shifrlash sxemasini quyidagi misolda ko‘rib chiqamiz. Ali (A) va Vali (V) nomli korrespondentlar bir-biri bilan xabar almashishmoqchi. Korrespondentlarning har biri o‘zining maxfiy kalitiga ega, bu kalitdan xabarni tarmoq orqali yuborishdan avval ma’lumotlarni shifrlashda foydalanishi mumkin. Shifrlash sxemasini ko‘rimliroq tasvirlash uchun, kalitni oddiy kalit, shifrlangan xabarni esa konvertga solingan hujjat ko‘rinishida tasvirlaymiz. Shifrlash va qayta shifrlash jarayoni quyidagi rasmda tasvirlangan. (2.1-rasm. Shifrlash va qayta shifrlash jarayoni)

.



2.1-rasm. Shifrlash va qayta shifrlash jarayoni

Simmetrik kalit yordamida shifrlash tizimi foydalanuvchi A o‘zining maxfiy kaliti bilan xabarni shifrlaydi va xabarni tarmoq orqali jo‘natadi, qabul qiluvchi V (xuddi shunday maxfiy kalitdan foydalanib) xabarni qayta tiklaydi. Rasmda sxemaning simmetrik ekanligi ko‘rinib turibdi. Chap va o‘ng tomondagi foydalanuvchilar bir xil (simmetrik) kalitlardan foydalanishmoqda, shuning uchun bunday turdagi shifrlash simmetrik kalit yordamida shifrlash deb yuritiladi. Maxfiy kalit yordamida shifrlash usuli ma’lum kamchiliklardan holi emas. Birinchi navbatda, simmetrik shifrlash autentifikatsiyalash muammosini hal qilib bermaydi. Masalan, Ali (A) Soli (S)ga xat yozib yuborishi, lekin bu xatni Vali (V) yozgan deb tan olmasligi mumkin. Bundan tashqari, simmetrik kalit xabar yuborilishidan oldin xabar jo‘natuvchi va qabul qiluvchi kompyuterlarda o‘rnatilgan bo‘lishi kerak.

Bu muammoni yechimini topish uchun asimmetrik shifrlash (ochiq (ommaviy) kalit yordamida shifrlash) sxemasi taklif etilgan. Ochiq kalitli shifrlash yoki shifrlashning asimmetrik algoritmlari deb ataluvchi algoritmlarda shifrlash uchun ishlatiladigan kalit shifrni ochish uchun ishlatiladigan kalitdan farq qiladi. Bundan tashqari, shifrlash kalitini bilgan holda, shifrni ochish uchun zarur kalitni juda katta muddat ichida hisoblab topish imkoni bo‘lmaydi. Ixtiyoriy foydalanuvchi shifrlash kaliti yordamida xabarni shifrlashi mumkin, lekin bu kalitga mos shifrni ochish kalitiga ega shaxsgina bu xabarni o‘qiy oladi. Shifrlash kalitini ochiq (ommaviy) kalit, shifrni ochish kalitini esa yopiq (maxfiy, xususiy) kalit deyiladi. Xabarni yopiq yoki ochiq kalit yordamida shifrlash mumkin, qayta tiklash esa ikkinchi kalit yordamida amalga oshiriladi. Ya’ni, yopiq kalit yordamida shifrlangan matn faqat ochiq kalit yordamida qayta tiklanishi mumkin va aksincha. Yopiq kalit faqat egasiga ma’lum, va u hech kimga berilmaydi, ochiq kalit esa ochiq tarqatiladi va u hammaga ma’lum bo‘lishi mumkin. Ikkita kalitni autentifikatsiyalash masalasining yechimini topish uchun hamda konfedensiallikni ta’minlashda qo‘llash mumkin.

Agar birinchi kalit yopiq bo‘lsa, u holda u elektron imzo sifatida ishlatiladi va bu usul bilan axborotni autentifikatsiyalash, ya’ni axborotning butunligini ta’minlash imkoni paydo bo‘ladi. Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

–foydalanuvchini autentifikatsiyalash, ya’ni kompyuter tizimi resurslariga kirmoqchi bo‘lgan foydalanuvchini aniqlash;

–tarmoq abonentlari aloqasini o‘rnatish jarayonida ularni o‘zaro autentifikatsiyalash.

Quyidagi sxemaga muvofiq, foydalanuvchi Ali (A) oldindan ochiq kalitni Vali (V) va Soli (S) nomli korrespondentlarga jo‘natadi, keyin esa yopiq kalit bilan shifrlangan matnni yuboradi.

Xabarni faqat Ali (A) jo‘natishi mumkin (yopiq kalit unga tegishli), bunda autentifikatsiya muammosi yechilgan. Lekin, masalan Vali (V)ning unga yo‘llangan xatni Soli (S) o‘qimaganligiga aniq ishonchi yo‘q. Demak, konfedensiallik ta’minlanmagan. Konfedensiallikni ta’minlash sxemasi quyidagi rasmda tasvirlangan. Xabarni faqat Ali (A) o‘qishi mumkin, chunki u xabarni qayta tiklash imkonini beruvchi yopiq kalitga ega, xabarni konfedensialligi ta’minlangan. Lekin, Ali (A) xabarni Soli (S) ubormaganiga aniq ishonchi yo‘q, chunki u Vali (V) nomidan xabarni yuborishi ham mumkin. Demak, autentifikatsiyalash ta’minlanmagan. Ikkita shaxs orasida xabar almashishda konfedensiallikni ta’minlash uchun ikkita kalit bo‘lishi shart. Juft kalit bilan shifrlashda Ali (A) tomonidan hammaga ochiq kalit jo‘natilishi shart emas. Ochiq kalit tarmoqdagi ochiq foydalanishni imkonini beruvchi serverga joylashtirilishi mumkin.

Simmetrik va asimmetrik kalit yordamida shifrlash. Shuni ta’kidlash lozimki, asimmetrik shifrlash algoritmida ma’lumotlarni shifrlash va qayta tiklash uchun simmetrik shifrlashga qaraganda ko‘p vaqt talab qilinadi, shuning uchun zamonaviy shifrlash tizimlarida asimmetrik shifrlash va an’anaviy simmetrik shifrlashning kombinatsiyalari qo‘llaniladi. Ochiq kalit yordamida shifrlash simmetrik kalitni uzatishda foydalaniladi, bu kalit yordamida uzatiladigan axborot shifrlanadi.

Raqamli sertifikatlar**.** Ochiq kalitli shirflash sxemasidan foydalanganda ochiq kalitni mijozlarga tarqatish yoki tarmoqdagi serverga o‘rnatmoq kerak. Lekin raqib sizning nomingiz bilan o‘zini tanitishi va ochiq kalitni sizning nomingizdan tarqatishi mumkin. Ommaviy kalitni haqiqiy egasi kimligini aniqlash uchun, hamma korrespondentlar ishonch bildiradigan uchinchi tomonga ehtiyoj paydo bo‘ladi. Bu masala sertifikatlashtirish markazlari (Certification Authority) orqali hal etiladi. Ular tomonidan sertifikatlar – egasini identifikatsiyalaydigan ochiq kalit va axborotning mosligini tasdiqlaydigan raqamli ma’lumotlar, kafolatchi imzolagan raqamli imzo beriladi. Sertifikatda ommaviy kalit, kalitning egasi haqidagi ma’lumot, sertifikatlashtirish markazining nomi, sertifikatni amal qilish muddati kabi ma’lumotlar bo‘ladi.

Sertifikatning har bir nusxasiga sertifikat bergan tashkilotning raqamli imzosi biriktiriladi, shuning uchun kim sertifikat olgan bo‘lsa, uning haqiqiyligiga ishonch hosil qilishi mumkin. Sertifikat shaxsni kimligini tasdiqlovchi hujjatning analogidir. Shaxsni identifikatsiya qilish muammosi (pasport, haydovchilik guvohnomasi va hokazo) uchrashuv paytida yuzaga keladi. Tarmoqda sherikni ko‘rmasdan turib muloqot qilishda, shaxsning kimligini bilish yanada muhimroqdir.

Kriptomustahkamlik shifrning tasnifi bo‘lib, u kalitni bilmasdan turib shifrni yechishga bo‘lgan mustahkamlikni bildiradi. Shifrlash orqali axborotni

himoyalashning samaradorligi kalitning yashirin saqlanishiga va shifrning kriptomustahkamligiga bog‘liq.

AES [advanced encryption standard (AES)]–AQShda ma’lumotlarni shifrlash standarti bo‘lib, simmetrik shifrtizimlarda foydalanish uchun qo‘llanadi. Blok o‘lchami 128 bit, kalit uzunligi 128, 192 yoki 256 bitdan iborat bo‘lgan bazaviy blokli shifrlash algoritmiga asoslagan. 2002-yildan beri amalda qo‘llanilmoqda. DES [data encryption standard] shifrlash standarti Amerika standart shifrlash tizimi bo‘lib, simmetrik shifrtizimlarda foydalanish uchun mo‘ljallangan. Dunyoda shifrlashning birinchi ochiq rasmiy standarti sifatida 1977-yildan 1997-yilgacha amal qilgan. Blok kattaligi 64 bit, kalit uzunligi 56 bitga teng bo‘lgan bazaviy blokli shifrlash algoritmi asosida qo‘llanilgan. Shifrlashning 4 rejimi va xabarni haqiqiyligini aniqlashtiruvchi kodni shakllantirishning 2 rejimiga ega. DES-algoritmi qo‘llashining asosiy sohalari:

1) kompyuterda ma’lumotlarni saqlash (parol va fayllarni shifrlash);

2) xabarlarni autentifikatsiyalash (xabar va nazorat guruhiga ega bo‘lib, xabarni haqiqiyligiga ishonch hosil qilish qiyinchilik tug‘dirmaydi);

3) elektron to‘lov tizimlarida (ko‘p sonli mijozlar va banklar o‘rtasidagi operatsiyalarda);

4) tijorat xabarlarni elektron almashinuvida (xaridor, sotuvchi va bank xodimi o‘rtasida ma’lumotlar almashinuvida o‘zgartirishlar kiritish va ushlab qolishlardan himoyalangan).

GOST 28147-89 shifrlash standarti–Rossiya shifrlash standarti bo‘lib, simmetrik shifrtizimlarda foydalanish uchun mo‘ljallangan. Blok kattaligi 56 bit, kalit uzunligi 256, 512 bitga teng bo‘lgan bazaviy blokli shifrlash algoritmiga asoslangan. Shifrlashning 4 rejimiga ega. Ko‘p sonli turli ochiq kalitli kriptotizimlar ichida keng tarqalgani 1977-yilda ixtiro qilingan va uning mualliflari Ron Rivest, Ada Shamir va Leonard Eydelman nomiga qo‘yilgan RSA kriptotizimidir. Ular, katta tub sonlarni aniqlash, hisoblash jihatdan oddiy ekanligidan hamda shunday ikkita katta sonlarning ko‘paytmasi bo‘lgan sonni ko‘paytuvchilarga ajratish judayam qiyin, amalda mumkin emasligidan foydalanishgan. RSA shifrini ochish shunday ko‘paytuvchilarga ajratishga tengligi isbotlangan (Rabin teoremasi). Shuning uchun kalit uzunligi qanday bo‘lishidan qat’i nazar shifrni ochish uchun talab qilinadigan amallarning quyi chegarasini baholash, zamonaviy kompyuterlarning tezligini bilgan holda shifrni ochish uchun kerak bo‘ladigan vaqtni ham aniqlash mumkin. RSA algoritmining himoyalanganlik kafolatini aniqlash imkoniyati, uning boshqa ochiq kalitli algoritmlar orasida mashhur bo‘lishining sababi hisoblanadi. Shuning uchun RSA algoritmidan bank kompyuter tizimlarida foydalanilmoqda, ayniqsa uzoq masofadagi mijozlar bilan ishlashda (kredit kartochkalarga xizmat ko‘rsatishda) qo‘llanilmoqda. Xabar xesh-funksiyasi – qiymati kirish ketma-ketligining, ya’ni ikkilik sanoq tizimida berilgan xeshlovchi sonning har bir bitiga yoki xeshlovchi dastlabki matnning har bir ramziga bog‘liq bo‘lgan funksiya1. Xeshlash algoritmi kirish matnidan bir xil uzunlikda natija chiqaradi. Bunda uzunlik deganda, ikkilik sanoq tizimida berilgan ifodadagi bitlar soni nazarda tutiladi.

Masalan, kirish matni «AKT lug‘ati» bo‘lsa va xeshfunksiya qiymati «10110111010100101»ga teng chiqsa, xesh-funksiya qiymati uzunligi 17 bitga teng bo‘ladi. Chiqish uzunligi 128, 192, 256 bit bo‘lgan xesh-funksiyalar ham mavjud. Xesh-funksiya samarali bo‘lishi uchun kirish xabari uchun natija noyob bo‘lishi lozim. Odatda, xeshfunksiyalar bir tomonli funksiyalardir. Chunki, chiqish qiymati asosida dastlabki matnni hisoblab topish juda qiyin. Xesh-funksiyalar axborot uzatish va saqlashda uning xavfsizligini muhofaza qilish uchun qo‘llaniladi.

Elektron raqamli imzo va ochiq kalitlar strukturasi. Elektron raqamli imzoni qo‘llashdan maqsad, birinchidan elektron hujjatdagi axborot asl nusxa ekanligini tasdiqlash, ikkinchidan uchinchi tarafga (arbitr, sudga va boshqalarga) hujjatni muallifi ushbu shaxs ekanligini isbotlash. Ushbu maqsadga erishish uchun muallif o‘zining maxfiy individual raqami (individual kalit, parol) bilan hujjatga o‘rnatilgan tartibda «elektron imzo qo‘yish» jarayonini bajarishi lozim. Bunday imzo qo‘yishda, har gal individual kalit elektron hujjatdagi ma’lumotlar bilan ma’lum qoidaga muvofiq aralashib ketadi. Bunday biriktirilish natijasida hosil bo‘lgan raqam (ma’lum razrad uzunligidagi raqamlar ketma-ketligi) ushbu hujjatga muallif tomonidan qo‘yilgan elektron raqamli imzo hisoblanadi. Shunday qilib, elektron raqamli imzo qo‘yish va uni tekshirish protsedurasining har birida ishlatiladigan ikkita kalitdan bittasi foydalaniladi. Lekin bunda imzo qo‘yish kalitini tekshirish kaliti yordamida aniqlash imkoniyati umuman mumkin emasligi kafolatlangan bo‘lishi kerak. Hozirda taklif etilgan usullarda, amalda imzo qo‘yish kalitini (yopiq kalit), tekshiruv kaliti yordamida (ochiq kalit) qayta tiklash uchun uzoq davom etadigan murakkab hisoblash ishlarini bajarish lozimligi nazarda tutiladi.

Elektron imzo g‘oyasi birinchi marta Diffi va Xellman asarida hujjatning asl nusxa ekanligini va muallif tomonidan imzolanganligini aniqlash uchun taklif etilgan. Hozirgi paytda raqamli imzo keng qo‘llanilmoqda (uzatiladigan yoki saqlanadigan shifrlangan matnga biriktirilgan raqam, bu axborotning butunligini va muallifni haqiqiyligini tekshirish imkoniyatini kafolatlaydi). Simmetrik shifrlash algoritmlariga asoslangan raqamli imzo modellari ham mavjud.

Mustaqil uchun savollar.

1. Kriptografiya nima?
2. Kriptografiya rivojlanishining qanday bosqichlari mavjud?

Nazorat savollari:

1. Kriptografiya deganda nimani tushunasiz?
2. Shifrlash va uni ochish funktsiyasini izoxlab bering?
3. Simmetrik va nosimmetrik shifrlashtirish bir—biridan qanday farq qiladi?
4. Kriptografiya kanday masalarni echilishini ta’minlash kerak?
5. Kriptotaxlil tushunchasiga ta’rif bering?

2.2. Axborotlarni himoyalashning vositalari.

Tayanch ibora va tushunchalar: Passiv metod va aktiv metod, ekranlash, nurlanish va ta’sirlanish quvvatini pasaytirish, nurlanish va ta’sirlanish

signallarini informativligini kamaytirish, lokal fazoviy shovqinlani, ob’ektli fazoviy shovqinlanish.

Mavzuga oid asosiy tushunchalar: Kompyuter malumotlarni himoyalashning texnik vositalari, kompyuter malumotlarni himoyalashning dastyriy vositalari.

Darsning maqsadi: Davlat xavfsizligi sohasida davlat siyosatini amalga oshirish, axborotni muhofaza qilishning davlat tizimi axborotni muhofaza qilish, davlat idoralari va tashkilotlarida axborotni muhofaza qilish holatini nazorat qilish.

Axborotni muhofaza qilishning davlat tizimi axborotni muhofaza qilish sohasida tashkilotlar faoliyatini litsenziyalash nimtizimini, axborotni muhofaza qilish vositalarini sertifikatsiyasini va axborot xavfsizligi talablari bo‘yicha axborotlashtirish obiektlarini attestatsiyasini, kadrlarni tayyorlash, maxsus aloqa tizimlari, ilmiy-tadqiqot va tajriba-konstruktorlik ishlarini tashkillashtirish tizimlarini o‘z ichiga oluvchi murakkab tizimdir. Axborotni muhofaza qilishning davlat tizimi ish yuritishi quyidagi qonun, me’yoriy hujjatlar asosida amalga oshiriladi:

– O‘zbekiston Respublikasining Konstitutsiyasi;
– “Davlat sirlarini saqlash to‘g‘risida”gi qonun;
– “Axborotlashtirish to‘g‘risida”gi qonun;
– “Mahsulotlar va xizmatlarni sertifikatlashtirish to‘g‘risida”gi qonun;
– “Faoliyat ayrim turlarini litsenziyalash to‘g‘risida”gi qonun;
– “Standartlashtirish to‘g‘risida”gi qonun;
– “Aloqa to‘g‘risida”gi qonun;
– “Telekommunikatsiyalar to‘g‘risida”gi qonun;
– “Axborot olish kafolatlari va erkinligi to‘g‘risida”gi qonun;
– “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonun;
– “Elektron hujjat aylanishi to‘g‘risida”gi qonun;
– “Elektron raqamli imzo to‘g‘risida”gi qonun;
– “Elektron tijorat to‘g‘risida”gi qonun;
– O‘zbekiston Respublikasi Prezidentining farmonlari va qarorlari;
– O‘zbekiston Respublikasi Vazirlar Mahkamasining qarorlari;
– Axborotni muhofaza qilish sohasidagi vazirlik, muassasa, agentlik va xo‘jaliklarning boshqa huquqiy aktlari.

Davlat xavfsizligi sohasida davlat siyosatini amalga oshirishga imkon beruvchi sharoitlarni yaratish, mamlakatni iqtisodiy va ilmiy-texnik taraqqiyotiga ko‘maklashish, axborotni muhofaza qilish usul va vositalarini qo‘llab, O‘zbekiston milliy xavfsizligiga bo‘lgan zararni jiddiy kamaytirish – bularning barchasi axborotni muhofaza qilishning davlat tizimida ko‘zlangan maqsad bo‘lib, ularni amalga oshirish uchun quyidagi vazifalarni bajarish kerak:

– yagona texnik siyosatni o‘tkazish, harbiy, iqtisodiy, ilmiy-texnik va boshqa sohalar faoliyatlarida axborotni muhofaza qilish bo‘yicha ishlarni muvofiqlash va tashkil etish;
– razvedkaning texnik vositalar yordamida axborotni qo‘lga kiritishni jiddiy qiyinlashtirish yoki yo‘l qo‘ymaslik;

– axborotni muhofaza qilish sohasida munosabatlarni tartibga soluvchi huquqiy hujjatlarni qabul qilish;
– axborotni muhofaza qilish vositalarini yaratish va ularning samaradorligini nazorat qilish kuchlarini tashkil etish;
– davlat idoralari va tashkilotlarida axborotni muhofaza qilish holatini nazorat qilish;

O‘zbekiston Respublikasining 2000-yil 25-maydagi “Faoliyatning ayrim turlarini litsenziyalash to‘g‘risida”gi 71-II-sonli Qonuni.

Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – Т., 2000.–№5-6. – 142. faoliyat sohasida litsenziyalashni amalga oshirish bo‘yicha asosiy hujjat hisoblanadi. Ushbu qonunning 3-moddasida quyidagi asosiy tushunchalar keltirilgan:

litsenziya–litsenziyalovchi organ tomonidan yuridik yoki jismoniy shaxsga berilgan, litsenziya talablari va shartlariga so‘zsiz rioya etilgani holda faoliyatning litsenziyalanayotgan turini amalga oshirish uchun ruxsatnoma (huquq);

litsenziya talablari va shartlari–faoliyatning litsenziyalanayotgan turini amalga oshirayotganda litsenziat tomonidan bajarilishi majburiy bo‘lgan, qonun hujjatlarida belgilangan talablar va shartlarning majmui;

litsenziyalovchi organlar–qonun hujjatlariga muvofiq litsenziyalashni amalga oshiruvchi maxsus vakolatli organlar;

litsenziat–faoliyatning litsenziyalanadigan turini amalga oshirish litsenziyasi bo‘lgan yuridik yoki jismoniy shaxs;

litsenziyalar reyestri–berilgan, to‘xtatib turilgan, qayta tiklangan, qayta rasmiylashtirilgan, bekor qilingan litsenziyalar, shuningdek amal qilishi tugatilgan litsenziyalar to‘g‘risidagi ma’lumotlarni o‘z ichiga olgan litsenziyalovchi organlarning ma’lumotlar bazalari majmui.

Litsenziyalash sohasini davlat tomonidan tartibga solishni ushbu qonunning 4-moddasiga ko‘ra O‘zbekiston Respublikasi Vazirlar Mahkamasi hamda litsenziyalovchi organlar amalga oshiradi.

O‘zbekiston Respublikasi Vazirlar Mahkamasi vakolatlari jumlasiga quyidagilar kiradi (5-modda):
– litsenziyalovchi organlarni va faoliyatning ayrim turlarini litsenziyalash tartibini belgilash, qonunda nazarda tutilgan hollar bundan mustasno;
– O‘zbekiston Respublikasi hududida litsenziyalar reyestrini yuritish tartibini belgilash;
– faoliyatning ayrim turlarini litsenziyalash sohasidagi qonun hujjatlariga litsenziyalovchi organlarning rioya etishlarini nazorat qilish;
– litsenziyalashning ayrim turlarini amalga oshirish.
Litsenziyalovchi organlarning vakolatlari jumlasiga quyidagilar kiradi (6-modda):
– faoliyatning ayrim turlarini qonun hujjatlariga muvofiq litsenziyalash;
– qonunda nazarda tutilgan hollarda faoliyatning tegishli turlarini litsenziyalash tartibi to‘g‘risidagi nizomlarni tasdiqlash;
– litsenziya talablari va shartlariga litsenziatlar rioya etishini nazorat qilish;

– litsenziyalarni qayta rasmiylashtirish;
– litsenziyalarning amal qilishini to‘xtatib turish, qayta tiklash;
– litsenziyalarning amal qilishini tugatish;
– litsenziyalarni bekor qilish;
– litsenziyalar reyestrini yuritish.

Litsenziya olish uchun litsenziya da’vogari tegishli litsenziyalovchi organga quyidagilarni taqdim etadi (14-modda):
–litsenziya berish to‘g‘risidagi ariza–unda: yuridik shaxs uchun–yuridik shaxsning nomi va tashkiliy-huquqiy shakli, joylashgan manzili (pochta manzili), bank muassasasining nomi va bank muassasasidagi hisob raqami; jismoniy shaxs uchun–familiyasi, ismi va otasining ismi, fuqaroning shaxsini tasdiqlovchi hujjatning ma’lumotlari; yuridik yoki jismoniy shaxs amalga oshirishni mo‘ljallagan faoliyatning litsenziyalanayotgan turi (uning bir qismi), shuningdek qonun hujjatlarida nazarda tutilgan hollarda faoliyatning mazkur turi;
– yuridik shaxslar uchun–yuridik shaxs davlat ro‘yxatidan o‘tkazilganligi to‘g‘risidagi guvohnomaning notarial tasdiqlangan nusxasi; jismoniy shaxslar uchun–yakka tartibdagi tadbirkor davlat ro‘yxatidan o‘tkazilganligi to‘g‘risidagi guvohnomaning nusxasi;
– litsenziyalovchi organ litsenziya da’vogarining arizasini ko‘rib chiqishi uchun litsenziya davogari yig‘im to‘laganligini tasdiqlovchi hujjat;
– faoliyatning ayrim turiga litsenziya olish uchun qo‘yiladigan talablar va shartlarni litsenziya davogari bajarishi mumkinligini tasdiqlovchi hamda qonun hujjatlarida belgilab qo‘yiladigan boshqa hujjatlar.

Litsenziya davogarining arizasini barcha zarur hujjatlar bilan birga olgan kundan e’tiboran o‘ttiz kundan oshmagan muddat ichida litsenziyalovchi organ namunaviy (oddiy) litsenziya berish haqida yoki berishni rad etish to‘g‘risida qaror qabul qiladi va litsenziyalovchi organ litsenziya davogarini qabul qilingan qaror to‘g‘risida uch kun ichida xabardor qilishi shart (16-modda).
O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilish (AKMQ) sohasida faoliyatni litsenziyalash tizimi Litsenziyalash talablari va shartlari O‘zbekiston Respublikasi Vazirlar Mahkamasining 2007-yil 21-noyabrdagi 242-sonli qarori1 bilan tasdiqlangan “Axborotning kriptografik himoya vositalarini loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta’mirlash va ulardan foydalanish faoliyatini litsenziyalash to‘g‘risidagi Nizom”ning II bo‘limida keltirilgan.

O‘zbekiston Respublikasi Vazirlar Mahkamasining “Toshkent axborot texnologiyalari universiteti faoliyatini tashkil etish to‘g‘risida”gi 2002-yil 7-noyabr 385-sonli qaroriga muvofiq bu universitet respublikaning aloqa va axborot texnologiyalari sohasida kadrlar tayyorlash, qayta tayyorlash va mutaxassislar malakasini oshirish bo‘yicha bazaviy oliy ta’lim muassasasi hisoblanadi.

O‘zbekiston Respublikasi Prezidentining “Milliy axborotkommunikatsiya tizimlarining kompyuter xavfsizligini ta’minlash borasidagi qo‘shimcha chora-tadbirlar to‘g‘risida”gi 2005-yil 5-sentabr 167-sonli qaroriga muvofiq

kompyuter va axborot texnologiyalarini rivojlantirish hamda joriy etish markazi “O‘zinfokom” huzurida “Kompyuter hodisalariga chora ko‘rish xizmati” tashkil etilgan. Ushbu xizmatning asosiy vazifalariga quyidagilar kiradi:
–kompyuter xavfsizligini ta’minlashda xalqaro tajribani o‘rganish va umumlashtirish asosida axborot tizimlariga noqonuniy kirish harakatlarini oldini olishni ta’minlovchi effektiv dasturiy-apparatli vositalarni qo‘llash bo‘yicha milliy foydalanuvchilarga tavsiyalar ishlab chiqish, ularga konsultativ xizmatlar va texnik yordam berish;
–ehtimoliy xavfni baholash, axborot tizimlarida va davlat korxona hamda tashkilotlarda kompyuter xavfsizligi holati bo‘yicha milliy foydalanuvchilarga konsultativ xizmatlar va texnik yordam berish, insident oqibati va sabablarini tahlil qilishda ko‘maklashish, kompyuter tizimlarini himoyalash uchun mexanizmlarni qidirish;
Kompyuter malumotlarni himoyalashning dastyriy vositalari.

Mamlakatning tahdidlarga mos aks ta’sir ko‘rsatish layoqatiga ega bo‘lgan axborot xavfsizlik tizimini yaratish uchun, rivojlangan chet el mamlakatlarida axborot urushining zamonaviy konsepsiyalari, o‘ziga xos xususiyatlari, axborot qurolining turlari va qo‘llash samaradorligi, shuningdek, chet el mamlakatlarida axborot xavfsizligini ta’minlash masalalari qay tarzda yechilishi haqida aniq bir tasavvurga ega bo‘lish kerak.

Axborot quroli deb nomlanuvchi vositalar:
- axborot massivlarini yo‘q qilish, buzish yoki o‘g‘irlash;
- himoya tizimlarini yengish;
- qonuniy foydalanuvchilar huquqlarini cheklash;
- kompyuter tizimlarini, texnik vositalarni ishini izdan chiqarish;
- shular kabi boshqa amallarni bajaradi.

Hozirda hujumkor axborot quroliga quyidagilarni keltirish mumkin:
– ko‘payish, dasturlarga kirish, aloqa liniyalari, ma’lumot uzatish tarmog‘i orqali uzatish, boshqaruv tizimini ishdan chiqarish va shu kabi boshqa qobiliyatlarga ega bo‘lgan kompyuter viruslari;
- mantiqiy bomba–dasturiy o‘rnatma qurilmalari, signal bo‘yicha yoki aniq vaqtda harakatga keltirish uchun harbiy yoki fuqarolik infratuzilma axborot-boshqaruv markazlariga oldindan kirgiziladi;
- telekommunikatsiya tarmoqlarida axborot almashishini susaytiruvchi, davlat yoki harbiy boshqarish kanallarida axborotni soxtalashtiruvchi vositalar;
- tekshiruvchi dasturlarni neytrallash vositalari;
-obiektning dasturiy ta’minotiga raqib tomonidan ongli ravishda turli xatoliklarni kiritish.

Axborot qurolini qo‘llash oqibatini kamaytirish yoki oldini olish uchun quyidagi chora-tadbirlarni ko‘rish kerak:
-axborot resurslarini fizik asosini tashkil etuvchi material-texnik obiektlarni himoyalash;
- ma’lumotlar bazasi va bankini normal va uzluksiz ishlashini ta’minlash;
-ruxsat etilmagan kirishlardan, buzish yoki yo‘q qilishdan axborotlarni himoyalash;

-axborot sifatini (vaqtidaligini, aniqligini, to‘laligini va foydalana olishlikni) saqlab qolish.

Axborot qurolidan himoyalovchi dasturiy tasnifdagi amaliy tadbirlarga quyidagilar kiradi:

1. Xalqaro tarmoq orqali turli xil axborot almashinuvida iqtisodiy va boshqa tuzilmalarning ehtiyojini bashoratlash va monitoringini tashkil qilish. Buning uchun transchegara, shu qatorda Internet orqali ham, almashinuvni nazorat qilish uchun maxsus tuzilmalarni yaratish; ochiq tarmoqlarda axborot xavfsizligi tahdidlarini bartaraf etish bo‘yicha davlat va nodavlat idoralarning chora-tadbirlarini koordinatsiya qilish; xalqaro hamkorlikni tashkil etish mumkin.
2. Axborot resurslarining xavfsizligi talablariga rioya qilgan holda milliy va korporativ tarmoqlarni jahon ochiq tarmog‘lariga ulanishini ta’minlovchi axborot texnologiyalarni takomillashtiruvchi davlat dasturini ishlab chiqish.
3. Jahon axborot tarmoqlarida ishlash uchun ommaviy foydalanuvchilarni va axborot xavfsizligi bo‘yicha mutaxassislarni tayyorlash va malakasini oshirish kompleks tizimini tashkil qilish.
4. Ochiq jahon tarmoqlari foydalanuvchilarining mas’uliyatlari va majburiyatlari, reglament huquqi va axborot resurslari bilan foydalanish qoidalarining milliy qonunchilik qismini ishlab chiqish. Jahon ochiq tarmoqlari ishlashining me’yoriy-huquqiy ta’minotini va xalqaro qonunchiligini ishlab chiqishda faol ishtirok etish.

Federal tekshirishlar byurosi (FTB-FBR) ham, eng avvalo AQSh infratuzilmasini himoyalash nuqtai nazaridan axborot urushi doktrinasini tatbiq qilishda ishtirok etadi. AQSh da kompyuter jinoyatchiligiga qarshi kurashish maqsadida 1996-yili «Kompyuterlarni qo‘llash orqali firibgarlik va suiiste’mol qilishlar to‘g‘risida»gi federal qonun qabul qilingan va ushbu turdagi jinoyatchilik bilan kurashish bo‘yicha FTB tarkibida bo‘linma tashkil etish ko‘zda tutilgan. FTB telekommunikatsiya tarmog‘i orqali amalga oshiriladigan ayg‘oqchilik, maxfiy ma’lumotlarni oshkor qilish, davlat instansiyalarni aldash, terrorizm, xiyla ishlatish va firibgarlik kabi noxush holatlarni tekshirish bilan shug‘ullanadi. Uning tarkibiga kompyuter jinoyatchiligi bilan shug‘ullanuvchi yettita bo‘linma kiradi, ularning shtati 300 kishini tashkil qiladi.

AQSh ning Mudofaa vazirligi (MV) xalqaro Internet tarmog‘ining ajdodi hisoblanib, birinchi bo‘lib mamlakatning xavfsizligiga yangi tahdidning va axborot qurolining kuchini anglab yetdi va hozirgi vaqtda harbiy sohada axborot urushi doktrinasini tatbiq qilishda yetakchi o‘rinni egallaydi. MV ilmiy kengashining ekspertlar komissiyasi axborot urushi hodisasiga qarshi harbiy telekommunikatsiya va kompyuter tarmoqlari xavfsizligini ta’minlovchi shoshilinch choralarni qabul qilish lozimligi haqida doklad tayyorladi. Pentagon harbiy avtomatlashtirilgan axborot tizimlarini “qizil buyruqlar” deb ataluvchi zaiflikka tekshirish uchun harbiy kompyuter tarmoqlarini himoyasini ta’minlash bilan shug‘ullanish maqsadida xakerlarni ishga qabul qiladi.

Secret Intelligence Service/MI6–Buyuk Britaniyaning asosiy razvedka xizmati. SIS Tashqi ishlar vazirligi (TIV) tizimiga kiritilgan bo‘lib xorijda 87 ta qarorgohga va Londonda shtab-kvartiraga ega. SISni Bosh direktor boshqaradi

va u bir vaqtning o‘zida Tashqi ishlar vazirining o‘rinbosari ham hisoblanadi. Shunday qilib, formal ravishda SIS Buyuk Britaniyaning TIV nazorati ostida hisoblanadi, biroq, shu bilan birga u to‘g‘ridan-to‘g‘ri premyer-ministrga chiqishi mumkin. Kontrrazvedka xizmati – Military Intelligence-5 (MI-5) 1909-yilda ichki xavfsizlikni ta’minlash bilan shug‘ullanuvchi maxfiy xizmatlar Byurosining ichki departamenti sifatida tuzilgan. Hukumat aloqa markazi Buyuk Britaniyaning maxsus xizmatlar tizimida radioayg‘oqchilik uchun javob beradi. Markaz TIV tarkibiga kiritilgan bo‘lib, xodimlarining soni va axborotni topish hajmi bo‘yicha mamlakatning yirik idoralaridan biri hisoblanadi.

Konstitutsiyani himoyalash federal byurosi (Verfassungsschutz /BfV/). Ushbu byuro BND va BSI bilan bir qatorda mamlakatning uchta maxsus xizmatlaridan biri hisoblanadi va u Germaniyaning ichki ishlar vazirligiga bo‘ysunadi. Barcha federal yerlarda mahalliy ichki ishlar vazirligiga bo‘ysunadigan o‘zining mos xizmatlari mavjud. Har yili to‘plangan axborotlar asosida Konstitutsiyaga rioya etilganligi doirasidagi ish holati haqida hukumatga hisobot taqdim etiladi, unda xulosalar va tavsiyalar qilinadi. Hukumat, o‘z navbatida, aniq choralarni amalga oshirish kerakligi haqida qaror qabul qiladi. zAxborotning yarmidan ko‘pini maxsus xizmat ochiq manbalardan: ommaviy axborot vositalarida chop etilgan nashrlar, Internet, majlis va mitinglarda ishtirok etish orqali yig‘adi. Axborotning bir qismi ayrim kishilardan va boshqa idoralardan kelib tushadi.

Fransiyada axborotni himoyalash tizimi. Fransiya kibermaydonda o‘zining fuqarolarini nazorat qilish bo‘yicha tuzilma tashkil etgan.
Fransuzlar “Eshelon” nomli Amerika tizimiga o‘xshash o‘z tizimini yaratdilar. U deyarli barcha xususiy global kommunikatsiyalarni tutib qolishga yo‘naltirilgan.

Milliy xavfsizlikni ta’minlash bo‘yicha siyosatning strategik yo‘nalishlarini ishlab chiqish bilan CLUSIF (Club de la securite informatique francaise) birlashmasi shug‘ullanadi. U o‘zining statusi bo‘yicha informatika sohasida ishlovchi yuridik va fizik shaxslarning ochiq assotsiatsiyasi hisoblanadi. CLUSIF davlat tomonidan to‘liq qo‘llab quvvatlanadi va maxsus xizmatlar bilan yaqin aloqaga ega. Fransiyaning maxsus xizmati strukturasi. Fransiya razvedka uyushmasining umumiy shtati, uchta har xil vazirlikka bo‘ysunuvchi xizmatlarda ishlaydigan 12779 ga yaqin xodimlardan iborat. Uchta xizmat Tashqi xavfsizlikning Bosh direksiyasi (DGSE); Harbiy razvedka boshqarmasi (DRM) va Harbiy kontrrazvedka boshqarmasi (DPSD) Mudofaa vazirligi himoyasida faoliyat olib boradi. Maxsus xizmatlarga jandarmeriyani (Gendarmerie) ham kiritish mumkin. Uning vazifalaridan biri bo‘lib razvedka faoliyatini yuritish hisoblanadi – jandarmeriyaning har bir qismida razvedka bo‘limi mavjud. Ikkita maxsus xizmat:
kontrrazvedka (DST) va Bosh razvedka xizmati (RG) Ichki ishlar vazirligiga bo‘ysungan.

Rossiya Federatsiyasi (RF)ning axborot xavfsizligini ta’minlovchi davlat idoralari strukturasi. Axborot xavfsizligining davlat siyosatini ishlab chiqish, qonunlar, normativ-me’yoriy hujjatlar tayyorlash, axborotni muhofaza qilishni

ta’minlash bo‘yicha o‘rnatilgan me’yorlarni bajarilishi ustidan nazoratni davlat idoralari amalga oshiradilar. RF Prezidenti axborot xavfsizligini ta’minlovchi davlat idoralariga boshchilik qiladi. U Xavfsizlik kengashini boshqaradi va davlatda axborot xavfsizligini ta’minlashga doir farmonlarni tasdiqlaydi.

Mamlakatning davlat xavfsizligiga oid boshqa masalalar bilan bir qatorda axborot xavfsizligi tizimining umumiy boshqaruvini RF Prezidenti va Hukumati amalga oshiradi. RF Prezidenti huzuridagi xavfsizlik Kengashi davlat xavfsizligi masalalari bilan bevosita shug‘ullanuvchi hokimiyat idorasi hisoblanadi. xavfsizlik Kengashi tarkibiga axborot xavfsizligi bo‘yicha idoralararo komissiya kiradi. Komissiya davlatning axborot xavfsizligi sohasida Prezident farmonlarini tayyorlaydi, qonun chiqarish tashabbusi bilan chiqadi, vazirlik va idoralar rahbarlarining faoliyatini muvofiqlashtiradi.

Axborot xavfsizligi bo‘yicha idoralararo komissiyaning ishchi idorasi bo‘lib RF Prezidenti huzuridagi Davlat texnik komissiyasi hisoblanadi. Bu komissiya qonun loyihalarini tayyorlashni amalga oshiradi, normative me’yoriy hujjatlarni ishlab chiqadi, axborotni muhofaza qilish vositalarini (kriptografik vositalardan tashqari) sertifikatlashtirishni tashkil etadi, himoya vositalarini ishlab chiqish sohasidagi faoliyatni litsenziyalashtiradi va axborotni muhofaza qilish bo‘yicha mutaxassislarni o‘qitadi. Axborotni muhofaza qilish sohasida izlanishlar olib boruvchi davlat ilmiy-tadqiqot tashkilotlari faoliyatini muvofiqlashtiradi. Bu komissiya Davlat sirini himoyalash bo‘yicha idoralararo komissiya ishini ham ta’minlaydi. Davlat sirini himoyalash bo‘yicha idoralararo komissiyasiga davlat sirini tashkil etadigan ma’lumotlardan foydalanish, axborotni muhofaza qilish vositalarini yaratish hamda davlat sirini himoyalash bo‘yicha xizmat ko‘rsatish bilan bog‘liq korxona, muassasa va tashkilotlarni litsenziyalashni boshqarish vazifasi yuklatilgan. RF vazirlik va idoralarida axborot xavfsizligi siyosatining mos darajalarini boshqarishni ta’minlovchi iyerarxiyaga asoslangan tuzilmalar mavjud. Bu tuzilmalar, turli-xil nomlangani bilan o‘xshash funksiyalarni bajaradilar.

Mustaqil tayyorgarlik uchun savollar

1. Axborotni muhofaza qilishning davlat tizimi nima?
2. Axborotni muhofaza qilishning davlat tizimi ish yuritishi qanday qonun, normativ-me’yoriy hujjatlar asosida amalga oshiriladi?

Nazorat savollari:

1. Axborot muhofaza qilish sohasida litsenziyalash va sertifikatsiyalash nima uchun beriladi.
2. Kompyuter malumotlarni himoyalashning dastyriy vositalari.
3. Germaniyaning axborotni himoyalash tizimi.
4. Fransiyada axborotni himoyalash tizimi.
5. Rossiya Federatsiyasi (RF)ning axborot xavfsizligini ta’minlovchi davlat idoralari strukturasi.

2.3. Simmetriyali kriptotizim asoslari.

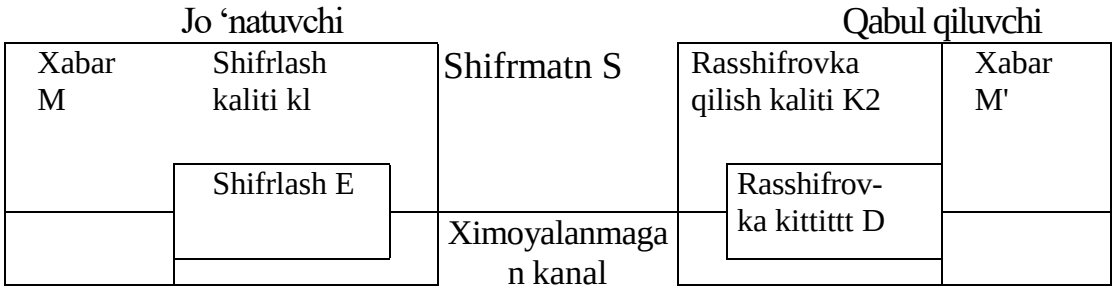
Tayanch ibora va tushunchalar: Xizmat kursatuvchi dasturlar, fizik zararlanish, mantiqiy zararlanish, virus, fayllar joylashuvi jadvali, klaster, sektor, prognoz.

Mavzuga oid asosiy muammolar: Axborotning ximoyalash shifrlash tashkil etadi. Axborotni shifrlash. Shifrlash kriptotizimi. Kriptotizimlarning ikkita sinfi simmetrik kriptotizim (bir kalitli), asimmetrik kriptotizim (ikkita kalitli).

Darasning maqsadi: Talabalarga kriptotizim asoslari va kriptografik himoyalar haqida tushuncha va ko‘nikmalar berish.

Simmetriyai kriptotizim kriptizim asoslari**.**

Axborotning ximoyalashning aksariyat mexanizmlari asosini shifrlash tashkil etadi. Axborotni shifrlash deganda ochiq, axborotni (dastlabki matnni) shifrlangan axborotga uzgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi. Shifrlash kriptotizimining umumlashtirilgan sxemasi quyidagi sxemada keltirilgan.



Uzatiluvchi axborot matni M kriptografik uzgartirish E_{kl} yordamida shifrlanadi, natijada shifrmatn S olinadi:

$$S = E_{k1}(M)$$

bu erda kg‘- shifrlash kaliti deb ataluvchi E funktsiyaning parametri.

Shifrlash kaliti yordamida shifrlash natijalarini uzgartirish mumkin. Shifrlash kaliti muayyan foydalanuvchiga yoki foydalanuvchilar guruxiga tegishli va ular uchun yagona bo‘lishi mumkin. Muayyan kalit yordamida shifrlangan axborot faqat ushbu kalit egasi (yoki egalari) tomonidan rasshifrovka qilinishi mumkin.

Axborotni teskari o‘zgartirish quyidagi ko‘rinishga ega:

$$M'+D_{k2}(C)$$

D funktsiyasi E funktsiyaga nisbatan teskari funktsiya bo‘lib, shifr matnni rasshifrovka qiladi. Bu funktsiya xam kl kalit kurinishidagi qo‘shimcha parametrga ega. kg‘ va k1 kalitlar bir ma’noli moslikka ega bo‘lishlari shart. Bu xolda rasshifrovka qilishgan M' axborot Mga ekvivalent bo‘ladi. k2 kaliti ishonchli bo‘lmasa D funktsiya yordamida M'+M dastlabki matnni olib bo‘lmaydi.

Kriptotizimlarning ikkita sinfi farqlanadi:

- simmetrik kriptotizim (bir kalitli);
- asimmetrik kriptotizim (ikkita kalitli). Shifrlashning simmetrik kriptotizimida shifrlash va rasshifrovka qilish uchun bitta kalitning o‘zi ishlatiladi. Demak, shifrlash kalitidan foydalanish xuquqiga ega bo‘lgan xar qanday odam axborotni rasshifrovka qilishi mumkin. Shu sababli, simmetrik kriptotizimlar maxfiy kalitli kriptotizimlar deb yuritiladi. Ya’ni shifrlash kalitidan faqat axborot atalgan odamgina foydalana olishi mumkin. Elektron xujjatlarni uzatishning konfidentsialligini simmetrik kriptotizim yordamida ta’minlash masalasi shifrlash kaliti konfidentsialligini ta’minlashga keltiriladi.

Simmetrik shifrlashning noqulayligi-axborot almashinuvi boshlanmasdan oldin barcha adresatlar bilan maxfiy kalitlar bilan ayirboshlash zaruriyatidir. Simmetrik kriptotizimda maxfiy kalitni aloqaning umumfoydalanuvchi kanallari orqali uzatish mumkin emas. Maxfiy kalit jo‘natuvchiga va qabul qiluvchiga kalitlar tarqatiluvchi ximoyalangan kanallar orqali uzatilishi kerak. Simmetrik shifrlash algoritmining ma’lumotlarni abonentli shifrlashda, ya’ni shifrlangan axborotni abonentga, masalan Internet orqali, uzatishda amalga oshirilgan variantlari mavjud. Bunday kriptografik tarmoqning barcha abonentlari ushbu bita kalitning ishlatilishi xavfsizlik nuqtai nazaridan nojoizdir. Xaqiqatan, kalit obro‘sizlantirilganda (yo‘qotilganida) barcha abonentlarning xujjat almashishi xavf ostida qo‘ladi. Bu xolda kalitlarning matritsasi quyidagicha ishlatilishi mumkin.

1	2	3	4	
kp	ki2	ko	...	km
k2i	k22	k23	...	k2„
k3i	k32	kzz	...	k3„
...	...	...	...	...
km	k„2	k„z	...	k„„

1-abonent uchun kalitlar to‘plami

2- abonent uchun kalitlar to‘plami

3- abonent uchun kalitlar to‘plami

n- abonent uchun kalitlar to‘plami

Kalitlar matritsasi abonentlarning juft-juft boglanishli jadvalidan iborat. Jadvalning xar bir elementi i va j abonentlarni bog‘lashga mo‘ljallangan va undan faqat ushbu abonentlar foydalana oladilar. Moc xolda, kalitlar matritsasi elementlari uchun quyidagi tenglik o‘rinli.

$$K_u + K_R$$

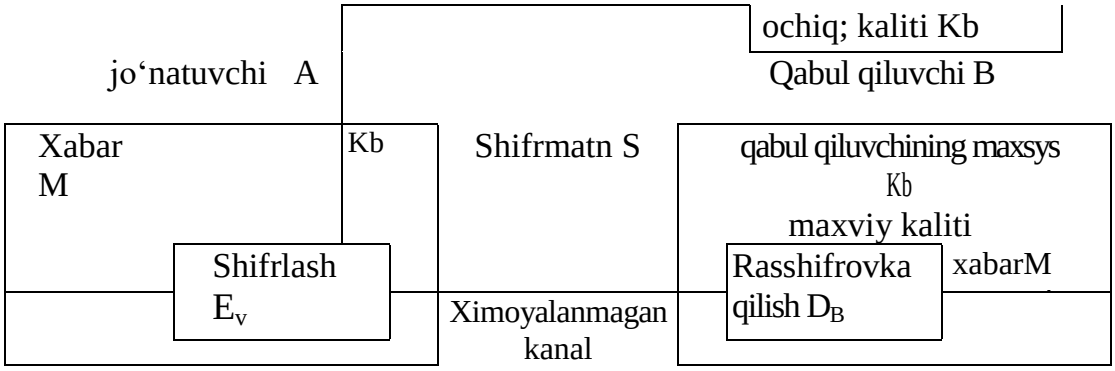
Matritsaning xar bir i- qatori muayyan i abonentning bolgan N-1 abonentlar bilan boglanishini ta’minlovchi kalitlar to‘plamidan iborat. Kalitlar to‘plami (tarmoq,to‘plamlari) kriptografik tarmoqning barcha abonentlari o‘rtasida taqsimlanadi. Taqsimlash aloqaning ximoyalangan kanallari orqali yoki qo‘ldan-qo‘lga tarzda amalga oshiriladi.

Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka kodlashshda turli kalitlardan foydalaniladi:

- ochiq kalit K axborotni shifrlashda ishlatiladi, maxfiy kalit k dan xisoblab chiqariladi;
- maxfiy kalit k uning jufti bo‘lgan ochiq kalit yordamida shifrlangan axborotni rasshifrovka qilishda ishlatiladi.

Maxfiy va ochiq kalitlar juft-juft generatsiyalanadi. Maxfiy kalit egasida krlishi va uni ruxsatsiz foydalanishdan ishonchli ximoyalash zarur (simmetrik algoritmdagi shifrlash kalitiga oxshab). Ochiq kalitning nusxalari maxfiy kalit egasi axborot almashinadigan kriptografik tarmoq abonentlarining xar birida bo‘lishi shart.

qabul qiluvchining



Bu sxemadan ko‘rinib turibdiki, asimmetrik kriptotizimda shifrlangan axborotni uzatish quyidagicha amalga oshiriladi:

1. Tayyorgarlik bosqichi:
- abonent B juft kalitni generatsiyalaydi: maxfiy kalit k_v va ochiq kalit K_v;
- ochiq, kalit K_v abonent A ga va kl gan abonentlarga jo‘natiladi.

2. A va V abonentlar o‘rtasida axborot almashish:
- abonent A abonent Yaning ochiq kaliti K_v yordamida axborotni shifrlaydi va shifrmatnni abonent 5ga jo‘natadi;
- abonent V uzining maxfiy kaliti k_v yordamida axborotni rasshifrovka qiladi. Xech kim (shu jumladan abonent A xam) ushbu axborotni rasshifrovka qilaolmaydi, chunki abonent Yaning maxfiy kaliti unda yo‘q.

Asimmetrik kriptotizimda axborotni ximoyalash axborot qabul qiluvchi kaliti k_v ning maxfiyligiga asoslangan.

Asimmetrik kriptotizimlarning asosiy xususiyatlari quyidagilar:

1. Ochiq kalitni va shifr matnni ximoyalangan kanal orqali jo‘natish mumkin, ya’ni niyati buzuq odamga ular ma’lum bo‘lishi mumkin.

2. Shifrlash E_v: M -> S va rasshifrovka qilish D_B: S > M algoritmlari ochiq.

Ikkala alfavitdagi simvollar o‘rtasidagi moslik ma’lum algoritm bo‘yicha K simvollar uzunligiga ega bo‘lgan dastlabki matn T_0 simvollarining raqamli ekvivalentlarini o‘zgartirish orqali amalga oshiriladi.

Monoalfafitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko‘rinishda ifodalanishi mumkin

l-qadam. [lxR] o‘lchamli dastlabki A_0 alfavitdagi har bir simvol $s_{oi} \in T(i=1,K)$ ni A_0 alfavitdagi s_{0i} simvol tartib raqamiga mos keluvchi $h_{0i}(s_{0i})$ songa almashtirish yo‘li bilan raqamlar ketma-ketligi L_{0h} ni shakllantirish.

2-qadam. L_{0h} ketma-ketligining har-bir sonini $h_{1i}=(k_1 x h_{0i}(s_{0i})+k_2)$ (mod R) formula o‘rqali hisoblanuvchi L_{1h} ketma-ketligining mos soni h_{1i} ga almashtirish yo‘li bilan L_{1h} son ketma-ketligini shakllantirirish; bu erda k_1-o‘nlik koeffisent; k_2- siljitish koeffisenti. Tanlangan k_1,k_2 koeffisentlar $h_{0i}h_{1i}$

sonlarning bir manoli mosligini taminlash lozim, $h_{1i}=0$ olinganida esa $h_{1i}=R$ almashinuvi bajarilishi kerak.

3-qadam. L_{1h} ketma-ketlikning har bir soni $h_{1i}(s_{1i})$ ni [lxR] o‘lchamli shifrlash alfafitining mos $s_{oi} \epsilon$ T(i=1,K) simvoli bilan almashtirish o‘rqali T_1 shifrmatnni hosil qilish.

4-qadam. Olingan shifrmatn o‘zgarmas b uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to‘liq bo‘lmasa blok orqasiga maxsus simvol-to‘ldiruvchilar joylashtiriladi(masalan, *).

Misol. Shifrlash uchun dastlabki ma’lumotlar quyidagilar:

T_0><XIMOYA_XIZMATI>

A_0=<ABVGDEYOJZIYKLMNOPRSTUFXTSCHSH’EYUYAUO‘X_> A_1<ORYOYATE-JMCHXAVDYFKKSEZPITSGXL’SHBUYUKGN> R=36; k_1 = 3; k_2=15; b=4

Algoritmning qadamba-qadam bajarilishi quyidagi natijalarni olinishiga olib keladi.

1-qadam. Lox=<35,10,14,16,31,36,23,10,9,14,1,20,10>

2-qadam. L_{lh}=<12,9,21,17,36,14,12,9,6,21,18,3,9>

3-qadam. T_1=<XJEFNVXJTEKYoJ>

4-qadam. T_1=<XJEF NVXJ TEKYO J***>

Rasshifrovka qilishda bloklar birlashtirilib K simvolli shifrmatn T_1 xosil qilinadi. Rasshifrovka qilish uchun quyidagi butun sonli tenglamani echish lozim:

$$k_1h_{01}+k_2=nR+h_{1i}$$

k_1 k_2, h_{1i} va R butun sonlar ma’lum bulganda h_{0i} kattaligi p ni saralash orkali xisoblanadi. Bu muolajani shifrmatnning barcha simvollariga tadbiq qilish uning rasshifrovka qilinishiga olib keladi.

Almashtirish usulining kamchiligi sifatida dastlabki va berilgan matnlar statistik xarakteristkalarining bir xilligidir. Dastlabki matn qaysi tilda yozilganligini bilgan kriptoanalitik ishlab ko‘rilngan axborotlarni statistik ishlab, ikkala alfavitdagi simvollar o‘rtasidagi muvofiqlikni aniqdashi mumkin.

Polialfavitli almashtirish usullari aytarlicha yuqori kripto-bardoshlikka ega. Bu usullar dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan. Rasman polialfavitli almashtirishni quyidagicha tasavvur etish mumkin. N-alfavitli almashtirishda dastlabki A_0 alfavitdagi s_{01} simvoli A, alfavitdagi s_n simvoli shifrlash takrorlanmaydigan M simvoldan iborat kalit yordamida amalga oshiriladi. Vijinerning to’liq matritsasidan [(M+1), H o‘lchamli shifrlash matritsasi $T_{(sh)}$ ajratiladi. Bu matritsa birinchi qatordan va birinchi elementlari kalit simvollariga mos keluvchi qatorlardan iborat bo‘ladi.

Agar kalit sifatida <FO‘ZA> so‘zi tanlangan bo‘lsa, shifrlash matritsasi beshta qatordan iborat bo‘ladi. O‘rin almashtirish usullari. O‘rin almashtirish usullariga binoan dastlabki matn belgilangan uzunlikdagi bloklarga ajratilib xar bir blok ichidagi simvollar o’rni ma’lum algoritm buyicha almashtiriladi.Eng oson urin almashtirishga misol tarikasida dastlabki axborot blokini matritsaga

qatori bo‘yicha yozishni, o‘qishni esa ustun bo‘yicha amalga oshirishni ko‘rsatish mumkin. Matritsa qatorilarini to‘ldirish va shifrlangan axborotni ustun bo‘yicha o‘qish ketma-ketligi kalit yordamida berilishi mumkin. Usulning kriptobardoshliga blok uzunligiga (matritsa o‘lchamiga) bogliq. Masalan uzunligi 64 simvolga teng bo‘lgan blok (matritsa o‘lchami 8x8) uchun kalitning 1,6. 10^9 kombinatsiya ham bo‘lishi mumkin. Uzunligi 256 simvolga teng bo‘lgan blok (matritsa o‘lchami 16x16) kalitning mumkin bo‘lgan kombinatsiya ham 14. 10^{26} ga etishi mumkin. Bu xolda kalitni saralash masalasi zamonaviy EXMlar uchun xam murakkab xisoblanadi. Gamilton marshrutlariga asoslangan usulda xam o‘rin almashtirishlardan foydalaniladi. Ushbu usul quyidagi qadamlarni bajarish orqali amalga oshiriladi.

1-qadam. Dastlabki axborot bloklarga ajratiladi. Agar shifrlanuvchi axborot uzunligi blok uzunligiga karrali bo‘lmasa, oxirga blokdagi bo‘sh o‘rinlarga maxsus xizmatchi simvollar to‘ldiruvchilar joylashtiriladi(masalan, *).

2-qadam. Blok simvollari yordamida jadval to‘ldiriladi va bu jadvalda simvolning tartib raqami uchun ma’lum joy ajratiladi.

3-qadam. Jadvaldagi simvollarni o‘qish marshrutlarning biri bo‘yicha amalga oshiriladi. Marshrutlar sonining oshishi shifr kriptobardoshligini oshiradi. Marshrutlar ketma-ket tanlanadi yoki ularning navbatlanishi kalit yordamida beriladi.

4-qadam. Simvollarning shifrlangan ketma-ketligi belgalangan L uzunlikdagi bloklarga ajratiladi. L kattalik 1-qadamda dastlabki axborot bo‘linadigan bloklar uzunligidan farqlanishi mumkin.

Rasshifrovka qilish teskari tartibda amalga oshiriladi. Kalitga mos xolda marshrut tanlanadi va bu marshrutga binoan jadval to‘ldiriladi.

Jadvaldan simvollar element nomerlari kelishi tartibida o‘qiladi.

Misol. Dastlabki matn T_0= “O‘RIN ALMASHTIRISH USULI”ni shifrlash talab etilsin. Kalit va shifrlangan bloklar uzunligi mos xolda quyidagilarga teng:

K=<2,1,1>, L=4.

1-qadam. Dastlabki matn uchta blokka ajratiladi. B_1=O‘RIN_ALM>, B_2 =ASHTIRISH>, B_3=<USULI**>;

2-qadam. 2,1,1 marshrutli uchta matritsa to‘ldiriladi;

3-qadam. Marshruttlarga binoan simvollarni joy-joyiga qo‘yish orqali shifrmatnni xosil qilish.

T_1=<NMLIURA_TISHARI_SHTOEMDI**>

4-qadam. Shifrmatnni bloklarga ajratish.

T_1=NMLI O‘RA_ TISHA RI_SH TOEM DI**>

Dastlabki axborot blokining parallel ikkili kodi (masalan, ikki bayt) sxemaga beriladi. Ichki kommutatsiya xisobiga sxemada bitlarning bloklardagi o‘rinlari almashtiriladi. Rasshifrovka qilish uchun esa sxemaning kirish va chiqish yo‘llari o‘zaro almashtiriladi.

O‘rin almashtirish usullarining amalga oshirilishi sodda bo‘lsada, ular ikkita jiddiy kamchiliklarga ega. Birinchidan, bu usullarni statistik ishlash orqali fosh qilish mumkin. Ikkinchidan, agar dastlabki matn uzunligi E simvollardan tashkil topgan bloklarga ajratilsa, shifrni fosh etish uchun shifrlash tizimsiga

bittasidan boshqa barcha simvollari bir xil bo‘lgan test axborotining E-1 blokini yuborish kifoya.

Shifrlashning additiv usullari. Shifrlashning additiv usullariga binoan dastlabki axborot simvollariga mos keluvchi raqam kodlarini ketma-ketligi gamma deb ataluvchi qandaydir simvollar ketma-ketligiga mos keluvchi kodlar ketma-ketligi bilan ketma-ket jamlanadi. Shu sababli, shifrlashinng additiv usullari gammalash deb xam ataladi.

Ushbu usullar uchun kalit sifatida gamma ishlatiladi. Additiv usulning kriptobardoshligi kalit uzunligiga va uning statistik xarakteristikalarining tekisligiga bogliq. Agar kalit shifrlanuvchi simvollar ketma-ketligidan qisqa bo‘lsa, shifrmatn kriptoanalitik tomonidan statistik usullar yordamida rasshifrovka qilishnishi mumkin. Kalit va dastlabki axborot uzunliklari qanchalik farqlansa, shifr-matnga muvaffaqiyatli xujum extimolligi shunchalik ortadi. Agar kalit uzunligi shifrlanuvchi axborot uzunligidan katta bo‘lgan tasodifiy sonlarning davriy bo‘lmagan ketma-ketligidan iborat bo‘lsa, kalitni bilmasdan turib shifrmatnni rasshifrovka qilish amaliy jixatdan mumkin emas. Almashtirish usullaridagidek gammalashda kalit sifatida raqamlarning takrorlanmaydigan ketma-ketligi ishlatilishi mumkin.

Amaliyotda asosini psevdo tasodifiy sonlar generatorlari (datchiklari) tashkil etgan additiv usullar eng ko‘p tarqalgan va samarali xisoblanadi. Generator psevdotasodifiy sonlarning cheksiz ketma-ketligini shakllantirishda nisbatan qisqa uzunlikdagi dastlabki axborotdan foydalanadi.

Psevdotasodifiy sonlar ketma-ketligini shakllantirishda kongruent generatorlardan xam foydalaniladi. Bu sinf generatorlari sonlarning shunday psevdotasodifiy ketma-ketliklarini shakllantiradiki, ular uchun generatorlarning davriyligi va chiqish yo‘li ketma-ketliklarining tasodifiyligi kabi asosiy xarakteristkalarini qattiy matematik tarzda ifodalash mumkin.

Kongruent generatorlar ichida o‘zining soddaligi va samaraliligi bilan chiziqli generator ajralib turadi. Bu generator quyidagi munosabat bo‘yicha sonlarning psevdotasodifiy ketma-ketliklarini shakllantiradi.

$$T(i + l) = (a*T(i) + c)\text{mod}m;$$

bu erda a va c – o‘zgarmaslar, T(0) –to‘ldiruvchi (sabab bo‘luvchi) son sifatida tanlangan dastlabki kattalik.

Bunday datchikning takrorlanish davri a va c kattaliklariga bogliq m qiymati odatda 2^s ga teng qilib olinadi, bu erda s-EXMdagi so‘zning bitlardagi uzunligi. Shakllantiruvchi son ketma-ketliklarining takrorlanish davri s-tok, son va a (mod4)+l bo‘lgandagina maksimal bo‘ladi. Bunday generatorlarni apparat yoki programm vositalari orqali osongina yaratish mumkin.

Shifrlashning kombinatsiyalangan usullari. Qudratli kompyuterlar, tarmoq texnologiyalari va neyronli xisoblashlarning paydo bo‘lishi xozirgacha umuman fosh qilinmaydi deb xisoblangan kriptografik tizimlarni obro‘sizlantirilishiga sabab bo‘ldi. Bu esa o‘z navbatida yuqori bardoshlikka ega kriptografik tizimlarni yaratish ustida ishlashni taqozo etdi. Bunday kriptografik tizimlarni yaratish usullaridan biri shifrlash usullarini kombinatsiyalashdir. Quyida eng kam vaqt sarfida kripto-bardoshlikni jiddiy oshishini ta’minlovchi shifrlashning kombinatsiyalangan usuli ustida so‘z boradi. Shifrlashning ushbu

kombinatsiyalangan usuliga binoan ma’lumotlarni shifrlash ikki bosqichda amalga oshiriladi. Birinchi bosqichda ma’lumotlar standart usul (masalan, DES usul) yordamida shifrlansa, ikkinchi bosqichda shifrlangan ma’lumotlar maxsus usul bo‘yicha qayta shifrlanadi. Maxsus usul sifatida ma’lumotlar vektorini elementlari noldan farqli bo‘lgan son matritsasiga ko‘paytirishdan foydalanish mumkin.

Ochiq kalitli tizimlarini qo‘llash asosida qaytarilmas yoki bir tomonli funktsiyalardan foydalanish yotadi. Bunday funktsiyalar quyidagi xususiyatlarga ega. Ma’lumki x ma’lum bo‘lsa y=f(x) funktsiyani aniqlash oson. Ammo uning ma’lum qiymati bo‘yicha x ni aniqlash amaliy jixatdan mumkin emas. Kriptografiyada yashirin deb ataluvchi yo‘lga ega bo‘gan bir tomonli funktsiyalar ishlatiladi. z parametrli bunday funktsiyalar quyidagi xususiyatlarga ega. Ma’lum z uchun E_z va D_z algoritmlarini aniqlash mumkin. E_z algoritmi yordamida aniqlik soxasidagi barcha x uchun $f_z(x)$ funktsiyani osongina olish mumkin. Xuddi shu tariqa D_z algoritmi yordamida joiz qiymatlar soxasidagi barcha u uchun teskari funktsiya $x=f_1(y)$xam osongina aniqdanadi. Ayni vaqtda joiz qiymatlar soxasidagi barcha z va deyarli barcha, u uchun xatto E_z ma’lum bo‘lganida xam $F^1(y)$ni xisoblashlar yordamida topib bo‘lmaydi. Ochiq kalit sifatida u ishlatilsa, maxfiy kalit sifatida x ishlatiladi.

Ochiq kalitni ishlatib shifrlash amalga oshirilganda o‘zaro muloaqatda bo‘lgan sub’ektlar o‘rtasida maxfiy kalitni almashish zaruriyati yo‘qoladi. Bu esa o‘z navbatida uzatiluvchi axborotning kriptoximoyasini soddalashtiradi.

Ochiq kalitli kriptotizimlarni bir tomonli funktsiyalar ko‘rinishi bo‘yicha farqlash mumkin. Bularning ichida RSA, El-Gamal va Mak-Elis tizimlarini aloxida tilga olish o‘rinli. Xozirda eng samarali va keng tarqalgan ochiq kalitli shifrlash algoritmi sifatida RSA algoritmini ko‘rsatish mumkin. RSA nomi algoritm yaratuvchilari familiyalarining birinchi xarfidan olingan (Rivest, Shamir va Adleman).

Algoritm modul arifmetikasining darajaga ko‘tarish amalidan foydalanishga asoslangan. Algoritmni quyidagi qadamlar ketma-ketligi ko‘rinishida ifodalash mumkin.

1-qadam. Ikkita 200 dan katta bo‘lgan tub son p va q tanlanadi.

2-qadam. Kalitning ochiq tashkil etuvchisi n xosil qilinadi

$$n=p*q.$$

3-qadam. Quyidagi formula bo‘yicha Eyler funktsiyasi xisoblanadi:

$$f(p,q)=(p-l)(q-l).$$

Eyler funktsiyasi n bilan o‘zaro tub, 1 dan n gacha bo‘lgan butun musbat sonlar sonini ko‘rsatadi. O‘zaro tub sonlar deganda 1 dan boshqa birorta umumiy bo‘luvchisiga ega bo‘lmagan sonlar tushuniladi.

4-qadam. f(p,q) qiymati bilan o‘zaro tub bo‘lgan katta tub son d tanlab olinadi.

5-qadam. Quyidagi shartni qanoatlantiruvchi e soni aniqlanadi

$$e^{-d}=l(\mathrm{modf}(p,q)).$$

Bu shartga binoan e^{-d} ko‘paytmaning f(p,q) funktsiyaga bo‘lishdan qo‘lgan qoldiq 1ga teng. e soni ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi. Maxfiy kalit sifatida d va n sonlari ishlatiladi.

6-qadam. Dastlabki axborot uning fizik tabiatidan qat’iy nazar raqamli ikkili ko‘rinishda ifodalanadi. Bitlar ketma-ketligi L bit uzunlikdagi bloklarga ajratiladi, bu erda L-L>Log_2(n+l) shartini qanoatlantiruvchi eng kichik butun son. Xar bir blok [0, n-1] oraliqqa taalluqli butun musbat son kabi ko‘riladi. Shunday qilib, dastlabki axborot X(i), i=1i sonlarning ketma-ketligi orqali ifodalanadi. i ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

7-qadam. Shifrlangan axborot quyidagi formula bo‘yicha aniqlanuvchi Y(i) sonlarning ketma-ketligi ko‘rinishida olinadi:

$$Y(i) = (X(i))^e \ (modn).$$

Misol. <GAZ> so‘zini shifrlash va rasshifrovka qilish talab etilsin.
Dastlabki so‘zni shifrlash uchun quyidagi qadamlarni bajarish lozim.

1-qadam. P=3 va q=11 tanlab olinadi.

2-qadam. N=3*11 = 33 xisoblanadi.

3-qadam. Eyler funktsiyasi aniqdanadi.

$$f(p.q) = (3-1)-(11-1) = 20$$

4-qadam. O‘zaro tub son sifatida d=3 soni tanlab olinadi.

5-qadam. (e-3)-(mod20) = 1shartini qanoatlantiruvchi e soni tanlanadi. Aytaylik, e=7.

6-qadam. Dastlabki so‘zning alfavitdagi xarflar tartib raqami ketma-ketligiga mos son ekvivalenti aniqdanadi. A harfiga -1, G harfiga-4, Z harfiga -9. O‘zbek alfavitida 36 ta xarf ishlatilishi sababli ikkili kodda ifodalash uchun 6 ta ikkili xona kerak bo‘ladi. Dastlabki axborot ikkili kodda quyidagi ko‘rinishga ega bo‘ladi:

000100 000001 001001.

Blok uzunligi L butun sonlar ichidan Z>log_2(33+l) shartini qanoatlantiruvchi minimal son sifatida aniqdanadi. p =33 bo‘ganligi sababli L=6.

Demak, dastlabki matn X(i)<< 4,1,9 > ketma-ketlik ko‘rinishida ifodalanadi.

7-qadam. X(i) ketma-ketligi ochiq kalit {7,33} yordamida shifrlanadi:

$$Y(1) = (4^7)(mod33) = 16384(mod33) = 16$$

$$Y(2) = (l^7)(mod33) = l(mod33) = 1$$

$$Y(1) = (9^7)(mod33) = 4782969(mod33) = 15$$

Shifrlangan so‘z Y(i)=<16,1,15>

Shifrlangan so‘zni rasshifrovka qilish maxfiy kalit {3,33} yordamida bajariladi.:

$$Y(1) = (16^3)(mod33) = 4096(mod33) =$$
$$4\,Y(1) = (l^3)(mod33) = l(mod33) = 1$$
$$Y7(1) = (15^3)(mod33) = 3375(mod33) = 9$$

Dastlabki son ketma-ketligi rasshifrovka qilingan X(i)=<4,1,9> ko‘rinishida dastlabki matn <GAZ> bilan almashtiriladi.

Keltirilgan misolda xisoblashlarning soddaligani ta’minlash maqsadida mumkin bolg‘an kichik sonlardan foydalanildi.

El-Gamal tizimi chekli maydonlarda diskret logarifmlarning xisoblanish murakkabligiga asoslangan. RSA va El-Gamal tizimlarining asosiy kamchiliga sifatida modul arifmetikasidagi murakkab amallarning bajarilishi zaruriyatini ko‘rsatish mumkin. Bu o‘z navbatida aytarlicha xisoblash resurslarini talab qiladi.

Mak-Elis kriptotizimida xatoliklarni tuzatuvchi kodlar ishlatiladi. Bu tizim RSA tizimiga nisbatan tezroq amalga oshirilsada, jiddiy kamchilikka ega. Mak-Elis kriptotizimsida katta uzunlikdagi kalit ishlatiladi va olingan shifrmatn uzunligi dastlabki matn uzunligidan ikki marta katta bo‘ladi.

Barcha ochiq kalitli shifrlash usullari uchun NP-to‘liq, masalani (to‘liq saralash masalasi) echishga asoslangan kriptotaxlil usulidan boshqa usullarining yo‘uqligi qat’iy isbotlanmagan. Agar bunday masalalarni echuvchi samarali usullar paydo bo‘lsa, bunday xildagi kriptotizim obro‘sizlantiriladi.

Yuqorida ko‘rilgan shifrlash usullarining kriptobardoshligi kalit uzunligiga bo‘gliq bo‘lib bu uzunlik zamonaviy tizimlar uchun, loaqal, 90 bitdan katta bo‘lishi shart.

Elektron xujjatlarni auentifikatsiyalashdan maqsad ularni mumkin bo‘lgan jinoyatkorona xarakatlardan ximoyalashdir. Bunday xarakatlarga quyidagilar kiradi:

-faol ushlab qolish-tarmoqqa ulangan buzgunchi xujjatlarni (fayllarni) ushlab qoladi va uzgartiradi.

- maskarad-abonent S xujjatlarni abonent V ga abonent A nomidan yuboradi;

- renegatlik-abonent A abonent V ga xabar yuborgan bo‘lsada, yubormaganman deydi;

- almashtirish- abonent V xujjatni o‘zgartiradi, yoki yangisini shakillantiradi va uni abonent A dan olganman deydi;

- takrorlash-abonent A abonent V ga yuborgan xujjatni abonent S takrorlaydi.

Jinoyatkorona xarakatlarning bu turlari o‘z faoliyatida kompyuter axborot texnologiyalaridan foydalanuvchi bank va tijorat tuzilmalariga, davlat korxona va tashkilotlariga xususiy shaxslarga ancha-muncha zarar etkazishi mumkin.

Elektron raqamli imzo metodologiyasi xabar yaxlitligini va xabar muallifining xaqiqiyligini tekshirish muammosini samarali xal etishga imkon beradi. Elektron raqamli imzo telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. Raqamli imzo ishlashi bo‘yicha oddiy qo‘l yo‘zma imzoga o‘xshash bo‘lib, quyidagi afzalliklarga ega:

-imzo chekilgan matn imzo qo‘ygan shaxsga tegishli ekanligini tasdiqlaydi;

- bu shaxsga imzo chekilgan matnga bo‘gliq majburiyatlaridan tonish imkoniyatini bermaydi;

- imzo chekilgan matn yaxlitligini kafolatlaydi.

Elektron raqamli imzo-imzo chekiluvchi matn bilan birga uzatiluvchi qo‘shimcha raqamli xabarning nisbatan katta bo‘lmagan sonidir.

Elektron raqamli imzo asimmetrik shifrlarning qaytaruvchanligiga xamda xabar tarkibi, imzoning o‘zi va kalitlar juftining o‘zaro bogliqligiga asoslanadi. Bu elementlarning xatto birining o‘zgarishi raqamli imzoning xaqiqiyligini tasdiqlashga imkon bermaydi. Elektron raqamli imzo shifrlashning asimmetrik algoritmlari va xesh-funktsiyalari yordamida amalga oshiriladi.

Elektron raqamli imzo tizimining qo‘llanishida bir-biriga imzo chekilgan elektron xujjatlarni jo‘natuvchi abonent tarmog‘ining mavjudligi faraz qilinadi. Xar bir abonent uchun juft-maxfiy va ochiq kalit generatsiyalanadi. Maxfiy kalit abonentda sir saqlanadi va undan abonent elektron raqamli imzoni shakllantirishda foydalanadi.

Ochiq kalit boshqa barcha foydalanuvchilarga ma’lum bo‘lib, undan imzo chekilgan elektron xujjatni qabul qiluvchi elektron raqamli imzoni tekshirishda foydalanadi.

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

- raqamli imzoni shakllantirish muolajasi;
- raqamli imzoni tekshirish muolajasi.

Imzoni shakllantirish muolajasida xabar jo‘natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo‘natuvchining ochiq kalitidan foydalaniladi. Xar qanday kriptografik tizim krpitografik kalitlardan foydalanishga asoslangan. Kalit axboroti deganda axborot tarmoqdari va tizimlarida ishlatiluvchi barcha kalitlar majmui tushuniladi. Agar kalit axborotlarining etarlicha ishonchli boshqarilishi ta’minlanmasa, niyati buzuq odam unga ega bo‘lib olib tarmoq va tizimdagi barcha axborotdan xoxlaganicha foydalanishi mumkin. Kalitlarni boshqarish kalitlarni generatsiyalash, saqlash va taqsimlash kabi vazifalarni bajaradi. Kalitlarni taqsimlash kalitlarni boshqarish jarayonidagi eng ma’suliyatli jarayon xisoblanadi.

Simmetrik kriptotizimdan foydalanilganda axborot almashinuvida ishtirok etuvchi ikkala tomon avval maxfiy sessiya kaliti, ya’ni almashinuv jarayonida uzatiladigan barcha xabarlarni shifrlash kaliti bo‘yicha kelishishlari lozim. Bu kalitni boshqa barcha bilmasligi va uni vaqti-vaqti bilan jo‘natuvchi va qabul qiluvchiida bir vaqtda almashtirib turish lozim. Sessiya kaliti bo‘yicha kelishish jarayonini kalitlarni almashtirish yoki taqsimlash deb xam yuritiladi.

Asimmetrik kriptotizimda ikkita kalit ochiq va yo‘piq (maxfiy) kalit ishlatiladi. Ochiq kalitni oshkor etish mumkin, yopiq kalitni yashirish lozim. Xabar almashinuvida faqat ochiq kalitni uning xaqiqiyligini ta’minlagan xolda jo‘natish lozim.

Kalitlarni taqsimlashga quyidagi talablar qo‘yiladi:

-taqsimlashning operativligi va aniqligi;

-taqsimlanuvchi kalitlarning konfidentsialligi va yaxlitligi.

Kompyuter tarmoqlaridan foydalanuvchilar o‘rtasida kalitlarni taqsimlashning quyidagi asosiy usullaridan foydalaniladi.

1. Kalitlarni taqsimlovchi bitta yoki bir nechta markazlardan foydalanish.
2. Tarmo‘q foydalanuvchilari o‘rtasida kalitlarni to‘g‘ridan-to‘g‘ri almashish.

Birinchi usulning muammosi shundaki, kalitlarni taqsimlash markaziga kimga, qaysi kalitlar taqsimlanganligi ma’lum. Bu esa tarmoq bo‘yicha uzatilayotgan barcha xabarlarni o‘qishga imkon beradi. Bo‘lishi mumkin bolg‘an suiste’mollar tarmoq xavfsizligining jiddiy buzilishiga olib kelishi mumkin.

Ikkinchi usuldagi muammo-tarmoq sub’ektlarining xaqiqiy ekanligiga ishonch xosil qilishidir.

Kalitlarni taqsimlash masalasi quyidagilarni ta’minlovchi kalitlarni taqsimlash protokolini ko‘rishga keltiriladi:

- seans qatnashchilarining xaqiqiyligiga ikkala tomonning tasdigi;
- seans xaqqiqiyliganing tasdigi;
- kalitlar almashinuvida xabarlarning minimal sonidan foydalanish.

Birinchi usulga misol tariqasida Kerberos deb ataluvchi kalitlarni autentifikatsiyalash va taqsimlash tizimini ko’tsatish mumkin.

Ikkinchi usulga-tarmoq foydalanuvchilari o‘rtasida kalitlarni to'g‘ridan-to'g‘ri almashishga batafsil toxtalamiz.

Simmetrik kalitli kriptotizimdan foydalanilganda kriptografik ximoyalangan axborot almashinuvini istagan ikkala foydalanuvchi umumiy maxfiy kalitga ega bo‘lishlari lozim. Bu foydalanuvchilar umumiy kalitni aloqa kanali bo‘yicha xavfsiz almashishlari lozim. Agar foydalanuvchilar kalitni tez-tez o‘zgartirib tursalar kalitni etkazish jiddiy muammoga aylanadi.

Bu muammoni echish uchun quyidagi ikkita asosiy usul qo‘llaniladi:

1. Simmetrik kriptotizimning maxfiy kalitini ximoyalash uchun ochiq kalitli asimmetrik kriptotizimdan foydalanish
2. Diffi-Xellmanning kalitlarni ochiq taqsimlash tizimidan foydalanish.

Birinchi usul simmetrik va asimmetrik kalitli kombinatsiyalangan kriptotizim doirasida amalga oshiriladi. Bunday yondashishda simmetrik kriptotizim dastlabki ochiq matnni shifrlash va uzatishda ishlatilsa, ochiq kalitli asimmetrik kriptotizim faqat simmetrik kriptotizimning maxfiy kalitini shifrlash, uzatish va keyingi rasshifrovka qilishda ishlatiladi. Shifrlashning bunday kombinatsiyalangan (gibrid) usuli ochiq kalitli asimmetrik kriptotizimning yo‘qori maxfiyligi bilan maxfiy kalitli simmetrik kriptotizimning yoqori tezkorligining uygunlashishga olib keladi. Bunday yondashish ba’zida elektron raqamli konvert sxemasi deb yuritiladi.

Faraz qilaylik foydalanuvchi A xabar M ni foydalanuvchi V ga ximoyalangan uzatish uchun shifrlashning kombinatsiyalangan usulidan foydalanmoqchi. Unda foydalanuvchilarning xarakatlari quyidagicha bo‘ladi.

Foydalanuvchi A ning xarakatlari:

1. Simmetrik seans maxfiy kalit K_s ni yaratadi (masalan, tasodifiy tarzda generatsiyalaydi).
2. Xabar M ni simmetrik seans maxfiy kalit K_sm shifrlaydi.
3. Maxfiy seans kalit K_s ni foydalanuvchi (xabar qabul qiluvchii) Yaning ochiq kaliti K_vt shifrlaydi.
4. Foydalanuvchi V adresiga aloqaning ochiq kanali bo‘yicha shifrlangan xabar M ni shifrlangan seans kaliti K_s bilan birgalikda uzatadi.

Olingan elektron raqamli konvertni faqat qo‘nuniy qabul qiluvchi-foydalanuvchi V ochishi mumkin. Faqat shaxsiy maxfiy kalit k_v egasi bo‘lgan foydalanuvchi V maxfiy seans kaliti K_s ni to‘g‘ri rasshifrovka qilish va so‘ngra bu kalit yordamida olingan xabar M ni rasshifrovka qilishi va o‘qishi mumkin.

Raqamli konvert usulida simmetrik va asimmetrik kriptoalgoritmlarning kamchiliklari quyidagicha kompensatsiyalanadi:

- simmetrik kriptoalgoritm kalitlarini tarqatish muammosi bartaraf qilinadi, chunki xabarni shifrlovchi seans kaliti K_s ochiq kanal bo‘yicha shifrlangan ko‘rinishda uzatiladi, kalit K_3vi rasshifrovka qilishi uchun asimmetrik kriptoalgoritmdan foydalaniladi;
- bu xolda asimmetrik shifrlash tezkorligining sekinligi muammosi paydo bo‘lmaydi, chunki asimmetrik algoritm bo‘yicha faqat qisqa kalit K_s shifrlanadi, barcha ma’lumotlar esa tezkor simmetrik kriptoalgoritm bo‘yicha shifrlanadi.

Natijada tezkor shifrlash bilan birgalikda kalitlarning qulay taqsimlanishi amalga oshiriladi. Shifrlashning kombinatsiyalangan usulida simmetrik xam asimmetrik kriptotizimlarning kriptografik kalitlaridan foydalaniladi. Ravshanki, kriptotizimning xar bir turi uchun kalitlar uzunligini shunday tanlash lozimki, niyati buzuq odamga kombinatsiyalangan kriptotizim ximoyasining xar qanday mexanizmiga xujum qilish bir xil qiyinchilik tugdirsin. Axborot almashinuvida ishtirok etuvchi foydalanuvchilar A va V mustaqil ravishda uzlarining maxfiy kalitlarini k_A va k_v ni generatsiyalaydilar (k_A va k_v kalitlar foydalanuvchilar A va V lar sir saqlovchi tasodifiy katta butun sonlar).

So‘ngra foydalanuvchi A o‘zining maxfiy kaliti k_A asosida ochiq kalitni xisoblaydi:

$$K_A = g^K * (\mathrm{mod} N).$$

Bir vaqtning o‘zida foydalanuvchi V o‘zining maxfiy kaliti k_v asosida ochiq kalitni xisoblaydi:

$$K_B = g^{K'} (\mathrm{mod} N).$$

By erda N va g-katta butun oddiy sonlar. Arifmetik amallar N ng moduliga keltirish orqali bajariladi. N va g sonlarni sir saqlash shart emas, chunki odatda, bu qiymatlar tarmoq va tizimdan foydalanuvchilarning barchasi uchun umumiy xisoblanadi.

So‘ngra foydalanuvchilar A va V o‘zlarining ochiq kalitlarini ximoyalanmagan kanal orqali almashtiradilar va umumiy sessiya maxfiy kalitini (bo‘linuvchi sirni) xisoblashda ishlatadilar:

foydalanuvchi A: $K = \{K_B f\text{-}(\mathrm{mod}\#) = (g^k \rangle\rangle)^{kl} (\mathrm{mod} N)$,

foydalanuvchi V: $Yu = (K_A f\rangle (\mathrm{mod} N) = (g^k *)^k \rangle\rangle$
(modN), bunda K = Kg‘ chunki ($g^k * f^A = (g^{kA} f^B$ (modiV)

Shunday qilib, ushbu amallar natijasida ikkala maxfiy kalit k_A va k_v larning funktsiyasi bo‘lgan umumiy sessiya maxfiy kaliti xosil qilinadi.

Ochiq kalitlar K_A va K_v qiymatlarini ushlab qollgan niyati buzuq odam sessiya maxfiy kaliti K ni xisoblay olmaydi, chunki u maxfiy kalitlar k_A va k_v qiymatlarini bilmaydi. Bir tomonlama funktsiyaning ishlatilishi sababli ochiq kalitni xisoblash amali qaytarilmaydigan amal, ya'ni abonentning ochiq kaliti qiymati bo'yicha uning maxfiy kalitini xisoblash mumkin emas.

Diffi-Xellman usulining noyobligi shundan iboratki, abonentlar jufti tarmoq orqali ochiq kalitlarni uzatganlarida faqat o'zlariga ma'lum maxfiy sonni olish imkoniyatiga ega. So'ngra abonentlar uzatilayotgan axborotni ma'lum tekshirilgan usulni-olingan umumiy sessiya maxfiy kalitidan foydalangan xolda simmetrik shifrlashni ishlatib ximoyalashga kirishishlari mumkin.

Diffi-Xellman sxemasi ma'lumotlarni xar bir seansda yangi kalitlarda shifrlash imkonini beradi. Bu sirlarni disketlarda yoki boshqa eltuvchilarda saqlamaslikka imkon beradi, chunki bunday saqlash ularni raqiblar yoki niyati buzuq odamlar qo'liga tushib qo'lish extimolligini oshiradi.

Diffi-Xellman sxemasi uzatilayotgan ma'lumotlarning konfidentsialligini va autentligini (asliga to'g'riligini) kompleks himoyalash usulini xam amalga oshirish imkonini beradi.

Ma'lumotlar yaxlitligini va konfidentsialligini bir vaqtda himoyalash uchun shifrlash va elektron raqamli imzodan kompleks foydalanish maqsadga muvofiq hisoblanadi. Diffi-Xellman sxemasi ishlashining oraliq natijalaridan uzatilayotgan ma'lumotlarning yaxlitligini va konfidentsiallagini kompleks himoyalash usulini amalga oshirishda foydalanish mumkin. Xaqiqatan, ushbu algoritmga binoan foydalanuvchilar À va Â avval o'zlarining maxfiy kalitlari k_A va k_B ni generatsiyalaydilar va ochiq kalitlari $\hat{E}_A$ va $\hat{E}_B$ ni hisoblaydilar. So'ngra abonentlar À va Â bu oraliq natijalardan ma'lumotlarni simmetrik shifrlashda foydalanilishi mumkin bo'lgan umumiy bo'linuvchi maxfiy kaliti Ê ni bir vaqtda hisoblash uchun ishlatadi.

Mustaqil uchun savollar.

1. Ochiq kalitli tizimlarini qo'llash?
2. Monoalfafitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi?

Nazorat savolari.

1. Elektron raqamli imzo qandau bo'lishi mumkin?
2. RSA va El-Gamal tizimlari qandau bo'ladi?
3. Diffi-Xellman sxemasi?

III BOB. IDENTIFIKATSIYA VA AUTENTIFIKATSIYA

3.1. Identifikatsiya va autentifikatsiya tushunchasi

Tayanch ibora va tushunchalar: Identifikatsiya (Identification), autentifikatsiya (authentication), avtorizatsiya (authorization), ma’murlash (accounting), parol, sertifikatlar va raqamli imzolar .

Mavzuga oid asosiy muammolar: Identifikatsiya (Identification)-foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni. Autentifikatsiya (Authentication) – ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi.

Darsning maqsadi: Kompyuter tizimida ro‘yxatga olingan xar bir sub’ekt indentifikatsiyalovchi axborot bog‘liqligi va autentifikatsiya ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi haqida ma’lumot berish.

Kompyuter tizimida ro‘yxatga olingan har bir sub’ekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma’noda indentifikatsiyalovchi axborot bog‘liq.

Bu ushbu sub’ektga nom beruvchi son yoki simvollar satri bo‘lishi mumkin. Bu axborot sub’ekt indentifikatori deb yuritiladi. Agar foydalanuvchi tarmoqda ro‘yxatga olingan indentifikatorga ega bo‘lsa u legal (qonuniy), aks holda legal bo‘lmagan (noqonuniy) foydalanuvchi hisoblanadi. Kompyuter resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o‘tishi lozim.

Identifikatsiya (Identification)-foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan funktsiyadir. Foydalanuvchi tizimga uning so‘rovi bo‘yicha o‘zining identifikatorini bildiradi, tizim esa o‘zining ma’lumotlar bazasida uning borligini tekshiradi.

Autentifikatsiya (Authentication)–ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o‘zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o‘tqazishda tekshiruvchi taraf tekshiriluvchi tarafning xaqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi.Odatda foydalanuvchi tizimga o‘z xususidagi noyob, boshqalarga ma’lum bo‘lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya va autentifikatsiya sub’ektlarning (foydalanuvchilarning) haqiqiy ekanligini aniqlash va tekshirishning o‘zaro bog‘langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog‘liq. Sub’ektni identifikatsiyalash va autentifikatsiyalashdan so‘ng uni avtorizatsiyalash boshlanadi.

Avtorizatsiya (Authorization)–sub’ektga tizimda ma’lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya sub’ekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli ajrata olmasa bu tizimda axborotning

konfidentsialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma’murlash muolajasi uzviy bog‘langan.

Ma’murlash (Accounting)– foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik xodisalarini oshkor qilish, taxlillash va ularga mos reaktsiya ko‘rsatish uchun juda muhimdir.

O‘zining haqiqiyligini tasdiqlash uchun sub’ekt tizimga turli axborotni taqdim etadi. Bunday axborot turi “Autentifikatsiya faktori” deb yuritiladi. Autentifikatsiyalashning quyidagi uchta faktori farqlanadi:

- biror narsani bilish asosida. Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda “so‘rov javob” xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko‘rsatish mumkin;
- biror narsaga egaligi asosida. Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va touch memory qurilmalari;
- qandaydir daxlsiz xarakteristikalar asosida. Ushbu faktor o‘z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko‘zining rangdor pardasi va to‘r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. Bu faktorda kriptografik usullar va vositalar ishlatilmaydi. Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

Sub’ektning haqiqiyligini tasdiqlash autentifikatsiyaning uchta faktoridan biri yordamida amalga oshirilishi mumkin. Masalan, foydalanuvchini autentifikatsiyalash jarayonida undan parol yoki barmoq izlari so‘ralishi mumkin. Autentifikatsiya jarayonida faqat bitta faktor ishlatilsa, bunday autentifikatsiya bir faktorli deb yuritiladi.

Autentifikatsiya jarayonida bir necha faktor ishlatilsa, bunday autentifikatsiya ko‘p faktorli deb yuritiladi. Masalan, autentifikatsiya jarayonida foydalanuvchi smart-kartadan va qo‘shimcha paroldan (yoki PIN-koddan) foydalanishi lozim. Ikki faktorli va uch faktorli autentifikatsiya tushunchalari ham ishlatiladi.

NCSC-TG-017 xujjatda ko‘p faktorli autentifikatsiya turlari uchun 1, 2 xilli, 2,3 xilli va 1,2,3 xilli autentifikatsiya atamalari kiritilgan. 1,2 xilli autentifikatsiya (bir ikki xilli autentifikatsiya deb yuritiladi) masalan autentifikatsiyaning ikki faktori ishlatadi: birinchi (bir narsani bilish asosida) va ikkinchi (bir narsaga egaligi asosida).

1,2,3 xilli autentifikatsiya (bir ikki uch xilli autentifikatsiya deb yuritiladi) autentifikatsiyaning uchta faktorining kombinatsiyasini ishlatadi (bir narsa bilish asosida, bir narsaga egaligi asosida va qandaydir daxlsiz xarakteristikalar asosida).

Parol–foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan narsa. O‘zaro autentifikatsiya uchun foydalanuvchi va uning sherigi o‘rtasida parol almashinishi mumkin. Plastik karta va smart-karta egasini autentifikatsiyasida shaxsiy identifikatsiya nomeri PIN sinalgan usul hisoblanadi. PIN – kodning mahfiy qiymati faqat karta egasiga ma’lum bo‘lishi

shart.

Dinamik–(bir martalik) parol-bir marta ishlatilganidan so‘ng boshqa umuman ishlatilmaydigan parol. Amalda odatda doimiy parolga yoki tayanch iboroga asoslanuvchi muntazam o‘zgarib turuvchi qiymat ishlatiladi.

“So‘rov-javob” tizimi-taraflarning biri noyob va oldindan bilib bo‘lmaydigan “so‘rov” qiymatini ikkinchi tarafga jo‘natish orqali autentifikatsiyani boshlab beradi, ikkinchi taraf esa so‘rov va sir yordamida hisoblangan javobni jo‘natadi. Ikkala tarafga bitta sir ma’lum bo‘lgani sababli, birinchi taraf ikkinchi taraf javobini to‘g‘riligini tekshirishi mumkin.

Sertifikatlar va raqamli imzolar-agar autentifikatsiya uchun sertifikatlar ishlatilsa, bu sertifikatlarda raqamli imzoning ishlatilishi talab etiladi. Sertifikatlar foydalanuvchi tashkilotining mas’ul shaxsi, sertifikatlar serveri yoki tashqi ishonchli tashkilot tomonidan beriladi. Internet doirasida ochiq kalit sertifikatlarini tarqatish uchun ochiq kalitlarni boshqaruvchi qator tijorat infrastrukturalari PKI (Public Key Infrastrusture) paydo bo‘ldi. Foydalanuvchilar turli daraja sertifikatlarini olishlari mumkin.

Autentifikatsiya jaryonlarini xavfsizlikning ta’minlanish darajasi bo‘yicha ham turkumlash mumkin. Ushbu yondashishga binoan autentifikatsiya jarayonlari quyidagi turlarga bo‘linadi:

-parollar va raqamli sertifikatlardan foydalanuvchi autentifikatsiya;

-kriptografik usullar va vositalar asosidagi qatiy autentifikatsiya;

-nullik bilim bilan isbotlash xususiyatiga ega bo‘lgan autentifikatsiya jarayonlari (protokollari);

-foydalanuvchilarni biometrik autentifikatsiyasi.

Autentifikatsiya protokollariga bo‘ladigan asosiy xujumlar quyidagilar:

-maskarad (impersonation). Foydalanuvchi o‘zini boshqa shaxs deb ko‘rsatishga urinib, u shaxs tarafidan xarakatlarning imkoniyatlariga va imtiyozlariga ega bo‘lishni mo‘ljallaydi;

-autentifikatsiya almashinuvi tarafini almashtirib qo‘yish (interleaving attack). Niyati buzuq odam ushbu xujum mobaynida ikki taraf orasidagi autenfikatsion almashinish jarayonida trafikni modifikatsiyalash niyatida qatnashadi. Almashtirib qo‘yishning quyidagi xili mavjud: ikkita foydalanuvchi o‘rtasidagi autentifikatsiya muvaffaqiyatli o‘tib, ulanish o‘rnatilganidan so‘ng buzg‘unchi foydalanuvchilardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;

-takroriy uzatish (replay attack). Foydalanuvchilarning biri tomonidan autentifikatsiya ma’lumotlari takroran uzatiladi;

-uzatishni qaytarish (reflection attak). Oldingi xujum variantlaridan biri bo‘lib, xujum mobaynida niyati buzuq protokolning ushbu sessiya doirasida ushlab qolingan axborotni orqaga qaytaradi.

majburiy kechikish (forsed delay). Niyati buzuq qandaydir ma’lumotni ushlab qolib, biror vaqtdan so‘ng uzatadi.

-matn tanlashli xujum (chosen text attack). Niyati buzuq autentifikatsiya trafigini ushlab qolib, uzoq muddatli kriptografik kalitlar xususidagi axborotni olishga urinadi.

Yuqorida keltirilgan xujumlarni bartaraf qilish uchun autentifikatsiya protokollarini qurishda quyidagi usullardan foydalaniladi:

“so‘rov–javob”, vaqt belgilari, tasodifiy sonlar, indentifikatorlar, raqamli imzolar kabi mexanizmlardan foydalanish;

-autentifikatsiya natijasini foydalanuvchilarning tizim doirasidagi keyingi xarakatlariga bog‘lash. Bunday yondashishga misol tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyingi o‘zaro aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko‘rsatish mumkin;

-aloqaning o‘rnatilgan seansi doirasida autentifikatsiya muolajasini vaqti-vaqti bilan bajarib turish va hk.

Vaqtni belgilash mexanizmi har bir xabar uchun vaqtni qaydlashni ko‘zda tutadi. Bunda tarmoqning har bir foydalanuvchisi kelgan xabarning qanchalik eskirganini aniqlashi va uni qabul qilmaslik qaroriga kelishi mumkin, chunki u yolg‘on bo‘lishi mumkin. Vaqtni belgilashdan foydalanishda seansning xaqiqiy ekanligini tasdiqlash uchun kechikishning joiz vaqt oralig‘i muammosi paydo bo‘ladi. Chunki, “vaqt tamg‘asi”li xabar, umuman, bir laxzada uzatilishi mumkin emas. Undan tashqari, qabul qiluvchi va jo‘natuvchining soatlari mutlaqo sinxronlangan bo‘lishi mumkin emas.

Autentifikatsiya protokollarini taqqoslashda va tanlashda quyidagi xarakteristikalarni hisobga olish zarur:

-o‘zaro autentifikatsiyaning mavjudligi. Ushbu xususiyat autentifikatsion almashinuv taraflari o‘rtasida ikkiyoqlama autentifikatsiyaning zarurligini aks ettiradi;

-hisoblash samaradorligi. Protokolni bajarishda zarur bo‘lgan amallar soni;

-kommunikatsion samaradorlik. Ushbu xususiyat autentifikatsiyani bajarish uchun zarur bo‘lgan xabar soni va uzunligini aks ettiradi;

-uchinchi tarafning mavjudligi. Uchinchi tarafga misol tariqasida simmetrik kalitlarni taqsimlovchi ishonchli serverni yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko‘rsatish mumkin;

-xavfsizlik kafolati asosi. Misol sifatida nullik bilim bilan isbotlash xususiyatiga ega bo‘lgan protokollarni ko‘rsatish mumkin;

-sirni saqlash. Jiddiy kalitli axborotni saqlash usuli ko‘zda tutiladi.

Mustaqil uchun savollar.

1. Identifikatsiya va audentifikasiya nima?
2. Sertifikatlar va raqamli imzolar .

Nazorat savollari:

1. Identifikatsiya va autentifikatsiya tushunchasi.
2. Autentifikatsiya texnologiyasining turlarini tushuntirib bering.
3. Autentifikatsiya protokollariga bo‘ladigan xujumlarni tavsiflab bering.
4. Autentifikatsiya protokollarini tanlashda qo‘llaniladigan mezonlarni yoritib bering.

3.2. Parollar asosida autentifikatsiyalash.

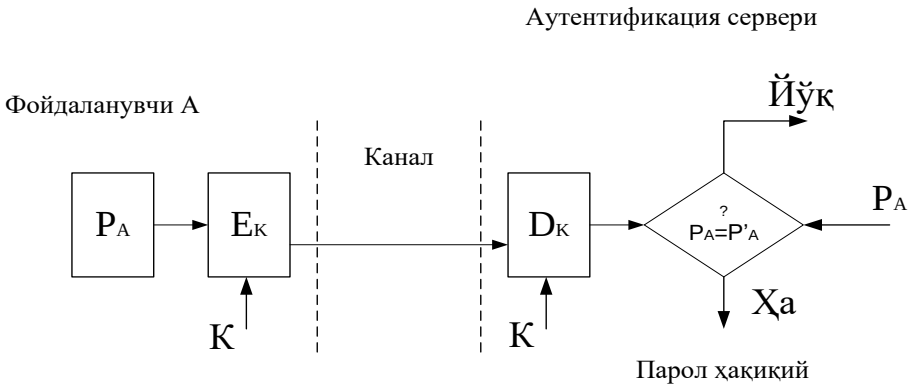
Tayanch ibora va tushunchalar: Bir martali parollarga asoslangan autentifikatsiyalash, ko‘p martali parollarga asoslangan oddiy autentifikatsiyalash sertifikatlar va raqamli imzolar.

Mavzuga oid asosiy muammolar: Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni qo‘llash, Masofadagi foydalanuvchi tarmoqdan foydalanish.

Darsning maqsadi: Parollar asosida autentifikatsiyalash, kompyuter tizimida ro’yxatga olingan xar bir sub’ekt indentifikatsiyalovchi axborot bog‘liq ligi va autentifikatsiya ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi haqida ma’lumot berish.

Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiyalash bo‘lib, u an’anaviy ko‘p martali parollarni ishlatishiga asoslangan. Tarmoqdagi foydalanuvchini oddiy autentifikatsiyalash muolajasini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan foydalanuvchi kompyuter klaviaturasida o‘zining identifikatori va parolini teradi. Bu ma’lumotlar autentifikatsiya serveriga ishlanish uchun tushadi. Autentifikatsiya serverida saqlanayotgan foydalanuvchi identifikatori bo‘yicha ma’lumotlar bazasidan mos yozuv topiladi, undan parolni topib foydalanuvchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikatsiya muvaffaqiyatli o‘tgan hisoblanadi va foydalanuvchi legal (qonuniy) maqomini va avtorizatsiya tizimi orqali uning maqomi uchun aniqlangan xuquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Ravshanki, foydalanuvchining parolini shifrlamasdan uzatish orqali autentifikatsiyalash varianti xavfsizlikning xatto minimal darajasini kafolatlamaydi. Parolni himoyalash uchun uni himoyalanmagan kanal orqali uzatishdan oldin shifrlash zarur. Buning uchun sxemaga shifrlash E_k va rasshifrovka qilish D_k vositalari kiritilgan. Bu vositalar bo‘linuvchi maxfiy kalit K orqali boshqariladi. Foydalanuvchining haqiqiyligini tekshirish foydalanuvchi yuborgan parol P_A bilan autentifikatsiya serverida saqlanuvchi dastlabki qiymat P'_A ni taqqoslashga asoslangan. Agar P_A va P'_A qiymatlar mos kelsa, parol P_A haqiqiy, foydalanuvchi A esa qonuniy hisoblanadi. Quyida paroldan foydalangan holda oddiy autentifikatsiyalash sxemasi keltirilgan.



Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul–foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir.

Bunda fayllarga o‘qish va yozishdan himoyalash atributlari o‘rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ro’yxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi– niyati buzuqning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

Ko‘p martali parollarga asoslangan oddiy autentifikatsiyalash tizimining bardoshligi past, chunki ularda autentifikatsiyalovchi axborot ma’noli so‘zlarning nisbatan katta bo‘lmagan to‘plamidan jamlanadi. Ko‘p martali parollarning ta’sir muddati tashkilotning xavfsizligi siyosatida belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular lug‘atda bo‘lmasin va ularni topish qiyin bo‘lsin.

Bir martali parollarga asoslangan autentifikatsiyalashda foydalanishga har bir so‘rov uchun turli parollar ishlatiladi. Bir martali dinamik parol faqat tizimdan bir marta foydalanishga yaroqli. Agar, hatto kimdir uni ushlab qolsa ham parol foyda bermaydi. Odatda bir martali parollarga asoslangan autentfikatsiyalash tizimi masofadagi foydalanuvchilarni tekshirishda qo‘llaniladi.

Bir martali parollarni generatsiyalash apparat yoki dasturiy usul oqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to‘lov plastik kartochkalariga o‘xshash mikroprotsessor o‘rnatilgan miniatyur qurilmalar ko‘rinishda amalga oshiradi. Odatda kalitlar deb ataluvchi bunday kartalar klaviaturaga va katta bo‘lmagan displey darchasiga ega.

Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni qo‘llashning quyidagi usullari ma’lum:

1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.
2. Legal foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro'yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish.
3. Foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

Birinchi usulni amalga oshirish misoli sifatida SecurID autentikatsiyalash texnologiyasini ko‘rsatish mumkin. Bu texnologiya SecurityDynamics kompaniyasi tomonidan ishlab chiqilgan bo‘lib, qator kompaniyalarning, xususan CiscoSystems kompaniyasining serverlarida amalga oshirilgan.

Vaqt sinxronizatsiyasidan foydalanib autentifikatsiyalash sxemasi tasodifiy sonlarni vaqtning ma’lum oralig‘idan so‘ng generatsiyalash algoritmiga asoslangan. Autentifikatsiya sxemasi quyidagi ikkita parametrdan foydalanadi:

- har bir foydalanuvchiga atalgan va autentifikatsiya serverida hamda foydalanuvchining apparat kalitida saqlanuvchi noyob 64-bitli sondan iborat maxfiy kalit;
- joriy vaqt qiymati.

Masofadagi foydalanuvchi tarmoqdan foydalanishga uringanida undan shaxsiy identifikatsiya nomeri PINni kiritish taklif etiladi. PIN to‘rtta o‘nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server foydalanuvchi tomonidan kiritilgan PIN-koddan foydalanib ma’lumotlar bazasidagi foydalanuvchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni generatsiyalash algoritmini bajaradi. So‘ngra server generatsiyalangan son bilan foydalanuvchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server foydalanuvchiga tizimdan foydalanishga ruxsat beradi.

Autentifikatsiyaning bu sxemasidan foydalanishda apparat kalit va serverning qat’iy vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda SecurityDynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

- apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me’yoridan chetlashishi aniq o‘lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;
- server muayyan apparat kalit generatsiyalagan kodlarni kuzatadi va zaruriyat tug‘ilganida ushbu kalitga moslashadi.

Autentifikatsiyaning bu sxemasi bilan yana bir muammo bog‘liq. Apparat kalit generatsiyalagan tasodifiy son katta bo‘lmagan vaqt oralig‘i mobaynida haqiqiy parol hisoblanadi. Shu sababli, umuman, qisqa muddatli vaziyat sodir bo‘lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

Bir martali paroldan foydalanib autentifikatsiyalashni amalga oshiruvchi yana bir variant "so‘rov-javob" sxemasi bo‘yicha autentifikatsiyalash. Foydalanuvchi tarmoqdan foydalanishga uringanida server unga tasodifiy son ko‘rinishidagi so‘rovni uzatadi. Foydalanuvchining apparat kaliti bu tasodifiy sonni, masalan DES algoritmi va foydalanuvchining apparat kaliti xotirasida va serverning ma’lumotlar bazasida saqlanuvchi maxfiy kaliti yordamida rasshifrovka qiladi. Tasodifiy son-so‘rov shifrlangan ko‘rinishda serverga qaytariladi. Server ham o‘z navbatida o‘sha DES algoritmi va serverning ma’lumotlar bazasidan olingan foydalanuvchining maxfiy kaliti yordamida o‘zi generatsiyalagan tasodifiy sonni shifrlaydi. So‘ngra server shifrlash natijasini apparat kalitidan kelgan son bilan taqqoslaydi. Bu sonlar mos kelganida foydalanuvchi tarmoqdan foydalanishga ruxsat oladi. Ta’kidlash lozimki, "so‘rov-javob" autentifikatsiyalash sxemasi ishlatishda vaqt sinxronizatsiyasidan foydalanuvchi autentifikatsiya sxemasiga qaraganda murakkabroq.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

- o‘zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;
- bir tomonlama funktsiyaga asoslangan parollar ketma-ketligi. Ushbu usulning mohiyatini bir tomonlama funktsiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o‘zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

Keng tarqalgan bir martali paroldan foydalanishga asoslangan autentifikatsiyalash protokollaridan biri Internet da standartlashtirilgan S/Key (RFC1760) protokolidir. Ushbu protokol masofadagi foydalanuvchilarning haqiqiyligini tekshirishni talab etuvchi ko‘pgina tizimlarda, xususan, Cisco kompaniyasining TACACSQ tizimida amalga oshirilgan.

Mustaqil uchun savollar.

1. Bir martali parollarga asoslangan autentifikasiyalsh.
2. Ko‘p martali porollarga asoslangan oddiy audentiffikasiyalsh.

Nazorat savollari:

1. Ko‘p martali parollarga asoslangan autentifikatsiya texnologiyasi.
2. Bir martali parollarga asoslangan autentifikatsiya texnologiyasi.

3.3. Sertifikatlar asosida autentifikatsiyalash.

Tayanch ibora va tushunchalar: Raqamli sertifikatlar ishlatiladigan computer tarmogi, sertifikatning electron shakli, ochiq kalitli sertifikatlar, sertifikatlar asosida audentifikasiyalash.

Mavzuga oid asosiy muammolar: Tarmoqda foydalanuvchilar soni parollarning tayinlashi va saqlanishi, raqamli sertifikatlar, foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar.

Darsning maqsadi: Raqamli sertifikatlar ishlatilganda computer tarmog‘i foydalanuvchilar xususida maxfiy axborotni, maxviy kalitni saqlash vazifasi foydalanuvchilarning o‘ziga yuklanishi haqida ma’lumot berish.

Tarmoqdan foydalanuvchilar soni millionlab o‘lchanganida parollarning tayinlanishi va saqlanishi bilan bog‘liq foydalanuvchilarni dastlabki ro’yxatga olish muolajasi juda katta va amalga oshirilishi qiyin bo‘ladi. Bunday sharoitda raqamli sertifikatlar asosidagi autentifikatsiyalash parollar qo‘llanishiga ratsional alternativa hisoblanadi.

Raqamli sertifikatlar ishlatilganida kompyuter tarmog‘i foydalanuvchilar xususidagi hech qanday axborotni saqlamaydi. Bunday axborotni foydalanuvchilarning o‘zi so‘rov-sertifikatlarida taqdim etadilar. Bunda maxfiy axborotni, xususan maxfiy kalitlarni saqlash vazifasi foydalanuvchilarning o‘ziga yuklanadi.

Foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar foydalanuvchilar so‘rovi bo‘yicha maxsus vakolatli tashkilot-sertifikatsiya markazi CA (CertificateAuthority) tomonidan, ma’lum shartlar bajarilganida beriladi. Ta’kidlash lozimki, sertifikat olish muolajasining o‘zi ham foydalanuvchining haqiqiyligini tekshirish (ya’ni, autentifikatsiyalash) bosqichini o‘z ichiga oladi.

Bunda tekshiruvchi taraf sertifikatsiyalovchi tashkilot (sertifikatsiya markazi SA) bo‘ladi.

Sertifikat olish uchun mijoz sertifikatsiya markaziga shaxsini tasdiqlovchi ma’lumotni va ochiq kalitini taqdim etishi lozim. Zaruriy ma’lumotlar ro‘yxati olinadigan sertifikat turiga bog‘liq. Sertifikatsiyalovchi tashkilot foydalanuvchining haqiqiyligi tasdig‘ini tekshirganidan so‘ng o‘zining raqamli imzosini ochiq kalit va foydalanuvchi xususidagi ma’lumot bo‘lgan faylga joylashtiradi hamda ushbu ochiq kalitning muayyan shaxsga tegishli ekanligini tasdiqlagan holda foydalanuvchiga sertifikat beradi.

Sertifikat elektron shakl bo‘lib, tarkibida qo‘yidagi axborot bo‘ladi:

- ushbu sertifikat egasining ochiq kaliti;
- sertifikat egasi xususidagi ma’lumot, masalan, ismi, elektron pochta adresi, ishlaydigan tashkilot nomi va h.;
- ushbu sertifikatni bergan tashkilot nomi;
- sertifikatsiyalovchi tashkilotning elektron imzosi–ushbu tashkilotning maxfiy kaliti yordamida shifrlangan sertifikatsiyadagi ma’lumotlar.

Sertifikat foydalanuvchini tarmoq resurslariga murojaat etganida autentifikatsiyalovchi vosita hisoblanadi. Bunda tekshiruvchi taraf vazifasini korporativ tarmoqning autentifikatsiya serveri bajaradi. Sertifikatlar nafaqat autentifikatsiyalashda, balki foydalanishning ma’lum xuquqlarini taqdim etishda ishlatilishi mumkin. Buning uchun sertifikatga qo‘shimcha hoshiyalar kiritilib ularda sertifikatsiya egasining foydalanuvchilarning u yoki bu kategoriyasiga mansubligi ko‘rsatiladi.

Ochiq kalitlarning sertifikatlar bilan uzviy bog‘liqligini alohida ta’kidlash lozim. Sertifikat nafaqat shaxsni, balki ochiq kalit mansubligini tasdiqlovchi xujjatdir. Raqamli sertifikat ochiq kalit va uning egasi o‘rtasidagi moslikni o‘rnatadi va kafolatlaydi. Bu ochiq kalitni almashtirish xavfini bartaraf etadi.

Agar abonent axborot almashinuvi bo‘yicha sherigidan sertifikat tarkibidagi ochiq kalitni olsa, u bu sertifikatdagi sertifikatsiya markazining raqamli imzosini ushbu sertifikatsiya markazining ochiq kaliti yordamida tekshirish va ochiq kalit adresi va boshqa ma’lumotlari sertifikatda ko‘rsatilgan foydalanuvchiga tegishli ekanligiga ishonch hosil qilishi mumkin. Sertifikatlardan foydalanilganda foydalanuvchilar ro’yxatini ularning parollari bilan korporatsiya serverlarida saqlash zaruriyati yo‘qoladi. Serverda sertifikatsiyalovchi tashkilotlarning nomlari va ochiq kalitlarining bo‘lishi etarli.

Sertifikatlarning ishlatilishi sertifikatsiyalovchi tashkilotlarning nisbatan kamligiga va ularning ochiq kalitlaridan qiziqqan barcha shaxslar va tashkilotlar foydalana olishi (masalan, jurnallardagi nashrlar yordamida) taxminiga asoslangan.

Sertifikatlar asosida autentifikatsiyalash jarayonini amalga oshirishda sertifikatsiyalovchi tashkilot vazifasini kim bajarishi xususidagi masalani echish muhim hisoblanadi. Xodimlarni sertifikat bilan ta’minlash masalasini korxonaning o‘zi echishi juda tabiiy hisoblanadi. Korxona o‘zining xodimlarini yaxshi biladi va ular shaxsini tasdiqlash vazifasini o‘ziga olishi mumkin. Bu sertifikat berilishidagi dastlabki autentifikatsiyalash muolajasini osonlashtiradi. Korxonalar sertifikatlarni generatsiyalash, berish va ularga xizmat ko‘rsatish

jarayonlarini avtomatlashtirishni ta’minlovchi mavjud dasturiy maxsulotlardan foydalanishlari mumkin. Masalan, Netscape Communications kompaniyasi serverlarini korxonalarga shaxsiy sertifikatlarini chiqarish uchun taklif etadi.

Sertifikatsiyalovchi tashkilot vazifasini bajarishda tijorat asosida sertifikat berish bo‘yicha mustaqil markazlar ham jalb etilishi mumkin. Bunday xizmatlarni, xusu san, Verisign kompaniyasining sertifikatsiyalovchi markazi taklif etadi. Bu kompaniyaning sertifikatlari halqaro standart X.509 talablariga javob beradi. Bu sertifikatlar ma’lumotlar himoyasining qator maxsulotlarida, jumladan himoyalangan kanal SSL protokolida ishlatiladi.

Mustaqil ish savollari.

1. Bir martali paroldan foydalangan holda oddiy autentifikasiyalsh.
2. Ko‘p martali paroldan foydalangan holda oddiy autentifikasiyalsh

Nazorat savollari:

1. Elektron sertifikatlar tarkibiga qanday axborotlarni oladi?
2. Elektron sertifikatlarni afzalliklari va kamchiliklari.
3. Elektron sertifikatlar qaysi asosiy halqaro standart talablariga javob berishi lozim.

3.4. Kalitlarni generatsiya qilish. Shifrlash kalitlari uzunligiga bo'lgan talablar.

Tayanch ibora va tushunchalar: Shifrlash algoritmi, kalitlar, simmetrik shifrlash tizimlari, ochiq kalitli kriptotizimlar, kalitlarni generasiya qilish**,** kalitlarni saqlash, kalitlarni tarqatish, kalitlarni almashtirish, kalitlarni yo'q qilib tashlash.

Mavzuga oid asosiy muammolar: Axborotlarni kritografik himoyalashda kalitlarga katta e'tibor berishda ochiq kalitli kriptotizimlarda shifrlash kalitlari ochiq bo'ladi sshifirlash algoritimlarini mustahkamligi kalitlarni bardoshligi qanday aniqlanishiga izoh berib o'ting.

Darsning maqsadi: Ochiq kalitli kriptotizimlarda shifrlash kalitlari ochiq bo'ladi, foydalanuvchi paroli asosida seansli kalitlarni generasiya qilinishini bayon qilish.

Axborotlarni kritografik himoyalashda kalitlarga katta e'tibor beriladi. Odatda shifrlash algoritmlari ma'lum deb faraz qilinadi. Demak, shifrni mustahkamligi kalitlarni bardoshligi bilan aniqlanadi. Simmetrik shifrlash tizimlarida va ularga asoslangan protokollarda shifrlashda va dastlabki matnga o'girishda ham kriptobardoshlik kalitning bardoshligiga bog'liq.

Ochiq kalitli kriptotizimlarda shifrlash kalitlari ochiq bo'ladi. Shu sababli ushbu turdagi kriptotizimlarning bardoshligi dastlabki matnga o'girish kalitlarini bardoshligi bilan to'liq xarakterlanadi.

Kalitlarni bosqarish masalasi kalitlarni hayotiyligi bilan bog'liq bo'lgan quyidagi jarayonlarni to'g'ri amalga oshirish bilan bog'liq:

- kalitlarni generasiya qilish;

- kalitlarni saqlash;
- kalitlarni tarqatish;
- kalitlarni almashtirish;
- kalitlarni yo'q qilib tashlash.

Shifrlash kalitlari uzunligi. Odatda kalitlarni bardoshligi kalitlarni bo'lishi mumkin bo'lgan barcha variantlarini hisoblash uchun sarf bo'ladigan vaqt va zarur bo'ladigan hisoblash texnikasi resurslari bilan baholanadi.

Simmetrik blokli shifrlarda kalitlarni aniqlash uchun kriptoanalitikka bir nyecha shifrmatn bloklari va unga mos keluvchi ochiq matn bloklari zarur bo'ladi. Agar kalit 8 bitdan iborat bo'lsa, u holda 8 bitli kalitlarni bo'lishi mumkin bo'lgan barcha variantlari soni 2^8 ga teng, ya'ni 256 ta 8 bitli kalitlar ichidan aynan zarur bo'lgan kalitni saralash lozim. Ushbu holda saralashni yarmini bajargandan so'ng 50% ehtimollik bilan zarur kalitni topish mumkin.

Agar kalit uzunligi 56 bit bo'lsa, u holda kalitlarni bo'lishi mumkin bo'lgan barcha variantlari soni 2^{56} ga teng. Sekundiga million kalitni tekshiruvchi kompyuterdan foydalanilsa, zarur bo'lgan kalitni aniqlash uchun o'rtacha 2285 yil kerak bo'ladi.

Shuningdek, agar kalit uzunligi 64 bit bo'lsa, u holda kalitlarni bo'lishi mumkin bo'lgan barcha variantlari soni 2^{64} ta kalitni ichidan zarur bo'lgan kalitni aniqlash uchun superkompyuterga 585000 yilga yaqin vaqt kerak bo'ladi.

Ko'rinib turibdiki, kalitlarni aniqlashda hisoblashlarda zarur bo'ladigan hisoblash texnikasi resurslari, aniqrog'i, ularga sarf bo'ladigan xarajatlat ham muhim o'rin egallaydi.

Agar buzg'unchi kalitni sindirishni juda xohlasa, u holda u mablag' sarflashiga to'g'ri keladi. Shu bois, kalitni “minimal” bahosini aniqlash lozim bo'ladi: kalitni ochish iqtisodiy manfaatli bo'lishi uchun kalitni ochishda qanday narx atrofidagi xarajatdan foydalanishni bilish kerak bo'ladi. Bundan tashqari ko'pgina xabarlarning narxi vaqt o'tishi bilan tez arzonlashadi.

Hozirgi vaqtda simmetrik kriptotizimlar uchun uzunligi 80 bitdan kam bo'lmagan va asimmetrik kriptotizimlar uchun uzunligi 768 bitdan kam bo'lmagan kalitlarni ishonchli deb hisoblash qabul qilingan. Albatta, bunday baholash shartli baholashdir. Bu yerda asosan kalitlarni bo'lishi mumkin bo'lgan barcha variantlari ichidan zarur bo'lgan kalitni aniqlash imkoniyati hisobga olingan.

Quyidagi jadvalda kalitlarni bo'lishi mumkin bo'lgan barcha variantlari usuliga nisbatan bir xil bardoshlilikka ega bo'lgan simmetrik va asimmetrik kriptotizimlar kalitlarining bitlari uzunligi haqida ma'lumotlar keltirilgan.

Simmetrik kalit uzunligi (bitlarda)	Asimmetrik kalit uzunligi (bitlarda)
56	384
64	512
80	768

112	1792
128	2304

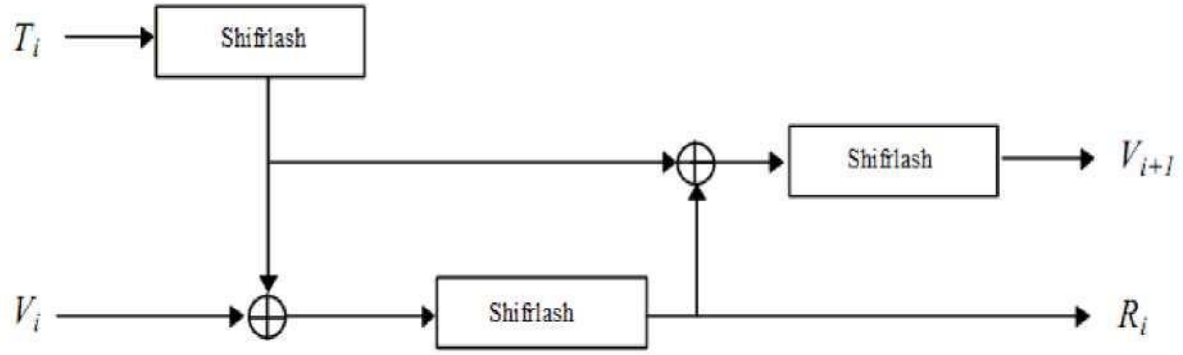
Seansli kalitlarni generasiya qilish.

Foydalanuvchi paroli asosida seansli kalitlarni generasiya qilish. Seansli kalitlarni yaratishning keng tarqalgan usullaridan biri foydalanuvchi paroli asosida kalitlarni generasiya qilishdir. Foydalanuvchi paroli ustida kriptografik almashtirishlar bajariladi. Natija kalit sifatida qabul qilinadi. Keynichalik ushbu kalitni foydalanuvchi tarmoq trafigini shifrlash uchun ishlatilishi mumkin.

Ushbu usulning yutug'i Shundan iboratki, maxfiy kalitlarni saqlashga zarurat bo'lmaydi. Maxfiy kalitni yaratishda foydalanilgan parolni foydalanuvchi eslab yurishi yetarli.

Usulning kamchiligi Shundaki, ushbu holatda raqibda lug'at yordamida hujum tashkil qilish imkoniyati paydo bo'ladi. Mazkur hujumning mohiyati eng katta ehtimolli so'zlarni saralash yo'li bilan raqib foydalanuvchi parolini aniqlashi mumkin. Chunki, parolni tanlashda ko'p hollarda esda oson saqlanishi mumkin bo'lgan so'zlardan yoki belgilar naboridan foydalaniladi.

Seansli kalitlarni generasiya qilishning X9.17 standarti. ANSI X9.17 standarti kalitlarni generasiya qilish usullarini aniqlaydi (3.4.1-rasm). Ushbu standart oson esda saqlanib qoladigan kalitlarni emas, balki seansli kalitlarni yoki psevdotasodifiy sonlarni generasiya qilishga mo'ljallangan. Kalitlarni generasiya qilishda DES kriptografik algoritmidan foydalaniladi, ammo uni o'rniga boshqa algoritmdan ham foydalanish mumkin.



3.4.1-rasm. ANSI X9.17 standarti bo'yicha kalitlarni generasiya qilish.

Faraz qilaylik, EK(X) bu maxfiy kalitlarni generasiya qilish uchun qo'llaniladigan, generasiya qilingan *K* kalit orqali DES kriptografik algoritmidan foydalanib *X* matnni shifrlash bo'lsin. V_0 - 64 bitli boshlang'ich ketma-ketlik, T - vaqt nishoni bo'lsin. Tasodifiy *Ri* kalitni generasiya qilishni quyidagicha bajarish mumkin:

$$Ri= E_K(E_K(T) F Vi.$$

Vi+1 ni generasiya qilish :

$$Vi+1= ErtEKTFR$$

Ri ni DES kalitiga aylantirish uchun, undagi har bir sakkizinchi bitni o'chirish orqali erishish mumkin. Agar 64 bitli kalit kerak bo'ladigan bo'lsa, u holda Ri ni o'zgartirmasdan foydalanish mumkin. Agar 128 bitli kalit kerak bo'ladigan bo'lsa, u holda bir jo'ft 64 bitli kalitlar yaratish va ularni birlashtirish lozim bo'ladi.

X9.17 standartiga asosan kalitlar 2 xil bo'ladi: kalitlarni shifrlash kalitlari va ma'lumotlarni shifrlash kalitlari. Kalitlarni shifrlash kalitlari yordamida kalitlarni tarqatish vaqtida boshqa kalitlar shifrlanadi. Simmetrik shifrlash algoritmlari uchun kalitli axboratlarni generasiya qilish. Kriptografik algoritmlardan foydalanishda eng murakkab masalalardan biri kalitlarni generasiya qilishdir. Bu holatda asosiy muammo yaratilayotgan kalitlarda ma'lum bir kriptografik xususiyatlarni mujassamlashtirishdir. Kalitlarni generasiya qilishning 2 xil usuli mavjud: determinallashgan va nodeterminallashgan. Determinallashgan usul. Ushbu usullarning mohiuati kichik uzunlikdagi tasodifiy ketma-ketliklardan statistik xususiyatlari bo'yicha dastlabki ketma-ketliklardan uncha farq qilmaydigan katta uzunlikdagi psevdotasodifiy ketma-ketliklarni shakllantirishdan iborat.

Psevdotasodifiy ketma-ketliklarni shakllantirishning eng keng tarqalgan usullaridan biri chiziqli teskari bog'lanishli siljitish registrlaridan foydalanish. Ular chiziqli rekurrent ketma-ketliklar vositasida ifodalanib, ulardan har doim ham psevdotasodifiy kalitlar ketma-ketligi generatori sifatida foydalanish mumkin emas. Shu sababli psevdotasodifiy xarakterga va fizikaviy tabiat (muskullarning harakati, kirish/chiqish qurilmalari bilan ishlashda foydalanuvchining ularga murojaat qilish vaqti) ga ega bo'lgan jarayonlardan foydalanish keng tarqalmoqda. Ixtiyoriy holatda ham kalitlarni generasiya qilishda quyidagilarga e'tibor qilish maqsadga muvofiq: k belgidan tashkil topgan ketma-ketlik (*k*-gramma) ni paydo bolish chastotasini /-kvadrat mezoniga tekshirish; natijalar chastotasini umumlashgan /-kvadrat mezoniga tekshirish; markirovka qilishning minimal va maksimal qiymatlarini tekshirish; ustma-ust tushmaslik oraliqlari uzunliklarini berilgan diapazon bilan solishtirish; monotonlikka tekshirish. Nodeterminallashgan usul. Natijalari keyinchalik kalitlarni generasiya qilishda qo'llaniladigan tasodifiy fizik jarayonlar ushbu usullar asosini tashkil qiladi. Tasodifiy natijalar hosil qilishga oddiy misol sifatida o'yin suyaklari yoki tangani tashlashni ko'rsatish mumkin. Kichik unumdorligi sababli amaliyotda ulardan foydalanish maqsadga muvofiq bo'lmasada, nazariy jihatdan ular kalitlar ketma-ketligi generatori sifatida xizmat qilishi mumkin.

Hozirgi vaqtda chiquvchi ketma-ketliklari tasodifiy tarqalgan fizikaviy shovqin generatorlari (masalan, shovqin soluvchi diodlar, impulsli generatorlar, Geyger hisoblagichlari) keng qo'llanilmoqda. Ushbu asbob yoki qurilmalardan olingan signallar raqamlashtiriladi. Ular keyinchalik oqimli shifratorlarda 2 modul bo'yicha qo'shish yoki kalitlarni shakllantirishda boshlang'ich ketma-ketlik sifatida xizmat qilishi uchun ikkilik ko'rinishidagi ketma-ketliklar sifatida ifodalanadi.

Asimmetrik (ochiq kalitli) shifrlash algoritmlari uchun kalitli axboratlarni generasiya qilish. Ochiq kalitli shifrlash algoritmlari uchun kalitli axboratlarni generasiya qilish simmetrik kriptotizimlarga nisbatan juda oddiy. Chunki, ochiq kalitli kriptotizimlarda maxfiy kalitlar ununig egasigagina tegishli bo'lib, ularni qandaydir aloqa kanali orqali uzatishga yoki boshqa foydalanuvchilarga tarqatishga hojat yo'q.

Asimmetrik kriptotizimlarda har bir foydalanuvchi o'zining ochiq va yopiq (maxfiy) kalitlar juftligiga ega. Xabarni jo'natuvchi xabarni qabul qiluvchining ochiq kalitlar jo'ftligidan foydalanib, ma'lumotlarni shifrlab, aloqa kanali orqali jo'natadi. Shifrlangan ma'lumotni qabul qilgan foydalanuvchi o'zining yopiq kalitlar juftligidan foydalanib, sifrmatnni dastlabki matnga o'giradi. Foydalanuvchilarning ochiq kalitlar juftligi tarmoqdagi boshqa foydalanuvchilar ishlatishlari uchun ochiq holda e'lon qilinishi yoki biror ma'lumotlar bazasida saqlanishi mumkin. Shu sababli asimmetrik kriptotizimlar ochiq kalitli kriptotizimlar deb ham nomlanadi.

Mustaqil ish savollari.

1. Asimmetrik (ochiq kalitli) shifrlash algoritmlari.
2. Nodeterminallashgan usul.

Nazorat savollari:

1. Ochiq kalitli kriptotizimlarda shifrlash kalitlari qanday bo'ladi?
2. Shifrlash kalitlari uzunligi qanday o'lchanadi.
3. Ochiq kalitli shifrlash algoritmlari uchun kalitlar qanday qo'llaniladi?

3.5. Kalitlarni boshqarish. Kalitlarni saqlash. Kalitlarni taqsimlash.

Tayanch ibora va tushunchalar: kritografik algoritmlarga hujum qilish kalitlar, fayl (direktoriya) larni shifrlash kalitlarni generasiya qilish**,** kalitlarni tarqatish sxemalari, kalitlarni birgalikda shakllantirish protokollari.

Mavzuga oid asosiy muammolar: Axborotni kritografik himoyalshninng ishonchli tizimini yaratishda birinchi navbatdagi asosiy masalalardan biri foydalanuvchining kalitini ish joyida ishonchli himoyasini ta'minlashdan iborat, buzgunchi boshqalarning kalitiga ega bo'lishi maxsus dasturiy vositalardan foydalaniladi, ushbu usul mustahkamligi kalitlarni bardoshligi qanday aniqlanishiga izoh berib o'ting.

Darsning maqsadi: Kalitlarni boshqarishda raqib xodimlarni og'dirish, viruslar va xotiraga to'g'ridan-to'g'ri murojaat qiladigan maxsus dasturiy vositalardan foydalanishni bayon qilish.

Axborotni kritografik himoyalshninng ishonchli tizimini yaratishda birinchi navbatdagi asosiy masalalardan biri foydalanuvchining kalitini ish joyida ishonchli himoyasini ta'minlashdan iborat. Buzg'unchiga boshqalarning kalitiga ega bo'lishning oson yo'llari raqib xodimlarini o'z tomoniga og'dirish, viruslar va xotiraga to'g'ridan-to'g'ri murojaat qiladigan maxsus dasturiy

vositalardan foydalanishdan iborat. Ushbu usullar kritografik algoritmlarga hujum qilish uchin qimmatbaho hisoblash texnikasi vositalari va katta vaqtni talab qilmaydilar.

Foydalanuvchi ish joyida kalitlarni saqlashni ishonchli tashkil qilishning asosiy usullarini quyidagicha keltirish mumkin:

- kalitlarni saqlashda ishlatiladigan xotirani ruxsat etilmagan kirishlardan himoyalaydigan kriptoqurilmalardan foydalanish;
- foydalanuvchi shaxsiy kompyuterida kalitlarni bevosita shifrlangan holatda saqlash;
- kalitlarni saqlashda tashqi qurilmalardan foydalanish.

Birinchi usul eng ishonchli bo'sada, foydalanuvchida har doim ham bunday qurilmalar bilan ishlashning imkoniyati yo'q. Bundan tashqari bunday kriptoqurilmalarning xotirasi uncha katta bo'lmaydi. Shu sababli bu turdagi qurilmalarda amalda shifrlash kalitlari yoki seans yoxud fayl (direktoriya)lar kalitlari saqlanadi.

Ikkinchi usulni batafsil izohlashning hojati yo'q. Bunday tarzda ko'pchilik hollarda fayl (direktoriya) larni shifrlash kalitlari saqlanadi.

Uchinchi usul hozirgi kunda eng istiqbolli usullardan biri hisoblanadi. Oxirgi vaqtlarda kalitli axborotlarni uzoq muddatda saqlash imkoniyatiga ega bo'lgan ko'plab qurilmalar paydo bo'lmoqda. Bunday qurilmalarni himoyalash tashkiliy usullar bilan oson hal qilinadi. Boz ustiga mazkur qurilmalarni zamonaviy hisoblash texnikasi vositalari bilan birgalikda foydalanilsh imkoniyati mavjud. Shu sababli bunday qurilmalarni amaliyotda qo'llash diapazoni kengayib bormoqda.

Simmetrik kriptotizimlarda kalitlarni tarqatish himoyalangan aloqa kanalidan va kriptpgrafik protokollardan foydalanishga asoslangan. Ochiq kalitli va gibridli kriptotizimlarda kalitlarni tarqatish ochiq kalitlarni autenfikasiya qilish, undan so'ng kriptpgrafik protokollardan foydalanishga asoslangan.

Kalitlarni tarqatish jarayoniga quyidagi talablar qo'yiladi:

1. Axborot almashinuvida ishtirok etuvchi har bir ishtirokchi protokollardan foydalanish jarayonida kalitlarni maxfiyligiga ishonch hosil qilishi lozim;
2. Kalit kimga mo'ljallangan bo'lsa, o'sha ishtirokchi kalitni qabul qilganligiga har bir ishtirokchi ishonch hosil qilishi lozim (qabul qilganligini tasdig'i talab qilinadi);
3. Kalit kimga jo'natilishi lozim bol'sa, o'sha ishtirokchiga kalit jo'natilganligiga har bir ishtirokchi ishonch hosil qilishi lozim (tomonlar autenfikasiyasi talab qilinadi).

Kalitlarni tarqatishning 2 xil protokoli mavjud:

- generasiya qilingan kalitlarni tarqatish protokollari;
- kalitlarni birgalikda shakllantirish protokollari.

Ikki va undan ortiq ishtirokchilar o'rtasida kalitlarni tarqatish protokollari va sxemalari ham turlicha bo'ladi. Ko'p ishtirokchilar o'rtasida kalitlarni tarqatishda markazlashtirilgan kalitlarni tarqatish sxemasidan foydalaniladi.
Bundan tashqari foydalanuvchilar bir-biriga ishongan va ishonmagan hollarda turli xil protokollardan foydalinaladi. Foydalanuvchilar bir-biriga ishongan

hollarda simmetrik va ochiq kalitli kriptotizimlardan foydalanishlari mumkin.

Foydalanuvchilar bir-biriga ishonmagan hollarda faqatgina ochiq kalitli kriptotizimlarga asoslangan protokollardan foydalanishlari mumkin.

Seansli kalitlarni tarqatishning muvaffaqiyatli yechimlaridan biri gibrid kriptotizimlardan foydalanishdir. Bunda ma'lumotlarni shifrlashda simmetrik, kalitlarni tarqatishda ochiq kalitli kriptotizimlardan foydalanish mumkin. Shu sababli gibrid kriptotizimlar simmetrik kriptotizimlarga xos bo'lgan yuqori tezlikda shifrlash, ochiq kalitli kriptotizimlarga xos bo'lgan kalitlarni qulay tarzda tarqatish bilan xarakterlanadi.

Faraz qilaylik, axborot almashiniuv tizimida N ta foydalanuvchi mavjud. Ushbu tizimdagi A va B foydalanuvchilar axborot almashishlari uchun K seans kalitiga ehtiyoj sezmoqdalar. Mazkur axborot almashiniuv tizimida odatdagi foydalanuvchilardan tashqari kalitlarni tarqatish markazi (KTM) deb nomlanuvchi ishonchli markaz ham ishtirok etmoqda.

KTM har bir abonent (foydalanuvchi) uchun turli K(i=1,N) maxfiy kalitlarni generasiya qiladi va himoyalangan aloqa kanali orqali ushbu kalitlar bilan abonentlarni ta'minlaydi. Ushbu mazkur K (i=1,N) maxfiy kalitlar bosh kalitlar deb nomlanadi va ulardan abonentlar KTM bilan aloqa qilishda foydalanishadi.

Seansli kalitlarni uzatishda shifrlashning maxsus algoritmi ishlatiladi. E_K (x) orqali ushbu shifrlash algoritmidan foydalanib, *x* ma'lumotni K kalit yordamida shifrlash tushuniladi.

Agar A_i va A abonetlar o'zaro maxfiy aloqa o'rnatmoqchi bo'lsalar, ular KTMga murojaat qilishadi. KTM esa ular uchun K umumiy seans kalitini ishlab orqali jo'natadi. Qabul qilingan ma'lumotlarni A_i va A abonetlar dastlabki matnga o'girib, K umumiy seans kalitiga ega bo'lishadi.

Bu yerda shifrlashda qo'llanilgan E kriptoalgoritmi isonchli, Shu sababli K_i va K kalitlarni bilmagan buzg'unchi K umumiy seans kalitini hosil qilolmaydi yoki uni boshqasi bilan almashtiriolmaydi.

Agar KTMdan foydalanuvchi abonentlar soni ko'p bo'lsa, ushbu KTM asosida ierarxik tomoyil bo'yicha bir nyecha ishonchli markazlar tashkil qilinishi mumkin. Natijada bosh KTM va uning mintaqaviy markazlari hosil qilinishi mumkin. Mintaqaviy KTMlar o'z guruh (hudud)laridagi abonentlarga xizmat ko'rsatishlari mumkin. Turli xil guruhdagi abonentlar bir-birlari bilan aloqa o'rnatmoqchi bo'lsalar, bosh KTM tomonidan ularga seans kalitlari taqdim qilinadi.

KTM tomonidan kalitlarni qayd qilish jurnali (alohida fayl) da kalitlar haqidagi ma'lumotlar kiritilib boriladi. Ushbu jurnalda odatda quyidagilar aks etgan bo'ladi:

KTM A_j abonentga E (K_{ij}), A abonentga Ek(K_{ij}) ni ochiq aloqa kanali chiqadi.

1. Kalitlarni generasiya qilinish sanasi;
2. Kalitlarni turi va nomi;
3. Kalitlarni amal qilish muddati;

4. Kalitlardan foydalanuvchi abonentlar ro'yxati;
5. Kalitlarni o'z foydalanuvchisiga jo'natilganligi haqidagi ma'lumotlar;
6. Kalitlarni qabul qilinganligi haqidagi foydalanuvchilarning tasdiqlari va shunga o'xshash ma'lumotlar.

Bayon etilgan KTM sxemasining yutug'i shundaki, abonentlar sifatli kalitlarni generasiya qilish uchun KTM kabi zamonaviy qurilmalarga, malakali mutaxassislarga ega emas. Kamchiligi esa agar KTM ishonchni yo'qotsa, ushbu markaz xizmat ko'rsatayotgan barcha abonentlar kalitlarining maxfiyligi shubha ostigai qoladi va ular kalitlar masalasida boshqa KTMga murojaat qilishlariga to'g'ri keladi.

Agar kalit foydalanuvchi tomonidan generasiya qilinsa va uni ishonchli markaz boshqa foydalanuvchi yetkazib bersa, kalitning xavfsizligiga tahdid kuchayadi. Shuningdek, seansli kalitning xavfsizligi u shifrlanadigan shifrlash algoritmining ishonchliligа ham bog'liq. Ammo, buzg'unchi kalitni uzatish protokolida aralashishi yoki o'zini qonuniy foydalanuvchi sifatida tutib, seansli kalitni o'zgartirish maqsadida o'zi shunday protokolni o'ylab topishi mumkin. Shu sababli abonentlarni o'zaro autentifikasiyasiga asoslangan karlitlni uzatishning mukammal protokoliga zaruriyat paydo bo'ladi.

Mavzuni bayon qilishda A abonent B abonentga kalitni uzatish ishonchli markaz T orqali amalga oshiriladi deb faraz qilinadi hamda quyidagi belgilashlardan foydalaniladi:

E_A, E_B orqali mos holda A va B abonentlarning bosh kalitlari bilan shifrlash ifodalanadi.

K,I,L-mos holda maxfiy seans kalitini, uning tartib nomerini va umri (foydalanish muddati) ni anglatadi.

T_A,T_B-mos holda A va B abonentlar tomonidan yaratilgan vaqt nishonlarini bildiradi.

RA, RB-mos holda A va B abonentlar tomonidan tasodifiy tanlangan sonlarni anglatadi.

X,Y-X va Y sonlarini konkatenasini bildiradi.

Shart bo'lmagan parametrlar yulduzcha bilan X^* kabi belgilanadi.

Wide-Mouth Frog protokoli.

Ushbu protokol kalitni ishonchli markaz orqali uzatishga misol bo'ladi. U quyida keltirilgan tartibda amalga oshiriladi:

1. A T: A, EA (TA, B,K);
2. T B: EB(TB,A,K).

Birinchi qadamda A abonent tomonidan T isonchli markazga kalitni uzatish va A abonentni T tomonidan autenfikasiyasilanishi amalga oshirilgan.

Ikkinchi qadamda T isonchli markazni B abonentga kalit uzatishi va T markazni B tomonidan autenfikasiyasilanishi amalga oshirilgan. Bundan tashqari T markaz A abonent tomonidan kalit uzatilgianligini B ga xabar qildi. Har ikki qadamda ham buzg'unchi ushlab olingan eski ma'lumotlardan foydalanishiga yo'l qo'ymaslik maqsadida shifrlangan vaqt nishonlaridan foydalanigan.

Ushbu protokolda A abonentni T tomonidan autenfikasiyasilanishi amalga oshirilgan. Ammo, kalitni muvaffaqiyatli qabul qilinganligi tasduqlovchi va B abonentni A tomonidan autenfikasiyalanishi amalga oshiruvchi qadamlar nazarda tutilmagan.

Yahalom protokoli.

1. A B: A, R_A ;
2. B T : B> EB (A,RA, RB);
3. T A: E_A (B, K, R_A , R_B), E_B (A, K);
4. A B: E_B (A, K), G = E_K (R_B).
5. B:G = $E_K(R_B)$ ekanligini tekshirib ko'radi, natija ijobiy bo'lsa, B K kalitni qabul qiladi.

Ushbu protokolning oldingi protokoldan farqi shundaki, unda xabar almashinuvuga tashabbuskor shaxs to'g'ridan-to'g'ri o'z hamkoriga murojaat qiladi (1-qadam) va u yakuniy kalit almashinuvuni amalga oshiradi (4-qadam). Ikkinchi tomondan seansli kalit T markaz tomonidan amalga oshiriladi. Shuningdek, vaqt nishonlari o'rniga bir martalik tasodifiy sonlar ishlatiladi. Bu esa bu protokolda ishlatiluvchi barcha ma'lumotlardan bir marta foydalanishni anglatadi.

A abonent orqali B abonentga kalitni uzatilishi B abonent tomonidan A abonentni autenfikasiyalashni ta'minlaydi. Haqiqatan ham, agar buzg'unchi o'zini A abonent o'rnida tutayotgan bo'lsa, u A abonentning kalitiga ega emasligi sababli 3-qadamda EA (B, K, RA,RB) ni dastlabki matnga o'gira olmaydi. Natijada undan R_B va K ni hosil qilolmaydi. Demakki, xabarni ham hosil qilolmaydi. Uni o'rniga boshqa xabarni jo'natsa, B abonent ushbu xabarni K kalit bilan dastlabki matnga o'girib, natija R_B bir xil emasligini ko'rib, buzg'unchi jo'natgan K kalitdan foydalanishni rad etadi.

B abonentni A abonent tomonidan autentifikasiyalanishi 2-3 qadamlarda T markaz orqali shifrlangan ma'lumotlarni uzatish yordamida amalga oshiriladi.

B abonent 4-qadamda qabul qiladigan EK (RB) nafaqat A abonentni B abonent tomonidan autentifikasiyalanishini, balki axborotni uzatish jarayonida o'zgartirilmaganligini tekshirishni ham ta'minlaydi.

Xulosa sifatida shuni aytish mumkinki, ushbu protokol nafaqat kalitni uzatishni amalga oshiradi, balki xabarlardan takroran foydalanishga to'sqinlik qilib, B abonentga A abonent olgan kalitni olganligiga ishonch hosil qilsh imkonini yaratadi. Protokolda xuddi shunga o'xshash tekshirishni A abonent ham o'tkazish imkoniyati mavjud emas.

Nidxem-Shreder protokoli.

Ushbu protokol A abonentni aldash maqsadida eski ma'lumotlarni takroran uzatish asosidagi hujumga to'sqinlik qiladi. Protokoldagi ixtiyoriy ma'lumotni qabul qilgan shaxs olingan ma'lumotni kutilayotgan ma'lumotga mosligini tekshirib ko'rishi lozim. Agar protokolni bajarilish vaqtida biror bir ziddiyatga duch kelinsa, u holda bu protokolni bajarilishini to'xtatish lozim va bu haqida boshqa ishtirokchilarga ham ma'lum qilishi kerak.

Protokol quyidagi tartibda amalga oshiriladi:

1. A -A: A, B, RA;

2. T-A: EA(RA, B, K, EB(K,A));

3. A- B: EB(K, A);

4. B- A: EK(RB);

5. A- B: EK(RB-1).

2-3 qadamlarda A abonent K kalit bilan shifrlangan xabardan EB(K,A) xabarni olib, uni B abonentga uzatish natijasida B abonent tomonidan autentifikasiyalanadi.

B abonent A abonent tomonidan autentifikasiyalanmaydi. Buzg'unchi o'zini A abonent sifatida namoyon qilib, 4-qadamda ixtiyoriy tasodifiy sonni B abonentga jo'natishi mumkin. Ammo, bu unga hech narsa bermaydi, chunki u maxfiy kalitni bilmaydi.

4-5 qadamlar B abonentga A abonent ham o'zi qabul qilgan aynan K kalitni olganligini tasdiqlaydi. Ammo, buzg'unchi o'zini A abonent sifatida namoyon qilib, B abonentga eski K' kalitni taqdim qilishi mumkin. Haqiqatan ham protokolda B va T bevosita muloqat qilishmaydi. Shu sababli M (buzg'unchi) 3-qadamdan boshlab B abonent bilan muloqat qilishni boshlaydi:

M(A nomidan)^B: EB(K',A);

(Ushbu xabarni A abonent B abonentga eski K' kalitni jo'natgan vaqtida tutib olgan edi.) B abonent qabul qilingan kalit oldin ishlatilgan yoki ishlatilmaganligini tekshirmasa, u holda B uni to'g'ri kalit sifatida qabul qiladi va A abonentga xabar jo'natadi:

4. B>A: EK'(RB);

B abonent tomonidan g'alati xabarlar kelayotgani haqida A abonent T markazga xabar qilmasligi uchun M buzg'unchi B abonent tomonidan A abonentga jo'natilayotgan barcha xabarlarni blokirovka qilishi lozim bo'ladi.

5. M(A nomidan)^B: EK'(RB-1).

Shunday qilib, B abonent tomonidan unga uzatilgan barcha kalitlar jurnalda qayd qilib borilgan hollardagina ushbu protokolni ishlatish mumkin.

Mustaqil ish savollari.

1. Generasiya qilingan kalitlarni tarqatish protokollari.
2. Kalitlarni birgalikda shakllantirish protokollari.

Nazorat savollari:

1. Axborotni kritografik himoyalshninng ishonchli tizimini yaratishda nimalarga etibor qaratish kerak?
2. Wide-Mouth Frog protokoliga tariff bering.
3. Nidxem-Shreder protokoli?

IV BOB. AXBOROTNI HIMOYALASHDA TARMOQLARARO EKRANLARNING O‘RNI.

4.1. Tarmoqlararo ekranlarning ishlash xususiyatlari

Tayanch ibora va tushunchalar: Brandmauer yoki firewall sistemasi, korporativ (lokal) tarmoq, OSI modeli, trafiklarni filtrlash, ochiq tashqi tarmoq, himoyalanadigan ichki tarmoq.

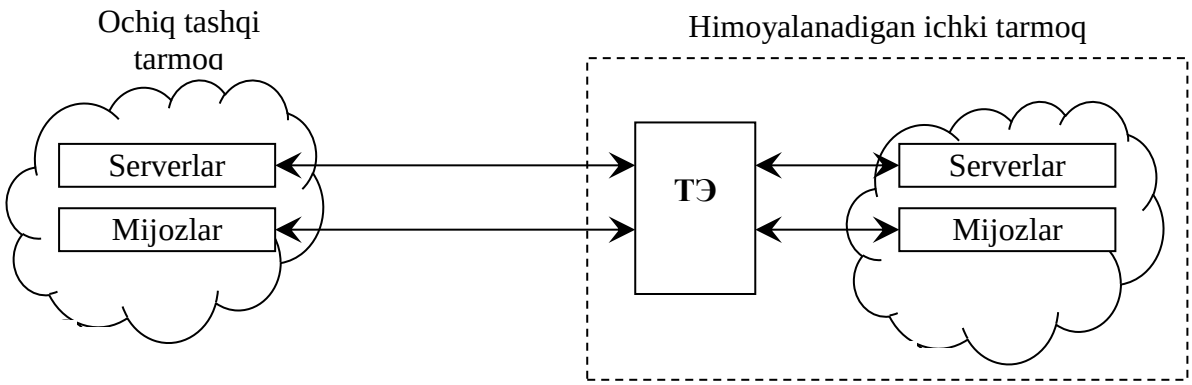
Mavzuga oid asosiy muammolar: Tarmoqda foydalanuvchilar soni parollarning tayinlashi va saqlanishi, raqamli sertifikatlar, foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar.

Darsning maqsadi: Raqamli sertifikatlar ishlatilganda computer tarmog‘i foydalanuvchilar xususida maxfiy axborotni, maxfiy kalitni saqlash vazifasi foydalanuvchilarning o‘ziga yklanishi haqida ma’lumot berish

Tarmoqlararo ekran (TE)-brandmauer yoki firewall sistemasi deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko‘p qismlarga ajratish va ma’lumot paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o‘tish shartlarini belgilovchi qoidalar to‘plamini amalga oshirish imkonini beradi. Odatda, bu chegara korxonaning korporativ (lokal) tarmog‘i va Internet global tarmoq orasida o‘tkaziladi. Tarmoqlararo ekranlar garchi korxona lokal tarmog‘i ulangan korporativ tarmog‘idan qilinuvchi hujumlardan himoyalashda ishlatilishlari mumkin bo‘lsada, odatda ular korxona ichki tarmog‘ini Internet global tarmoqdan suqilib kirishdan himoyalaydi. Aksariyat tijorat tashkilotlari uchun tarmoqlararo ekranlarning o‘rnatilishi ichki tarmoq xavfsizligini ta’minlashning zaruriy sharti hisoblanadi.

Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta’sir ko‘rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning himoyalanuvchi tarmog‘i va tashqi g‘anim tarmoq orasida joylanishi lozim. Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtai nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga

kiradi. Bundan kelib chiqib tarmoqlararo ekranni ulash sxemasini quydagicha keltirishimiz mumkin



4.1-rasm. Tarmoqlararo ekranni ulash sxemasi.

Ichki tarmoqning ko‘pgina uzellarini birdaniga himoyalovchi tarmoqlararo ekran quyidagi ikkita vazifani bajarishi kerak:

-tashqi (himoyalanuvchi tarmoqqa nisbatan) foydalanuvchilarning korporativ tarmoqning ichki resurslaridan foydalanishini chegaralash. Bunday foydalanuvchilar qatoriga tarmoqlararo ekran himoyalovchi ma’lumotlar bazasining serveridan foydalanishga urinuvchi sheriklar, masofadagi foydalanuvchilar, xakerlar, hatto kompaniyaning xodimlari kiritilishi mumkin;

-himoyalanuvchi tarmoqdan foydalanuvchilarning tashqi resurslardan foydalanishlarini chegaralash. Bu masalaning echilishi, masalan, serverdan xizmat vazifalari talab etmaydigan foydalanishni tartibga solishga imkon beradi.

Hozirda ishlab chiqarilayotgan tarmoqlararo ekranlarning tavsiflariga asoslangan holda, ularni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

OSI modeli sathlarida ishlashi bo‘yicha:

- paketli filtr (ekranlovchi marshrutizator – screening router);
- seans sathi shlyuzi (ekranlovchi transport);
- tatbiqiy sath shlyuzi (application gateway);
- ekspert sathi shlyuzi (stateful inspection firewall).

Ishlatiladigan texnologiya bo‘yicha:

- protokol holatini nazoratlash (Stateful inspection);
- vositachilar modullari asosida (proxy);

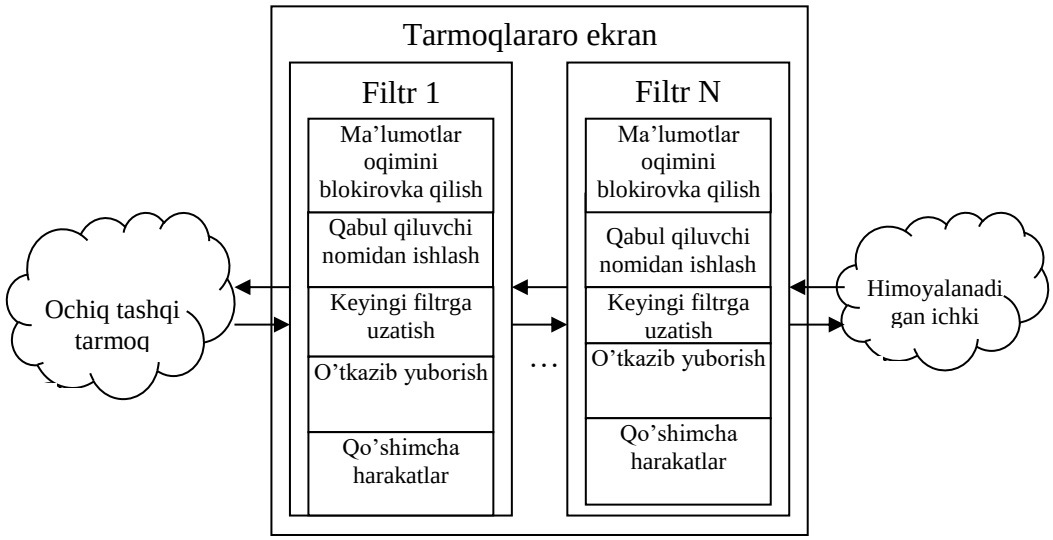
Bajarilishi bo’yicha:

- apparat-dasturiy;
- dasturiy;

Ulanish sxemasi bo‘yicha;

- tarmoqni umumiy himoyalash sxemasi;
- tarmoq segmentlari himoyalanuvchi berk va tarmoq segmentlari himoyalanmaydigan ochiq sxema;
- tarmoqning berk va ochiq segmentlarini alohida himoyalovchi sxema.

Trafiklarni filtrlash. Axborot oqimlarini filtrlash ularni ekran orqali, ba’zida qandaydir o‘zgartirishlar bilan, o‘tkazishdan iborat. Filtrlash qabul qilingan xavfsizlik siyosatiga mos keluvchi, ekranga oldindan yuklangan qoidalar asosida amalga oshiriladi. Shu sababli tarmoqlararo ekranni axborot oqimlarini ishlovchi filtrlar ketma-ketligi sifatida tasavvur etish qulay. Tarmoqlararo ekran tuzilmasi.



4.2-rasm. Tarmoqlararo ekran tuzilmasi.

Filtrlarning har biri quyidagi harakatlarni bajarish orqali filtrlashning alohida qoidalarini izohlashga atalgan:

1. Axborotni izohlanuvchi qoidalardagi berilgan mezonlar bo‘yicha tahlillash, masalan, qabul qiluvchi va jo‘natuvchi adreslari yoki ushbu axborot atalgan ilova xili bo‘yicha.

2. Izohlanuvchi qoidalar asosida quyidagi echimlardan birini qabul qilish:

- ma’lumotlarni o‘tkazmaslik;
- ma’lumotlarni qabul qiluvchi nomidan ishlash va natijani jo‘natuvchiga qaytarish;
- taxlillashni davom ettirish uchun ma’lumotlarni keyingi filtrga uzatish;
- keyingi filtrlarga e’tibor qilmay ma’lumotlarni uzatish.

Filtrlash qoidalari vositachilik funktsiyalariga oid qo‘shimcha, masalan ma’lumotlarni o‘zgartirish, xodisalarni qaydlash va hk.., kabi harakatlarni ham berishi mumkin. Mos holda, filtrlash qoidalari quyidagilarning amalga oshirilishini ta’minlovchi shartlar ro‘yxatini aniqlaydi:

- ma’lumotlarni keyingi uzatishga ruxsat berish yoki ruxsat bermaslik;
- himoyalashning qo‘shimcha funktsiyalarini bajarish.

Ishlatiluvchi taxlillash mezonlari filtrlashni amalga oshiruvchi OSI modelining sathlariga bog‘liq. Umumiy holda, paketni filtrlashni amalga oshiruvchi OSI modelining sathi qanchalik yuqori bo‘lsa, ta’minlanuvchi himoyalash darajasi ham shunchalik yuqori bo‘ladi.

Vositachilik funktsiyalarining bajarilishi**.** Tarmoqlararo ekran vositachilik funktsiyalarini ekranlovchi agentlar yoki vositachi dasturlar deb ataluvchi maxsus dasturlar yordamida bajaradi. Bu dasturlar rezident dasturlar hisoblanadi va tashqi va ichki tarmoq orasida xabarlar paketini bevosita uzatishni taqiqlaydi.

Tashqi tarmoqdan ichki tarmoqning va aksincha foydalanish zaruriyati tug‘ilganda avval tarmoqlararo ekran kompyuterida ishlovchi vositachi-dastur bilan mantiqiy ulanish o‘rnatilishi lozim. Vositachi-dastur so‘ralgan tarmoqlararo aloqaning joizligini tekshiradi va ijobiy natijada o‘zi suralgan kompyuter bilan alohida ulanish o‘rnatadi. So‘ngra tashqi va ichki tarmoq kompyuterlari orasida axborot almashish, xabarlar oqimini filtrlashni hamda boshqa himoyalash funktsiyalarini bajaruvchi dasturiy vositachi orqali amalga oshiriladi.

Umuman, vositachi-dasturlar, xabarlar oqimini shaffof uzatilishini blokirovka qilgan holda, quyidagi funktsiyalarni bajarishi mumkin:

- uzatiluvchi va qabul qilinuvchi ma’lumotlarning haqiqiyligini tekshirish;
- ichki tarmoq resurslaridan foydalanishni chegaralash;
- tashqi tarmoq resurslaridan foydalanishni chegaralash;
- tashqi tarmoqdan so‘raluvchi ma’lumotlarni kesh xotiraga saqlash;
- xabarlar oqimini filtrlash va o‘zgartirish, masalan, viruslarni dinamik tarzda qidirish va axborotni shaffof shifrlash;
- foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;
- ichki tarmoq adreslarini translyatsiyalash;
- xodisalarni qaydlash, xodisalarga reaksiya ko‘rsatish, xamda qaydlangan axborotni taxlillash va hisobotlarni generatsiyalash.

Uzatiluvchi va qabul qilinuvchi ma’lumotlarning haqiqiyligini tekshirish nafaqat elektron xabarlarni, balki soxtalashtirilishi mumkin bo‘lgan migratsiyalanuvchi dasturlarni (Java, ActiveXControls) autentifkatsiyalash uchun dolzarb hisoblanadi. Xabar va dasturlarning haqiqiyligini tekshirish ularning raqamli imzosini tekshirishdan iboratdir.

Ichki tarmoq resurslaridan foydalanishni chegaralash usullari operatsion tizim sathida madadlanuvchi chegaralash usullaridan farq qilmaydi.

Tashqi tarmoq resurslaridan foydalanishni chegarlashda ko‘pincha quyidagi yondashishlardan biri ishlatiladi:

-faqat tashqi tarmoqdagi berilgan adres bo‘yicha foydalanishga ruxsat berish;

-yangilanuvchi nojoiz adreslar ro‘yxati bo‘yicha so‘rovlarni filtrlash va o‘rinsiz kalit so‘zlari bo‘yicha axborot resurslarini qidirishni blokirovka qilish:

-ma’mur tomonidan tashqi tarmoqning qonuniy resurslarini brandmauerning diskli xotirasida to‘plash va yangilash va tashqi tarmoqdan foydalanishni to‘la taqiqlash.

Tashqi tarmoqdan so‘raluvchi ma’lumotlarni keshlash maxsus vositachilar yordamida madadlanadi. Ichki tarmoq foydalanuvchilari tashqi tarmoq resurslaridan foydalanganlarida barcha axborot, proxy-server deb ataluvchi brandmauer qattiq diski makonida to‘planadi. Shu sababli, agar navbatdagi so‘rovda kerakli axborot proxy-serverda bo‘lsa, vositachi uni tashqi tarmoqqa murojaatsiz taqdim etadi. Bu foydalanishni jiddiy tezlashtiradi. Ma’murga faqat proxy-server tarkibini vaqti-vaqti bilan yangilab turish vazifasi qoladi.

Xabarlar oqimini filtrlash va o‘zgartirish vositachi tomonidan qoidalarning berilgan to‘plami yordamida bajariladi. Bunda vositachi-dasturlarning ikki xili farqlanadi:

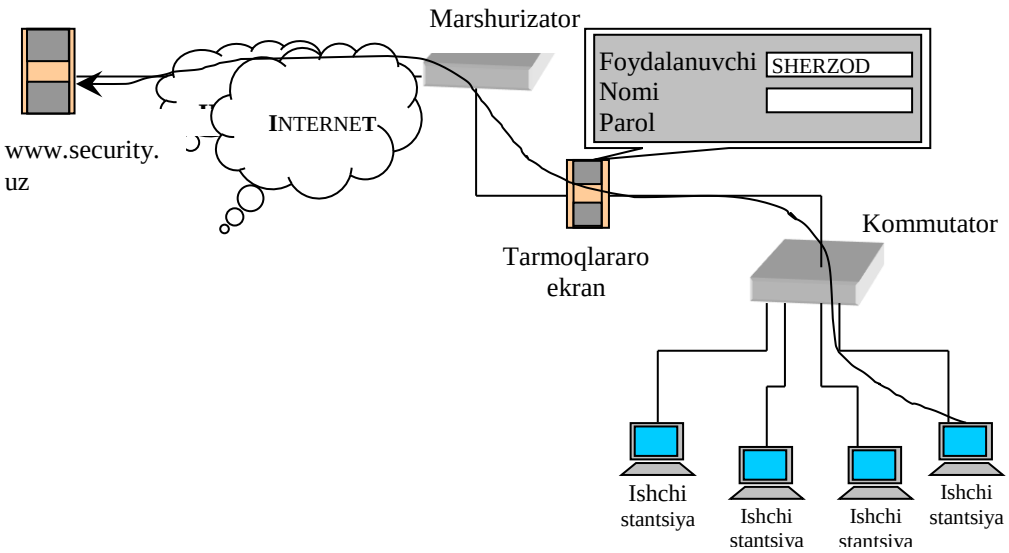
- servis turini aniqlash uchun xabarlar oqimini taxlillashga mo‘ljallangan ekranlovchi agentlar, masalan, FTP, HTTP, Telnet;
- barcha xabarlar oqimini ishlovchi universal ekranlovchi agentlar, masalan, kompyuter viruslarini qidirib zararsizlantirishga yoki ma’lumotlarni shaffof shifrlashga mo‘ljallangan agentlar.

Dasturiy vositachi unga keluvchi ma’lumotlar paketini taxlillaydi va agar qandaydir ob’ekt berilgan mezonlarga mos kelmasa, vositachi uning keyingi siljishini blokirovka qiladi yoki mos o‘zgarishini, masalan, oshkor qilingan kompyuter viruslarni zararsizlantirishni bajaradi. Paketlar tarkibini taxlillashda ekranlovchi agentning o‘tuvchi faylli arxivlarni avtomatik tarzda ocha olishi muhim hisoblanadi.

Autentifikatsiyalashning ishonchliroq usuli bir marta ishlatiluvchi parollardan foydalanishdir. Bir martali parollarni generatsiyalashda apparat va dasturiy vositalardan foydalaniladi. Apparat vositalari kompyuterning stoliga o‘rnatiluvchi qurilma bo‘lib, uni ishga tushirish uchun foydalanuvchi qandaydir maxfiy axborotni bilishi zarur. Masalan, smart-karta yoki foydalanuvchi tokeni axborotni generatsiyalaydi va bu axborotni xost an’anaviy parol o‘rnida ishlatadi. Smart-karta yoki token xostning apparat va dasturiy ta’minoti bilan birga ishlashi sababli, generatsiyalanuvchi parol har bir seans uchun noyob bo‘ladi.

Tarmoqlararo ekranlar tarmoqdan foydalanishni boshqarishni

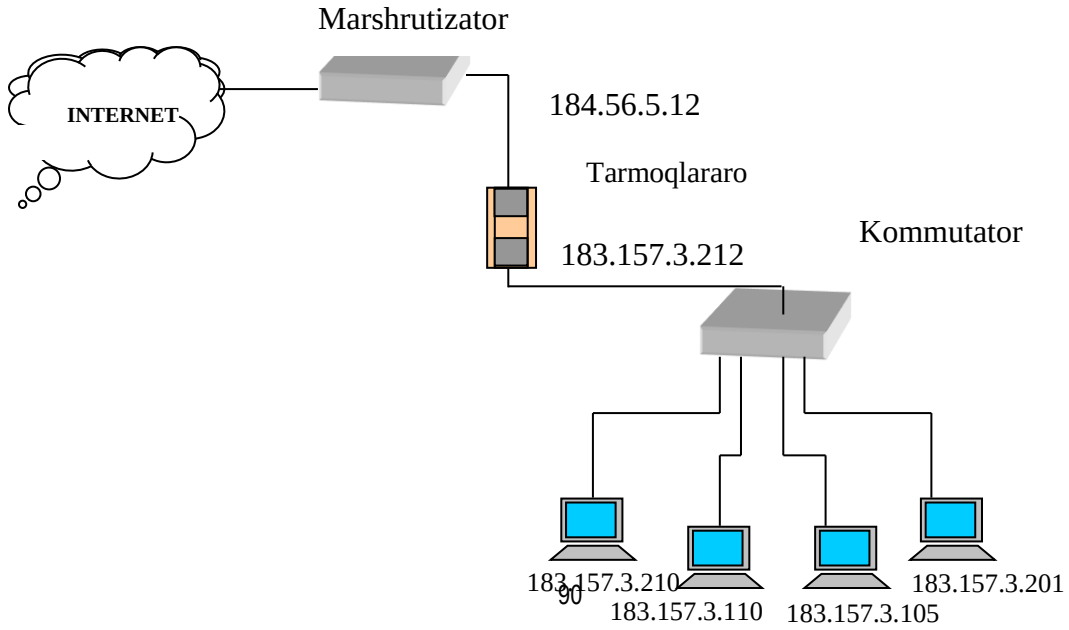
markazlashtirishlari mumkin. Demak, ular kuchaytirilgan autentifikatsiyalash dasturlari va qurilmalarini o‘rnatishga munosib joy hisoblanadi. Garchi kuchaytirilgan autentifikatsiya vositalari har bir xostda ishlatilishi mumkin bo‘lsada, ularning tarmoqlararo ekranlarda joylashtirish qulay. Kuchaytirilgan autentifikatsiyalash choralaridan foydalanuvchi tarmoqlararo ekranlar bo‘lmasa, Telnet yoki FTP kabi ilovalarning autentifikatsiyalanmagan trafigi tarmoqning ichki tizimlariga to‘g‘ridan-to‘g‘ri o‘tishi mumkin.



4.3– rasm. Parol bo’yicha foydalanuvchini autentifikatsiyalash sxemasi

Qator tarmoqlararo ekranlar autentifikatsiyalashning keng tarqalgan usullaridan biri–Kerberosni madadlaydi. Odatda, aksariyat tijorat tarmoqlararo ekranlar autentifikatsiyalashning turli sxemalarini madadlaydi. Bu esa tarmoq xavfsizligi ma’muriga o‘zining sharoitiga qarab eng maqbul sxemani tanlash imkonini beradi.

Ichki tarmoq adreslarini translyatsiyalash. Ko‘pgina xujumlarni amalga oshirishda niyati buzuq odamga qurbonining adresini bilish kerak bo‘ladi. Bu adreslarni hamda butun tarmoq topologiyasini bekitish uchun tarmoqlararo ekranlar eng muhim vazifani – ichki tarmoq adreslarini translyatsiyalashni bajaradi (4.4-rasm).



4.4– rasm. Tarmoq adreslarini translyatsiyalash

Bu funktsiya ichki tarmoqdan tashqi tarmoqqa uzatiluvchi barcha paketlarga nisbatan bajariladi. Bunday paketlar uchun jo‘natuvchi kompyuterlarning IP-adreslari bitta "ishonchli" IP adresga avtomatik tarzda o‘zgartiriladi.

Ichki tarmoq adreslarini translyatsiyalash ikkita usul-dinamik va statik usullarda amalga oshirilishi mumkin. Dinamik usulda adres uzelga tarmoqlararo ekranga murojaat onida ajratiladi. Ulanish tugallanganidan so‘ng adres bo‘shaydi va uni korporativ tarmoqning boshqa uzeli ishlatishi mumkin. Statik usulda uzel adresi barcha chiquvchi paketlar uzatiladigan tarmoqlararo ekranning bitta adresiga doimo bog‘lanadi. Tarmoqlararo ekranning IP-adresi tashqi tarmoqqa tushuvchi yagona faol IP-adresga aylanadi. Natijada, ichki tarmoqdan chiquvchi barcha paketlar tarmoqlararo ekrandan jo‘natilgan bo‘ladi. Bu avtorizatsiyalangan ichki tarmoq va xavfli bo‘lishi mumkin bo‘lgan tashqi tarmoq orasida to‘g‘ridan-to‘g‘ri aloqani istisno qiladi.

Xodisalarni qaydlash, xodisalarga reaktsiya ko‘rsatish, hamda qaydlangan axborotni taxlillash va hisobotlarni generatsiyalash tarmoqlararo ekranlarning muhim vazifalari hisoblanadi. Korporativ tarmoqni himoyalash tizimining jiddiy elementi sifatida tarmoqlararo ekran barcha harakatlarni ro‘yxatga olish imkoniyatiga ega. Bunday harakatlarga nafaqat tarmoq paketlarini o‘tkazib yuborish yoki blokirovka qilish, balki xavfsizlik ma’muri tomonidan foydalanish qoidasini o‘zgartirish ham taalluqli. Bunday ro‘yxatga olish zaruriyat tug‘ilganda (xavfsizlik mojarosi paydo bo‘lganida yoki sud instantsiyalariga yoki ichki tergov uchun dalillarni yig‘ishda) yaratiluvchi jurnallarga murojaat etishga imkon beradi.

Ko‘pgina tarmoqlararo ekranlar statistikani qaydlovchi, yig‘uvchi va taxlillovchi quvvatli tizimga ega. Mijoz va server adresi, foydalanuvchilar identifikatori, seans vaqtlari, ulanish vaqtlari, uzatilgan va qabul qilingan ma’lumotlar soni, ma’mur va foydalanuvchilar harakatlari bo‘yicha hisob olib borilishi mumkin. Hisob tizimlari statistikani taxlillashga imkon beradi va ma’murlarga batafsil hisobotlarni taqdim etadi. Tarmoqlararo ekranlar maxsus protokollardan foydalanib, ma’lum xodisalar to‘g‘risida real vaqt rejimida masofadan xabar berishni bajarishi mumkin.

Ruxsatsiz harakatlarni qilishga urinishlarni aniqlanishiga bo‘ladigan majburiy reaktsiya sifatida ma’murning xabari, ya’ni ogohlantiruvchi signallarni berish belgilanishi lozim. Xujum qilinganligi aniqlanganda ogohlantiruvchi signallarni yuborishga qodir bo‘lmagan tarmoqlararo ekranni tarmoqlararo himoyaning samarali vositasi deb bo‘lmaydi.

Mustaqil ish savollari.

1. Trafikli filtrlashda nimani tushunasiz.
2. Tarmoqlararo ekranda vositachilik funksiyalarning bajarilishi.

Nazorat savollari:

1. Tarmoqlararo ekran vositalari tushunchasi va uning vazifalari.
2. Tarmoqlararo ekranlarning OSI modeli sathlari bo‘yicha turkumlanishi.
3. Trafiklarni filtrlash funktsiyasining ishlashini tushuntirib bering.
4. Tarmoq adreslarini translyatsiyalash qanday amalga oshiriladi?

5. Tarmoqlararo ekranlarning vositachilik funktsiyalarining mohiyati nimadan iborat?

4.2. Tarmoqlararo ekranlarning asosiy komponentlari.

Tayanch ibora va tushunchalar: Ekranlovchi marshruzator, seans sathi shlyzi, tarmoqlarda ishlatiladigan protokollar(TCP/IP, SPS/IPX), OSI modeli, ekranlovchi marshruzator, paketli filtning ishlash sxemasi.

Mavzuga oid asosiy muammolar: Tadbiqiy ekran xabarlarining tashqi tarmoqqa uzatish, shifirlashni, qabul qiluvchi kriptografik tarzda berkitilgan ma’lumotlarni avtomatik tarzda razshifrovka qilish, seans sathi shylizinig ishlashi tadbiqiy shyluzning ishlash sxemasi.

Darsning maqsadi: Tarmoqlararo ekranlar tarmoqlararo aloqa xavfsizligini OSI modelining satxlarda ishlashi, ekranlovchi marshruzator(screeningrouter) paketli filtr(pasketfilter) xabarlar paketini filtrlashga atalgan ichki va tashqi tarmoqlar orasida aloqani ta’minlash.

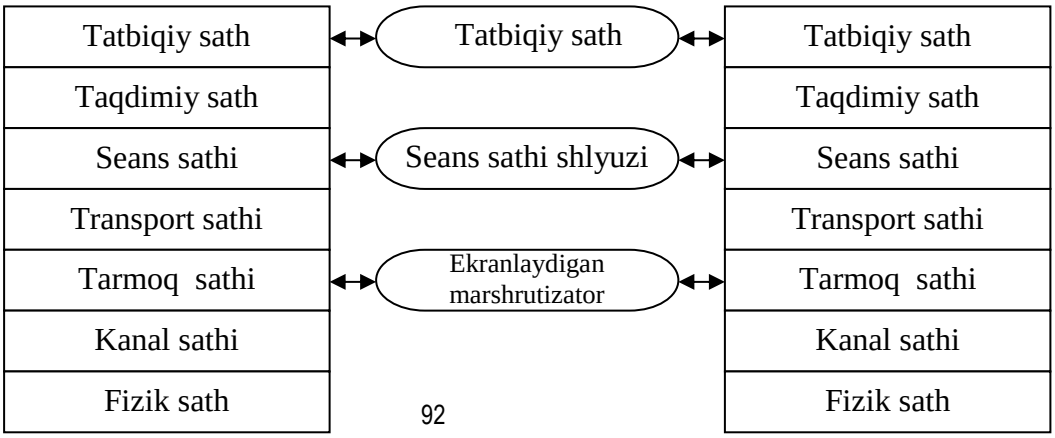
Tarmoqlararo ekranlar tarmoqlararo aloqa xavfsizligini OSI modelining turli sathlarida madadlaydi. Bunda etalon modelning turli sathlarida bajariladigan himoya funktsiyalari bir-biridan jiddiy farqlanadi. Shu sababli, tarmoqlararo ekranlar kompleksini, har biri OSI modelining alohida sathiga mo‘ljallangan, bo‘linmaydigan ekranlar majmui ko‘rinishida tasavvur etish mumkin.

Ekranlar kompleksi ko‘pincha etalon modelning tarmoq, seans, tatbiqiy sathlarida ishlaydi. Mos holda, quyidagi bo‘linmaydigan brandmauerlar farqlanadi (4.2.1-rasm).

- ekranlovchi marshrutizator;
- seans sathi shlyuzi (ekranlovchi transport);
- tatbiqiy sath shlyuzi (ekranlovchi shlyuz).

Tarmoqlarda ishlatiladigan protokollar (TCP/IP, SPX/IPX) OSI etalon modeliga batamom mos kelmaydi, shu sababli sanab o‘tilgan ekranlar xili funktsiyalarini amalga oshirishda etalon modelining qo‘shni sathlarini ham qamrab olishlari mumkin. Masalan, tatbiqiy ekran xabarlarning tashqi tarmoqqa uzatilishida ularni avtomatik tarzda shifrlashni, hamda qabul qilinuvchi kriptografik bekitilgan ma’lumotlarni avtomatik tarzda rasshifrovka qilishni amalga oshirishi mumkin. Bu holda, bunday ekran OSI modelining nafaqat tatbiqiy sathida, balki taqdimiy sathida ham ishlaydi.

Seans sathi shlyuzi ishlashida OSI modelining transport va tarmoq sathlarini qamrab oladi. Ekranlovchi marshrutizator xabarlar paketini taxlillashda ularning nafaqat tarmoq, balki transport sathi sarlavhalarini ham tekshiradi.

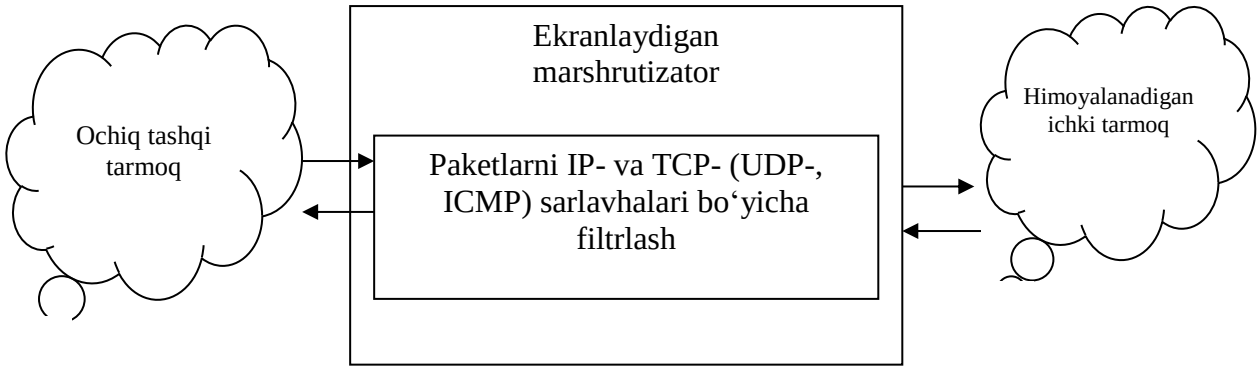


4.2.1-rasm. OSI modelining alohida sathlarida ishlaydigan tarmoqlararo ekranlar turi

Yuqorida keltirilgan tarmoqlararo ekranlarning xillari o‘zining afzalliklari va kamchiliklariga ega. Ishlatiladigan brandmauerlarning ko‘pchiligi yoki tatbiqiy shlyuzlar, yoki ekranlovchi marshrutizatorlar bo‘lib, tarmoqlararo aloqaning to‘liq xavfsizligini ta’minlamaydi. Ishonchli himoyani esa faqat har biri ekranlovchi marshrutizator, seans sathi shlyuzi, hamda tatbiqiy shlyuzni birlashtiruvchi tarmoqlararo ekranlarning kompleksi ta’minlaydi.

Ekranlovchi marshrutizator (screeningrouter) (paketli filtr (packetfilter) deb ham ataladi) xabarlar paketini filtrlashga atalgan va ichki va tashqi tarmoqlar orasida shaffof aloqani ta’minlaydi. U OSI modelining tarmoq sathida ishlaydi, ammo o‘zining ayrim funktsiyalarini bajarishida etalon modelining transport sathini ham qamrab olishi mumkin.

Ma’lumotlarni o‘tkazish yoki brakka chiqarish xususidagi qaror filtrlashning berilgan qoidalariga binoan har bir paket uchun mustaqil qabul qilinadi. Qaror qabul qilishda tarmoq va transport sathlari paketlarining sarlavhalari taxlil etiladi. (4.2.2-rasm).



4.2.2-rasm. Paketli filtrning ishlash sxemasi

Har bir paketning IP-va TCP/UDP–sarlavhalarining taxlillanuvchi hoshiyalari sifatida quyidagilar ishlatilishi mumkin:

- jo‘natuvchi adresi;
- qabul qiluvchi adresi;
- paket hili;
- paketni fragmentlash bayrog‘i;
- manba porti nomeri;
- qabul qiluvchi port nomeri.

Birinchi to‘rtta parametr paketning IP-sarlavhasiga, keyingilari esa TCP-yoki UDP sarlavhasiga taalluqli. Jo‘natuvchi va qabul qiluvchi adreslari IP-adreslar hisoblanadi. Bu adreslar paketlarni shakllantirishda to‘ldiriladi va uni tarmoq bo‘yicha uzatganda o‘zgarmaydi.

Paket xili hoshiyasida tarmoq sathiga mos keluvchi ICMP protokol kodi yoki taxlillanuvchi IP-paket taalluqli bo‘lgan transport sathi protokolining (TCP yoki UDP) kodi bo‘ladi.

Paketni fragmentlash bayrog‘i IP-paketlar fragmentlashining borligi yoki yo‘qligini aniqlaydi. Agar tahlillanuvchi paket uchun fragmentlash bayrog‘i o‘rnatilgan bo‘lsa, mazkur paket fragmentlangan IP-paketning qismpaketi

hisoblanadi.

Manba va qabul qiluvchi portlari nomerlari TCP yoki UDP drayver tomonidan har bir jo‘natiluvchi xabar paketlariga qo‘shiladi va jo‘natuvchi ilovasini, hamda ushbu paket atalgan ilovani bir ma’noda identifikatsiyalaydi. Portlar nomerlari bo‘yicha filtrlash imkoniyati uchun yuqori sath protokollariga port nomerlarini ajratish bo‘yicha tarmoqda qabul qilingan kelishuvni bilish lozim.

Har bir paket ishlanishida ekranlovchi marshrutizator berilgan qoidalar jadvalini, paketning to‘liq assotsiatsiyasiga mos keluvchi qoidani topgunicha, ketma-ket ko‘rib chiqadi. Bu erda assotsiatsiya deganda berilgan paket sarlavhalarida ko‘rsatilgan parametrlar majmui tushuniladi. Agar ekranlovchi marshrutizator jadvaldagi qoidalarning birortasiga ham mos kelmaydigan paketni olsa, u xavfsizlik nuqtai nazaridan, uni yaroqsiz holga chiqaradi.

Paketli filtrlar apparat va dasturiy amalga oshirilishi mumkin. Paketli filtr sifatida oddiy marshrutizator, hamda kiruvchi va chiquvchi paketlarni filtrlashga moslashtirilgan, serverda ishlovchi dasturdan foydalanish mumkin. Zamonaviy marshrutizatorlar har bir port bilan bir necha o‘nlab qoidalarni bog‘lashi va kirishda, ham chiqishda paketlarni filtrlashi mumkin.

Paketli filtrlarning kamchiligi sifatida quyidagilarni ko‘rsatish mumkin. Ular xavfsizlikning yuqori darajasini ta’minlamaydi, chunki faqat paket sarlavhalarini tekshiradi va ko‘pgina kerakli funksiyalarni madadlamaydi. Bu funktsiyalarga, masalan, oxirgi uzellarni autentifikatsiyalash, xabarlar paketlarini kriptografik bekitish, hamda ularning yaxlitligini va haqiqiyligini tekshirish kiradi. Paketli filtrlar dastlabki adreslarni almashtirib qo‘yish va xabarlar paketi tarkibini ruxsatsiz o‘zgartirish kabi keng tarqalgan tarmoq xujumlariga zaif hisoblanadilar. Bu xil brandmauerlarni "aldash" qiyin emas-filtrlashga ruxsat beruvchi qoidalarni qondiruvchi paket sarlavhalarini shakllantirish kifoya.

Ammo, paketli filtrlarning amalga oshirilishining soddaligi, yuqori unumdorligi, dasturiy ilovalar uchun shaffofligi va narhining pastligi, ularning hamma erda tarqalishiga va tarmoq xavfsizligi tizimining majburiy elementi kabi ishlatilishiga imkon yaratdi.

Seans sathi shlyuzi, (ekranlovchi transport deb ham yuritiladi) virtual ulanishlarni nazoratlashga va tashqi tarmoq bilan o‘zaro aloqa qilishda IP-adreslarni translyatsiyalashga atalgan. U OSI modelining seans sathida ishlaydi va ishlashi jarayonida etalon modelning transport va tarmoq sathlarini ham qamrab oladi. Seans sathi shlyuzining himoyalash funksiyalari vositachilik funksiyalariga taalluqli.

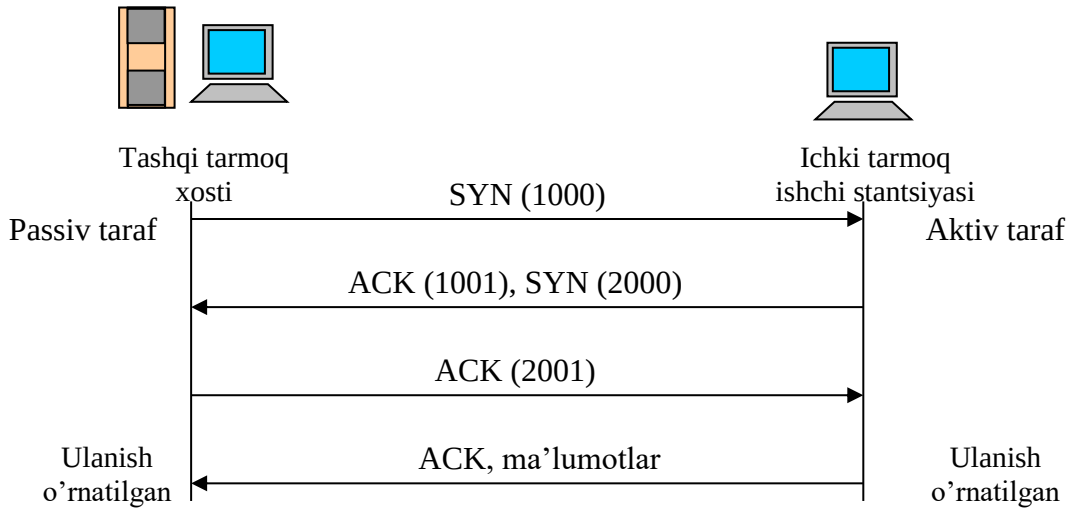
Virtual ulanishlarning nazorati aloqani kvitirlashni kuzatishdan hamda o‘rnatilgan virtual kanallar bo‘yicha axborot uzatilishining nazoratlashdan iborat. Aloqani kvitirlashning nazoratida seans sathida shlyuz ichki tarmoq ishchi stantsiyasi va tashqi tarmoq kompyuteri orasida virtual ulanishni kuzatib, so‘ralayotgan aloqa seansining joizligini aniqlaydi.

Bunday nazorat TCP protokolining seans sathi paketlarining sarlavhasidagi axborotga asoslanadi. Ammo TCP-sarlavhalarni taxlillashda paketli filtr faqat manba va qabul qiluvchi portlarining nomerini tekshirsa,

ekranlovchi transport aloqani kvirtirlash jarayoniga taalluqli boshqa hoshiyalarni tahlillaydi.

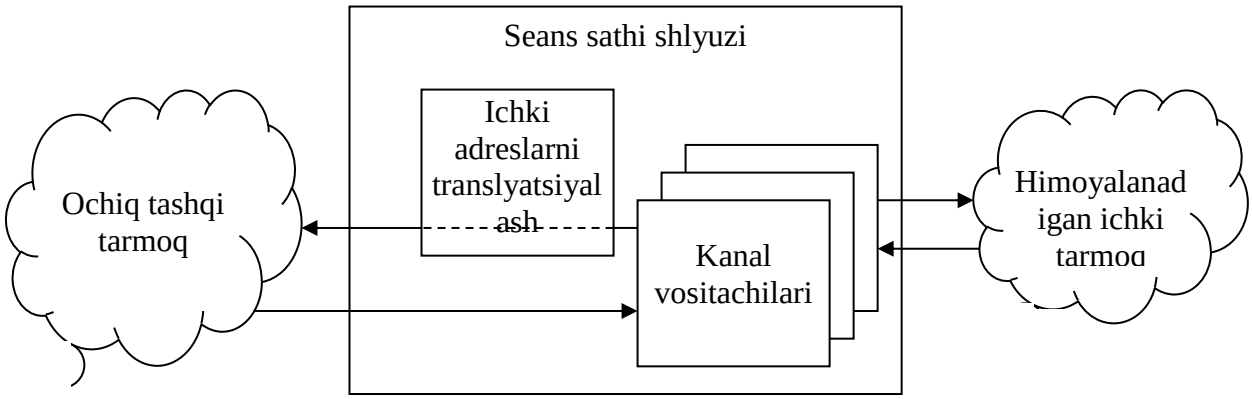
Bu muolaja SYN (Sinxronlash) va ACK (Tasdiqlash) bayroqlari orqali belgilanuvchi TCP-paketlarni almashishdan iborat (4.2.3-rasm).

SYN bayroq bilan belgilangan va tarkibida ixtiyoriy son, masalan 1000, bo‘lgan TCP seansining birinchi paketi mijozning seans ochishga so‘rovi hisoblanadi. Bu paketni olgan tashqi tarmoq kompyuteri javob tariqasida ACK bayroq bilan belgilangan va tarkibida olingan paketdagidan bittaga katta (bizning holda 1001) son bo‘lgan paketni jo‘natadi. Shu tariqa, mijozdan SYN paketi olinganligi tasdiqlanadi. So‘ngra, teskari muolaja amalga oshiriladi: tashqi tarmoq kompyuteri ham mijozga uzatiluvchi ma’lumotlar birinchi baytining tartib raqami bilan (masalan, 2000) SYN paketini jo‘natadi, mijoz esa uni olganligini, tarkibida 2001 soni bo‘lgan paketni uzatish orqali tasdiqlaydi. Shu bilan aloqani kvirtirlash jarayoni tugallanadi.



4.2.3– rasm. TCP protokoli bo‘yicha aloqani kvitirlash sxemasi.

Seans sathi shlyuzi (4.2.4-rasm) uchun so‘ralgan seans joiz hisoblanadi, qachonki aloqani kvirtirlash jarayoni bajarilishida SYN va ACK bayroqlar, hamda TCP-paketlari sarlavhalaridagi sonlar o‘zaro mantiqiy bog‘langan bo‘lsa.



4..2.4- rasm. Seans sathi shlyuzining ishlash sxemasi

Ichki tarmoqning ichki stantsiyasi va tashqi tarmoqning kompyuteri TCP seansining avtorizatsiyalangan qatnashchilari ekanligi hamda ushbu seansning

joizligi tasdiqlanganidan so‘ng shlyuz ulanishni o‘rnatadi. Bunda shlyuz ulanishlarining maxsus jadvaliga mos axborotni (jo‘natuvchi va qabul qiluvchi adreslari, ulanish holati, ketma-ketlik nomeri xususidagi axborot va h.) kiritadi.

Shu ondan boshlab shlyuz paketlarni nusxalaydi va ikkala tomonga yo‘naltirib, o‘rnatilgan virtual kanal bo‘yicha axborot uzatilishini nazorat qiladi. Ushbu nazorat jarayonida seans sathi shlyuzi paketlarni filtrlamaydi. Ammo u uzatiluvchi axborot sonini nazorat qilishi va qandaydir chegaradan oshganida ulanishni uzishi mumkin. Bu esa, o‘z navbatida, axborotning ruxsatsiz eksport qilinishiga to‘siq bo‘ladi. Virtual ulanishlar xususidagi qaydlash axborotining to‘planishi ham mumkin.

Seans sathi shlyuzlarida virtual ulanishlarni nazoratlashda kanal vositachilari (pipeproxy) deb yuritiluvchi maxsus dasturlardan foydalaniladi. Bu vositachilar ichki va tashqi tarmoqlar orasida virtual kanallarni o‘rnatadi, so‘ngra TCP/IP ilovalari generatsiyalagan paketlarning ushbu kanal orqali uzatilishini nazoratlaydi. Kanal vositachilari TCP/IPning muayyan xizmatlariga mo‘ljallangan. Shu sababli ishlashi muayyan ilovalarning vositachi-dasturlariga asoslangan tatbiqiy sath shlyuzlari imkoniyatlarini kengaytirishda seans sath shlyuzlaridan foydalanish mumkin.

Seans sathi shlyuzi tashqi tarmoq bilan o‘zaro aloqada tarmoq sathi ichki adreslarini (IP-adreslarini) translyatsiyalashni ham ta’minlaydi. Ichki adreslarni translyatsiyalash ichki tarmoqdan tashqi tarmoqqa jo‘natiluvchi barcha paketlarga nisbatan bajariladi.

Amalga oshirilishi nuqtai nazaridan seans sathi shlyuzi etarlicha oddiy va nisbatan ishonchli dastur hisoblanadi. U ekranlovchi marshrutizatorni virtual ulanishlarni nazoratlash va ichki IP-adreslarni translyatsiyalash funktsiyalari bilan to‘ldiradi.

Seans sathi shlyuzining kamchiliklari–ekranlovchi marshrutizatorlarning kamchiliklariga o‘xshash. Ushbu texnologiyaning yana bir jiddiy kamchiligi ma’lumotlar hoshiyalari tarkibini nazoratlash mumkin emasligi. Natijada, niyati buzuq odamlarga zarar keltiruvchi dasturlarni himoyalanuvchi tarmoqqa uzatish imkoniyati tug‘iladi. Undan tashqari, TCP-sessiyasining (TCP hijacking) ushlab qolinishida niyati buzuq odam xujumlarini hatto ruxsat berilgan sessiya doirasida amalga oshirishi mumkin.

Amalda aksariyat seans sath shlyuzlari mustaqil mahsulot bo‘lmay, tatbiqiy sath shlyuzlari bilan komplektda taqdim etiladi.

Tatbiqiy sath shlyuzi (ekranlovchi shlyuz deb ham yuritiladi) OSI modelining tatbiqiy sathida ishlab, taqdimiy sathni ham qamrab oladi va tarmoqlararo aloqaning eng ishonchli himoyasini ta’minlaydi. Tatbiqiy sath shlyuzining himoyalash funktsiyalari, seans sathi shlyuziga o‘xshab, vositachilik funktsiyalariga taalluqli. Ammo, tatbiqiy sath shlyuzi seans sathi shlyuziga qaraganda himoyalashning ancha ko‘p funktsiyalarini bajarishi mumkin:

-brandmauer orqali ulanishni o‘rnatishga urinishda foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;

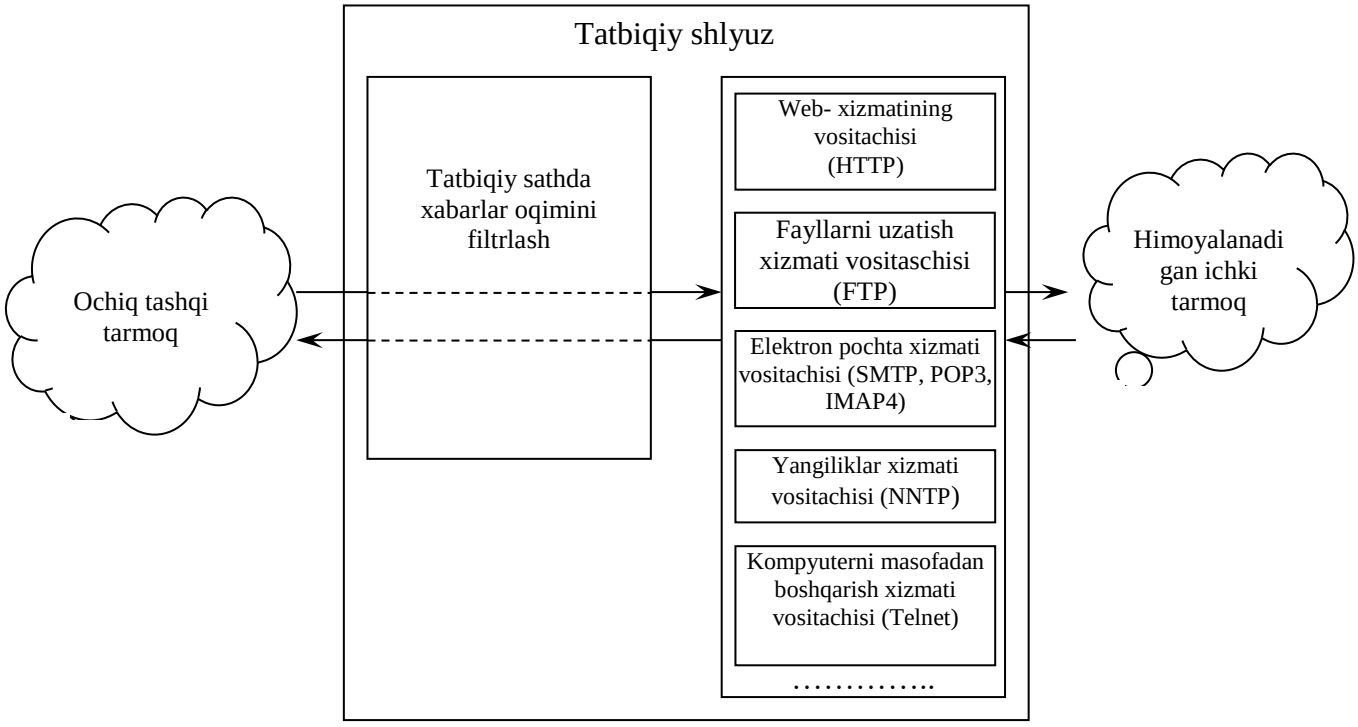
- shlyuz orqali uzatiluvchi axborotning haqiqiyligini tekshirish;
- ichki va tashqi tarmoq resurslaridan foydalanishni cheklash;
- axborot oqimini filtrlash va o‘zgartirish, masalan, viruslarni dinamik tarzda

qidirish va axborotni shaffof shifrlash;

- xodisalarni qaydlash, xodisalarga reaktsiya ko‘rsatish, hamda qaydlangan axborotni taxlillash va xisobotlarni generatsiyalash;
- tashqi tarmoqdan so‘raluvchi ma’lumotlarni keshlash.

Tatbiqiy sath shlyuzi funktsiyalari vositachilik funksiyalariga taalluqli bo‘lganligi sababli, bu shlyuz universal kompyuter hisoblanadi va bu kompyuterda har bir xizmat ko‘rsatiluvchi tatbiqiy protokol (HTTP, FTP, SMTP, NNTP va h.) uchun bittadan vositachi dastur (ekranlovchi agent) ishlatiladi. TCP/IPning har bir xizmatining vositachi dasturi (application proxy) aynan shu xizmatga taalluqli xabarlarni ishlashga va himoyalash funksiyalarini bajarishga mo‘ljallangan.

Tatbiqiy sath shlyuzi mos ekranlovchi agentlar yordamida kiruvchi va chiquvchi paketlarni ushlab qoladi, axborotni nusxalaydi va qayta jo‘natadi, ya’ni ichki va tashqi tarmoqlar orasidagi to‘g‘ridan-to‘g‘ri ulanishni istisno qilgan holda, server-vositachi funktsiyasini bajaradi (4.2.5-rasm).



4.2.5- rasm. Tatbiqiy shlyuzning ishlash sxemasi.

Tatbiqiy sath shlyuzi ishlatadigan vositachilar seans sathi shlyuzlarining kanal vositachilaridan jiddiy farqlanadi. Birinchidan, tatbiqiy sath shlyuzlari muayyan ilovalar (dasturiy serverlar) bilan bog‘langan, ikkinchidan ular OSI modelining tatbiqiy sathida xabarlar oqimini filtrlashlari mumkin.

Tatbiqiy sath shlyuzlari vositachi sifatida mana shu maqsadlar uchun maxsus ishlab chiqilgan TCP/IPning muayyan xizmatlarining dasturiy serverlari HTTP, FTP, SMTP, NNTP va hk. serverlaridan foydalanadi. Bu dasturiy serverlar brandmauerlarda rezident rejimida ishlaydi va TCP/IPning mos xizmatlariga taalluqli himoyalash funksiyalarini amalga oshiradi. UDP trafigiga UDP-paketlar tarkibining maxsus translyatori xizmat ko‘rsatadi.

Ichki tarmoq ishchi serveri va tashqi tarmoq kompyuteri orasida ikkita

ulanish amalga oshiriladi: ishchi stansiyadan brandmauergacha va brandmauerdan belgilangan joygacha. Kanal vositachilaridan farqli holda, tatbiqiy sath shlyuzining vositachilari faqat o‘zlari xizmat qiluvchi ilovalar generatsiyalagan paketlarni o‘tkazadi. Masalan, HTTP xizmatining vositachi-dasturi faqat shu xizmat generatsiyalagan trafikni ishlaydi.

Agar qandaydir ilovada o‘zining vositachisi bo‘lmasa, tatbiqiy sathdagi shlyuz bunday ilovani ishlay olmaydi va u blokirovka qilinadi. Masalan, agar tatbiqiy sathdagi shlyuz faqat HTTP, FTP va Telnet vositachi-dasturlaridan foydalansa, u faqat shu xizmatlarga tegishli paketlarni ishlaydi va qolgan xizmatlarning paketlarini blokirovka qiladi.

Tatbiqiy sath shlyuzi vositachilari, kanal vositachilaridan farqli holda, ishlanuvchi ma’lumotlar tarkibini tekshirishni ta’minlaydi. Ular o‘zlari xizmat ko‘rsatadigan tatbiqiy sath protokollaridagi komandalarning alohida xillarini va xabarlardagi axborotlani filtrlashlari mumkin.

Tatbiqiy sath shlyuzini sozlashda va xabarlarni filtrlash qoidalarini tavsiflashda quyidagi parametrlardan foydalaniladi: servis nomi, undan foydalanishning joiz vaqt oralig‘i, ushbu servisga bog‘liq xabar tarkibiga cheklashlar, servis ishlatadigan kompyuterlar, foydalanuvchi identifikatori, autentifikatsiyalash sxemalari va hk..

Tatbiqiy sath shlyuzi quyidagi afzalliklarga ega:

- aksariyat vositachilik funktsiyalarini bajara olishi tufayli lokal tarmoq himoyasining yuqori darajasini ta’minlaydi;
- ilovalar sathida himoyalash ko‘pgina qo‘shimcha tekshirishlarni amalga oshirishga imkon beradi, natijada dasturiy ta’minot kamchiliklariga asoslangan muvaffaqiyatli xujumlar o‘tkazish ehtimolligi kamayadi;
- tatbiqiy sath shlyuzining ishga layoqatligi buzilsa, bo‘linuvchi tarmoqlar orasida paketlarning to‘ppa-to‘g‘ri o‘tishi blokirovka qilinadi, natijada, rad qilinishi tufayli himoyalanuvchi tarmoqning xavfsizligi pasaymaydi.

Tatbiqiy sath shlyuzining kamchiliklariga quyidagilar kiradi:

- narxining nisbatan yuqoriligi;
- brandmauerning o‘zi, hamda uni o‘rnatish va konfiguratsiyalash muolajasi etarlicha murakkab;
- kompyuter platformasi unumdorligiga va resurslari hajmiga quyiladigan talablarning yuqoriligi;
- foydalanuvchilar uchun shaffoflikning yo‘qligi va tarmoqlararo aloqa o‘rnatilishida o‘tkazish qobiliyatining susayishi.

Tatbiqiy sath shlyuzining foydalanuvchilar uchun shaffofligining yo‘qligi va tarmoqlararo aloqa o‘rnatilishida o‘tkazish qobiliyatining susayishi kabi jiddiy kamchiliklarini bartaraf etish maqsadida paketlarni filtrlashning yangi texnologiyasi ishlab chiqilgan. Bu texnologiyani ba’zida ulanish xolatini nazoratlashli filtrlash (statefulinspection) yoki ekspert sathidagi filtrlash deb yuritishadi. Bunday filtrlash paketlar holatini ko‘p sathli tahlillashning maxsus usullari (SMLT) asosida amalga oshiriladi.

Ushbu gibrid texnologiya tarmoq sathida paketlarni ushlab qolish va undan ulanishni nazorat qilishda ishlatiluvchi tatbiqiy sath axborotini chiqarib olish orqali ulanish holatini kuzatishga imkon beradi.

Ishlashi asosini ushbu texnologiya tashkil etuvchi tarmoqlararo ekran ekspert sath brandmaueri deb yuritiladi. Bunday brandmauerlar o‘zida ekranlovchi marshrutizatorlar va tatbiqiy sath shlyuzlari elementlarini uyg‘unlashtiradi. Ular har bir paket tarkibini berilgan xavfsizlik siyosatiga muvofiq baholaydilar.

Shunday qilib ekspert sathidagi brandmauerlar quyidagilarni nazoratlashga imkon beradi:

- mavjud qoidalar jadvali asosida har bir uzatiluvchi paketni;
- holatlar jadvali asosida har bir sessiyani;
- ishlab chiqilgan vositachilar asosida har bir ilovani.

Ekspert sath tarmoqlararo ekranlarining afzalliklari sifatida ularning foydalanuvchilar uchun shaffofligini, axborot oqimini ishlashining yuqori tezkorligini hamda ular orqali o‘tuvchi paketlarning IP-adreslarini o‘zgartirmasligini ko‘rsatish mumkin. Oxirgi afzallik. IP-adresdan foydalanuvchi tatbiqiy sathning har qanday protokolining bunday brandmauerlardan hech qanday o‘zgarishsiz yoki maxsus dasturlashsiz birga ishlay olishini anglatadi.

Bunday brandmauerlarning avtorizatsiyalangan mijoz va tashqi tarmoq kompyuteri orasida to‘g‘ridan-to‘g‘ri ulanishga yo‘l qo‘yishi, himoyaning unchalik yuqori bo‘lmagan darajasini ta’minlaydi. Shu sababli amalda ekspert sathini filtrlash texnologiyasidan kompleks brandmauerlar ishlashi samaradorligini oshirishda foydalaniladi. Ekspert sathning filtrlash texnologiyasini ishlatuvchi kompleks brandmauerlarga misol tariqasida FireWall-1 va ON Guardlarni ko‘rsatish mumkin.

Mustaqil ish savollari:

1. Tarmoqlarda ishlatiladigan protokollar (TCP/IP, SPX/IPX) OSI etalon modeli bo‘yicha ekranlar xili qanday funksiyalarni qamrab o‘lishi mumkin.
2. TCP/IP protokoli bo‘yicha aloqani kvitlash sxemasini izoxlang.

Nazorat savollari:

1. Ekranlovchi marshrutizatorlarning ishlash printsipini tushuntirib berin.
2. Seans sathi shlyuzining funktsiyalarini yoritib bering.

4.3. Tarmoqlararo ekranlar asosidagi tarmoq himoyasining sxemalari

Tayanch ibora va tushunchalar: Tarmoqlararo aloqa, tarmoq servisidan foydalanish, tarmoqlararo ekran iashlash siyosati, local tarmoqni umumiy himoyalash sxemasi, ochiq tashqi tarmoq, himoyalangan ichki tarmoq, ochiq serverlar.

Mavzuga oid asosiy muammolar: Tarmoq servislaridan foydalanish siyosati himoyalanuvchi kompyter tarmoqlarining barcha servisidan foydalanish, “oshkora ruxcat etilmagani man qilinmagan” prinsipi tanlanganida tarmoqlararo ekran qanday sozlanadi.

Darsning maqsadi: Tarmoqlararo aloqani samarali himoyalash, brandmauer tizimi to‘g‘ridan-to‘g‘ri o‘rnatilishi va konfigurasiyalanish, tarmoqlararo aloqa siyosatini shakillantirish, brandmauerni ulash sxemasini tanlash va parametrlarini sozlash.

Tarmoqlararo aloqani samarali himoyalash uchun brandmauer tizimi to‘g‘ri o‘rnatilishi va konfiguratsiyalanishi lozim. Ushbu jarayon quyidagilarni o‘z

ichiga oladi:
- tarmoqlararo aloqa siyosatini shakllantirish;
- brandmauerni ulash sxemasini tanlash va parametrlarini sozlash.
Tarmoqlararo aloqa siyosatini shakllantirish.
Tarmoqlararo aloqa siyosatini shakllantirishda quyidagilarni aniqlash lozim:
- tarmoq servislaridan foydalanish siyosati;
- tarmoqlararo ekran ishlashi siyosati.

Tarmoq servislaridan foydalanish siyosati himoyalanuvchi kompyuter tarmog‘ining barcha servislarini taqdim etish, hamda ulardan foydalanish qoidalarini belgilaydi. Ushbu siyosat doirasida tarmoq ekrani orqali taqdim etiluvchi barcha servislar va har bir servis uchun mijozlarning joiz adreslari berilishi lozim. Undan tashqari, foydalanuvchilar uchun qachon va qaysi foydalanuvchilar qaysi servisdan va qaysi kompyuterda foydalanishlarini tavsiflovchi qoidalar ko‘rsatilishi lozim. Foydalanish usullariga cheklashlar ham beriladi. Bu cheklashlar foydalanuvchilarning Internetning man etilgan servislaridan aylanma yo‘l orqali foydalanishlariga yo‘l qo‘ymaslik uchun zarur. Foydalanuvchilar va kompyuterlarni autentifikatsiyalash qoidalari, hamda tashkilot lokal tarmog‘i tashqarisidagi foydalanuvchilarning ishlash sharoitlari alohida belgilanishi lozim.

Tarmoqlararo ekran ishlashi siyosatida tarmoqlararo aloqani boshqarishning brandmauer ishlashi asosidagi bazaviy printsipi beriladi. Bunday printsiplarning quyidagi ikkitasidan biri tanlanishi mumkin:
- oshkora ruxsat etilmagani man qilingan;
- oshkora man etilmaganiga ruxsat berilgan.

"Oshkora ruxsat etilmagani man qilingan" printsipi tanlanganida tarmoqlararo ekran shunday sozlanadiki, harqanday ruxsat etilmagan tarmoqlararo aloqalar blokirovka qilinadi. Ushbu printsip axborot xavfsizligining barcha sohalarida ishlatiluvchi foydalanishning mumtoz modeliga mos keladi. Bunday yondashish, imtiyozlarni minimallashtirish printsipini adekvat amalga oshirishga imkon berishi sababli, xavfsizlik nuqtai nazaridan yaxshiroq hisoblanadi. Mohiyati bo‘yicha "oshkora ruxsat etilmagani man qilingan" printsipi zarar keltirishi faktini e’tirof etishdir. Ta’kidlash lozimki, ushbu printsipga asosan ta’riflangan foydalanish qoidalari foydalanuvchilarga ma’lum noqulayliklar tug‘dirishi mumkin.

"Oshkora man etilmaganiga ruxsat berilgan" printsipi tanlanganida tarmoqlararo ekran shunday sozlanadiki, faqat oshkora man etilgan tarmoqlararo aloqalar blokirovka qilinadi. Bu holda, foydalanuvchilar tomonidan tarmoq servislaridan foydalanish qulayligi oshadi, ammo tarmoqlararo aloqa xavfsizligi pasayadi. Foydalanuvchilarning tarmoqlararo ekranni chetlab o‘tishlariga imkon tug‘iladi, masalan ular siyosat man qilmagan (hatto siyosatda ko‘rsatilmagan) yangi servislaridan foydalanishlari mumkin. Ushbu printsip amalga oshirilishida ichki tarmoq xakerlarning xujumlaridan kamroq himoyalangan bo‘ladi. Shu sababli, tarmoqlararo ekranlarni ishlab chiqaruvchilari odatda ushbu printsipdan foydalanmaydilar.

Oddiy tarmoqlararo ekranlar bu funktsiyalarning birini bajarishga mo‘ljallangan. Kompleks tarmoqlararo ekranlar himoyalashning ko‘rsatilgan

funksiyalarining birgalikda bajarilishini ta’minlaydi.

Tarmoqlararo ekranlarni ulashning asosiy sxemalari. Korporativ tarmoqni global tarmoqlarga ulaganda himoyalanuvchi tarmoqning global tarmoqdan va global tarmoqning himoyalanuvchi tarmoqdan foydalanishini cheklash, hamda ulanuvchi tarmoqdan global tarmoqning masofadan ruxsatsiz foydalanishidan himoyalashni ta’minlash lozim. Bunda tashkilot o‘zining tarmog‘i va uning komponentlari xususidagi axborotni global tarmoq foydalanuvchilaridan bekitishga manfaatdor. Masofadagi foydalanuvchilar bilan ishlash himoyalanuvchi tarmoq resurslaridan foydalanishning qat’iy cheklanishini talab etadi.

Tashkilotdagi korporativ tarmoq tarkibida ko‘pincha himoyalanishning turli sathli birnecha segmentlarga ega bo‘lishi ehtiyoji tug‘iladi:

- bemalol foydalaniluvchi segmentlar (masalan, reklama WWW-serverlari);
- foydalanish chegaralangan segmentlar (masalan, tashkilotning masofadagi uzellari xodimlarining foydalanishi uchun);
- yopiq segmentlar (masalan, tashkilotning moliya lokal qism tarmog‘i)

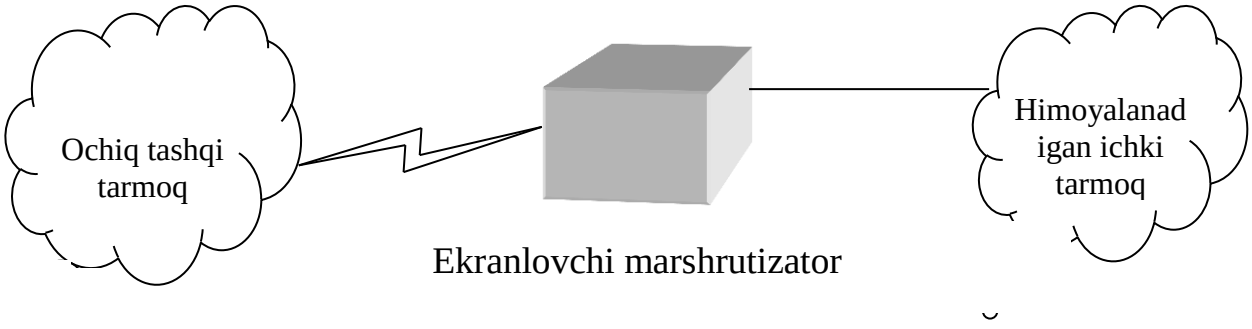
Tarmoqlararo ekranlarni ulashda turli sxemalardan foydalanish mumkin. Bu sxemalar himoyalanuvchi tarmoq ishlashi sharoitiga, hamda ishlatiladigan brandmauerlarning tarmoq interfeyslari soniga va boshqa xarakteristikalariga bog‘liq. Tarmoqlararo ekranni ulashning quyidagi sxemalari keng tarqalgan:

- ekranlovchi marshrutizatordan foydalanilgan himoya sxemalari;
- lokal tarmoqni umumiy himoyalash sxemalari;
- himoyalanuvchi yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemalar;
- yopiq va ochiq qism tarmoqlarni alohida himoyalovchi sxemalar.

Ekranlovchi marshrutizatordan foydalanilgan himoya sxemasi.

Paketlarni filtrlashga asoslangan tarmoqlararo ekran keng tarqalgan va amalga oshirilishi oson. U himoyalanuvchi tarmoq va bo‘lishi mumkin bo‘lgan g‘anim ochiq tarmoq orasida joylashgan ekranlovchi marshrutizatordan iborat (4.3.1-rasm).

Ekranlovchi marshrutizator (paketli filtr) kiruvchi va chiquvchi paketlarni ularning adreslari va portlari asosida blokirovka qilish va filtrlash uchun konfiguratsiyalangan.



4.3.1-расм. Tarmoqlararo ekran–ekranlovchi marshrutizator.

Himoyalanuvchi tarmoqdagi kompyuterlar Internetdan to‘g‘ridan-to‘g‘ri foydalana oladi, Internetning ulardan foydalanishining ko‘p qismi esa

blokirovka qilinadi. Umuman, ekranlovchi marshrutizator yuqorida tavsiflangan himoyalash siyosatidan istalganini amalga oshirishi mumkin. Ammo, agar marshrutizator paketlarni manba porti va kirish yo‘li va chiqish yo‘li portlari nomeri bo‘yicha filtrlamasa, "oshkora ruxsat etilmagani man qilingan" siyosatini amalga oshirish qiyinlashadi.

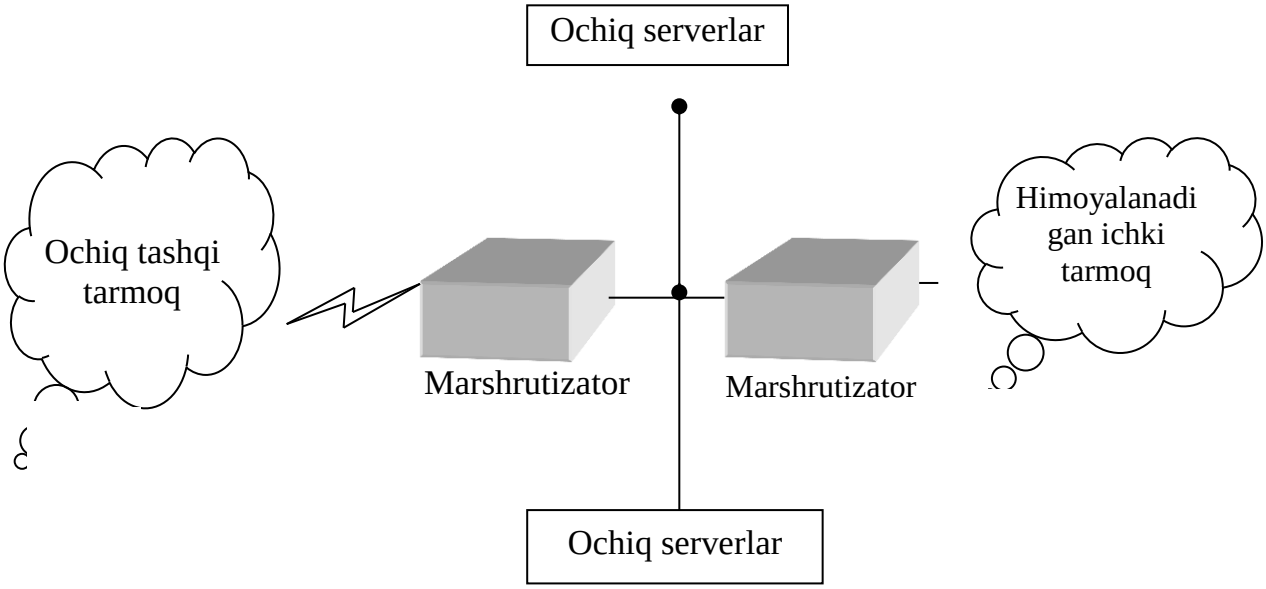
Paketlarni filtrlashga asoslangan tarmoqlararo ekranning kamchiliklari quyidagilar:

- filtrlash qoidalarining murakkabligi; ba’zi hollarda bu qoidalar majmui bajarilmasligi mumkin;
- filtrlash qoidalarini to‘liq testlash mumkin emasligi; bu tarmoqni testlanmagan xujumlardan himoyalanmasligiga olib keladi;
- xodisalarni ro‘yxatga olish imkoniyatining yo‘qligi; natijada ma’murga mashrutizatorning xujumga duch kelganligini va obro‘sizlantirilganligini aniqlash qiyinlashadi.

Lokal tarmoqni umumiy himoyalash sxemalari. Bitta tarmoq interfeysli brandmauerlardan foydalanilgan himoyalash sxemalari xavfsizlik va konfiguratsiyalashning qulayligi nuqtai nazaridan samarasiz hisoblanadi. Ular ichki va tashqi tarmoqlarni fizik ajratmaydilar, demak, tarmoqlararo aloqaning ishonchli himoyasini ta’minlay olmaydilar.

Lokal tarmoqni umumiy himoyalash sxemasi eng oddiy echim bo‘lib, unda brandmauer lokal tarmoqni tashqi g‘anim tarmoqdan butunlay ekranlaydi. Marshrutizator va brandmauer orasida faqat bitta yo‘l bo‘lib, bu yo‘l orqali butun trafik o‘tadi. Brandmauerning ushbu varianti "oshkora ruxsat etilmagani man qilingan" printsipiga asoslangan himoyalash siyosatini amalga oshiradi. Odatda marshrutizator shunday sozlanadiki, brandmauer tashqaridan ko‘rinadigan yagona mashina bo‘ladi.

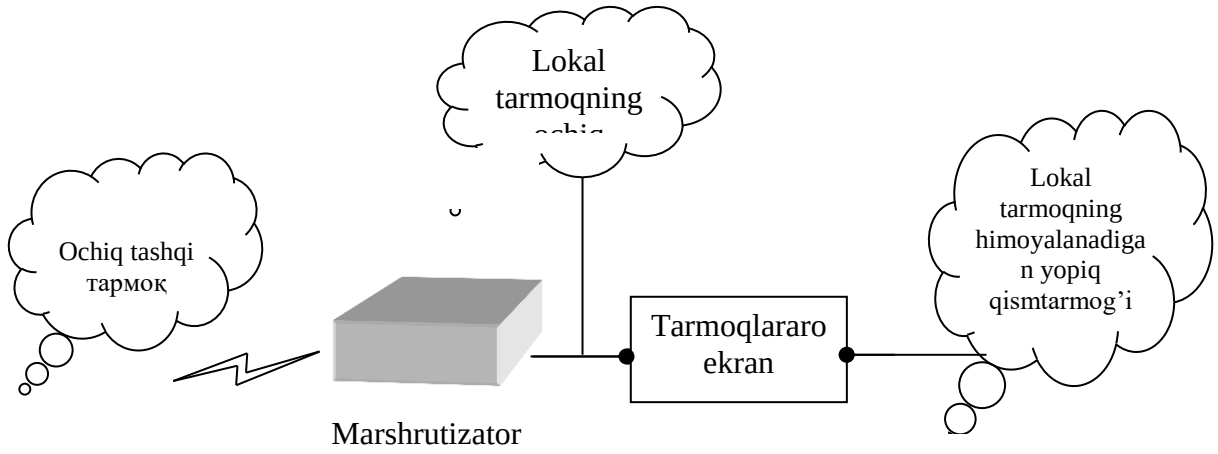
Lokal tarmoq tarkibidagi ochiq serverlar ham tarmoqlararo ekranlar tomonidan himoyalanadi. Ammo, tashqi tarmoq foydalana oladigan serverlarni himoyalanuvchi lokal tarmoqlarning boshqa resurslari bilan birlashtirish tarmoqlararo aloqa xavfsizligini jiddiy pasaytiradi.



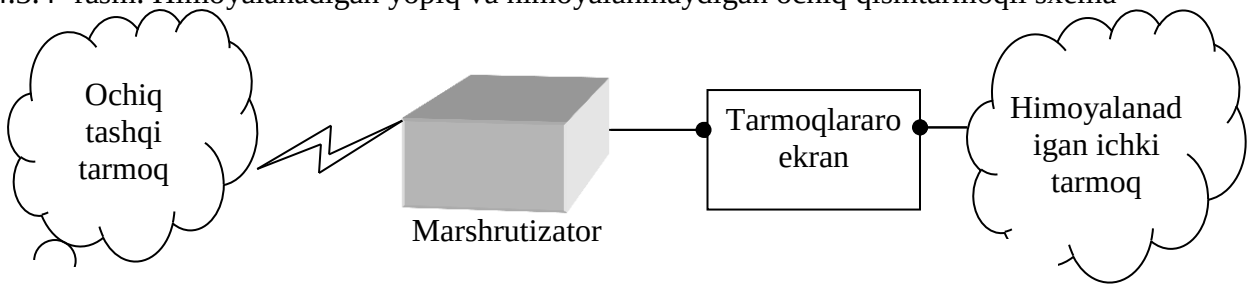
4.3.2- rasm. Bitta tarmoq interfeysli firewall yordamida lokal tarmoqni himoyalash

Tarmoqlararo ekran foydalanadigan xostga foydalanuvchilarni kuchaytirilgan autentifikatsiyalash uchun dastur o‘rnatilishi mumkin.

Himoyalanuvchi yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemalar. Agar lokal tarmoq tarkibida umumfoydalanuvchi ochiq serverlar bo‘lsa ularni tarmoqlararo ekrandan oldin ochiq qismtarmoq sifatida chiqarish maqsadga muvofiq hisoblanadi (4.3.3-rasm).



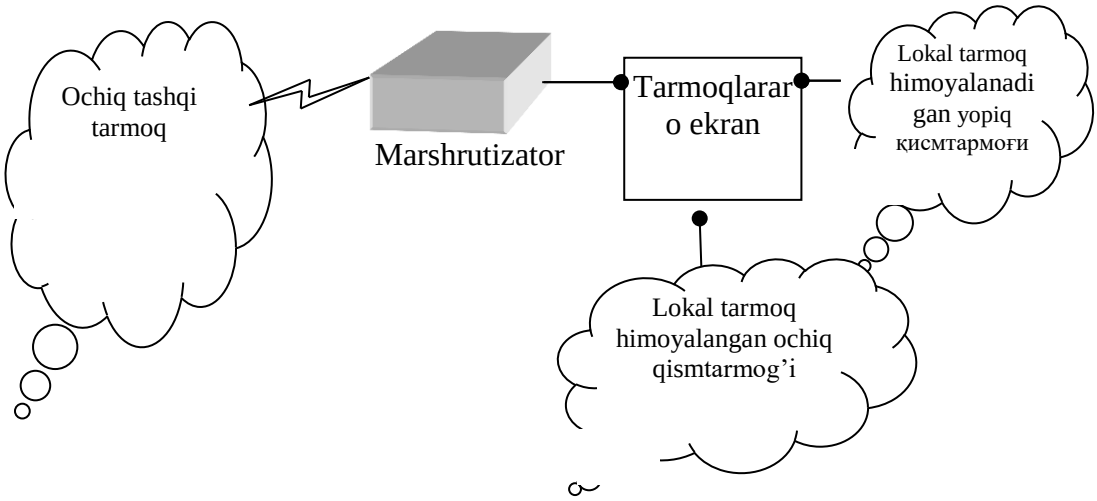
4.3.4- rasm. Himoyalanadigan yopiq va himoyalanmaydigan ochiq qismtarmoqli sxema



4.3.3- rasm. Lokal tarmoqni umumiy himoyalash sxemasi

Ushbu usul lokal tarmoq yopiq qismining kuchli himoyalanishini, ammo tarmoqlararo ekrangacha joylashgan ochiq serverlarning pasaygan himoyalanishini ta’minlaydi.

Ba’zi brandmauerlar bu serverlarni o‘zida joylashtiradi. Ammo bu brandmauerning xavfsizligi va kompyuterning yuklanishi nuqtai nazaridan yaxshi echim hisoblanmaydi. Himoyalanuvchi yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemani ochiq qismtarmoq xavfsizligiga qo‘yiladigan talablarning yuqori bo‘lmagan hollarida ishlatilishi maqsadga muvofiq hisoblanadi. Agar ochiq server xavfsizligiga yuqori talablar qo‘yilsa, yopiq va ochiq qismtarmoqlarni alohida himoyalash sxemalaridan foydalanish zarur.



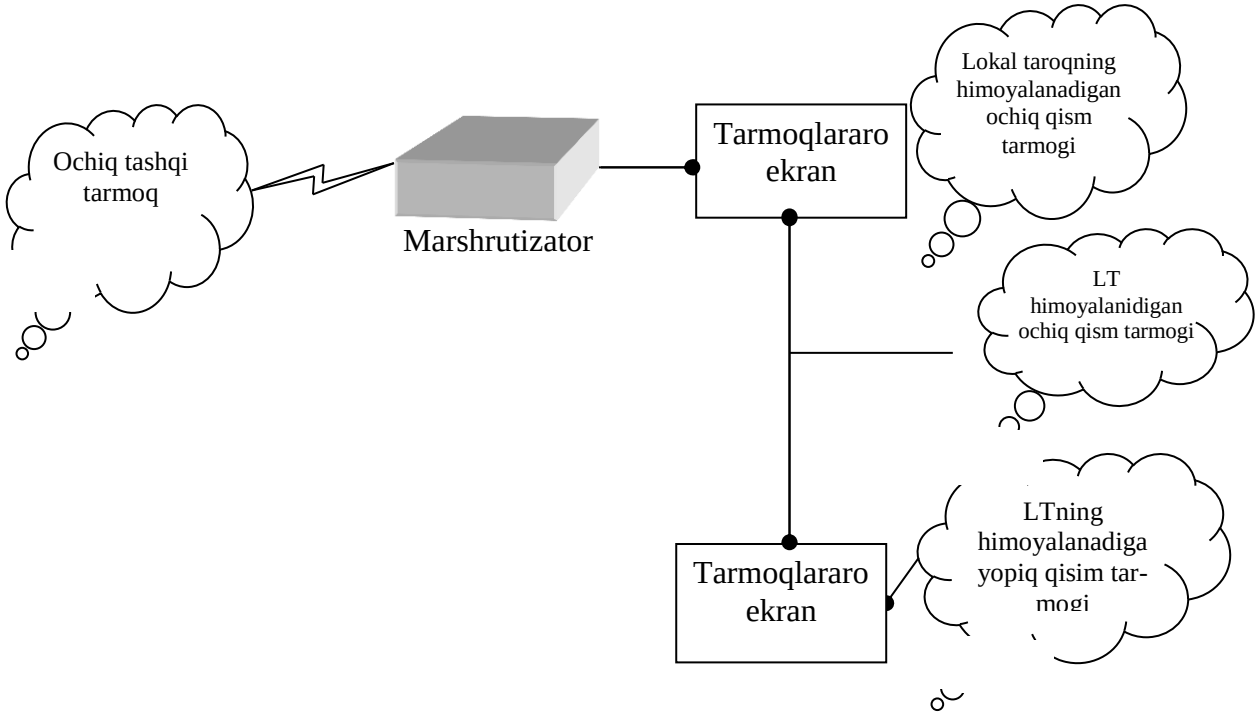
4.3.5 - rasm. Uchta tarmoq interfeysli bir brandmauer asosida yopiq va ochiq qismtarmoqlarni alohida himoyalash sxemasi

Bunday sxemalar uchta tarmoq interfeysli bitta brandmauer (4.3.6-rasm) yoki ikkita tarmoq interfeysli ikkita brandmauer (4.3.7-rasm) asosida qurilishi mumkin. Ikkala holda ham ochiq va yopiq qismtarmoqlardan faqat tarmoqlararo ekran orqali foydalanish mumkin. Bunda ochiq qismtarmoqdan foydalanish yopiq qism tarmoqdan foydalanishga imkon bermaydi.

Ikkita brandmauerli sxema tarmoqlararo aloqa xavfsizligining yuqori darajasini ta'minlaydi. Bunda har bir brandmauer yopiq tarmoqni himoyalashning alohida eshelonini hosil qiladi, himoyalanuvchi ochiq qismtarmoq esa ekranlovchi qismtarmoq sifatida ishtirok etadi. Odatda ekranlovchi qismtarmoq shunday konfiguratsiyalanadiki, qismtarmoq kompyuteridan g'anim tashqi tarmoq va lokal tarmoqning yopiq qismtarmog'i foydalana olsin. Ammo tashqi tarmoq va yopiq qismtarmoq orasida to'g'ridan-to'g'ri axborot paketlarini almashish mumkin emas.

Ekranlovchi qismtarmoqli tizimga xujum qilishda, bo'lmaganida himoyaning ikkita mustaqil chizig'ini bosib o'tishga to'g'ri keladi. Bu esa juda murakkab masala hisoblanadi. Tarmoqlararo ekran holatlarini monitoringlash vositalari bunday urinishni doimo aniqlashi va tizim ma'muri o'z vaqtida ruxsatsiz foydalanishga qarshi zaruriy choralar ko'rishi mumkin.

Ta’kidlash lozimki, aloqaning kommutatsiyalanuvchi liniyasi orqali



4.3.7-rasm. Ikkita tarmoq interfeysli ikkita brandmauer asosida yopiq va ochiq qismtarmoqlarni alohida himoyalash sxemasi

ulanuvchi masofadagi foydalanuvchilarning ishi ham tashkilotda o‘tkaziluvchi xavfsizlik siyosatiga muvofiq nazorat qilinishi shart. Bunday masalaning namunaviy hal etilishi–zaruriy funktsional imkoniyatlarga ega bo‘lgan masofadan foydalanish serverini (terminal serverni) o‘rnatish. Terminal server bir necha asinxron portlarga va lokal tarmoqning bitta interfeysiga ega bo‘lgan tizim hisoblanadi. Asinxron portlar va lokal tarmoq orasida axborot almashish faqat tashqi foydalanuvchini autentifikatsiyalashdan keyin amalga oshiriladi.

Terminal serverni ulashni shunday amalga oshirish lozimki, uning ishi faqat tarmoqlararo ekran orqali bajarilsin. Bu masofalagi foydalanuvchilarning tashkilot axborot resurslari bilan ishlash xavfsizligining kerakli darajasini ta’minlashga imkon beradi.

Shaxsiy va taqsimlangan tarmoq ekranlari. Oxirgi bir necha yil mobaynida korporativ tarmoq tuzilmasida ma’lum o‘zgarishlar sodir bo‘ldi. Agar ilgari bunday tarmoq chegaralarini aniq belgilash mumkin bo‘lgan bo‘lsa, hozirda bu mumkin emas. Yaqindayoq bunday chegara barcha marshrutizatorlar yoki boshqa qurilmalar (masalan, modemlar) orqali o‘tar va ular yordamida tashqi tarmoqlarga chiqilar edi. Ammo hozirda tarmoqlararo ekran orqali himoyalanuvchi tarmoqning to‘la huquqli egasi – himoyalanuvchi perimetr tashqarisidagi xodim hisoblanadi. Bunday xodimlar sirasiga uydagi yoki mehnat safaridagi xodimlar kiradi. Shubxasiz, ularga ham himoya zarur. Ammo barcha an’anaviy tarmoqlararo ekranlar shunday qurilganki, himoyalanuvchi foydalanuvchilar va resurslar ularning himoyasida korporativ yoki lokal tarmoqning ichki tomonida bo‘lishlari shart. Bu esa mobil foydalanuvchilar uchun mumkin emas.

Bu muammoni echish uchun quyidagi yondashishlar taklif etilgan:

- taqsimlangan tarmoqlararo ekranlardan (distributed firewall) foydalanish;
- virtual xususiy tarmoqVPNlar imkoniyatidan foydalanish.

Taqsimlangan tarmoqlararo ekran tarmoqning alohida kompyuterini himoyalovchi markazdan boshqariluvchi tarmoq mini-ekranlar majmuidir.

Taqsimlangan brandmauerlarning qator funktsiyalari (masalan markazdan boshqarish, xavfsizlik siyosatini tarqatish) shaxsiy foydalanuvchilar uchun ortiqcha bo‘lganligi sababli, taqsimlangan brandmauerlar modifikatsiyalandi. Yangi yondashish shaxsiy tarmoqli ekranlash texnologiyasi nomini oldi. Bunda tarmoqli ekran himoyalanuvchi shaxsiy kompyuterda o‘rnatiladi. Kompyuterning shaxsiy ekrani (personal firewall) yoki tarmoqli ekranlash tizimi deb ataluvchi bunday ekran, boshqa barcha tizimli himoyalash vositalariga bog‘liq bo‘lmagan holda butun chiquvchi va kiruvchi trafikni nazoratlaydi. Natijada, shu tariqa himoyalanuvchi kompyuter ichki servislarining zaifligi pasayadi, chunki chetki niyati buzuq odam oldin, himoyalash vositalari sinchiklab va qat’iy konfiguratsiyalangan ekranni bosib o‘tishi lozim.

Taqsimlangan tarmoqlararo ekranlar, an’anaviy tarmoqlararo ekranlardan farqli ravishda, qo‘shimcha dasturiy ta’minot bo‘lib, xususan korporativ serverlarni, masalan Internet-serverlarni ishonchli himoyalashi mumkin. Korporativ tarmoqni himoyalashning oqilona echimi – himoyalash vositasini u himoya qiluvchi serveri bilan bir platformada joylashtirishdir. 4.3.6-rasmda korporativ serverlarni taqsimlangan tarmoqlararo ekranlar yordamida himoyalash sxemasi keltirilgan.

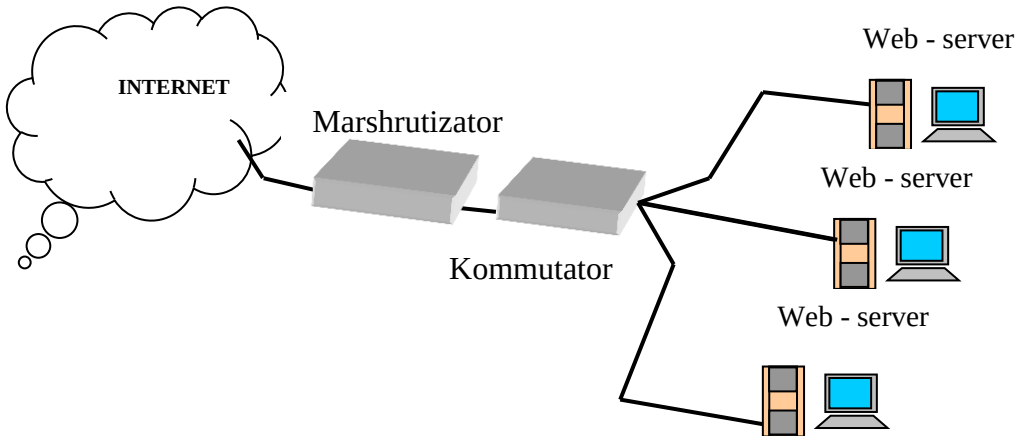
An’anaviy va taqsimlangan tarmoqlararo ekranlar quyidagi ko‘rsatkichlari bo‘yicha taqqoslanadi.

Samaradorlik. An’anaviy brandmauer ko‘pincha tarmoq perimetri bo‘yicha joylashtiriladi, ya’ni u himoyaning bir qatlamini ta’minlaydi xolos. Agar bu yagona qatlam buzilsa, tizim har qanday xujumga bardosh bera olmaydi. Taqsimlangan brandmauer operatsion tizimning yadro sathida ishlaydi va barcha kiruvchi va chiquvchi paketlarni tekshirib korporativ serverlarni ishonchli himoyalaydi.

O‘rnatilishining osonligi. An’anaviy brandmauer korporativ tarmoq konfiguratsiyasining bo‘limi sifatida o‘rnatilishi lozim. Taqsimlangan brandmauer dasturiy ta’minot bo‘lib, sanoqli daqiqalarda o‘rnatiladi va olib tashlanadi.

Boshqarish. An’anaviy brandmauer tarmoq ma’muri tomonidan boshqariladi. Taqsimlangan brandmauer tarmoq ma’muri yoki lokal tarmoq foydalanuvchisi tomonidan boshqarilishi mumkin.

Unumdorlik. An’anaviy brandmauer tarmoqlararo almashishni ta’minlovchi qurilma bo‘lib, unumdorligi paket/daqiqa bo‘yicha belgilangan cheklashga ega. U bir-biri bilan kommunikatsiyalanuvchi mahalliy tarmoq orqali bog‘langan o‘suvchi server parklari uchun to‘g‘ri kelmaydi.



4.3.8- rasm. Taqsimlangan tarmoqlararo ekranlar yordamida

An’anaviy brandmauer, odatda funktsiyalari belgilangan, narxi etarlicha yuqori tizim hisoblanadi. Brandmauerning taqsimlangan mahsulotlari dasturiy ta’minot bo‘lib, an’anaviy tarmoqlararo ekranlar narxining 1/5 yoki 1/10 gateng.

Mustaqil ish savollari:

1. Tarmoqlararo ekran ishlashi sxemasini qanday ishlash prinsipi mavjud.
2. Bitta va uchta tarmoq interfeysli firewell yordamida local tarmoqni himoyalash.

Nazorat savollari:

1. Tarmoqlarni ekranlovchi marshrutizatorlar yordamida himoyalash sxemasini tushuntirib bering.
2. Tarmoqlararo ekran yordamida lokal tarmoqni himoyalash sxemasini yoritib bering.
3. Himoyalanadigan yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemani tushuntirib bering.

V BOB. AMALIY MASHG‘ULOTLAR.

1-amaliy mashg‘ulot.

Mavzu: O‘rin almashtirish shifrlari.

Almashtirish (podstanovka) usullarining moxiyati bir alfavitda yozilgan axborot simvollarini boshqa alfavit simvollari bilan ma’lum qoida bo‘yicha almashtirishdan iboratdir. Eng sodda usul sifatida to‘gridan-to‘g‘ri o‘rin almashtirishni ko‘rsatish mumkin. Dastlabki axborot yoziluvchi A_0 alfavitning s_{oi} simvollariga shifrlovchi Aj alfavitning simvollari mos qo‘yiladi. Oddiy xolda ikkala alfavit xam bir xil simvollar to‘plamiga ega bo‘lishi mumkin.

Ikkala alfavitdagi simvollar o‘rtasidagi moslik ma’lum algoritm bo‘yicha K simvollar uzunligiga ega bo‘lgan dastlabki matn T_0 simvollarining raqamli ekvivalentlarini o‘zgartirish orqali amalga oshiriladi.

Monoalfavitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko‘rinishda ifodalanishi mumkin

1-qadam. [lxR] o‘lchamli dastlabki A_0 alfavitdagi xar bir simvol s_0 € T i=1k) ni A_0 alfavitdagi s_{0l} simvol tartib raqamiga mos keluvchi h_0 (s_0j) songa almashtirish yoli bilan raqamlar ketma-ketligi L_{0h} ni shakllantirish.

2-qadam. L_{0h} ketma-ketligining xar bir sonini h_{1h}= (k_1xh_0i(s_0i)+k_2)(modR) formula orqali xisoblanuvchi L_{1h} ketma-ketlikning mos soni h_{ji} ga almashtirish yo‘li bilan L_{lh} son ketma-ketligini shakllantirish, bu erda k_1- o‘nlik koeffitsent; k_2-siljitish koeffitsenti. Tanlangan k_1k_2 koeffitsentlar h_{oi}, h_{ij} sonlarning bir ma’noli mosligini ta’minlashi lozim, h_{ij}=0 olinganida esa h_{ij}=R almashinuvi bajarilishi kerak.

1-qadam. L_{ih} ketma-ketlikning xar bir soni h_{ih}(s_{li}) ni [lxR] o‘lchamli shifrlash alfavitning mos S_{ji}, € Ti($i^{=1k}$) simvoli bilan almashtirish yo‘li bilan Ti shifrmatnni xosil qilish.

2-qadam. Olingan shifrmatn o‘zgarmas B uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to‘liq bo‘lmasa blok orqasiga maxsus simvol-to‘ldiruvchilar joylashtiriladi (masalan:*).

Shifrlovchi jadval usulida kalit sifatida quyidagilar qo‘llaniladi:

-jadval o‘lchovlari;

-so‘z yoki so‘zlar ketma-ketligi;

-jadval tarkibi xususiyatlari.

Masalan:

T_0=KADRLAR TAYYORLASH MILLIY DASTURI

K=4x7; B=4;

Ushbu axborot ustun bo‘yicha ketma-ket jadvalga kiritiladi:

K	L	A	L	I	Y	T
A	A	Y O	A	L	D	Y
D	R	E	S H	L	A	R
R	T	R	M	I	S	I

Natijada, 4x7 o‘lchovli jadval tashkil qilinadi. Endi shifrlangan matn qatorlar bo‘yicha aniqlanadi, ya’ni o‘zimiz uchun 4 tadan belgilarni ajratib yozamiz.

KLAL_IYTA_AYAL_DUDR_YoShLA_RRTR_MISI Bu erda kalit sifatida jadval o‘lchovlari xizmat qiladi. Oddiy o‘rin almashtirish usulidan tashqari kalit yordamida o‘rin almashtirish usuli xam mavjud. Shifrlash jadvalidan kalit orqali foydalaniladi.

Bu erda kalit simvollariga mos xolda jadvalning o‘lchamiga qarab NxM jadvali tuziladi va ochiq matnni (T_0) ustun bo‘yicha joylashtirilib chiqiladi. So‘ngra kalit simvollari alfavit tartibida tartiblanib, ustun bo‘yicha o‘rin almashtiriladi, qator bo‘yicha o‘qilib shifrlangan matnga (T_1) ega bo‘linadi va bloklarga bo‘linadi.

T_0= O‘zbekistan kelajagi buyuk davlat;
K = Toshkent;
B=4;
Matnda 28-ta va kalitda 7-ta xarflar borligi uchun 6x7 jadval tuzamiz.

T	o	sh	k	e	n	t
5	4	7	2	1	3	6
O ‘	k	o	l	g	yu	v
z	i	n	a	i	k	l
b	s	k	j	b	d	a
e	t	e	a	u	a	t

Raqam bo‘yicha ustunlarni o‘zgartirib chiqamiz.

e	k	n	o	T	т	sh
1	2	3	4	5	6	7
g	l	yu	k	u	b	o
i	a	k	i	z	l	n
b	j	d	s	b	a	k
u	a	a	t	e	t	e

Qator bo‘yicha 4 tadan bloklarga bo‘lib, simvollar ketma-ketligidagi shifrlangan matnni olamiz.

Ketma- keraki agar qatorda ikkita bir xil simvollar ketma - ketligi kelsa, chap tarafdan kelayotgan birivchi raqamlanadi, keyin esa ikkinchisi raqamlanadi va shifrlangan matn xosil qilinadi.

T_1= GLYUK_ UVOI_AKIZ_LNBJ_DSBA_KUUA_TETE Shifrni ochishda teskari jarayon amalga oshiriladi. Shifrlanish jarayoni qadamma qadam amalga oshirila maqsadga mufofiq bo‘lar edi.

2-amaliy mashg‘ulot.

Mavzu: Ikki tomonlama o‘rin almashtirish usuli.

Bu usulda kalit sifatida ustun va qatordagi xarflar tartibdagi sonlardan foydalaniladi. Avvalom bor kalit simvollariga qarab jadval tuziladi va ochiq T_o matn joylashtirib chiqiqiladi, so‘ngra esa raqamlar navbatma navbat tartiblanib, avval ustun, so‘ngra esa qatorlar o‘rni almashtiriladi va jadvaldagi ma’lumot qator bo‘yicha o‘qilib T_1 ga ega bo‘linadi. Masalan: “Malakali xizmatchi” ochiq matnni shifrlash talab etilsin. Bu erda kalit bo‘lib 1342 va 2314 xizmat qiladi. Yaxshiroq izoxlanishi uchun K_1=1342 va K_2=2314, B=4 deb belgilab olamiz.

4x4 jadval yaratib T_0 qator bo‘yicha yozamiz (1-jadval). 2-jadvaldagi ko‘rinish bo‘yicha qator va ustunlar tartibbilan o‘rinlari almashtiriladi.

2	3	1	4
M	a	l	a
k	a	l	i
x	i	z	m
a	t	ch	i

1-jadval

M	a	l	a
a	t	ch	i
k	a	l	i
x	i	z	m

2- jadval

a	m	a	l
i	a	t	ch
i	k	a	l
m	x	i	z

3- jadval

3- jadvalga asosan shifrlaтgan matni yozamiz va bloklarga bo‘lib chiqamiz.

T_1 =AMAL_IATCH_IKAL_MXIZ

Ikki tomonlama almashtirishda jadval kattaligiga qarab variantlar xam ortib boradi. Jadval o‘lchamining kattaligi shifr chidamliligini oshiradi,

Sexrli kvadrat deb, katakchalariga 1 dan boshlab sonlar yozilgan, undagi xar bir ustun, satr va diagonal bo‘yicha sonlar yigindisi bitga songa teng bo‘lgan kvadrat shaklidagi jadvalga aytiladi. Sexrli kvadratga sonlar tartibi bo‘yicha belgilar kiritiladi va bu belgilar satrlar bo‘yicha ukilangan matn xosil bo‘ladi.

Sexrli kvadrat-qadimgi Xitoy tarixiga borib taqaladi. Afsonalarga ko‘ra Yu imperatori boshqaruvi vaqtida (bizning asrimizdan 2200 yil ilgari) Xuanxe (Sariq daryo) suvi ostidan toshbaqa suzib chiqadi va bu toshbaqa ustidagi toshi(pantsiri)da maxfiy ierogliflar chizilgan bo‘lib, keyinchalik bu belgilar «lo-shu» atamasi bilan nomlangan.

XI asrga kelib sexrli kvadrat bilan Xindiston, keyinchalik esa Yaponiya olimlari shugillanishgan. Evropaga sexrli kvadrat xaqida ma’lumotlar XV asrdan etib kelgan.

4	9	2
3	5	7
8	1	6

Sexrli kvadrat yigindisini topish quyidagi tartibda amalga oshirildi:1+ 2 + ... + p +p2

1) Shuning uchun dioganallar (qator va ustun xam) yigindisi M(n)=n(n2+1)2 ga teng. Quyidagi jadvalda mumkin bo‘lgan n*n jadvallarning yigindisi ko‘rsatilgan.

n tartibi	3	4	5	6	7	8	9	10	11	12	13
M(n)	15	34	65	111	175	260	369	505	671	870	1105

Misol.

4_X4 o‘lchovli sexrli kvadratni olamiz, bu erda sonlarning 880 ta har xil kombinasiyasi mavjud. Quyiagicha ish yuritamiz.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Boshlangich matn sifatida quyidagi matnni olamiz:

T_0= D A S T U R L A SH T I L L A R I

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

ga jadvalga joylashtiramiz.

i	s	a	l
u	t	i	a
sh	p	l	l
t	p	a	d

Shifrlangan matn jadval elementlarini satrlar bo‘yicha o‘qish natijasida tashkil topadi:

T1=ISAL_UTIA_ShRLL_TRAD

Klassik maxfiy kriptotizimlarga xam olishimiz mumkin. Siljitish shifri ikki turga bo‘linadi. Ular oddiy va murakkab siljitish shifrlaridir. Oddiy siljitish shifrida alfavit bo‘yicha siljigan xarflar bilan shifrlanayotgan matn xarflari alfavitga mos ravishda almashtirish orqali shifrlash amalga oshiriladi. Bir turli almashtirish shifri oddiy siljitish shifrining bir qismi xisoblanadi.

Oddiy almashtirishli shifr. Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin: Sezar usuli, Affin tizimidagi Sezar usuli, tayanch so‘zli Sezar usuli va boshqalar.

Sezar shifri oddiy siljitish shifrining bir qismi xisoblanadi. Bu shifrni rimlik imperator Gole Yuliy Sezar o‘ylab toptan. Shifrlashda matnning xar bir xarfi boshqa xarf bilan quyidagi qoida asosida almashtiriladi. Xarflarni almashtirishda kelayotgan yozuv xarflarini K-ga siljitib almashtiriladi. Bu erda K-butun son xisoblanib uni quyidagicha ifodalash mumkin. K=K (modm), t - alfavit soni. Yuliy Sezar bevosita
k = 3 bo‘lganda ushbu usuldan foylangan.

Sezar usulining kamchiligi bu bir xil xarflarning o‘z navbatida, bir xil xarflarga almashishidir.

Masalan, matn sifatida T_0=KOMPUTER so‘zini va K=3 deb oladigan bo‘lsak Sezar usuli natijasida quyidagi shifrlangan yozuv xosil bo‘ladi:

T_1 =NRPSXWHU. m=26, a=3, b=5 bo'lganda Shunga moc ravishda qilinadi: quyidagicha almashadi:

Affin tizimidagi Sezar usulida xar bir xarfga almashtiriluvchi xarflar maxsus formula bo‘yicha aniqlanadi: at+b (modm), bu erda a, b-butun sonlar,

T	3t+5		A	F
0	5		B.	J
1	8		C	N
2	11		D	R
3	14		E	S
4	17		F	V
5	20		G	Z
6	23		H	D
7	26		1	H
8	29		J	L
9	32		K	P
10	35		L	T
11	38		м	X
12	41		N	B
13	44		0	F
14	47		p	J
15	50		Q	N
16	53		R	R
17	56		S	V
18	59		T	Z
19	62		и	D
20	65		V	H
21	68		W	L
22	71		x	P
23	74		Y	T
24	77		Z	X
25	80			
26	83			

$0<a, b<m.$

Natijada yuqorida keltirilgan matn quyidagicha shifirlanadi:

T_1=PFXJDZSR

Kalit so‘zli Sezar tizimi. Sezarning kalit so‘zli shifrlash tizimi bitta alfavitli almashtirish tizimi xisoblanadi. Bu usulda kalit so‘zi orqali xarflarning surishda va tartibini o‘zgartirishda foydalanadi.

Lotin alifbosi asosida shifrlash. Kalit so‘zini tanlashda takrorlanmaydigan xar xil xarflardan iborat bo‘lgan so‘zni tanlash maqsadga muvofiqdir. Bu usul amaliyotda qo‘llanilmaydi. Chunki kalit so‘zli Sezar shifrini kiriptotaxlil asosida ochish mumkin.

3 amaliy mashg‘ulot.

Mavzu: Murakkab almashtirish shifri.

Murakkab almashtirishli shifri ko‘p alfavitli bo‘lib, shifrlashda keluvchi matnning xar bir xarfi o‘zining oddiy almashtirish shifri kabi shifrlanadi. Ko‘p alfavitli almashtirishda alfavit ketma-ketligi va siklidan foydalaniladi.

A-alfavitli almashtirishda kiruvchi axborotning X_0-xarfi B_o-alfavitning Y_0-xarfi bilan almashtiriladi, X_1-xarfi esa B_1-alfavitning Y_1-xarfi bilan almashtiriladi, X_{p-1}-xarfi B_{p-1} alfavitning $Y_{p.1}$-xarfi bilan almashtiriladi va xokazo.

Ko‘p alfavitli almashtirishning r=4 bo‘lgan xol uchun umumiy ko‘rinishi quyidagi jadvalda keltirilgan.

Kiruvchi xarflar	XO	XI	X2	X3	X4	X5	X6	XI	X8	X9
Alfavit almashtirish	BO	B1	B2	B3	BO	B1	B2	B3	BO	B1

Bu usul bilan shifrlangan matnni ochishda etarli qiyinchiliklar tugdiradi, endi k-kalit bir-necha marotaba o‘zgaradi. Gamma shifri ixtiyoriy ko‘rinishda xar-bir shifrlanayotgan bo‘lakni o‘zgartiradi. Bunda dushman xar bir matn bo‘lagini qanday qilib ochishni bunday shifrlashda ximoyalanganlik darajasi foydalaniyotgan Bj-alfavit ketma-ketligiga bog‘liqdir. Ko‘p alfavitli almashtirish shifrini Leon Batist Al’bert kriptografiyaga kiritdi.

Vijinerning shifrlash tizimi. Birinchi bo‘lib Vijiner tizimi 1586-yilda chop etilgan va u ko‘p alfavitli tizimga nisbatan yuqoriroq o‘rinda turadi. Bleza Vijinera o‘zini XVI asrning frantsuz diplomata deb xisoblaydi. U kriptografiya tizimiga, ya’ni uning rivojlanishiga o‘z xissasini qo‘shgan. Vijiner tizimi Sezar shifrlash tizimiga qaraganda mukammalroq xisoblanib, unda kalit xarfidan xarfga almashtiriladi. Bunday ko‘p alfavitli almashtirish shifrini shifrlash jadvali orqali ifodalash mumkin. Quyidagi jadvalda Vijinerning ingliz alfaviti uchun mos keluvchi jadval ko‘rsatilgan.

Bu jadvaldan matnni shifrlash va uni ochish uchun ishlatiladi. Jadvalning ikkita kirishi bo‘lib: Yuqori qatordagi xarflardan kiruvchi ochiq yozuv uchun foydalaniladi.

Chap ustundan esa kalit xarflaridan foydaniladi.

Misol uchun kalit ketma-ketligini p-deb olaylik, u xolda kalit p-alfavitli p-satrdan iborat bo‘ladi.

$$P=(p_0, p_1...,p_{nr-1});$$

Vijinerning shifrlash tizimida ochiq matn $x=(x_0,x_1...,x_{n.1})$ va shifrlanganp matn $y=(y_o,y_1\ldots,y_{n-1}$ ko’rinishga ega. $p=(p_o,p_{1,}...,p_{r-1}.,)$ kalit yordamida quyidagicha munosabatda bo‘ladi.

$$X=(x_0,x_i,... ,x_{n-i}) \qquad y=(y_o,y_1---,y_{n-1});$$

$$(y_o,y_1,\ldots,y_{p-1})=(p_o(X_o),p_1(p_1),... ,p_{n-1},,(X_{n-1}));$$

Yuqoridagi ifodadan ma’lumki Vijiner jadvali orqali shifrlashda matnning (axborotning) xar bir xarfiga moc keluvchi kalitning xar bir xarfi orqali ularning ustun va satrlari kesishmasiga moc keluvchi xarflar olinadi. Agar

o‘zbek - kiril alfaviti ishlatilsa, Vijiner matritsaci [36x36] o‘lchamga ega bo‘ladi.

Masalan, Agar kalit sifatida <KO‘ZA> so‘zi tanlangan bo‘lsa, shifrlash matritsaci beshta qatordan iborat bo‘ladi.

ABVGDEYOJZIYKLMNOPRSTUFXTSChSh’EYUYAUKGX_
KLMNOPRSTUFXTSChSh’EYUYAUK,EX^_ABVGDEYOJZIY
O’QG‘H_AABIGDEYOJZIYKLMNOPRSTUFXTSCHSH'EYUYA
ZIYKLMNOPRSTUFXTSCHSH’EYUYAUKG^ABVGDEYOJ
ABVGDEYOJZIYKLMNOPRSTUFXTSChSh’EYUYAUKG^

Misol. K=<KO‘ZA> kaliti yordamida T=<BAYRAM KUNI> dastlabki matni shifrlansin.

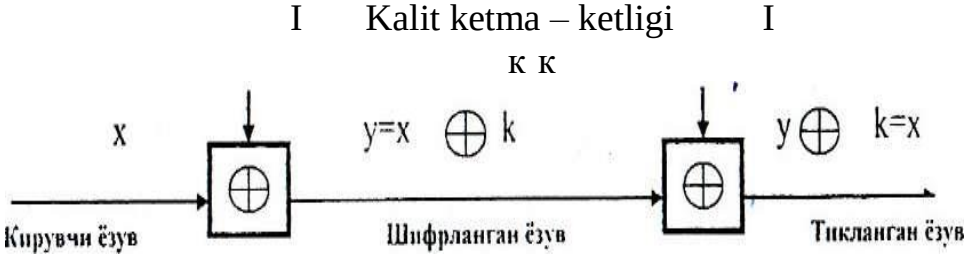
Ochiq matn	B	A	Y	R	A	M	_	K	U	N	I
Kalit	K	U	3	A	G	U	Z	A	K	U	Z
Shifrlangan matn	L	U	S	R	K	Z	J	K	U	I	R

T_1=LO’SR_KZJK_O‘IR.

4- amaliy mashg‘ulot

Mavzu: Vernamning shifrlash usuli.

Vernamning shifrlash tizimi modul kiymati m=2 bo‘lgan Vijiner shifrlash tizimining bir qismi xisoblanib, 1926-yilda bu usulning aniq ko’rinishi ishlab chiqiladi. Gilbertom Vernam AT&SSHA firmasi xomiyligi ostida kiruvchi matn sifatida ikkilik sanoq sistemasidan foydalandi. Shifrlashda birinchi ingliz alfavitidagi (A,B,….Z) matnning xir bir xarfi 5-bit bo‘lakli (b_0,b_1...b_4) Bado raqami bilan kodlanadi. Ixtiyoriy ketma-ketlikdagi ikkilik kalitlar k_0, k k_2, avval kitobsimon lentaga yo‘ziladi. Quyidagi rasmda uzatilayotgan axborotni Vernam usuli orqali shifrlash ko‘rsatilgan.



Kiruvchi matnni shifrlashda X-kiruvchi matn ikkilik ko‘rinishiga o‘tkaziladi va ikkilik modul ostida ikkilik ketma-ketlikdagi k-kalit bilan shifrlash amalga oshiriladi. U shifrlangan yozuv:

$$y=x + k$$

Shifrni ochishda yozuvdagi xar bir ikkilik modul ostidagi belgilar k-kalit ketma-ketligi bilan tuziladi.

$$Y+ k=x + k+ k=x;$$

Vernam ishlab chikkan bu tizimni aylanali lenta yordamida tekshirgan, uzatgich va qabul qilgichlarni ko‘rinishda bir xil yoki shunga o‘xshagan kalit ketma-ketlig‘idan foydalangan. Vernam shifrlash tizimining kamchiligi uzatuvchi orqali qabul qilish tomoniga kalit ketma-ketligini qanday uzatish edi. Chunki dushman kalitni olsa, u yuborgan shifrlangan matnni bemalol ochib o‘kiy oladi. Shuning uchun xam Vernamning shifrlash tizimi etarli emasligi sababli buni xal qilish uchun shifrlashni gammalashtirish usuliga o‘tilgan.

Gammalash usuli bilan shifrlash. Gammalashtirish xam kriptografii akslantirishda keng qo‘llaniladi. Aslida gammalashtirish, Vijiner shifri xamda cheksiz kalitdan foydalanish bir-biriga juda o‘xshash.

Gammalashtirishda tasodifiy sonlar generatori yordamida gamma generatsiya qilinadi va u ochiq matnga qayta tiklanadigan usulda (masalan, 2 ga modul bo’yicha qo‘shish) qo‘shiladi.

Ma’lumotlarni deshifrlash jarayoni shifr gammasini ma’lum kalit yordamida qaytadan generatsiya qilish va bu gammani shifrlangan ma’lumotdan olib tashlash bilan amalga oshiriladi.

Agar shifr gammasida takrorlanuvchi bitli ketma-ketlik mavjud bo‘lmasa shifrlangan matnni ochish juda qiyin. Umuman olganda, shifr gammasi xar bir shifrlanadigan so‘z uchun tasodifiy ravishda o‘zgarishi kerak. Agar gamma uzunligi butun shifrlanadigan matn uzunligidan oshib ketsa va ochiq matnning xech qanday qismi ma’lum bo‘lmasa, u xolda shifrni faqat mumkin bo‘lgan kalitlarni to‘la k o‘rib chikish bilan ochish mumkin. Bu xolda kriptobardoshlilik kalit uzunligi bilan o‘lchanadi.

Agar raqibga ochiq matnning bo‘lagi va unga mos keluvchi shifrogrammasi ma’lum bo‘lsa gammalashtirish usuli kuchsiz bo‘lib qoladi. Modul bo‘yicha oddiy ayirish orqali tasodifiy sonlar kema-ketligi qismi olinadi va bu qism bo‘yicha butun ketma-ketlik tiklanadi. Raqiblar buni ochiq matnning tashkil etuvchilari asosida taxmin bilan topishlari xam mumkin. Quyida amaliyotda qo‘llash mumkin bo‘lgan gamma generatsiyasining keng tarqalgan usullari qaraladi. Gamma shifri quyidagi ko‘rinishdagi ketma-ketlikda olinadi.

$T^{(i)}sh$

Shifrlashni quyidagi ko‘rinishda yozish mumkin.

$T^{((i)}\ T^{0)}+$, i=l..m;

B.

$T^{(0}sh$ i-shifrlangan matn;

$G^{(i)}sh$ i-gamma shifri bo‘ladi;

$T^{(i)}0$ i-ochiq matn bo‘ladi;

M-(ochiq) matnni sifat darajasi.

Shifrni ochishda qayta gamma shifridan foydalaniladi:

$$T_o=G_{sh} + T_{sh}.$$

Bu usul bilan shifrlangan matnni ochishda etarli qiyinchiliklar tugdiradi, endi k-kalit bir-necha marotaba o‘zgaradi. Gamma shifri ixtiyoriy ko‘rinishda xar bir

shifrlanayotgan bo‘lakni o‘zgartiradi. Bunda dushman xar bir matn bo‘lagini qanday qilib ochishni bilmaydi. Chunki dushman xar bir turdagi kalitni topishi uchun ancha vaqt ketadi. Bu xolatda shifrlangan matn bardoshliligi ko‘pligiga bog‘liq bo‘ladi.

5-amaliy mashg‘ulot.

Mavzu: Axborotlarni kriptografik himoyalash usullari.

Ushbu axborot ustun buyicha ketma – ket jadvalga kiritiladi*:*

M	M	K	A	Y	I	N
A	A	V	B	I	Y	L
T	T	A	I	L	F	A
E	I	T	I	M	A	R

Sehrli kvadrat deb, katakchalariga 1 dan boshlab sonlar yozilgan, undagi har bir ustun, satr va diagonal buyicha sonlar yigindisi bitga songa teng bo‘lgan kvadrat shaklidagi jadvalga aytilali.

4x4 ulchovli sehrli kvadratni olamiz, bu erda sonlarning 880 ta har xil kombinatsiyasi mavjud. Quyidagicha ish yuritamiz:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Boshlangich matn sifatida quyidagi matnni olamiz:

Komyuter tamog'i va jadvalga joylashtiramiz:

I	M	O	M

Y	T	A	E
R	U	T	R
P	G'	O	K

SHifrlangan matn jadval elementlarini satrlar bo‘yicha o‘qish natijasida tashkil topadi:

ISAL UTIA SHRLL TRAD

Almashtirish usullari

Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin:

- Sezar usuli;
- Affin tizimidagi Sezar usuli;
- Tayanch so‘zli Sezar usuli va boshqalar.

Sezar usulida almashtiruvchi harflar k va siljish bilan aniqlanadi. YUliy Sezar bevosita k = 3 bo‘lganda ushbu usuldan foylalangan.

k = 3 bo‘lganda va alifbodagi harflar m = 26 ta bo‘lganda quyidagi jalval hosil qilinadi:

6-amaliy mashg‘ulot.

Mavzu: Ochiq kalitli RSA kriptoalgoritmi.

RSA bir tomonli funktsyasiga asoslangan tartib va qoidalarni boshqarish kriptotizimi xisoblanadi. Bu kriptotiz'imini kalitlarni taqsimlash tartib va qoidalarini boshqarish kriptotizimi uchun xam qo‘llash mumkin. Tartib va qoidalarni boshqarish masalalari, kriptotizimilariga doir kriptologik ilmiy izlanishlar xozirda, zamonaviy, bardoshli kriptografik tizimlarni yaratishda keng va jadal rivojlanib bormoqda. Bu soxada RSA bir tomonli funktsiyasidan foydalanishning qulayligi o‘zini xar tomonlama oqlab kelmoqda.

RSA algoritmini ko‘llanishiga doir kichik bir misol keltiramiz.

Misol: Uchta xarfdan iborat bo‘lgan "CAB" ma’lumotini shifrlaymiz.

Biz qulaylik uchun kichik tub sonlardan foydalanamiz. Amalda esa mumkin qadar katta tub sonlar bilan ish ko‘riladi.

1.Tub bo‘lgan p=3 va q=11 sonlarini tanlab olamiz.

2. Ushbu n=pq=3*11=33 sonini aniqlaymiz.

So‘ngra, $\varphi(33) = (p-1)(p-1) = 2*10 = 20$ sonini topamiz, xamda bu son bilan 1 dan farqli biror umumiy bo‘luvchiga ega bo‘lmagan d sonini, misol uchun

d= 3 sonini, olamiz.

3. Yuqorida keltirilgan (24) shartni qanoatlantiruvchi e sonini 3e=1 (mod 20) tenglikdan topamiz. Bu son e=7

4. Shifrlanishi kerak bulgan «SAB» ma’lumotini tashkil etuvchi xarflarni: A—I, B-»2, S-»3 mosliklar bilan sonli ko‘rinishga o‘tkazib olib, bu

ma’lumotni musbat butun sonlarning, ketma-ketligidan iborat deb qaraymiz. U xolda ma’lumot (3,1,2) ko‘rinishda bo‘ladi va uni {e;n}={7;33} ochiq kalit bilan $f_z(x) = x^7 \pmod{33}$ bir tomonli funksiya bilan shifrlaymiz:

X=3da ShM1=(3^7)(mod33)=2187(mod33)=9,
X=1 da ShM2=(1^7) (mod33)=l,
x=2 da ShM3=(2^7) (mod33)=128(mod33)=29

5. Bu olingan shifrlangan (9,1,29) ma’lumotni maxfiy {d;n}={3;33} kalit bilan

$f^{-1}{}_z(y) = y^3 \pmod{33}$ ifoda orqali deshifrlaymiz:

y=9 da OM1=(9^3) (mod33)=729(mod33)=3,
y=1da OM2=(1^3) (mod33)=l(mod33)=l,
y=29 da OM3=(29^3) (mod33)=24389(mod33)=2.

Shunday qilib, kriptotizimilarda RSA algoritmining qo‘llanishi quyidagicha: xar bir foydalanuvchi ikkita etarli darajada katta bo‘lmagan p va q tub sonlarni tanlaydilar va yuqorida keltirilgan algoritm bo‘yicha d va e tub sonlarini xam tanlab oladi. Bunda n=pq bo‘lib, {e; n} ochiq kalitni {d; n} esa maxfiy kalitni tashkil etadi. Ochiq kalit ochiq ma’lumotlar kitobiga kiritiladi. Ochiq kalit bilan shifrlangan kaliti faqat shifr ma’lumotining xaqiqiy egasigagina ma’lum.

7-amaliy mashg‘ulot.

Mavzu: El-Gamal kriptotizimi.

El-Gamal kriptotizimi. El-Gamal tizimi RSA tizimiga muqobil (alternativ) bo‘lib, bu kriptotizimilarning kalitlarining o‘lchov uzunlnklari teng bo‘lganda bir-xil kriptobardoshlilikga ega bo‘ladilar.

El-Gamal kriptotizimi Diffi-Xellman algoritmiga o‘xshash bo‘lib, diskret logarifmlarni xisoblash masalasi echimining murakkabligiga asoslangan. Bu kriptotizimi asosini tub bo‘lgan r va butun bo‘lgan g sonlari tashkil etadi. Quyida ushbu tizimning moxiyatini ochib beruvchi misolni keltiramiz.

Biror foydalanuvchi (A) maxfiy kalit a sonini tanlab oladi va $y = g^a$ modp bo‘lgan ochiq kalitni xisoblaydi. Agarda mana shu foydalanuvchi (A) bilan biror boshqa foydalanuvchi (B) maxfiy ma’lumotni jo‘natmoqchi bo‘lsa, u xolda (B) p sonidan kichik bo‘lgan biror kriptotizimi sonini tanlab olib

$$Y_1 = g^k \text{ modp va } y_2 = m \circledR y^k,$$

sonlarini xisoblaydi, bu erda + belgisi 2 modul bo‘yicha bitlarni qo‘shish amalini bildiradi, ya’ni m va y^k sonlari ikkilik sanoq tizimida, deb tushiniladi. So‘ngra (B) ($y_1 > y_2$) ma’lumotlarini (A) ga jo‘natadi. O‘z navbatida (A) bu shifrlangan ma’lumotni qabul qilib, quyidagi

$$(y^a{}_1 \bmod p) \circledR y_2 = m$$

bo‘lgan xisoblash bilan ma’lumotning ochiq matnini tiklaydi.

Shifrlashni kombinatsion usuli. Shifrlashning kombinatsiyalangan usullari. Qudratli kompyuterlar, tarmoq texnologiyalari va neyronli xisoblashlarning paydo bo‘lishi xozirgacha umuman fosh qilinmaydi deb xisoblangan kriptografik tizimlarni obro'sizlantirilishiga sabab bo‘ldi. Bu esa o‘z navbatida yuqori bardoshlikka ega kriptografik tizimlarni yaratish ustida ishlashni taqozo etdi. Bunday kriptografik tizimlarni yaratish usullaridan biri shifrlash usullarini kombinatsiyalashdir. K^G‘ yida eng kam vaqt sarfida kriptobardoshlikni jiddiy. oshishini ta’minlovchi shifrlashning kombinatsiyalangan usuli ustida so‘z boradi. Shifrlashning ushbu kombinatsiyalangan usuliga binoan ma’lumotlarni shifrlash ikki bosqichda amalga oshiriladi. Birinchi bosqichda ma’lumotlar standart usul (masalan, DES usul) yordamida shifrlansa, ikkinchi bosqichda shifrlangan ma’lumotlar maxsus usul bo‘yicha qayta shifrlanadi. Maxsus usul sifatida ma’lumotlar vektorini elementlari noldan farqli bo‘lgan son matritsasiga ko‘paytirishdan foydalanish mumkin.

Gammalashni qo‘llashda agar shifr gammasi sifatida raqamlarning takrorlanmaydigan ketma-ketligi ishlatilsa shifrlangan matnni fosh qilish juda qiyin. Odatda shifr gammasi xar bir shifrlanuvchi so‘z uchun tasodifiy o‘zgarishi lozim. Agar shifr gammasi shifrlangan so‘z uzunligidan katta bo‘lsa va dastlabki matnning xech qanday qismi ma’lum bo‘lmasa, shifrni faqat to‘g‘ridan-to‘g‘ri saralash orqali fosh etish mumkin. Bunda kriptobardoshlik kalit o‘lchami orqali aniqlanadi. Shifrlashning bu usulidan ko‘pincha ximoya tizimining dasturiy amalga oshirilishida foydalaniladi va shifrlashning bu usuliga asoslangan tizimlarda bir sekundda ma’lumotlarning bir necha yuz Kbaytini shifrlash imkoniyati mavjud. Rasshifrovka jarayoni-kalit ma’lum bo‘lganida shifr gammasini qayta generatsiyalash va uni shifrlangan ma’lumotlarga singdirishdan iborat.

Shifrlangan ma’lumotlar vektorini matritsaga ko‘paytirishni qo‘llashda shifrlangan matn bir bayt uzunlikdagi f_i vektorlarga ajratiladi va xar bir vektor kvadrat matritsa M^i_j ga ko‘paitiriladi va shifrlangan vektorlar shakllantiriladi:

$$F^{j}_{i} = f_i * M_{ij}$$

Bu usulning asosiy afzalligi sifatida uning ma’lumotlar ishlanishining turli jabxalaridagi moslanuvchanligini ko‘rsatish mumkin. Xar bir vektor aloxida shifrlanganligi sababli ma’lumotlar blokini uzatish va dasturlangan ma’lumotlardan ixtiyoriy foydalanish imkoniyati tugiladi. Ushbu usulni apparat yoki dasturiy usulda amalga oshirish mumkin.

Deshifrlash jarayonida shifrlangan f^j vektorlarni teskari matritsa (M_{ij}^{-1}) ga ko‘paitiriladi.

$$F_{ji} = f_i * M_{ij}$$

Kombinatsiyalangan usullarning yuqori samaradorligiga uning ikkala bosqichini apparat usulda amalga oshirish orqali erishish mumkin. Ammo bu uskuna xarajatlarining jiddiy oshishiga olib keladi. Dasturiy usulda amalga oshirilishida esa ma’lumotlarni shifrlash va deshifrlash vaqti oshib ketadi. Shu sababli kombinatsiyalangan usularni apparat-dasturiy usulda, ya’ni usulning bir

bosqichi apparat usulda, ikkinchi bosqichi dasturiy usulda amalga oshirilishi maqsadga muvofiq xisoblanadi.

8-Amaliy mashgulot

Mavzu: Simmetrik kriptotizimlar.

DES algoritmining asosiy ishlash tartibi. DES algoritmu 64-bitli ma’lumotlar blokini turli o‘rin almashtirish va akslantirishlar kombinatsiyasiga asoslanib 56 bitli k kalit bilan shifrlashni amalga oshiradi, xamda oxirgi bitlarni boshlangich o‘rin almashtirish, 16 marta shifrlash siklini takrorlanishi xamda oxirgi bitlarni o‘rin almashtirishdan iborat.

Algoritmda keltirilgan barcha o‘rin almashtirish va akslantirishlar jadvallari standart qabul qilingan, algoritm bajarilishida bular xech qanday o‘zgartirishlarsiz o‘z xolicha saqdanadi.

Foydalanilgan belgilashlar:

Lj BaRi -64 bitli bloklni chap va yong qismlari;

Q-2 modul bo‘yicha ko‘shish amali;

Kj – 48 bitli i-sikllar kaliti;

f-shifrlash funktsiyasi;

IP -boshlangich o‘rin almashtirish.

Ma’lumotning T blokini shifrlashda uning barcha bitlari quyidagi jadvalga ko‘ra IP boshlangich o‘rin almashtiriladi.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	14
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	34	25	17	9	1
59	51	43	34	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Bunda 58-bit T blokning 1-biti, 50-bit, 2-biti va xak..., ko‘rinishda almashtirish bajariladi. O‘rin almashtirishdan keyin xosil bo‘lgan IP(T) blok mos ravishda ikki: L_0 1-bitdan 32-bitgacha va R_0 33-bitdan 64-bitgacha bo‘lgan bloklarga ajraladi. Keyin Feystel akslantirishlariga asoslangan 16 marta takrorlanuvchi iterativ shifrlash jarayoni bajariladi.

$T_{i-1}=L_{i-1}$ $-R_{i+1}$-(i-1) - iteratsiya natijasi bo‘lsin. U xolda, i- iteratsiya natijasi $T_i=L_iR_i$ quyidagi formuladan aniqlanadi.

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

$R_i=L_{i-1}+f(R_{i-1,}k_{i\,),}$ i=l,2,…l

f shifrlash funktsiyasi deyiladi. Funktsiya argumenta 32 bitli R_{i-1} vektor va 56 bitli shifrlash k kalitdan akslantirishlar asosida olingan 48 bitli Ki kalitdir. $T_{16}=K_{16}L_{16}$ oxirgi iteratsiya natijasi. Shifrlash tugashi bilan bitlarning o‘z joylarini qayta tiklash maqsadida T_{16} ga IP^{-1} qayta o‘rin almashtirishlar qilinadi. Ma’lumotni qayta shifrlash uchun yuqoridagi qilingan ishlar teskari tartibda bajariladi, shunga ko‘ra (1) munosabat o‘rniga quyidagi munosabatni qo‘llashga to‘g‘ri keladi.

$$R_{i-1}=L_1$$

L_{i-1} = Ri+f(L_i k_i), i=16,....1

F(R_{i-1},k_i shifrlash funktsiyasini qiymatini xisoblash sxemasi.

F(Rj-i,ki) shifrlash funktsiyasining sxemasi f shifrlash funktsiyasining qiymatini xisoblashda E «kengaytma» funktsiyasi, S1, S2...S8 bloklardan iborat. S va P o‘rin almashtirishlardan foydalaniladi. R_{i-1} (32 bit) vektor va k_i (48 bit) kalitlar f funktsiyasi argumenti xisoblanadi.

E «kengaytma» funksiyasi 32 bitli R_{i-1} vektorni quyidagi jadvalga ko‘ra bir xil bitlarni takrorlash yoli bilan E(R_{i-1}) 48 bitli vektor xosil qiladi.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

E(R_{i-1}) vektorning birinchi uchta biti mos ravshida R_{i-1} vektorni 32,1 va 2-bitlar, oxirgi uchta biti esa R_{i-1} vektorni 31, 32,1-bitlardir.

Xosil bo‘lgan nagija mavjud k_i kalitga 2 moduli bo‘yicha bitma-bit qo‘shiladi va 6 bitlik 8 ta B_1, B_2…B_8 bloklar ketma-ketligini xosil qilinadi.

$$E(R_{i-1})+ ki = B_1.B_2….B_8.$$

So‘ngra xar bir B_j blok 4-bitli B_j bloka mos kelgan S_j S - bloklar jadvali yordamida o‘zgartiriladi, S-bloklar ro‘yxati quyida jadval asosida akslantirilgan.

S (l)

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S(2)

15	11	8	14	6	11	3	4	9	7	2	13	12	0	5	10
33	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	3	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S(3)

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	3
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S(4)

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	3	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

B_i blokning B_j ga o‘zratirilishini bitta misol orqali keltiramiz.

Masalan B_2 blok 111010 dan iborat bo‘lsin. B_2 blokni birinchi razryadi a_1 =1 $a=a_1a_6$ sonining ikkilik sanoq sistemasidagi yozuvi bo‘lsa, bu sonning o‘nlik sanoq sistemasidagi qiymati 4 dan katta bo‘lmaydi, ya’ni $0<a<4$. Oradagi 4 ta $b=a_1a_2a_3a_4a_5$=1101 dan tashkil topgan b soni esa $0<b<16$ munosabatni qanoatlantiradi. Bizning misolda a=2, b=13.

S_2 blokning satrlari 0 dan a gacha bo‘lgan sonlar bilan ustunlari esa 0 dan b gacha bo‘lgan sonlarda raqamlab chiqilgan. Shunday qilib, (a,b) sonlar juftligi jadvaldagi a-satr va b-ustunning kesishmasidagi biror sonini anikqlaydi. Ushbu xolatda kesishmada turgan son 3. Bu sonni ikkilik sanoq sistemasiga o‘tkazib B_2ni xosil qilamiz.(0011)

$F(R_{i-1}.k_i)$ qiymati P bitli o‘rin almashtirishlarni quyida keltirilgan jadvaldan foydalanib qo‘llagan xolda xosil qilinadi.

16	7	20	21
24	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Xar bir iteratsiya k_i (48 bit) kalitning ayni paytdagi qiymati foydalaniladi. Ushbu qiymatlar dastlabki k kalitdan quyidagicha olinadi. Dastlab foydalanuvi 56 ta ixtiyoriy bitli kalitni tanlaydi. 8.16....64 o‘rinlarda turgan 8 ta bit kalitga shunday qo‘yiladiki, undagi xar bir bayt toq sondagi birlik raqamlarni o‘z ichiga olsin. Lekin bu bitlar shifrlashda qatnashmaydi. Bu kalitlarni uzatish va saqlashda uchraydigan ayrim xatoliklarni topishda juda qo‘l keladi. 56 bit kalit quyidagi jadvalga ko‘ra o‘rin almashtirishlar asosida olinadi.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Bu o‘rin almashtirish xar bir 28 bitdan iborat bo‘lgan ikkita S_0 va D_0 bloklar bilan aniqdanadi (ular mos ravishda jadvalning yuqori va pastki qismlarni egallagan). S_0 ni uchta oldingi bitlari kalitning 57,49,41 uchta bitlariga mos keladi va jadval asosida davom ettirilady. Keyin induktiv yo‘l bilan S_i va D_i (i=l,....16) bloklar aniqlanadi. Agar C_{i-1} va D_{i-1} lar aniqlangan bo‘lsa, u xolda C_i va D_i lar ulardan quyida keltirilgan jadvalga asosan bir yoki ikkita chapga siklik surash bilan xosil qilinadi.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Surishlar soni	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Endi, k_i ($1< i< 16$) kalitni aniqlaymiz. k_i kalit 48 bitdan tashkil topgan bo‘lib, ular 2.7-jadvalga asosan S_i D_i blok bitlaridan tanlab olingan. Takidlash joizki, S_i D_i dagi 56 bitdan 8 tasi (9,18,22,25,35,38,43,54 raqamli) k_i, da yoq.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

9-Amaliy mashg‘ulot.

Mavzu: Elektron raqamli imzo.

Elektron xujjatlarni tarmoq orqali almashishda ularni ishlash va saqlash xarajatlari kamayadi, qidirish tezlashadi. Ammo, elektron xujjat muallifini va xujjatning o‘zini autentifikatsiyalash, ya’ni muallifning xaqiqiyligini va olingan elektron xujjatda o‘zgarishlarning yoqligini aniqlash muammosi paydo bo‘ladi.

Elektron xujjatlarni auentifikatsiyalashdan maqsad ularni mumkin bo‘lgan jinoyatkorona xarakatlardan ximoyalashdir. Bunday xarakatlarga quyidagilar kiradi:

-faol ushlab qolish-tarmoqqa ulangan buzgunchi xujjatlarni (fayllarni) ushlab qoladi va o‘zgartiradi.

-maskarad-abonent S xujjatlarni abonent B ga abonent A nomidan yuboradi;

-renegatlik-abonent A abonent B ga xabar yuborgan bulsada, yubormaganman deydi;

-almashtirish-abonent B xujjatni o‘zgartiradi, yoki yangisini shakillantiradi va uni abonent A dan olganman deydi;

-takrorlash-abonent A abonent B ga yuborgan xujjatni abonent S takrorlaydi.

Jinoyatkorona xarakatlarning bu turlari o‘z faoliyatida kompyuter axborot texnologiyalaridan foydalanuvchi bank va tijorat strukturalariga, davlat korxona va tashkilotlariga xususiy shaxslarga ancha-muncha zarar etkazishi mumkin.

Elektron raqamli imzo metodologiyasi xabar yaxlitligini va xabar muallifining xaqiqiyligini tekshirish muammosini samarali xal etishga imkon beradi.

Elektron raqamli imzo telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. Raqamli imzo ishlashi bo‘yicha oddiy qo‘lyozma imzoga o‘xshash bo‘lib, quyidagi afzalliklarga ega:

-imzo chekilgan matn imzo qo‘ygan shaxsga tegishli ekanligini tasdiqlaydi;

-bu shaxsga imzo chekilgan matnga bogliq majburiyatlaridan tonish imkoniyatini bermaydi;

-imzo chekilgan matn yaxlitligini kafolatlaydi.

Elektron raqamli imzo-imzo chekiluvchi matn bilan birga uzatiluvchi qo‘shimcha raqamli xabarning nisbatan katta bo‘lmagan sonidir.

Elektron raqamli imzo asimmetrik shifrlarning qaytaruvchanligiga xamda xabar tarkibi, imzoning o‘zi va kalitlar juftining o‘zaro bogliqligiga asoslanadi. Bu elementlarning xatto birining o‘zgarishi raqamli-imzoning xaqiqiyligini tasdiqlashga imkon bermaydi. Elektron raqamli imzo shifrlashning asimmetrik algoritmlari va xesh-funktsiyalari yordamida amalga oshiriladi.

Elektron raqamli imzo tizimining qo‘llanishida bir-biriga imzo chekilgan elektron xujjatlarni jo‘natuvchi abonent tarmogining mavjudligi faraz qilinadi. Xar bir abonent uchun juft-maxfiy va ochiq kalit generatsiyalanadi. Maxfiy kalit abonentda sir saqlanadi va undan abonent elektron raqamli imzoni shakllantirishda foydalanadi.

Ochiq kalit boshqa barcha foydalanuvchilarga ma’lum bo‘lib, undan imzo chekilgan elektron xujjatni qabul qiluvchi elektron raqamli imzoni tekshirishda foydalanadi.

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

-raqamli imzoni shakllantirish muolajasi;

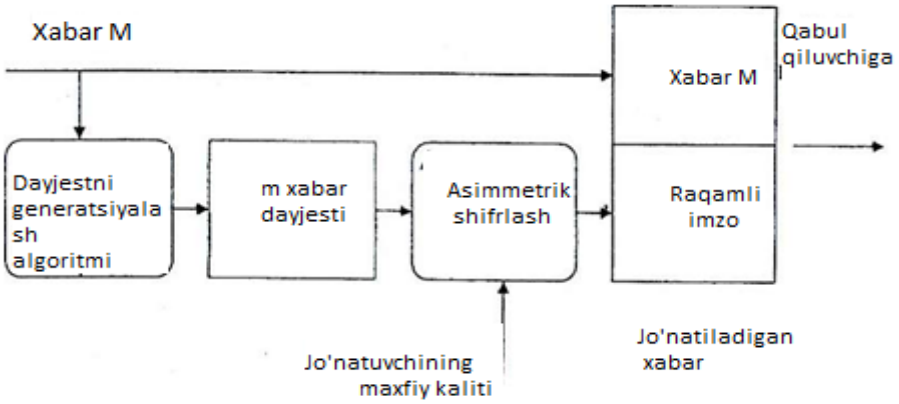
-raqamli imzoni tekshirish muolajasi.

Imzoni shakllantirish muolajasida xabar jo‘natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo‘natuvchining ochiq kalitidan foydalaniladi.

Raqamli imzoni shakllantirish muolajasi. Ushbu muolajani tayyorlash bosqichida xabar jo‘natuvchi abonent A ikkita kalitni generatsiyalaydi: maxfiy kalit k_A va ochiq kalit K_A. Ochiq kalit K_A uning jufti bo‘lgan maxfiy kaliti k_A dan xisoblash orqali olinadi. Ochiq kalit K_A tarmoqning boshqa abonentlariga imzoni tekshirishda foydalanish uchun tarqatiladi.

Raqamli imzoni shakllantirish uchun jo‘natuvchi A avvalo imzo chekiluvchi matn M ning xesh funktsiyasi L(M) qiymatini xisoblaydi (9.1-rasm).

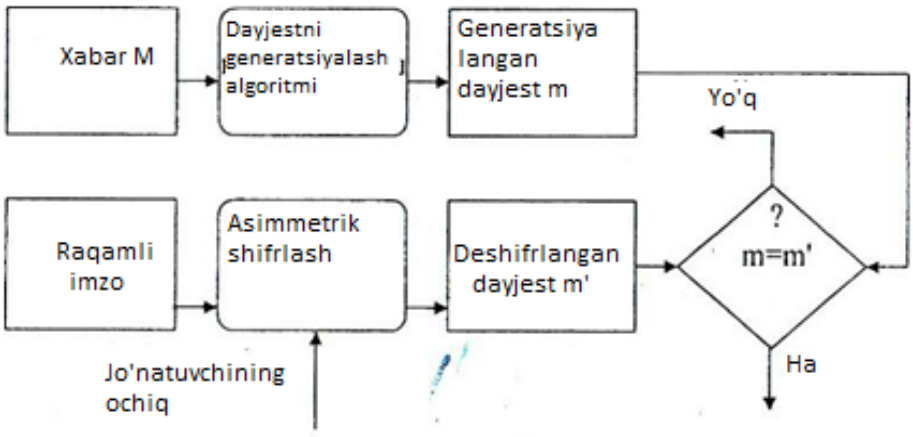
Xesh-funktsiya imzo chekiluvchi dastlabki matn "M" ni daydjest "t" ga zichlashtirishga xizmat qiladi. Daydjest M-butun matn "M" ni xarakterlovchi bitlarning belgilangan katta bo‘lmagan sonidan iborat nisbatan qisqa sondir. So‘ngra jo‘natuvchi A uzining maxfiy kaliti k_A bilan daydjest "t" ni shifrlaydi. Natijada olingan sonlar jufti berilgan "M" matn uchun raqamli imzo xisoblanadi. Xabar "M" raqamli imzo bilan birgalikda qabul qiluvchining adresiga yuboriladi.



K_A

9.1-rasm. Elektron raqamli imzoni shakllantirish sxemasi

Raqamli imzoni tekshirish muolajasi. Tarmoq abonentlari olingan xabar "M" ning raqamli imzosini ushbu xabarni jo‘natuvchining ochiq kaliti K_A yordamida tekshirishlari mumkin.



kaliti K_A

9.2- rasm. Elektron raqamli imzoni tekshirish sxemasi.

Elektron raqamli imzoni tekshirishda xabar "M"ni qabul qiluvchi "B" qabul qilingan daydjestni jo‘natuvchining ochiq kaliti "K_A" yordamida deshifrlaydi. Undan tashqari, qabul qiluvchini o‘zi xesh-funktsiya h(M) yordamida qabul qilingan xabar "M" ning daydjesti "t" ni xisoblaydi va uni deshifrlangani bilan taqqoslaydi. Agar ikkala daydjest "m" va "m"' mos kelsa raqamli imzo xaqiqiy xisoblanadi. Aks xolda imzo qalbakilashtirilgan, yoki axborot mazmuni o‘zgartirilgan bo‘ladi.

Elektron raqamli imzo tizimining printsipial jixati-foydalanuvchining elektron raqamli imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirishning mumkin emasligidir. Shuning uchun imzo chekishdagi maxfiy kalitni ruxsatsiz foydalanishdan ximoyalash zarur. Elektron raqamli

imzoning maxfiy kalitini, simmetrik shifrlash kalitiga o‘xshab, shaxsiy kalit elituvchisida, ximoyalangan xolda saqlash tavfsiya etiladi.

Elektron raqamli imzo imzo chekiluvchi xujjat va maxfiy kalit orqali aniqlanuvchi noyob sondir. Imzo chekiluvchi xujjat sifatida xar qanday fayl ishlatilishi mumkin. Imzo chekilgan fayl imzo chekilmaganiga bir yoki bir nechta elektron imzo qo‘shilishi orqali yaratiladi.

Imzo chekiluvchi faylga joylashtiriluvchi elektron raqamli imzo imzo chekilgan xujjat muallifini identifikatsiyalovchi qo‘shimcha axborotga ega. Bu axborot xujjatga elektron raqamli imzo xisoblanmasidan oldin qo‘shiladi. Xar bir imzo quyidagi axborotni o‘z ichiga oladi:

-imzo chekilgan sana;

-ushbu imzo kaliti ta’sirining tugashi muddati;

-faylga imzo chekuvchi shaxs xususidagi axborot (F.I.Sh., mansabi, ish joyi);

-imzo chekuvchining indentifiqatori (ochiq kalit nomi);

-raqamli imzoning o‘zi.

Asimmetrik shifrlashga o‘xshash, elektron raqamli imzoni tekshirish uchun ishlatiladigan ochiq kalitning almashtirilishiga yol qo‘ymaslik lozim. Faraz qilaylik, niyati buzuq odam "n" abonent "B" kompyuterida saqlanayotgan ochiq kalitlardan, xususan, abonent A ning ochiq kaliti K_A dan foydalana oladi. Unda u quyidagi xarakatlarini amalga oshirishi mumkin:

-ochiq kalit K_A saqlanayotgan fayldan abonent A xususidagi indentsifikatsiya axborotini o‘qishi;

-ichiga abonent A xususidagi indentifikatsiya axborotini yozgan xolda shaxsiy juft kalitlari k_n va K_n ni generatsiyalashi;

-abonent B da saqlanayotgan ochiq kalit $K_A$ni o‘zining ochiq kaliti K_p bilan almashtirishi.

So‘ngra niyati buzuq odam "n" abonent B ga xujjatlarni o‘zining maxfiy kaliti k_n yordamida imzo chekib jo‘natishi mumkin. Bu xujjatlar imzosini tekshirishda abonent B abonent A imzo chekkan xujjatlarni va ularning elektron raqamli imzolarini to‘g'ri va xech kim tomonidan modifikatsiyalanmagan deb xisoblaydi. Abonent A' bilan munosabatlarini bevosita oydinlashtirilishigacha B abonentda olingan xujjatlarning xaqiqiyligiga shubxa tugilmaydi.

Elektron raqamli imzoning qator algoritmlari ishlab chiqilgan. 1977 yilda AQSh da yaratilgan RSA tizimi birinchi va dunyoda mashxur elektron raqamli imzo tizimi xisoblanadi va yuqorida keltirilgan printsiplarni amalga oshiradi. Ammo raqamli imzo algoritmi RSA jiddiy kamchilikka ega. U niyati buzuq odamga maxfiy kalitni bilmasdan, xeshlash natijasini imzo chekib bo‘lingan xujjatlarning xeshlash natijalarini ko‘paytirish orqali xisoblash mumkin bo‘lgan xujjatlar imzosini shakllantirishga imkon beradi.

Ishonchliligining yuqoriligi va shaxsiy kompyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmli 1984 yilda El Gamal tomonidan ishlab chiqildi. El Gamalning raqamli imzo algoritmi (EGSA) RSA raqamli imzo algoritmidagi kamchiliklardan xoli

bo‘lib, AQSh ning standartlar va texnologiyalarning Milliy universiteta tomonidan raqamli imzoning milliy standartiga asos kabi qabul qilindi.

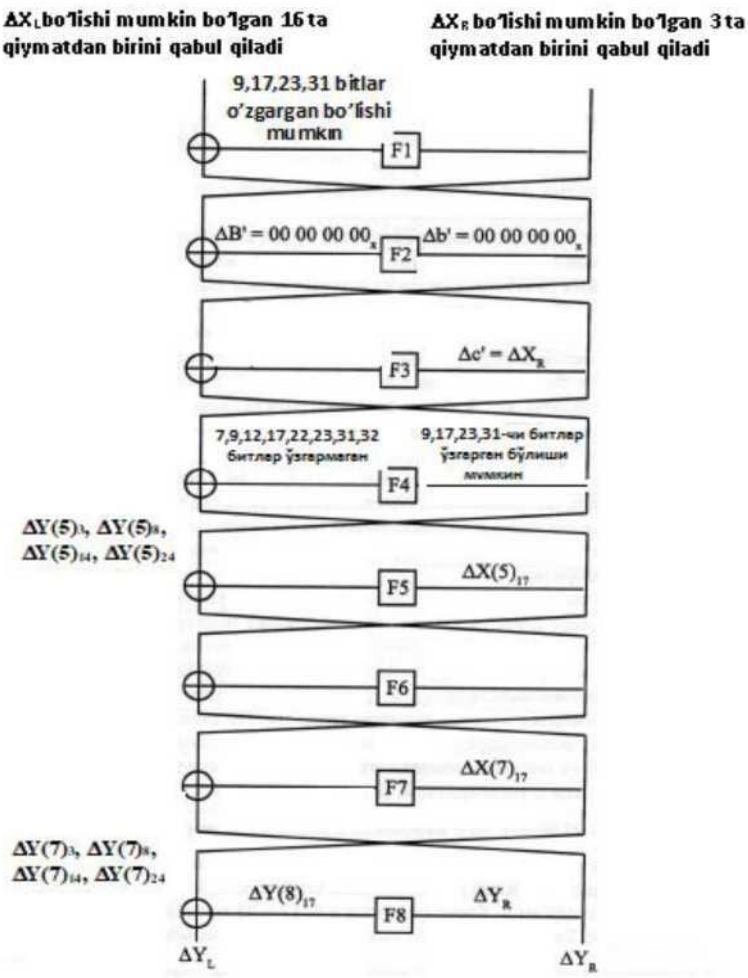
10-Amaliy mashg‘ulot.

Mavzu: DES shifrlash algoritmi uchun chiziqli-differensial kriptotahlil.

S blokka kiruvchi ayirmani va S blokdan chiquvchi ikkinchi bit ayirmasini bilgan holda ikkinchi chiquvchi bitga mos kelmaydigan, S_1 blokdan chiquvchi ayirmaning yarmini aniqlash mumkin. Masalan, agar S1 blokdan chiquvchi ayirmaning ikkinchi biti 1 ga teng bo'lsa, u holda tahlil uchun bo'lishi mumkin bo'lgan 16 qiymatdan quyidagi 8 ta chiquvchi qiymatlarni qoldiramiz: 0100, 0101, 0110, 0111, 1100, 1101, 1110, 1111. Biroq, kalit bitlarini aniq topishda bu ma'lumotlar etarli emas. Shu sababli S.Langford va M.Xellman sakkiz raundli DES shifrlash algoritmiga hujum qilish variantini taklif qildilar. Bundan oldingi paragrafda ko'rilgan etti raundga ular qo'shimcha birinchi raundni kiritdilar. Ushbu holatda ikkinchi raundga kiruvchi ayirmalarni to'g'ri saqlab qolish uchun kiruvchi xabarlarning o'ng qismlari ikkinchi yoki uchinchi bitda farqlanishi yoki bir vaqtning o'zida ikkinchi va uchinchi bitlarda farqlanishi lozim.

F shifrlash funksiyasiga shunday ayirma kirishi mumkinki, natijada 9,17,23 va 31-chi bitlarning qiymatlari o'zgarishi mumkin. Shifrlash algoritmining ikkinchi raundiga kiruvchi ayirmaning o'ng qismi nolga teng bo'lishi lozim. Biz birinchi raund F shifrlash funksiyasi chiqishining ayirmasini bilmaymiz, ammo bu ayirma bo'lishi mumkin bo'lgan 16 ta qiymatdan birini qabul qilishini bilamiz.

S.Langford va M.Xellmanlar kiruvchi qiymatlarning bo'lishi mumkin bo'lgan barcha qiymatlarini saralashni taklif qildilar. Natijada har bir kiruvchi juftligi uchun birinchi raund S1 blokining qismiy kaliti bitlarini saralab, ular dastlabki kalitning 10 bitini qiymatini aniqlashga muvaffaq bo'ldilar. Gap shundaki, birinchi raund S1 bloki qismiy kaliti 6 ta bitining 2 tasi sakkizinchi raund S1 bloki qismiy kaliti 6 ta bitida ishtirok etar ekan. Ushbu faktni bilish qismiy kalitlarni saralashda o'z natijasini ko'rsatdi. Albatta, kalitning o'n biti ko'p emas, ammo bundan ham nimagadir foydalanish mumkin.


ΔX_L bo'lishi mumkin bo'lgan 16 ta qiymatdan birini qabul qiladi
ΔX_R bo'lishi mumkin bo'lgan 3 ta qiymatdan birini qabul qiladi
9,17,23,31 bitlar o'zgargan bo'lishi mumkin
F1
ΔB' = 00 00 00 00x
F2
Δb' = 00 00 00 00x
F3
Δc' = ΔX_R
7,9,12,17,22,23,31,32 битлар ўзгармаган
9,17,23,31-чи битлар ўзгарган бўлиши мумкин
F4
ΔY(5)3, ΔY(5)8, ΔY(5)14, ΔY(5)24
F5
ΔX(5)17
F6
F7
ΔX(7)17
ΔY(7)3, ΔY(7)8, ΔY(7)14, ΔY(7)24
ΔY(8)17
F8
ΔY_R
ΔY_L
ΔY_R

10.1-rasm. 8 raundli DES shifrlash algoritmiga chiziqli-differensial kriptotahlilni qo'llash.

Langford va Xellmanlarning tadqiqotlarini kuzatgan Eli Bixam, Orr Dunkelman i Natai Keller 8 raundli DES shifrlash algoritmini chiziqli-differensial kriptotahlilini o'tkazishda o'zlarining yondoshuvlarini taklif qildilar. Quyida biz ular tomonidan taklif qilingan tahlil qilish usuli bilan tanishamiz (10.1-rasm).

Shifrlash algoritmi kirishiga (AX_L, AX_R)= (00 80 82 00, 60 00 00 00) ayirma tushadi. Natijada birinchi raund F shifrlash funksiyasiga qiymati 60 00 00 00 bo'lgan ayirma kiradi. Ilgari bunday holda birinchi S blokdan boshqa barcha S bloklarning chiqishida nol qiymatli ayirmalar chiqishini ta'kidlagan edik. Ma'lumki, S1 blokka 001100 qiymat kirsa (aynan ushbu qiymat kiradi, chunki AXR=60 00 00 00 qiymat kengaytirib, o'rin almashtirishga uchragandan so'ng S0 00 00 00 00 00 ga o'zgaradi) eng katta p=14/64 ehtimollik bilan chiqishda qiymati 1110 bo'lgan ayirma paydo bo'ladi. F shifrlash funksiyasidan chiqishdan oldin S bloklar chiqishlari o'rin almashtiishga uchraydi, S1 blokdan chiqqan ayirmadagi 1 lar ayirmaning 9,17 va 23 pozisiyalarida joylashadi. SHunday qilib, DES algoritmi birinchi raund F shifrlash funksiyasi chiqishida p = 14/64 ehtimollik bilan AA'=00 80 82 00 ayirma paydo bo'ladi.

Birinchi raundni kirish ayirmasini chap qismi bilan chiqish ayirmasining ikkining moduli bo'yicha yig'indisi ikkinchi raundni F shifrlash funksiyasiga kirganligi sababli ushbu ayirmaning qiymati quyidagicha bo'ladi:

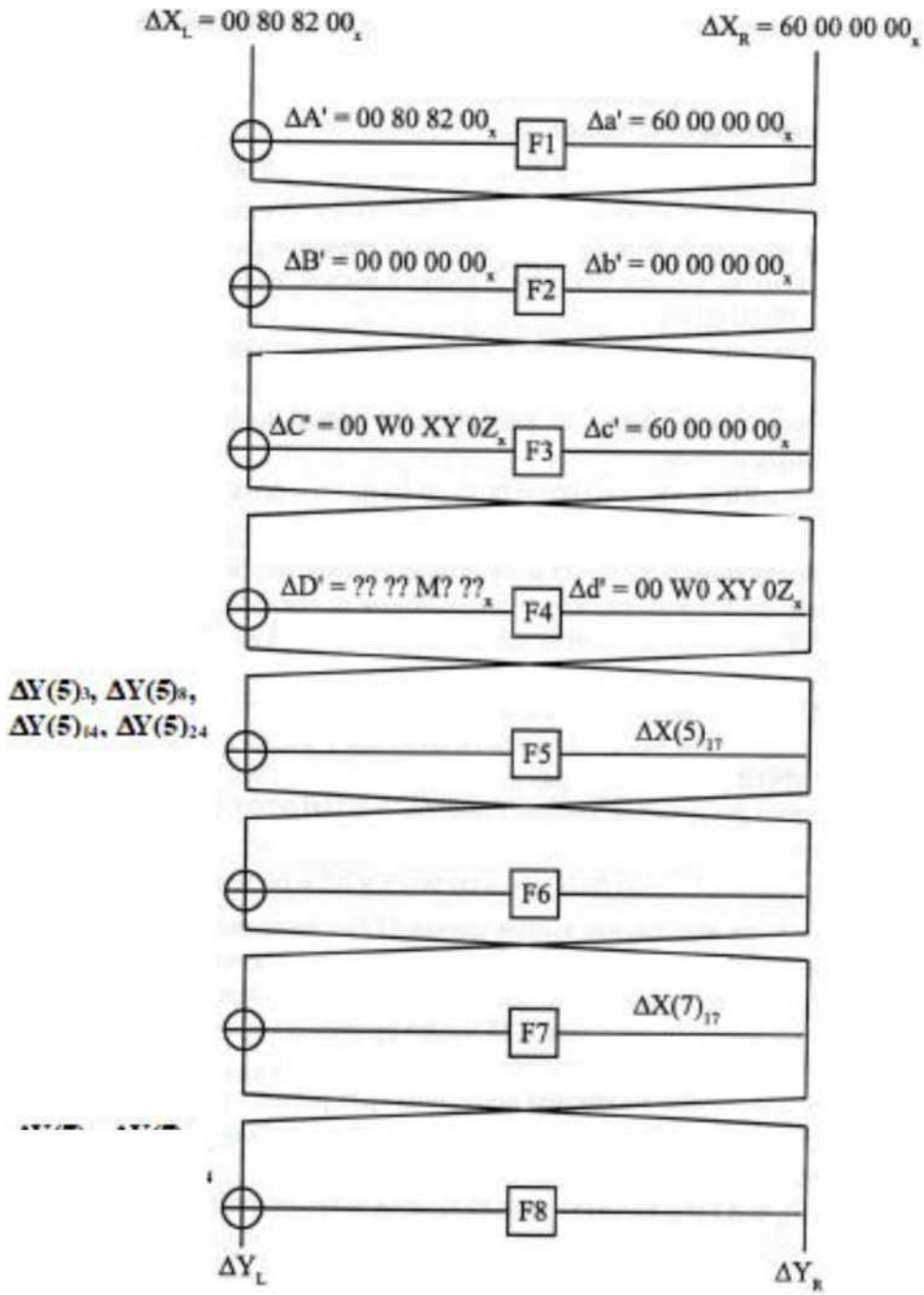
Ab'=AXL©AA'=00 80 82 00 Φ 00 80 82 00 = 00 00 00 00.

Agar F shifrlash funksiyasiga qiymati noldan iborat ayirma kiradigan bo'lsa, ushbu funksiyadan ham qiymati noldan iborat ayirma chiqadi. Shu sababli ikkinchi raund F shifrlash funksiyasidan AB'= 00 00 00 00 ayirma chiqadi.

Birinchi raundni kirish ayirmasini o'ng qismi bilan ikkinchi raundni chiqish ayirmasining ikkining moduli bo'yicha yig'indisi uchinchi raundni F shifrlash funksiyasiga kirganligi sababli ushbu ayirmaning qiymati quyidagicha bo'ladi:

AC'=AXR©AB'=60 00 00 00 Φ 00 00 00 00 =60 00 00 00.

Ushbu holda biz bilamizki, F shifrlash funksiyasidan chiquvchi ayirmaning 9, 17, 23 va 31 pozisiyalardagi qiymatlari 1 dan iborat bo'lishi mumkin. Shu bois, shuni aytish mumkinki, uchinchi raund F shifrlash funksiyasidan chiquvchi ayirmaning qiymati AC'=00 W0 XY 0Z bo'ladi. Bu erda W va X lar 0 yoki 8, Y va Z lar 0 yoki 2 qiymatlarni qabul qilishlari mumkin.



ДУ(7)ч AY(7>, $AY(7)_{H}$, AY(7)м

10.2-rasm. 8 raundli DES shifrlash algoritmi uchiin Eli Bixam, Orr Dunkelman va Natai Keller tomonidan taklif qilingan chiziqli-differensial kriptotahlil usuli.

To'rtinchi raundni F shifrlash funksiyasiga ikkinchi raundni kirish ayirmasini o'ng qismi bilan uchinchi raund F shifrlash funksiyasini chiqish ayirmasining ikkining moduli bo'yicha yig'indisi kiradi. Ikkinchi raundni kirish ayirmasini o'ng qismi Ab'= 00 00 00 00 bo'lganligi sababli to'rtinchi raundni F shifrlash funksiyasiga qiymati quyidagicha bo'lgan ayirma kiradi:

Ad'=AbWC'= 00 00 00 00 Ф 00 W0 XY 0Z = 00 W0 XY 0Z.

11-Amaliy mashgulot.

Mavzu: Odatdagi slaydli hujumni s-des-1 shifrlash algoritmiga qo'llanilishi.

S-DES-1 shifri bo'yicha ma'lumotlar oldingi seminarlarda keltirilgan va muhokama qilingan edi. S-DES-1 shifrlash algoritmi Feystel tarmog'i asosida qurilganligi sababli tanlangan ochiq matn asosidagi hujumni bemalol unga nisbatan qo'llash mumkin. Ushbu algoritmda ochiq matn bloki uzunligi 16 bitni tashkil qiladi. Shifrlash jarayoni uchun algoritmga kiruvchi ochiq matn bloki har birining uzunligi 8 bitdan bo'lgan chap va o'ng qismiy bloklarga bo'linadi. S-DES-1 algoritmida dastlabki shifrlash kaliti uzunligi 10 bit bo'lib, undan ma'lum bir qoida asosida 8 bitli raund kalitlari hosil qilinadi. Mavzuni bayon qilish jarayonini soddalashtirish uchun to'g'ridan to'g'ri 8 bitli K raund kalitdan foydalanamiz (ya'ni, 10 bitli dastlabki shifrlash kalitidan 8 bitli qismiy kalit hosil qilish jarayonidan foydalanmaymiz). Shuningdek, shifrlanuvchi ma'lumotlarni raund kaliti bilan ikkining moduli bo'yicha qo'shish amali F-funksiyadan oldin emas, balki ushbu funksiyaning ichida bo'ladi. Algoritmning kriptografik bardoshligiga ta'sir qilmaganligi uchun boshlang'ich va yakuniy almashtirishlarni ham tushirib qoldiramiz hamda 20 raundan iborat kriptografik almashtirishdan foydalanamiz.

11.1-jadval. Ri=(x,ui) ochiq matnlar massivini K kalit bilan shifrlash natijalari.

№	X_L	X_R	Y_L	Y_R
1	1101	0110	0101	1100
2	1101	0001	1101	1110
3	1101	0010	1001	1010
4	1101	1000	0000	0111

11.2-jadval. R i' = (u i', x) ochiq matnlar massivini Krlash

№	XL'	X R'	Y_L'	Y_R'
1	1010	1101	1010	1101
2	0010	1101	0101	1111
3	1110	1101	1100	1000
4	1100	1101	0000	0011

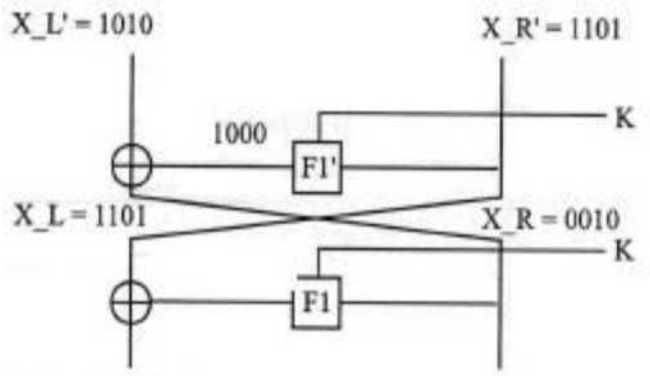
Birinchi navbatda ixtiyoriy ravishda to'rt bitli x=1101 matnni tanlaymiz. Undan so'ng bir-birlari bilan faqatgina tasodifiy tanlangan o'ng va chap qismlari bilan farqlanadigan $2^{n/l} = 2^{84} = 2^2 = 4$ ta sondagi Ri=(x=X_L, Ui=X_R) va Rj'=(Uj'=X_L', x=X_R') ochiq matnlardan iborat massivlarni shakllantiramiz. Endi tanlangan matnlarni 4 bitli qismlar (ularni har biri S-blok kirishiga ta'sir qiladi) dan iborat, tasodifiy tanlangan 8 bitli K = (K_1, K_2) kalit bilan shifrlaymiz. Ri = (x, nj va R j' = (u j', x) ochiq matnlardan iborat massivlarni shifrlash natijalari mos holda 11.1- va 11.2-jadvallarda keltirilgan.

Shunday qilib, bizning ixtiyorimizda sakkiz juft matnlar mavjud. 11.1- va 11.2- jadvallarda keltirilgan shifrlash natijalarini tahlil qilib, slayd juftlik shartini

ikkita matnlar juftligi qanoatlantirishini aniqlash mumkin.

Aniqlangan juftlikni tahlil qilishda S-DES-1 shifrlash algoritmi o'rniga qo'yish jadvali, ya'ni S bloklaridan foydalanishga to'g'ri keladi. 11.1-jadvaldagi №1 va 11.2-jadvaldagi №3 matnlar birinchi slaydli juftlikni tashkil qiladi. 11.1-rasmda keltirilgan shifrlash jarayonining birinchi ikki raundini o'rganib, ushbu juftlikni tahlil qilamiz.

X_R' va X_L matnlarning ma'lumligi F_1' funksiyaga kiruvchining qiymati haqida ma'lumot beradi. Shuningdek, X_R va X_L' matnlarning ham qiymati ma'lum. U holda F-funksiyadan chiquvchining qiymati, ya'ni 1000 ni osongina aniqlash mumkin.



11.3-rasm. Birinchi slaydli juftlik birinchi raundlarini tahlili.

F-funksiyadan chiqishdan oldin ma'lumotlar 11.3-jadvalga asosan o'rin almashtirishga uchraydi. Bir qadam orqaga qaytib, S blokdan chiqishda 0100 qiymat paydo bo'lishini aniqlash mumkin, ya'ni ushbu vaziyatda 01 va 00 qiymatlar mos holda S0 va S1 bloklardan chiqishlar hisoblanadi.

11.4-jadval. S-DES-1 shifrlash algoritmining S bloklariga kirish va chiqish mosliklari.

S-blokka kirish	S_0 blokdan chiqish	S_1 blokdan chiqish
0000	01	01
0001	11	10
0010	00	01
0011	10	00
0100	11	10
0101	01	01
0110	10	11
0111	00	11
1000	00	11
1001	11	10
1010	10	00
1011	01	01
1100	01	01
1101	11	00

1110	11	00
1111	01	11

F-funksiyaga kiruvchi xabar 11.4-jadvalga asosan kengaytirib o'rin almashtirishga uchraydi. Buning natijasida F-funksiyaga kiruvchi 1101 ma'lumot 11101011 ga almashadi. Kengaytirish natijasi K=(Ki,K2) kalit bilan qo'shilib, ya'ni So blokka 1110Φ K1 kirib, S1 blokka 1011 ϕ1<2 kirib, ushbu bloklardan mos holda 01 va 00 qiymatlar chiqadi.

Agar 0000, 0101, 1011, 1100 va 1111 qiymatlardan biri S_0 blokka kirsagina, undan chiqishda 01 qiymat paydo bo'lishini aniqlash mumkin. U holda S_0 blokka kiruvchi 0000, 0101, 1011, 1100 yoki 1111 qiymatlarning har birini 1110 bilan ikkining moduli bo'yicha qo'shib, K_1 qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 1110, 1011, 0101, 0010 yoki 0001 ni hosil qilish mumkin.

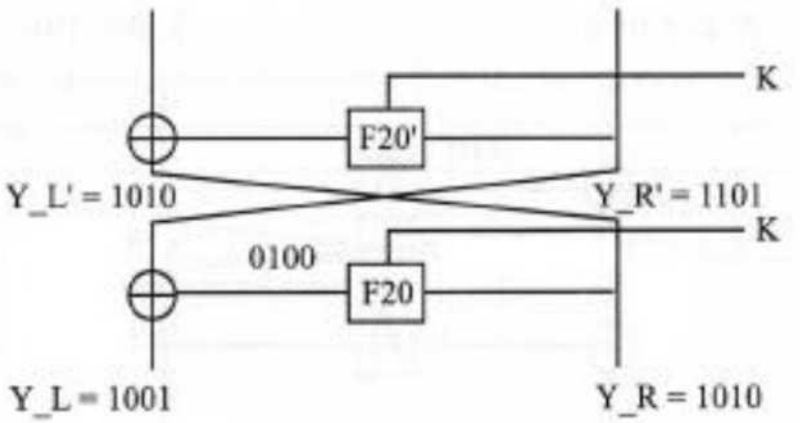
Xuddi shuningdek, 0011, 1010, 1101 yoki 1110 qiymatlardan biri S1 blokka kirsagina, undan chiqishda 00 qiymat paydo bo'lishini payqash mumkin. U holda S_1 blokka kiruvchi 0011, 1010, 1101 yoki 1110 qiymatlarning har birini 1011 bilan ikkining moduli bo'yicha qo'shib, K_2 qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 1000, 0001, 0110 yoki 0101 ni hosil qilish mumkin.

11.3-jadval. S-DES-1 shifrlash algoritmi o'rin almashtirish jadvali.

P4			
2	4	3	1

11.4-jadval. E/P kengaytirib almashtirish jadvali.

E/>							
4	1	2	3	2	3	4	1



11.5-rasm. Birinchi slaydli juftlik oxirgi raundlarini tahlili.

Endi ushbu slaydli juftlik uchun shifrlashning oxirgi ikki raundi (bizning holimizda 20-chi round) ni ko'rib chiqamiz (11.5-rasm).

Y_L' va Y_R matnlarning ma'lumligi F_{20}' funksiyaga kiruvchining qiymati haqida ma'lumot beradi. Shuningdek, Y_R' va Y_L matnlarning ham qiymati ma'lum. U holda F-funksiyadan chiquvchining qiymati, ya'ni 0100 ekanligini osongina aniqlash mumkin.

F-funksiyadan chiqishdan oldin ma'lumotlar 4-jadvalga asosan o'rin almashtirishga uchraydi. Bir qadam orqaga qaytib, S blokdan chiqishda 0001 qiymat paydo bo'lishini aniqlash mumkin, ya'ni ushbu vaziyatda 00 va 01 qiymatlar mos holda S_0 va S_1 bloklardan chiqishlar hisoblanadi.

F-funksiyaga kiruvchi xabar 11.5-jadvalga asosan kengaytirib o'rin almashtirishga uchraydi. Buning natijasida F-funksiyaga kiruvchi 1010 ma'lumot 01010101 ga almashadi. Kengaytirish natijasi K=(K_1,K_2) kalit bilan qo'shilib, ya'ni S0 blokka 0101 f K1 kirib, S1 blokka 0101 ®K_2 kirib, ushbu bloklardan mos holda 00 va 01 qiymatlar chiqadi.

Agar 0010, 0111 yoki 1000 qiymatlardan biri S0 blokka kirsagina, undan chiqishda 00 qiymat paydo bo'lishini aniqlash mumkin. U holda S_0 blokka kiruvchi 0010, 0111 yoki 1000 qiymatlarning har birini 0101 bilan ikkining moduli bo'yicha qo'shib, K_1 qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 0111, 0010 yoki 1000 ni hosil qilish mumkin.

Xuddi shuningdek, 0000, 0010, 0101, 1011 yoki 1100 qiymatlardan biri S1 blokka kirsagina, undan chiqishda 01 qiymat paydo bo'lishini payqash mumkin. U holda S_1 blokka kiruvchi 0000, 0010, 0101, 1011 yoki 1100 qiymatlarning har birini 0101 bilan ikkining moduli bo'yicha qo'shib, K_2 qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 0101, 0111,0000, 1110 yoki 1001 ni hosil qilish mumkin.

Shifrlashning barcha raundlarida bir xil kalitdan foydalanilgani uchun birinchi va oxirgi raundlarda K1 va K2 qismiy kalitlarning qiymatlari o'zgarmasdan qolishi lozim. K_1 va K_2 qismiy kalitlarning bo'lishi mumkin barcha qiymatlarini tekshirib ko'rish orqali faqatgina bitta K1=0010 va K2=0101 qiymatlardangina birinchi va oxirgi raundlarda foydalanish mumkinligi aniqlandi. Bu esa qidirilayotgan kalit aynan K=00100101 ekanligini anglatadi. Yuqorida generasiya qilingan ochiq matnlarni ushbu kalit bilan shifrlab, shifrlash natijalarini taqqoslash orqali shifrlash kaliti to'g'ri topilganligiga ishonch hosil qilish mumkin. 10.1-jadvaldagi №3 va 10.2- jadvaldagi №1 matnlar ikkinchi slaydli jultlikni tashkil qiladi. Ushbu matn jultliklarini tahlil qilish ham yuqoridagi natijaga olib keladi. Buni o'quvchining o'zi mustaqil bajarib, ishonch hosil qilishi mumkin.

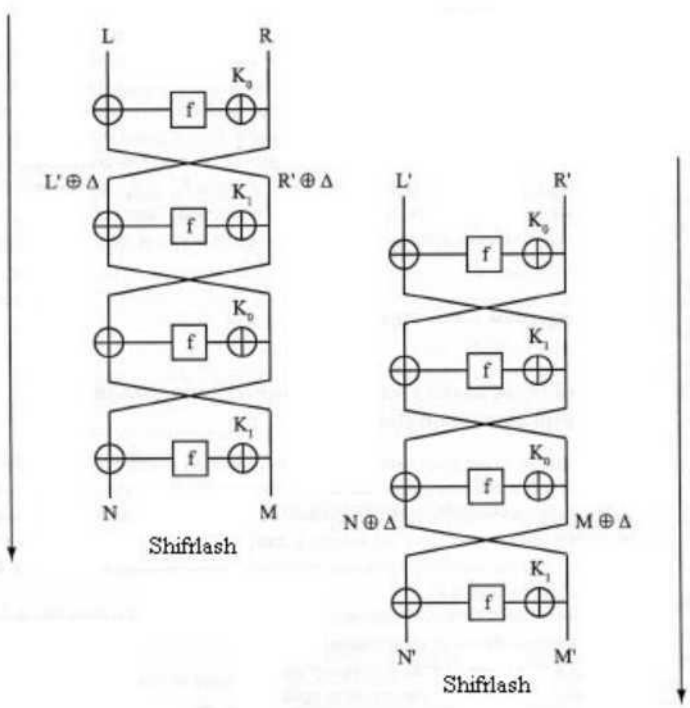
12-Amaliy mashgulot

Mavzu: Yaxshilangan slaydli hujumning asosiy g'oyasi.

Qo'shimcha ma’lumotlardan foydalanuvchi slaydli hujum (Comrlemeptatiop slide). Ushbu mavzuda ko'plab shifrlash algoritmlariga qo'llash uchun oddiy slaydli hujumni kengaytirishning bir necha usullari keltiriladi. Birinchi navbatda Feystel tarmog'iga asoslangan, ikki raundli o'z-o'ziga o'xshash shifrlash algoritmini tahlil qilishga mo'ljallangan usul bayon etiladi. Bu erda o'z-o'ziga o'xshash shifrlash algoritmi deyilganda 12.1-rasmda

ko'rsatilgani kabi shifrlash jarayonida ikkita doimo almashinuvchi K0 va K1 qismiy kalitlardan foydalanuvchi algoritm nazarda tutiladi.

Odatdagi slaydli hujumni ikki raundli o'z-o'ziga o'xshash shifrlash algoritmi qo'llashda ikki raundga «kechikuvchi» ikkita shifrlash jarayonini taqqoslash mantiqan to'g'ri bo'lar edi, ammo ushbu holda hujum samarasiz bo'lar edi. Agar har bir raundda ikkita shifrlash jarayoni o'rtasida A= K0®K1 ayirmadan foydalanilsa, bir raundga «kechikuvchi» shifrlash jarayonlarini taqqoslash imkoni mavjud. Ushbu holda ikki raundli o'z-o'ziga o'xshashlikdan bir raundli o'z- o'ziga o'xshashlikka o'tish mumkin. Shu bilan birgalikda slaydli juftliklarda shifrlash raundlari o'rtasida ayirmaga ega bo'lish mumkin.



12.1-rasm. O'z-o'ziga o'xshash shifrlash algoritmi.

Hujum qilish uchun shunday slaydli juftlikni tanlash kerakki, natijada ochiq matnlar ayirmasi kalitlar ayirmasini kompensasiya qilsin. Buning uchun slaydli ayirmasi (D, D) bo'lgan ochiq matnlarni topish lozim bo'ladi. Ma'lumki, agar F(P)®R'=A bo'lsa, u holda R va R' ochiq matnlar juftligi Д slaydli ayirmaga ega bo'ladi. Bunday slaydli ayirma p=1 ehtimollik bilan raunddan raundga o'tadi va natijada shifr matnlarni shu ayirmaga olib keladi. 6.1-rasmda ushbu kriptotahli usuli ochiq ko'rsatilgan.

Xuddi oldingi mavzularga o'xshab, $2^{n/2}$ ta ochiq matndan tashkil topgan massivdan slaydli juftlik ajratib olinishi mumkin. Agar ochiq va shifr matnlarni mos holda R = (L, R) va S = (N, M) bilan belgilasak, u holda quyidagi tengliklarga ega bo'lish mumkin:

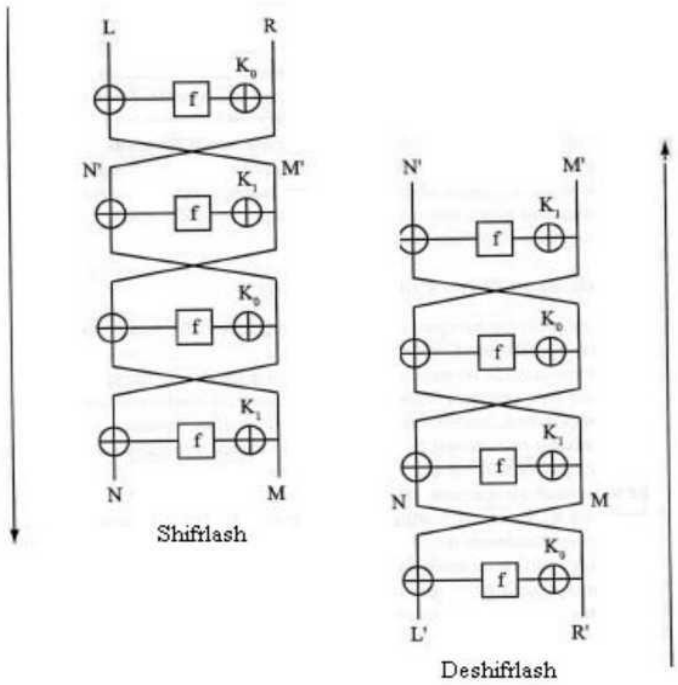
$$(L',R') = (R,L \text{ F } f\ (Ko \text{ F } R\ ))\ F(A, A), \qquad (10.1)$$

$$(N',M') = (M \text{ F } f(K \text{ F } N \text{ F } A),N)\ F(A, A). \qquad (10.2)$$

Keltirilgan tenglamalardan ko'rinib turibdiki, L'=R fD va M'= N fD. Natijada L'fM-RfDfNfD = R©N ni hosil qilish mumkin. Bu esa slaydli juftlikni aniqlashning n/2 bitli shartidir. Topilgan slaydli juftlik L, R, M, N, L', R', M' va

N' laming qiymatlarini beradi.

Ma'lumki, R=LfD (11.1-rasm), demak, A=R©L. Ikkining moduli bo'yicha ikkita qiymat kfLfK' ni qo'shib, shifrlash raundining F funksiyasi chiqishida slaydli juftlikni hosil qilish mumkin. Bizga F funksiyaning almashtirishlari ma'lum va ular kalitga bog'liq emas. U holda slaydli juftlik shifrlashining birinchi raundi F funksiyasi kirishiga qanday qiymat kelib tushganligi haqida faraz qilish mumkin. Chunki ushbu funksiyaning kirishiga RфK0 yig'indi kelib tushadi, bu esa K_0 ning qiymati haqida faraz qilish imkonini beradi. Xuddi shunday mulohazalarni ikkinchi slaydli juftlikning oxirgi raundi haqida ham yuritib, F funksiyaning chiqishida MfLfI yig'indi paydo bo'lishini aniqlash mumkin. Ushbu funksiyaning kirishiga WK' yig'indi kelib tushadi. Demak, Ki ning qiymati haqida faraz qilish mumkin bo'ladi. Ko va Ki qismiy kalitlarning ilgari faraz qilingan qiymatlaridan ikkining moduli bo'yicha A qiymatni beradigan qiymatlarigina haqiqiy bo'ladi. Ko'rinib turibdiki, tahlildagi asosiy qiyinchilik to'g'ri slaydli juftliklarni topish bilan bog'liq bo'lib qolmoqda.



12.2-rasm. Ilmoqli slaydli hujum.

Ilmoqli slaydli hujum (Sliding with a Twist). Ushbu mavzuda Feystel tarmog'iga asoslangan, ikki raundli o'z-o'ziga o'xshash shifrlash algoritmini tahlil qilish uchun yana bitta slaydli hujum usuli keltiriladi.

Agar blokli shifrlash algoritmlariga ko'pchilik hollarda qo'llaniladigan boshlang'ich va yakuniy almashtirishlar e'tiborga olinmasa, Feystel tarmog'iga asosida qurilgan shifrlash algoritmlari uchun K_0 va K_1 qismiy kalitlardan foydalanuvchi deshifrlash jarayoni K1 va K0 qismiy kalitlardan foydalanuvchi shifrlash jarayoniga o'xshash bo'ladi. Shuni ham aytish mumkinki, Feystel tarmog'i asosidagi algoritmlar yordamida K0 va K1 qismiy kalitlardan foydalanuvchi shifrlash jarayoni ushbu algoritm bilan K1, K0 qismiy kalitlardan foydalanib, shifrlash jarayoniga juda yaqin, ya'ni bunda jarayonlardan biri ikkinchisiga nisbatan bitta raundga «kechiktirilib» bajariladi. Shu boisdan,

shifrlash va deshifrlash jarayonlaridan biri ikkinchisiga nisbatan bitta raundga «kechiktirilib», taqqoslanadi. Ushbu holda shifrlashning birinchi va deshifrlashning oxirgi raundlaridan boshqa barcha raundlarda slaydli jultliklar qisman ustma-ust tushadi.

Kriptotahlil hech bo'lmaganda bitta slaydli jultlikni topish uchun $2^{n/2}$ ta ochiq matndan iborat massivni yaratishdan boshlanadi. Izlanayotgan slaydli jultlik uchun quyidagi tengliklar o'rinli bo'lishi lozim:

$$(N',M') = (R,L\ F\ f(K \circledR R)). \quad (11.3)$$

$$(L',R') = (M\ F\ f\ (K \circledR N),N), \quad (11.4)$$

(12.3), (12.4) tenglamalar slaydli juftlik (ya'ni, N' = R va R'=N) ni ajratish uchun n-bitli shartni beradi. Slaydli juftdikni aniqlab, bundan oldingi mavzuda bayon qilingan usul bilan K_0 qismiy kalitni bitlarini topish mumkin. Shifrlashning ikki raundiga «kechiktirilib», slaydli hujum qilish natijasida K_1 qismiy kalitni aniqlash mumkin. Bunda tahlil uchun ilgari yaratilgan matnlar massividan foydalanish mumkin.

Shuningdek, tanlangan ochiq matn-shifr matn asosida hujum qilish mumkin. Ushbu holda talab qilinadigan matnlar soni $2^{n/4}$ tagacha kamayadi. Buning uchun faqatgina chap yarim qismi bilangina farqlanadigan $2^{n/4}$ sondagi (Li,R) ochiq matnlardan tashkil topgan massivni yaratish va ularga mos keluvchi shifr matnlar qiymatini hosil qilish lozim bo'ladi. Shuningdek, faqatgina chap yarim qismi bilangina farqlanadigan $2^{n/4}$ sondagi (Mj',N') (bu erda N'=R) shifr matnlardan tashkil topgan massivni yaratish va ularga mos keluvchi ochiq matnlar qiymatini hisoblash kerak. Bunday sondagi ochiq va shifr matnlarga ega bo'lgandan keyin hech bo'lmaganda bitta slaydli juftlikni topish mumkin bo'ladi. Keyingi bo'ladigan tahlillar oldingilariga o'xshash tarzda olib boriladi.

13-Amaliy mashgulot.

Mavzu: Kvant kriptografiyasining ma’lumot kaliti taqsimoti tizimini protokollari

Kvantli ob’ektlar bilan axborotlarni soxtalashtirish va ruxsat etilmagan kirishdan ximoya qilish fikrini birinchi bo‘lib 1970 yil Stefan Veysner tomonidan aytilgan. 10 yildan so‘ng, Veysner bilan tanish bo‘lgan Bennet va Brassard Veysnerning ishini davom etib, kvantli obektlar yordamida maxfiy kalitlarni yuborishda ishlatgan. 1984 yili IBM firmasi xodimi Charlz Bennet va Monrela universiteta olimi Jil Brassor fotonlarning kriptografiya soxasida fundamental ximoyalangan aloqa kanalini tashkil qilishi mumkinligini aniqlashgan. 0 va 1 larni tashkil qilish uchun fotonlarni olishga qaror qilishdi, bu fotonlarning turli qutblari orqali tashkil qilinadi. BB84 deb nomlanuvchi kvantli shifrlash kalitlarini aniqlash sxemasini tuzib chiqishdi. Keyinroq, 1991 yilda bu goya Ekert tomonidan shakllantirildi. Bu sxema kvantli kanalni qo‘llaydi, qaysiki aloqani ximoyalangan seansi ishtirokchilari bir birlari bilan ma’lumot almashish uchun ularni qutblangan fotonlar ko‘rinishida yuboradi.

Kvantli kriptografiya texnologiyasi kvant tizimining quyidagi xossasiga asoslangan-bir vaqtning o‘zida kordinata va impuls qismlarini qabul qila

olmaydi va fotonning bir parametrini boshqa bir fotonni buzmasdan o‘zgartirib bo‘lmaydi. Bu tabiatning fundamental xususiyati fizikada Geyzenberg noaniqlik printsipi bilan ma’lum. Bu printsip 1927 yilda ishlab chiqilgan. Bu printsipga asosan, kvant tizimidagi parametrlarning o‘zaro bog‘liqligini aniqlash uning buzilishiga olib keladi va bu o‘zgartirish natijasida qabul qilinadigan axborot dezinformatsiya shaklida aniqlanadi.

Agar fotonni biror bir xususiyatini o‘zgartirsak, masalan deylik qutblanish darajasi yoki yoruglik uzunligini o‘zgartirish natijasida fotonning tuzilishi o‘zgaradi. Bir vaqdning o‘zida kvantning ikkita kattaligini berilgan aniqlik bo‘yicha o‘zgartirib bo‘lmaydi va qutblanish darajasining o‘zgarishi ikkinchisining xam mos ravishda o‘zgarishiga olib keladi. Agar ma’lumotni yuboruvchi va qabul qiluvchi tomonlar qutblanishning biror bir usulini tanlab olishmagan bo‘lsa, qabul qiluvchi yuboruvchi tomonidan berilgan ma’lumotlardan xech qanday foydali ma’lumot olisha olmaydi.

Shunga asoslanib, axborotni uzatishda boshqa kimsalar tomonidan ushlab qolinishida ximoya qilish uchun ma’lumot uzatish kanallari ko‘riladi. Qabul qiluvchi kelayotgan axborotni boshqa odamlar tomonidan ushlab qolinganligini aniqlashi mumkin va bu aniqlanganidan keyin uzatuvchi tomonga ma’lumotlarni boshqa kalit bo‘yicha qayta uzatishni so‘raydi.

Yuboruvchi ma’lumotlarni biror bir kvantli tuzilish bo‘yicha kodlashtiradi. Qabul qiluvchi esa, bu tuzilishlarni ro‘yxatdan o‘tkazadi. Keyin yuboruvchi va qabul qiluvchi tomonlar birgalikda kuzatish natijalarini taxlil qilishadi. Natijada, yuborilgan va qabul qilingan ma’lumotlarning bir xilliliga ishonch xosil qilinadi. Natijalarni taxlil qilishda quyidagilarga e’tibor beriladi: xatoliklar, shovqin va buzgunchilar keltirib chiqargan xatoliklar. Ma’lumotlarni aniqligi taxlil qilinadi, lekin bit bo‘yicha taxlil qilinmaydi. Ma’lumotlarni uzatish vaqtida fotonlarning joylashuvi nazorat qilinadi.

Yoruglikni qutblanishini o‘lchash uchun u qaysi qutb sistemasi bo‘yicha uzatilganligini oldindan bilishimiz kerak. Agar bizga yoruglik vertikal yoki gorizontal uzatilgan bo‘lsa, uni gorizontal filtrdan o‘tkazganimizda u 0 yoki 90 gradusda qutblanganligini aniqlashimiz mumkin. Agar qutblanish dioganal va filtrni gorizontal qo‘ygan bo‘lsa, u xolda yoruglik +45 yoki -45 gradusda o‘tkanligini aniqlay olmaymiz.

Shuning uchun yoruglik impulslari orqali shakllantirilgan kanalda boshqa shaxslar tomonidan ushlab qolinmaydi. Noto‘g‘ri filtr o‘rnatilganda kanal buziladi. Kvant kriptografiyasidan foydalanish jarayonida quyidagi kvantli protokollardan foydalaniladi:

1. Kvantli protokol BB84

Bu sistema o‘zida qabul qilgich va uzatkichdan tashkil topgan. Uzatkich o‘zida fotonlarni turt qutbdan biriga jo‘natishda generator ishlata oladi.O, 45, 90 yoki 135 graduslar tanlanayotgan bitga bogliq. Qabul qilgich esa, qutblanishni o‘lchaydigan fiksatorni ishlatadi. Kvant mexanikasini qonunlariga ko‘ra qabul qilgich, to'g'ridan-to'g'ri qutblanish (0,..,90) yoki dioganal qutblanish(45,..,135)larni farqlay oladi, lekin ikkalasini birgalikda

xech qachon farqlay olmaidi. Kalitlarni taqsimlash bir necha qadamlarda iborat:

1- qadam: Uzatkich fotonlarni ixtiyoriy tanlangan 4 qutblardan 1 tasiga yuboradi.

2- qadam: Xar bir qabul qilingan foton uchun qabul qiluvchi ixtiyoriy tipdagi qutblanish olchamini tanlaydi: to‘g‘ri yoki dioganal. Qabul qiluvchi o‘lchangan natijani yozib oladi va ularni maxfiy ravishda saqlaydi.

3- qadam: Qabul qiluvchi (ochiq kanal) oshkora fotonlarni o‘lchashda ishlatiladigan tiplarni e’lon qiladi (natijani e’lon qilmaydi).

4- qadam: Uzatuvchi yuboruvchiga (ochiq kanal bo‘yicha) to‘g‘ri tipdagi o‘lchashlarni xabar qiladi.

5- qadam: Foydalanuvchilar (qabul qiluvchi va uzatuvchi) o‘lchashlar xaqida xamma to‘g‘ri tipdagi xodisalarni tanlaydi.

Bu xodisalarni bitlarga yog‘irib, kalitlarni oladi. Xabarni yog‘irlamoqchi bo‘lgan buzgunchi, albatta shu xatolikni bajaradi chunki u oldindan fotonning qutblanish tipini bilmaydi. Kvant mexanikasi esa, bu ikkita noma’lum bir-biriga bog‘lik bo‘lmagan qutb tiplarini o‘lchash imkonini bermaydi (to‘g‘ri va dioganal qutblar) Ikkita qonuniy foydalanuvchi kvantli kanalda eshitish imkoniyati, ochiq kanal orqali ixtiyoriy bitli kalitlar va xatoliklarni testdan o‘tkazadi. Ular yashirincha eshitishni oldini ololmasa xam, buzgunchilar tomonidan aldanmaydi, chunki kanalga xar bir ulanish aniqlanadi.

Masalan, buzgunchi kabelni kesib uskunalar yordamida adresatni analogik jixozlari xaqida o‘lchashlarni olib boradi. Shundan so‘ng, u o‘lchashlar natijasiga ko‘ra qabul qiluvchiga foton jo‘natadi. Shunda buzgunchi xolatning 50% da noto‘g‘ri analizator tanlaydi va adresatga tasodifan tanlangan xolda jo‘natadi. Natijada 25% muxim xabarlar bitlari yuboruvchi tomonidan adresatnikidan farq qiladi.

Endi foydalanuvchilar yarim bitli satr kalitini tanlash orqali va oshkora ularni ma’nosini e’lon qilish orqali buzgunchi borlig‘ini bila oladi. Agar e’lonlarning xamma ma’nosi bir-biriga mos tushsa, foydalanuvchilar ularni xech kim eshitmayotganini ishonch xosil qilishi mumkin. Chunki, ularni eshitib turish extimolligi (3/4)N/2 ~=10-125 bo‘lganda, N = 1000

Alisa ma’lumotlari	1	0	1	0	1	0
Alisa filtiri	/	|	/	|	/	|
Bobni filtiri	\	\	-	-	-	\
Bobni natijalari	N	N	Y	N	N	Y
Kalit	-	-	1	-	-	0

Masalan, Alisa quyidagilarni yuboryapti: | \ / - \ - |.

Bob uzining detektorini ixtiyoriy sozlab olgan.

Maxfiy kalit algoritmining generatsiyasi.

Bob qutblanishni to‘g‘ri aniqlaganda (Xuddi Alisa yuborgan qutblarday), u to‘g‘ri natija oladi qolgan vaziyatlarda esa, natija tasodifiy bo‘ladi.

Bob va Alisa ochiq kanal orqali bir-biriga qaysi qutblanish tipidan foydalanayotganini aytadi (dioganal yoki ortogonal). Faqatgina to‘g'ri natijalarni qoldiradi.

Bizning keltirilgan misolimizda Bob 2, 5, 6, 7 - impulslar qutblanishini topdi. Shunday qilib, | \ \ - | qoladi.

Oldindan kelishilgan shartlarga ko‘ra, natija bitlar davomiyligiga aylanadi (Masalan, 0 va 45 birini qabul qiladi. 90 va -45 esa, 0).

Xabarni ogirlanganligini Bob va Alisa xatolarini tekshirish orqali aniqlashi mumkin, tasodifiy xabarlar betini taqqoslab. To‘g‘ri kelmagani, xabar o‘g‘irlanganini ko‘rsatadi, oshanda kalit o‘zgartiriladi va qayta yuboriladi.

Agar farq bo‘lmasa, taqqoslash uchun ishlatilgan bitlar tashlanadi va kalit qabul qilinadi.

1. Kvantli protokol B92

0 va 1larni bu protokolda tasavvur qilish uchun ikki yonalishli qutblangan fotonlar ishlatiladi. Uzatuvchi bitlarni kodlashda ikkita qutblangan filtrdan foydalaniladi. Bu ikkita qutbli filtrlar yonalishi orasidagi burchak 45 gradusni tashkil qiladi. Bu yonalishlar ortogonal emas. Qabul qiluvchi fotonlarni qabul qilishda 90, 135 gradusli filtrdan foydalaniladi. Agar foton qutbi va filtri orasidagi farqi 90 gradusni tashkil qilsa, u xolda foton filtr orqali o‘tmaydi. Agarda 45 bo‘lsa, fotonni filtrdan o‘tish extimolligi 0.5 ga teng.

Endi, B92 protokolini ishlash ketma-ketligini ko‘rib chiqamiz:

1-qadam: Manba ikki filtr orqali 0 va 45 gradusda 0 va 1li xabarni yuboradi.

2-qadam: Adresatning filtri 90, 135 gr. yonalishda bo‘ladi. Yuboruvchi shu yonalishdagi fotonlarni jo‘natadi.

3-qadam: Qabul qiluvchi qutblanishni aniqlashda shu yoki boshqa filtr orqali fotonni o‘tkazadi. Tasavvur qilaylik, masalan bitta filtr orqali (135gradus) foton o‘tmadi. Adresat nima yuborilganini bilmaydi. Agarda foton filtrdan o‘tsa, adresat ishonch bilan qabul qilingan foton 0 ekanligini bildiradi. Agar foton yaxshi qabul qilinsa, navbatdagi kalit biti 0 yoki 1 bilan ishlatiladigan filtrga qarab kodlanadi.

2-qadam: Adresat yuborilgan fotonlardan taxminan 4 dan birini olganini aniqlash oson.

3-qadam: Davomiylikni qabul qilib, adresat jo‘natuvchiga 100 dan 25 ta qabul qilingan fotonni aytish mumkin. Ular navbatdagi xabarda kalit bo‘lib xizmat qilishi mumkin. Shuning bilan filtr va qabul qilingan qutblarni aytmasdan turib bajaradi. Shuning uchun buzgunchi telefon orqali so‘zlashuvni eshitib tursa xam, kalitni tuza olmaydi.

4-qadam: Kalitni muvofaqiyatli jo‘natishdan so‘ng, jo‘natuvchi o‘zining xabarlarini shu kalit yordamida kodlab yuborishi mumkin. Adresatdan boshka xech kim kodni ocha olmaydi. Buzgunchi tomonidan xabarni kalitini o‘girlanganligi xaqidagi ma’lumotni, foydalanuvchilar xatolikni nazorat qilish orqali topib olishi mumkin. Buning uchun ular xuddi BB84 dagidek, kalitdan

tanlangan xolatlarni taqqoslash orqali aniqlaydi. Agarda bir-biriga to‘gri kelmagan xollar aniqlanganda, xabar o'g'irlanganligini ko'rsatadi va yuborish protsedurasi boshqatdan qaytariladi. Agarda to'g'ri kelsa, tekshirilayotgan bit, kalit ekspluatatsiyaga qabul qilinadi.

2. Ekkert tomonidan taklif qilingan kvantli protrokol.

1991 yil Ekkert maxfiy kalit yaratishda o‘zaro bo‘g‘langan kvantli zarrachalarni ishlatishni taklif qildi. Bunday xususiyat birinchi bo‘lib, Eynshteyn tomonidan 1935 yil mantiqiy paradoks deb aytib o‘tilgan, keyinroq 1969 yilda Bell tomonidan tushuntirilgan. Bir-biriga boglik zarrachalar (EPR zarrachalar) xarakatchan xolatda bo‘ladi. Bunday zarrachalarning to‘lqin funktsiyasiga ko‘ra:

$$|Y> = (1/2)1/2*(|0>|1> - |1>|0>)$$

Bu erda zarrachalar o‘lchanayotgan EPR paradoksiga ko‘ra yozilgan. Bu ikki juftlikdan birining xolati ma’lum bo‘lsa (misol uchun, qandaydir bazasiga asosan o‘lchashlar olib borilayotg‘an bo‘lsa), u xolda ikki xolatini 100% lik aniqliq bilan aniqlash mumkin va bu ikki zarraning bir - biriga bo‘g‘lik ortoganal bo‘ladi. Agar birinchi zarraning xolatini o‘lchashi |0> ni bersa, u xolda ikkinchi zarraniki xuddi shu bazisda |1>.

Ekkert protokolini ishlashi uchun, ikkita EPR zarrani generatsiyalovchi qurulma zarur bo'ladi. Bulardan tashqari maxfiy kalitlarni shakllantirishda kvantlarini qatnashuvchilarga uzatuvchi kanal zarur, qatnashuvchilarda esa qabul qilingan zarralarning xolatini o'lchaydigan qurilma bo‘lishi kerak.

1-qadam:Qurilma ikki bir-birig‘a bogliq zarralarni ishlab chiqaruvchi qurilma (A va B).

2-qadam:A zarracha birinchi foydalanuvchiga yuboriladi (odatda uni Alisa deb nomlaymiz), B zarracha esa ikkinchi foydalanuvchiga (uni xam Bob deb nomlaymiz).

3-qadam:Alisa va Bob o‘z zarralarini o‘lchaydi, o‘lchashlar natijasi esa EPR paradoksiga to‘g‘ri kelishi kerak va Bellaga teng bo‘lmasligi kerak.

4-qadam:Davomiyligidan olingan bitlarni bir qismini ochiq kanal bo‘yicha o‘lchanadi. Agarda ular kvantlar korelyatsiyasini buzilganligini aniqlamasa, u xolda e’lon qilinmay qolgan bitlar kalit deb e’lon qilinadi.

Kamchiligi: ayirboshlovchi qatnashuvchilardan biri qabul qilingan ketma - ketlikni invertlab turishi kerak.

Masalan shpion kvantlar uzatish kanalini topib oldi va kvantlarni xolatini o‘lchay boshladi. Lekin u qaysi bazisda o‘lchashlar olib borishini qaerdan bilsin? Shu tariqa buzgunchi kamida 50% vaziyatda EPR bog‘liqligini buzadi. Buzgunchining borligini xuddi BB84 dagiday, kalitli ketma - ketlikdagi ko'p xatolar orqali aniqlanadi.

3. Zichlab kodlash protokoli.

Tasavvur qilaylik, juft qutiblarni ketma-ketligini $|00>+|11>$ xolatda yaratuvchi qurilma mavjud va xar bir juftlikda bitta qutibni Alisada saqlash uchun, boshqasini Bobda saqlash uchun yubormoqda. Bungacha Alisa va Bob uchun xech qachon bir-biri o‘rtasida bo‘g‘lanish o‘rnatilmasligi talab qilingan edi. Bu xolda esa, Alisa Bobga bitta qutib yordamida, ikki klassik bitlar xaqida xabar berishi mumkin. Bu xolat shunday tushuntiriladi, bir - birig‘a bog‘liq

bo‘lgan to‘rt orthogonal |00> + |11>, |00> -|11>, |01> + |10>, |01> -|10> xolat bir xolatdan boshqa xolatga o‘tishdabir qutib vositasida taminlanishi mumkin.

Berilgan xolat juda kuchli Bell-EPR ketma-ketlgini ko‘rsatgani uchun Bella bazisi deb ataladi (Braunstein et. al. 1992). |00> + |Ts> xolatdan boshlab, Alisa Bella bazisi xolatida kvantlarning bir geyt {1, X, Y, Z } yordamida ma’lum bo‘lgan qutibga ta’sir ko‘rsata oladi. Operatsiyalarda 4 imkoniyat bo‘lgani uchun 2 bitli klassik axborot bilan ta’sirda aniqlanadi.

Zichlab kodlash protokolini ko‘rib chiqaylik:

1-qadam: Alisa va Bob qurulmadan bir-birig‘a bo‘g‘liq bo‘lgan juft qutiblardan (a va b) birini olishadi.

2-qadam: Alisa o‘zining qutibi a ga geyt bilan ta’sir ko‘rsatadi. Xar qanday geyt ishlatishga yuborilayotgan 2 bit axborotga bogliq.

3-qadam: Bob Alisadan qutib qabul qilgandan so‘ng, u qutib Bella bazisini qaysi xolatidaligini aniqlashi kerak. Buni juft qutibga XOR geyti tasiri vositasida qilish mumkin va natijalovchi bitni o‘lchash orqali. Shu tariqa Bob |00>+-|N> xolatni |01>+-|10> xolatdan farqlay oladi.

4-qadam: Bob superpozitsiya belgisini aniqlashi uchun, u Admara "X" o‘zgartirishini ishlatishi kerak [misol uchun 7] va shundan so‘ng natijani o‘lchashi kerak. Shunday qilib Bob ikki klassik bitlar xaqida axborot oladi.

Zich kodlashni amalga oshirish qiyin. Shunaqa fikrlar borki standart boglanish metodidan boshqa amaliy ma’nosi yo‘q, lekin bunaqa emas. Bu protokol aloqa ximoya qiladi. Ikki klassik bitlardagi axborotlarni olish uchun, yuboruvchi Alisani qutibini ikki juftiga ega bo‘lsag‘ina axborotni oladi. Shunday qilib buzgunchi xam markazdan Bobga yuborilayotgan juft qutib olishi kerak, Alisa xam bobga yuborayotgan qutibni olishi kerak. Ko‘rinib turibdiki, bu qutiblar xar xil KKS bilan yuboriladi. Bundan tashqari, agar bugungi bitta qutibni olishga muvaffaq bo‘lsa, uni ushlab topib olishadi, chunki qutib ikkinchi qutibga to‘liq emas.

Buzgunchi Bobga olingan juft qutibdan bosh biriktirilgan juft qutiblarni yuborishi mumkin. U xolda Alisaning xabari xaqiqatdan xam og‘irlangan bo‘ladi. U xolda buzgunchi biriktirilgan juftlikni ishlab chiqaradigan generatorga kirishga ega bo‘lishi kerak. Alisa va Bob o‘zlarida ishlab chiqaradigan mavjud qutblarni tekshirish xaqida kelishish mumkin. Bunday tekshirish buzgunchini ishiga 50% xolatda salbiy natijani ko‘rsatishi mumkin. Bundan tashqari buzgunchi Alisa yuboradigan qutibni kodlashi uchun qanchadir vaqt yoqotadi, bunday yoqotishdan so‘ng, u almashtirilgan qutibni yubora olmaydi. Faqatgina 2 bitli axborotni olgachgina buzgunchi qutibni o‘z qutibiga o‘zgartirib Bobga yuborishi mumkin. Kanaldagi qutiblarni kechikishi buzgunchi borligi xaqida shubxa oyg‘otadi va Alisaga u xaqida xabar qilinadi.

14-Amaliy mashg‘ulot.

Mavzu: Kvant kriptografiyasining ishlash prinsipi va uning eksperiment tadqiqoti.

Optik tolali kabellar paydo bo‘lishi natijasida (bir necha Gbit/s), uzatish tezligi B chiziqli traktlarda (ChT), raqamli uzatish traktlarida (RUT) bir vaqtda

qayta tiklash bo‘limlarining uzayishi bilan birga (100 km gacha va undan yuqori) yuqori ko‘rsatkichlarga erishish mumkin bo‘ldi. Optik tolali kabellarda raqamli traktning metall juftli kabellardagi ishchanligi 100 baravardan ko‘proqqa ortiq qaysiki iqtisodiy tomondan xam foydalidir. Ko‘pchilik qayta tiklagichlar oxirgi yoki tranzit stansiyalar bilan birlashtirilishi mumkin. Shuning uchun qayta tiklagichlarni masofadan ta’minlashni osonlashtiradi. Shuning uchun optik tolali kabellar transport tarmoqlarida signallarni tarqatishdagi asosiy muxit xisoblanadi.

Transport tarmoqlari telekommunikatsiya tarmoqlari miqyosi bo‘yicha quyidagicha bo‘linadi.

1. Milliy miqyos-bunday transport tarmoqlari mintaqalar (viloyat)aro aloqani ta’minlaydi, bu tarmoq tugunlari viloyat markazlari va yirik sanoatlashgan shaxarlarda joylashadi.
2. Mintaqaviy miqyos-bunday miqyosdagi transport tarmoqlari bir mintaqa (viloyat)da joylashgan turli tumanlar orasidagi aloqani ta’minlaydi va bu tarmoq tugunlari odatda tuman markazlarida joylashadi.

Milliy va mintaqaviy miqyosdagi transport tarmoqlarida uzatilish xajmining trafigi bo‘yicha farqlanadi, ma’lum miqdorda milliy miqyosda ko‘proqdir. Shunga binoan bunday tarmoqlarni loyixalashtirish va ko‘rishda optik tolali kabellarni to‘g‘ri tanlash zarur shuningdek, shu transport tarmog‘ida uzatilishi zarur bo‘lgan trafik va bir paytda uning iqtisodiy qiymatining oshib ketmasligini ta’minlash zarur.

Transport tarmoqlaridagi kabellarni to‘g‘ri tanlash, shu tarmoqda ishlatiladigan tarmoq qurilmalarining texnologiyasi bilan uzviy bo‘gliqdir. Qaysiki, transport tarmogi raqamli traktni xosil qilishini ta’minlashi kerak.

Transport tarmogining qurilishida turli xil tarmoq texnologiyalari ishlatiladi:

-sinxron raqamli ierarxiya SDH texnologiyasi;
-asinxron turidagi axborot tashish ATM texnologiyasi;
-to‘lqinli multipleksor WDM texnologiyasi.

SDH texnologiyasi uchun asosiy uzatish muxiti bo‘lib G652 MSE-T tavsifnomasiga javob beradigan optik-tolali kabellarning standartlari ishlatiladi. ATM texnologiya xam shu optik tolali kabellarni ishlatish mumkin, lekin odatda ATM, SDH bilan birgalikda ishlatiladi. Optik tolalarda dispersiya kattaliklarini kichraytirish va SDH texnologiyasining qayta tiklanish maydonini uzaytirish uchun surilgan dispersiyali va G653 MSE-T tavsifnomasiga javob bera oladigan optik tolalar ishlab chiqarilgan. Bunday optik-tolalarda dispersiyaning nuqtasi (0) to‘lqin uzunligi 1.3 mkm dan ish uzunligi 1.55 mkm tomon surilgan.

WDM (DWDM) to‘lqinning multipleksorlari texnologiyasining va G652 tavsifnomaga javob beruvchi disperiyasi surilgan (G653) optik tolaning qo‘llanilishi natijasida optik signallarning uzatilishi yomonlashuviga olib keladigan nochiziqli effektlar xosil bo‘ladi. Shunga o‘xshash effektlarni bartaraf etish uchun WDM va DWDM texnologiyalarning ishlatilishida G655

tavsifnomasiga javob bera oladigan dispersiya siljishi (0) ga teng bo‘lgan optik tolali kabellar ishlab chiqarilgan.

Bunday tolaga True Wave optik tolasi misol bo‘la oladi. Xozirgi vaqtda O‘zbekistan Respublikasi transport tarmog‘ining xar xil miqiyosida tarmoq texnologiyasining sinxron raqamli SDH ierarxiyasi ishlatilgan, shu bilan birga G652 tavsifnomasiga mos keluvchi standart optik tolalar qo'llanilgan. Bunday tarmoqlarda raqamli axborotning blok l siklik tuzilishi asosida uzatiladigan STM transport moduli deb ataladi. Transport moduli o‘zining miqyosi bo‘yicha raqamli axborotni uzatish tezligi va tashkil etiladigan kanallari bo‘yicha ajratiladi. Ular 4 bosqichdan iborat (14.1.-jadval).

SDH transport moduli darajasi	Transport moduli	Uzatish tezligi (Mbit/s)	Telefon kanallar soni
SDH birinchi daraja	STM- 1	155.52	1890
SDH ikkinchi daraja	STM-4	622.08	7560
SDH uchinchi daraja	STM- 16	2488.32	30240
SDH to‘rtinchi daraja	STM- 64	9953.28	120960

Ma’lumki, telekomunikatsion transport tarmoqlari global, milliy, mintaqaviy va maxalliylarga bo‘linadi. 14.2,- jadvalda tarnsport modullari va tarnsport tarmoqlarining o‘zaro bog‘liqlig‘i ko‘rsatilgan.

14.2.-jadval

Transport tarmogi	Transport moduli
Global	STM-64, STM- 16
Milliy	STM- 16, STM- 4
Mintaqaviy	STM- 4, STM-1
Maxalliy	STM- 1, STM- 4

Loyixalashtirilayotgan tarmoq bosqich miqiyosiga qarab kerakli kanallar tashkil eta oladisgan transport moduli tanlanadi. Shuning uchun kerakli modullar soni quyidagicha aniqlanadi: $Ish.mod = (N_{ish}k_a)/(N_{tr}mod)$:

Bu erda: $N_{ish}k.$ - ishchi kanallar soni; $N_{tr}mod$ – transport xosil qiladigan kanallar soni.

Transport moduli asosida raqamli axborotni uzatish uchun 2 ta optik tolali tanlash zarur. Shunda kabeldagi kerakli tolalar soni $N_{10}i = Ish_0mod * (2+2_{zax})$ ga teng bo’ladi.

Bu erda Ish_0mod transport modullar soni $2+2_{zax}$ zaxira tola. Kabeldagi ishchi tolalar sonini aniqlab, kabelning markazi va uning turini bilamiz.

Kabelni tanlashda uning etkazilish sharoiti, ya’ni telefon kanalizatsiyasini, er yoki suvdan o‘tish joylari bo‘lishini inobatga olishi zarur.

Nemis kabellari 3 sinfga bo‘linadi.

Birinchi, eng axamiyatlisiga chiziqli optik tolali kabellar kiradi. (Fiber Optic Outdoor Sables). Bu kabellar telefon kanalizatsiyalari, erda va kollektorlarda ishlatilish uchun mo‘ljallangan.

Ikkinchi sinf o‘zida stansiya optik tolali kabellarini aks ettirgan (Fiber Optic Outdoor Sables). Bu kabellar faqat bino inshoatlari ichida ishlatilishiga mo‘ljallangan.

Uchinchi sinfga faqat maxsus ishlatilishi uchun muljallangan kabellar kiradi. Bular osiladigan (Fiber Optic Outdoor Cables) va suv ostida ishlatiladigan (Fiber Optic Outdoor Cables) kabellar, shunga binoan tayanchlarga osiladi yoki dariyo, suv xavzalari tagidan o‘tkaziladi. Keltirilgan sinfdagi kabellar tuzilishi, modullar soni, tola soni, toplami soni, ishlatilgan maxsuloti bilan farqlanadi. Aniq turni tanlash kabel ishlatiladigan bir necha omilga bo‘g‘liq bular qaysi tarmoqda ishlatilishi, kanallar soni, uzatish parametrlari, etkizilish sharoitlari, tashqi ta’sir, kabel qiymati va xokazolardir.

Optik kabellar markirovkasini ko‘rib chiqaylik. Kabelning markasi deb shartli belgilashlarga aytiladi. Bularga xarflar guruxi va raqamlar kiradi. Ularning ma’lum tartibda yozilishi kabelning tuzilishi va uni ishlatilish sharoitini ko‘rsatadi. Germaniya kabel sanoatida VDE (Verband Deutscher Elecktrotechniker-Association of German Electrical Engineers) Germaniya elektro muxandislar tashkiloti tomonidan standart marka-belgilashlar ishlab chiqilgan. Optik-tolali kabellar uchun xarfli va raqamli belgilashlar ishlatiladi.

Shaxarlararo moderlar optik tolali aloqa liniyalarining o‘rtasida etkazilish uchun ishlatiladi. Aholi yashash joylarida bu kabellar mavjud bo‘lgan telefon kanalizatsiyalari va metro kollektorlari, undan tashqqarida er, ya’ni tuproq orqali o‘tkaziladi.

Shaxarlararo optik-tolali aloqa liniyalarida telefon kanalizatsiyalari va erda yotqizish uchun quyidagi kabel turlari ishlatiladi. A- DF (ZN) 2Y (SR) 2Y. A-DF (ZN) 2Y (SR) 2Y 3x6E9/125 0.36F3.5+0.22N18 LG turdagi kabel tuzilishi keltirilgan. Kabelning markaziy kuch elementi shishaplastikdan yasalgan bir modli tolalar turi E9/125 termobardosh ftoroplast naylarda joylashtirilib, modul deb yuritiladi. Kabel o‘zagida qavatli mustaxkamlashtirilgan qog‘oz va sanoat tolasi yotqizilgan. Kabelning ichki qoplami polietilendan, qalaydan qilingan qoplama ostida mustaxkamlashgan qogozdan yostiqcha joylashgan. Polat qoplama tashqari qobiq polietilen shlang bilan qoplangan kabel to‘ldirg‘ichlar bilan germitizatsiyalangan.

ADSL (Asymetric Digitel Subecriber Line) abbreviaturasi-asimmetrik raqamli abonentlik liniyasi deb kengaytirib izoxlanadi. Nomining o‘zi texnologiyaga avvaldan joylashtirilgan abonentga va teskari yonalishlarda tezliklar almashinuvi turlarini ko‘rsatadi. Ma’lumotlar uzatish tezligi foydalanilayotgan jixoz, telefon liniyasi uzunligi va sifatiga bo‘g‘liq.

Ma’lumotlar uzatishning asimmetrik xususiyati maxsus amalga oshirilgan, bunda Internetdan tipik foydalanuvchi sifatida ma’lumotlarni o‘z kompyuteriga joylashtiradi, boshqaruv buyruqlari va foydalaniladigan ma’lumotlarning uncha

katta bo‘lmagan oqimi (elektron pochta, saxifalarning yangilanishi va boshqalar) teskari yo‘nalishda boradi.

O‘z sifatiga ko‘ra ADSL-texnologiyasi qimmatbaxo tolali-optik tarmoqlarning alternativ qurilmasi xisoblanadi. Tarmoqdan foydalanuvchi uchun ADSL dan foydalanish quyidagilari bilan diqqat talab etadi:

- kechayu-kunduz Internetga ulanish mumkin, bunda qo‘ng‘iroq qilish shart emas, sababi ulanish doimiydir;
- internet-aloqa turgun va u telefon liniyasi xususiyatlarining o‘zgarishiga bogliq bo‘lmaydi, bu esa aloqa uzilishisiz juda katta xajmdagi ma’lumotlar olish imkoniny beradi.

Ma’lumotlar uchun: ADSL-abonentlik ulanishining eng zamonaviy texnologiyalaridan biri bo‘lib, bir vaqtning o‘zida oddiy telefon liniyasi orqali xam ovoz, xam ma’lumotlarni uzata oladi. Boshqacha qilib aytganda, Internet ishlayotgan vaqtda telefon liniyasi oddiy qo‘ngiroqlar uchun erkin bo‘lib qolaveradi va aloqa sifati xam o‘zgarmaydi. Nazariy jixatdan ADSL-servis tarmoqdagi abonentga ma’lumotlar uzatish tezligi 8 Mbit/s dan, teskari yo‘nalishda 1.5Mbit/s ga teng bo‘ladi.

15-Amaliy mashgulot.

Mavzu: Berilgan ma'lumotlarni autentifikatsiyalash muammosi.

RSA asosidagi ERI algoritmi Butun dunyo miqyosida birinchi va juda mashhur elektron imzo algoritmi bu RSA sistemasiga asoslangan ERI bo'lib hisoblanadi. Uning matematik sxemasi 1977 yilda AQShning Massachusset texnologiya instetutida ishlab chiqilgan. Bu sistema quyidagicha amalga oshiriladi.

Dastlab sirli va ochiq kalitlarni hisoblab chiqish lozim. Uning uchun elektron hujjat muallifi ikkita katta P va Q tub sonlarini saylaydi, so'ngra ularning ko'paytmasini hisoblaydi.

$$<PW = (P -!)(<?-!) \quad (1.1.)$$

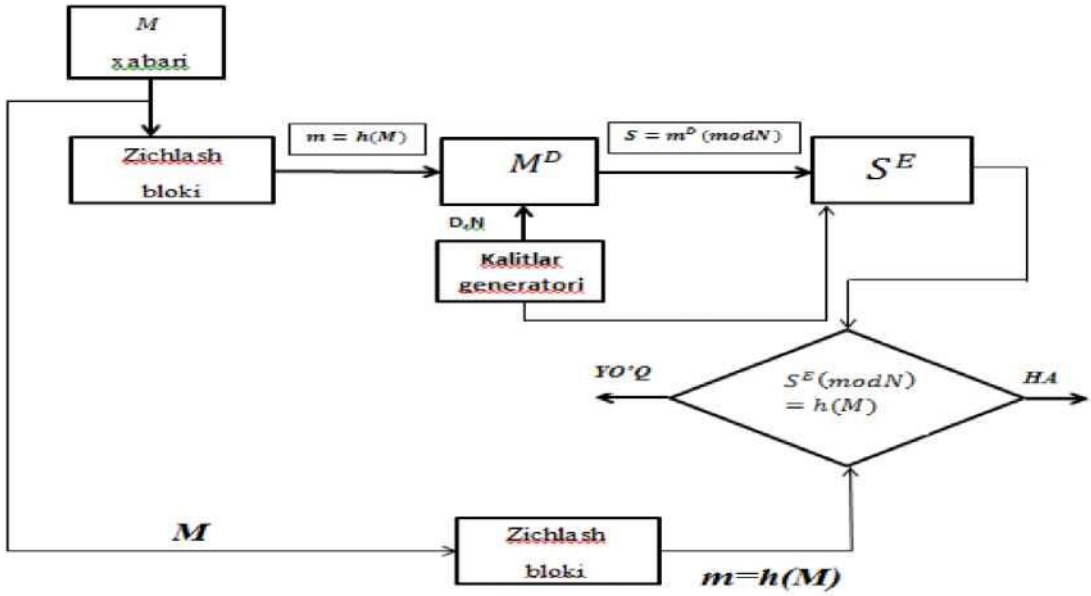
(1.1) va undan so'ng Eyler funksiyasi hisoblanadi. Keyinchalik hujjatni yuboruvchi abonent E sonini

$$E \leq \varphi(N), \quad EKUB\ (E,\varphi(N))=1 \quad (1.2.)$$

saylab olinadi. So'ngra D soni,

$$D < N,\ E * D = lmodQpQNy)$$

Shartlari qanoatlantiradiganday qilib saylab olinadi. Bunda, (E,N) juftligi ochiq kalitlar bo'lib topiladi. Bu sonlar elektron imzoni tekshirish uchun qo'llaniladi. *D* soni imzolash uchun muallif tomonidan maxfiy kalit sifatida saqlanadi. RSA asosidagi ERIni tekshirishning umumlashgan sxemasi 2- rasmda keltririlgan.



2 - rasm

RSA elektron imzo algoritmining umumlashtirilgan sxemasi

Mayli, xabar yuboruvchi shaxs *M* xabarini yubormay turib, xabarni imzolamoqchi bo'lsin. U dastlab *M* xabarni *h* xesh - funksiya yordamida *m* butun soniga zichlaydi.

$$m = h(M)$$

Shundan elektron imzosini,

$$S = m^D(\text{mod}N') \qquad (3.3)$$

formulasi yordamida hisoblaydi va *(M,S)* juftligi *S* elektron imzosi bilan imzolangan M elektron hujjati sifatida adreslovchiga yuboriladi. *(M,S)* juftligi qabul qilingandan so'ng M xabarning xesh - qiymati ikki usul yordamida hisoblanadi. Dastlab *E* ochiq kalitidan foydalanib *S* imzosiga kriptografik o'zgartirishlar qo'llab, *m'* xesh - qiymatini qayta tiklaydi.

$$m'=S^E(\text{mod}N) \qquad (3.4)$$

Bundan tashqari, *h* xesh - funksiyasi yordamida olingan *M* xabarning xeshlash natijasini oladi.

$$m = /i(M)$$

Agarda hisoblangan qiymatlar teng bo'lsa, ya'ni

$$S^E(\text{mod } N) = h(M) \qquad (3.5)$$

U holda hujjatni qabul qiluvchi (M,S) juftligining rost ekanligini tan oladi.

Bu yerda faqat D sirli kalitga ega shaxsgina M hujjatga S imzosini qo'yishi mumkin. D sirli kalitini E orqali aniqlashda N moduli bo'yicha ko'paytuvchilarga ajratish oson bo'lmagan masala bo'lib topiladi. E kaliti odatda imzolovchining "identifikatori" deb ham ataladi.

EL-GAMAL elektron raqamli imzo (ERI) algoritmi (EGSA)

Ilm fan rivojlanishi , axborot kommunikatsiya texnologiya(AKT)larining qollanilishi kriptografiya sohasiga katta hissa qo'shdi. 1984-yili Amerikalik olim Taxer El-Gamal, shaxsiy kompyuterlarda imzoni ishonchli va turg'un holda foydalanish uchun, «EL-GAMAL» ERI algoritmini ishlab chiqdi.

Bu algoritm, boshqa algoritmlardan farq qilgan holda kriptomustahkamligi yuqori deb topidi va 1991 - yili «EL-GAMAL» algoritmi AQShning milliy standarti sifatida qabul qilindi. «EL-GAMAL» ERI algoritmi asosini, butun sonlarni tub ko'paytuvchilarga ajratishdan ham murakkab bo'lgan diskret logarifmlash masalasini hisoblashni tashkil qiladi. Bu esa RSA elektron raqamli imzo algoritmining ba'zi bir kamchiliklarini tuzatadi. «EL-GAMAL» ERI algoritmiga ko'ra, juft kalitlarni generatsiyalash uchun ba'zi bir katta tub *P va Q(Q<P)* sonlarini saylab olamiz. Imzolangan hujjatni, yuboruvchi va qabul qiluvchi abonentlar bir hil qiymatdagi butun katta sonlardan,

$$P\ (\approx 10^{308}\ yoki\ 2^{1024}),\quad Q(\approx 10^{154}\ yoki\ 2^{512})$$

oraliqdagi sonlarni foydalanadi.

Hujjatni yuboruvchi abonent tasodifiy x- x - (p 1)) sonini saylab oladi va

$$Y — Q^{x} modP$$

Ifodasini hisoblaydi. Bunda, Y soni xabar yuboruvchi abonentning imzosini tekshirish uchun foydalaniladigan ochiq kalit hisoblanadi. Y soni hujjatni oluvchi abonentlarga ochiq kanallar orqali yuboriladi. Bunda, X soni hujjatlarni imzolash uchun sirli kalit bo'lib, u boshqa yovuz niyatli abonentlardan sir saqlanishi lozim. Endi, hujjatlani imzolash jarayonini ko'rib chiqamiz. Berilgan M hujjatni imzolash uchun dastlab uni H xesh - funksiyasi yordamida m butun soniga xeshlaydi,

$$m = H(M),\ (1 < m < (P - 1))$$

bunda, K va P -1 o'zaro tub sonlar. So'ngra xabar yuboruvchi abonent a butun sonni quyidagicha hisoblaydi.

$$a=QkmodP \quad (3.2)$$

va Evklidning kengaytirilgan algoritmidan foydalanib X maxfiy kaliti yordamida b butun sonni hisoblab topadi:

$$m = X*a + K + b(mod(P — 1)) \quad (3.3.)$$

(a,b) juftligi M hujjatga qo'yiladigan S elektron raqamli imzosini hosil qiladi.(M,a,b) sonlar uchligi adresatga yuboriladi, (X,K) juftligi esa maxfiy saqlanadi. Imzolangan hujjat qabul qilinganda so'ng S(a,b) imzosining M xabariga mosligi tekshiriladi. Moslikni tekshirish uchun qabul qilingan M xabari bo'yicha m=h(M) ni hisoblaydi, ya'ni M xabarini xeshlaydi.

$$A = Yaab(modP) \quad (3.4.)$$

ifodasining qiymati hisoblanadi. Agarda, faqat A ~ Q (m<->dP) ifodasi mavjud bo'lsa, u holda elektron raqamli imzo haqiyqiy deb topiladi, aks holda quyidagi munosabat tekshiriladi, agar tenglik bajarilmasa imzo qalbaki degan hulosaga kelinadi. Eng so'nggi tengligi

$$Yaab(modP)=Qm(modP) \quad (3.5.)$$

(3.5) faqatgina quyidagicha holatda bajariladi.

Agarda hujjatdagi S(a,b) imzosi Y ochiq kaliti va X maxfiy kaliti yordamida olingan bo'lsa. EL-GAMAL algoritmi bilan imzolangan har bir habar hujjat tasosifiy K qiymatini yangidan saylab olishni talab qiladi. Agarda K qiymati

takroran qo'llanilsa, unda unda yovuz niyatli abonent X maxfiy kalitini topishi mumkin. EL-GAMAL algoritmining amaliyotga qo'llanilishi quyidagicha misol tariqasida ko'ramiz.

Misol: Mayli, p = n. q = 2 va X = 8 sonlari berilgan bo'lsin. Bundan quyidagicha ifodani hisoblaymiz:

Y = QxmodP = 28modll = 3

Shunday M xabari m=5 xesh-qiymati bilan harakterlanadigan, dastlabki tasodifiy K soni tanlab olinadi. Dastlab, K va (P-1) sonlarining o'zaro tub ekanligini tekshirib ko'ramiz.

Haqiqatan,

E KU B (9,10) = 1

eng katta bo'luvchisi 1 ga tengligidan bu sonlar o'zaro tub.

So'ngra imzoning a va b elementlarini hisoblaymiz:

A= QKmodP - 2gmodll-6

b elementini esa Evklidning kengaytirilgan algoritmidan foydalanib aniqlaymiz,

m = X * a + K * b(mod(P- 1))

bunda, '*! 5* c’■ 6, X 8, K 9, P 11 bo'lganligidan

5 = (6 *7 + 9* b)modlO

yoki

9 * b - - 43modl0

hisoblagan holda, b=3 natijaga ega bo'lamiz.

Endi, imzolangan xabar yuboriladi. Xabarni qabul qiluvchi abonent, bu habarni va Y=3 ochiq kalitni olib, M xabari uchun xesh - qiymatni hisoblaydi: Natijada, m=5 topiladi.

So'ngra,

1. Yaab(modP') - 3663(modll) - lOmodll
2. Qm(modP) = 25(modll) = lOmodll

hisoblash natijalari solishtiriladi. Bizning hisoblashlarinmizda (3.5) tengliklari tekshiriladi, tenglik teng sonlarga ega bo'lganligi sababli, imzo haqiyqiy deb topildi. Aks holda bajarilmasa, imzo qalbaki bo'ladi.

Endi, EL-GAMAL ERI algoritmini RSA ERI algoritmi bilan solishtirgandagi imkoniyatlarini ko'rib o'tamiz.

Elektron raqamli imzo algoritmining berilgan turg'unlik shartini qanoatlantirishida hisoblashlarda qatnashadiganbutun sonlar 25% ga qisqa. Bu bizga hisoblashlardagi qiyinchiliklarni ikki karra qisqartirishga va foydalanilayotgan hotira hajmini sezilarli darajada kamaytirishga imkoniyat beradi.

P modulini saylab olganda, uning tub ekanligi va (P-1) sonining katta tub ko'paytuvchisi mavjudligini tekshirish zarurli va yetarli.

EL-GAMAL ERI sistemasi bo'yicha, RSA sistemasi kabi maxfiy kalitni bilmay turib hisoblash mumkin emas.

Lekin, EL-GAMAL sxemasining RSA ERI sxemasiga solishtirganda ba'zi kamchiliklarga ega. Kamchilik mazmuniga ko'ra, ERI uzunligi 1,5 karra katta, bu o'z navbatida ERIni hisoblash vaqtini sezilarli darajada ortiradi.

MUSTAQIL ISH TOPSHIRIQLARI.

1-mavzu: Axborot xavfsizligiga taxdidlar**.**

Topshiriqlar:

1. Axborot xavfsizligida bo‘ladigan tahdidlar qanday bo‘lishini ifodalang.
2. Tabiiy va sun’iy tahdidlarni ifodalab bering.
3. Bilmasdan va atayin qilinadigan tahdidlarni tushuntirib bering.

Foydalanilgan adabiyo‘tlar:

1. S.K.Ganiyev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil.
2. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. - Санкт-Петербург,2009.
3. Романец Ю.Б.,Тимофеев П.А.Защита информации в компьютерных системах и сетях. Санкт-Петербург, 2006.

2-mavzu: Axborotning mahfiyligi, yaxlitligini va foydalanuvchanligini buzish usullari.

Topshiriqlar:

1. Tarmoq trafidini tahlillashda asoslangan buzish usullarini tushuntirib bering.
2. Tarmoqning yolg‘on obektini kiritishga asoslangan buzush usulini ishlash prinsipini izohlang.
3. Yo‘lgon marshrutni kiritish qanday amalga oshiriladi.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.
2. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. Санкт-Петербург,2009.
3.Романец Ю.Б.,Тимофеев П.А. Защита информации в компьютерных системах и сетях. Санкт-Петербург, 2006.

3-mavzu: Axborot xavfsizligi soxasiga oid xalqaro standartlar.

Topshiriqlar:

1. Axborot xavfsizligi soxasida standartlar va me’yoriy hujjatlarning tutgan o‘rni.
2. ISO/IEC 27001:2005 xalqaro standartning mohiyatini tushuntirib bering.
3. O‘z DSt ISO/IEC 15408:2008 xalqaro standartt nechta qiqismdan iborat va ularda yoritilgan masalalar nimadan iborat.

Foydalanilgan adabiyo‘tlar:

Баричев С. Основы современной криптографии. Учебний курс. Горячая линия Телеком 2002 г.
Ganiyev C.K., Karimov M.M., Tashev K.A., Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.

4-mavzu: Shifirlash, maxfiy va ochiq kalitlar.

Topshiriqlar:

1. Simmetrik shifrlash tizimlarining ishlash sxemasini tushuntirib bering.
2. AQShning axborotni shifrlash standarti DES algoritmini izoxlab bering.

Foydalanilgan adabiyo‘tlar:

1. S.K. Ganiyev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil.
2. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. Санкт-Петербург, 2009.

5-mavzu: Asimmetrik shifirlash tizimlari.

Topshiriqlar:

1. Asimmetrk shifirlash tizimlarini ishlash prinsipini tushuntiring.
2. RSA asimmetrik algoritmik algoritmining shifirlash qadamlarini yoritib bering.

Foydalanilgan adabiyo‘tlar:

1. S.K. Ganiyev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil.
2. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. - Санкт-Петербург, 2009.

6-mavzu: Xeshlash funksiyalari.

Topshiriqlar:

1. Xeshlash funksiyaning ishlash sxemasini tushuntirib bering.
2. GOST R 34.11 Rossiyaning xeshlash algoritmini aytib bering.

Foydalanilgan adabiyo‘tlar:

1. S.K.Ganiyev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil.
2. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. Санкт-Петербург, 2009.

7-mavzu: Elektron raqamli imzo.

Topshiriqlar:

1. Elektron raqamli imzoni shakillantirish sxemasini tavsiflab bering.
2. Elektron raqamli imzoni tekshirish jarayoning sxemasini tushuntirib bering.

Foydalanilgan adabiyo‘tlar:

3. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik.Fan va texnologiya T.: 2017.

8-mavzu: Stegonografiya usullari.

Topshiriqlar:

1. Stegonografiyaning axborotni kriptografik himoyalash sohadagi o‘rnini izoxlang.
2. Moddiy stenografik usullarni tushuntirib bering.

3. Axborot stenografik usullarining turlarini tavsiflab bering.

Foydalanilgan adabiyo‘tlar:

1. S.K. Ganiyev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil.

9-mavzu: Kriptotaxlil usullari.

Topshiriqlar:

1. Kriptotaxlil usullari tushunchasi va usullarini tushuntirib bering.
2. Taxlillash murakkabligini qanday koeffitsientlar yordamida o‘lchash mumkin.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.

2. Арипов М., Пудовченко Ю. «Основы криптологии» Ташкент, УзМУ 2004 г.

10-mavzu: Identifikasiya va autentifikatsiya tushunchasi.

Topshiriqlar:

1. Identifikasiya va autentifikatsiya tushunchasi.
2. Autentifikatsiya texnologiyasining turlarini tushuntirib bering.
3. Autentifikasiya protokollariga bo‘ladigan hujumlarni tavsiflab bering.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.

2. Арипов М., Пудовченко Ю. «Основы криптологии» Ташкент, УзМУ 2004 г.

11-mavzu: Parollar asosida audentifikatsiya.

Topshiriqlar:

1. Ko‘p martali parollarga asoslangan audentifikatsiya texnologiyasi.
2. Bir martali parollarga asoslangan audentifikatsiya texnologiyasi.

Foydalanilgan adabiyo‘tlar:

1. Олифер В.Г., Олифер Н.А., Компьютерные сети. Принципы, технологии протоколы 4-изд. Питер, 2010,

2. P.Y.A. Ryan, S.A. Schneider, M.H. Goldsmith, G. Lowe and A.W. Roscoe. The Modelling and Analysis of Security Protocols: the CSP Approach. The original version is in print December 2010 with Pearson Education.

12-mavzu: Kompyuter viruslari va virusdan himoyalanish muommalari.

Topshiriqlar:

1. Komputer virusi va zarar keltiruvchi dasturlar tushunchasi.
2. Komputer firusini bajarish davri qanday bosqichlarni o‘z ichiga oladi.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik.Fan

va texnologiya T.: 2017.

13-mavzu: Virusga qarshi himoya tizzimini qurish.

Topshiriqlar:

1. Virusga qarshi himoyaga ega korporativ tarmoqning namunaviy arxitekturasini tariflab bering.
2. Virus va zarar keltiruvchi dasturlardan himoyalovchi korporativ tizimni qurushda bajariladigan virusga qarshi siyosatni ishlab chiqish afzalliklarini tushuntiring.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik.Fan va texnologiya T.: 2017.

14-mavzu: Tarmoqlataro ekranlarning ishlash xususiyatlari.

Topshiriqlar:

1. Tarmoqlararo ekran vositalari tushunchasi va uning vazifalarini izoxlang.
2. Tarmoqlararo ekranning OSI modeli sathlari bo‘yicha turkumlanishi.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.
2. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. O‘quv qo‘llanma - T.: TDIU, 2005.

15-mavzu: Tarmoqlararo ekranlarning asosiy komponentlari.

Topshiriqlar:

1. Ekranlovchi marshrutizatorlarning ishlash prinsipini tushuntirib bering.
2. Ekranlovchi marshrutizatorlar, seans sathi shluzi va tatbiqiy sath shuluzi qo‘llaniladigan funkssiyalarning bir-biridan farqi nimada.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.
2. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. O‘quv qo‘llanma - T.: TDIU, 2005.

16-mavzu: Operatsssiyon tizim xavfsizligini ta’minlash muammolari.

Topshiriqlar:

1. Himoyalangan operatsiyon tizim tushunchasini ta’riflang.
2. Himoyalangan operatsiyon tizimni yaratishdagi yondashishlarni tushuntirib

bering.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.
2. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. O‘quv qo‘llanma - T.: TDIU, 2005.

17-mavzu: Axbototlarni himoyalashda dasturiy ilovalarning qo‘llanilishi.

Topshiriqlar:

1. Axborotlarni himoyalashda qo‘llaniladigan dasturiy vositalarning shartli ravsda qanday guruxlarga ajratish mumkinligini tushuntiring.
2. Axborotlarni kriptografik himoyalashning dasturiy vositalarini ishlash prinsipini tushuntiring bering.
3. Tarmoqni himoyalashning dasturiy vositalarini tavsiflab bering.

Foydalanilgan adabiyo‘tlar:

1. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya T.: 2017.
2. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. O‘quv qo‘llanma - T.: TDIU, 2005.

18-mavzu: Axborot sirqib chiqarilgan texnik kanallar va ularning turkumlanishi.

Topshiriqlar:

1. Axborot siqib chiqaradigan texnik kanallar tushunchasini ta’riflang.
2. Axborot siqib chiqaradigan texnik kanal stukturasini tushuntirib bering.

Foydalanilgan adabiyo‘tlar:

1. Шнайер Брюс. Прикладная криптография. Протоколи, алгоритми, исходние тексти на язике Си. –М.: Издательство Триумф – 2008г.
2. Баричев С. Основи современной криптографии. Учебний курс. Горячая линия Телеком 2002 г.
3. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik.Fan va texnologiya Toshkent.: 2017.

19-mavzu: Ob’yektlarni injener himoyalash va texnik qo‘iqlash.

Topshiriqlar:

1. Axborot manbalarini fizik himoyalash tizimi tushunchasini tushuntirib bering.
2. Obektlarni injener himoyalash va texnik qo‘riqlash tizimi tarkibini ta’riflang.

Foydalanilgan adabiyo‘tlar:

1. Шнайер Брюс. Прикладная криптография. Протоколи, алгоритми, исходние тексти на язике Си. –М.: Издательство Триумф – 2008г.

2. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya Toshkent.: 2017.

20-mavzu: Axborot sirqib chiqarilgan texnik kanallarni aniqlash usullari va vositalari.

Topshiriqlar:

1. Elektromagnit nurlanish indikatorining ishlash sxemasini tushunchasini ta’riflang.

2. Radiyo chastotomerlarning ishlash rejimlarini tushuntirib bering.

Foydalanilgan adabiyo‘tlar:

1. Мельников Д.А. Информационная безопасстность открытых систем: учебник-М:. Флинта: Наука, 2013.

2. Баричев С. Основи современной криптографии. Учебний курс. Горячая линия Телеком 2002 г.

3. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. Fan va texnologiya Toshkent.: 2017.

FOYDALANILGAN ADABIYOTLAR:

1. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд.4-е М: Ленанд, 2015.
2. Richard E.Smith. Elementary Information Security. Jones &Barlett Learning. USA, 2015.
3. Шаньгин В.Ф. информационная безопасность.-М:. ДМК Пресс. 2014.
4. Платонов В.В. программно-аппаратные средства защиты информации: учебник для студ. учреждений выс. Образования-М: Издательский центр ”Академия”, 2014.
5. Мельников Д.А. Информационная безопасстность открытых систем: учебник-М:.Флинта: Наука, 2013.
6.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии протоколы 4-изд.- Питер,2010,
7. P.Y.A. Ryan, S.A. Schneider, M.H. Goldsmith, G. Lowe and A.W. Roscoe. The Modelling and Analysis of Security Protocols: the CSP Approach. The original version is in print December 2010 with Pearson Education.
8. Шнайер Брюс. Прикладная криптография. Протоколи, алгоритми, исходние тексти на язике Си. –М.: Издательство Триумф – **2008г.**
9. Баричев С. Основи современной криптографии. Учебний курс. Горячая линия Телеком 2002 г.
10. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik.Fan va texnologiya Toshkent.: 2017.372 b.
11. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. - Санкт-Петербург,2009.
12. Романец Ю.Б.,Тимофеев П.А. Защита информации в компьютерных системах и сетях. - Санкт-Петербург,2006.
13. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. O‘quv qo‘llanma - T.: TDIU, 2005.
14. Ganiyev C.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi.Aborot-kommunikasiyon tizimlar xafvsizligi. O‘quv qo‘llanma T.:”Aloqachi”, 2008.
15. Арипов М., Пудовченко Ю. «Основы криптологии» Ташкент, УзМУ 2004 г.
16. Хорошко В.А., Чекатков А.А. Методи средства защити информации. Учебное пособие. - К.: Издательство Юниор, 2006.
17. несанкционированного доступа. - СПб.: Наука и техника, 2004.
18. www.ziyonet.uz - Axborot ta’lim portali
19. www.edu.uz —Oliy va o‘rta maxsus ta’lim vazirligi portali
20. www.nasa.gov\statistics\
21. www.security.uz
22. www.cert.uz

GLOSSARIY

LMS (LearningManagementSystem)-Virtual ta’lim jarayonini boshqaruvchi tizim.

CMS (ContentManagementSystems)-Ichki kontentni boshqaruv tizimlari Brauzer-internet bilan ishlashni ta’minlaydigan dastur.

IP (Internetprotocol) manzili- kompyuterning internet tarmog‘idagi manzili.

On-line mashg‘ulot–barcha qatnashuvchi (talabalar va o‘qituvchi)lar internet orqali axborotalmashinish yo`li bilan o`zaro aloqaqiladigan o`quv mashg‘uloti ko‘rinishi.

On-line muhokama-elektron doskalarda biror mavzuni ayni vaqtdagi muhokamasi.

On-line o‘qish-internet texnologiyalariga asoslangan ta’lim muhitidan foydalanib o‘quv materiallarini o‘rganish jarayonini tashkil etish usuli.

Administrator-elektron axborot-ta’lim resurslarini moslashtirish va boshqarish uchun keng huquqlarga ega bo‘lgan mutaxassis.

Animatsiya-dinamik va ovozli jarayonlarni ifodalashga imkoniyat beradigan grafik axborotlarni tashkil etish usuli.

Audioanjuman-tarmoq texnologiyasi tizimi va telefondan foydalangan xolda turli geografik nuqtalarda joylashgan bir qancha shaxslarning ma’lumotlarni ovozli-raqamli ko‘rinishda almashinish jarayoni.

Axborot-(lat.Informatio-tushuntirish, bayon qilish)-shartli belgilar yordamida shaxslar, predmetlar, dalillar, voqealar, hodisalar va jarayonlar haqida, ularni tasvirlash shaklidan qat’iy nazar uzatiladigan va saqlanadigan ma’lumotlar.

Videoanjuman-turli geografik manzillardagi foydalanuvchi guruhlari orasida raqamli videoyozuv yoki oqimli video ko‘rinishida ma’lumotlarni almashinish asosida yigilish va munozaralar o‘tkazish jarayoni.

Virtual laboratoriya–o‘rganilayotgan haqiqiy ob’ektlarda bo‘layotgan jarayonlarni kompyuter imitatsiyasi orqali taqdim etish va masofaviy kirish imkoniyatiga ega bo‘lgan dasturiy majmua.

Virtual auditoriya-o‘quv jarayonining o‘qituvchisi va boshqaruvchisining maslahatini olish uchun tarmoq texnologiyasi yordamida turli geografik joylarda yashayotgan talabalarni birlashtirish.

Virtual haqiqiylik-o‘rganishga mo‘ljallangan murakkab jarayonlarda bo‘ladigan hodisalarni audiovideo tizimi orqali o‘quvchi tassavuridagi mavhum ko‘rinishi.

Gipermatnli tizim-elektron hujjatlar kutubxonasini yaratishni ta’minlaydigan vosita.

Gipermedia-matndan tashqari multimedia imkoniyatlarini ham o‘zida mujassamlashtirgan ma’lumotlarga yo‘l ko‘rsatuvchi xujjatlar.

Gipermurojaat-tagiga chizilgan yoki qandaydir boshqa usulda ajratib ko‘rsatilgan so‘z yoki jumla bo‘lib, gipermatnli tizimning boshqa blok xujjat, gipermuhit sahifasi, gipermatnini ko‘rsatish imkoniyatini beradi.

Gipermuhit-bir-biri bilan assotsiativ bog‘langan nisbatan katta bo‘lmagan bloklar ko‘rinishidagi axborotning ixtiyoriy ko‘rinishini taqdim etgan texnologiya.

Global tarmoq-mintaqaviy (qit’alardagi) kompyuterlarni o‘zida birlashtirish imkoniga ega bo‘lgan tarmoq.

Grafik muharrir-tasvirlarni tahrirqilishni ta’minlaydigan amaliy dastur.

Didaktik vositalar-o‘quv fanini o‘zlashtirish samaradorligini oshiruvchi pedagogik vositalar.

Didaktik material-foydalanilganda o‘quvchilarning bilim olishini faollashtirish, o‘quv vaqtini iqtisod qilishni ta’minlaydigan o‘quv mashg‘uloti uchun mo‘ljallangan qo‘llanmalarning maxsus ko‘rinishi.

Didaktik tamoyillar-natijaviylikni ta’minlaydigan ta’lim jarayoniga qo‘yilgan eng umumiy talablar tizimi.

Dizayn-o‘quv materialni ifodalash (tavsiflash, namoyish) usuli.

Differensiallashgan ta’lim-o‘quvchilarning moyilligi qiziqishi va qobiliyatini hisobga olgan holda o‘quv faoliyatni tashkil etish shakli.

Jarayon-qo‘yilgan maqsadga erishish uchun yo‘naltirilgan amallar yig‘indisi. Individual (yakkama-yakka tartibda) masofaviy o‘qitish-telekommunikatsiya va ta’limni ta’minlash uchun zarur dasturiy vositalariga ega bo‘lgan masofaviy o‘qitish.

Interaktiv o‘zaro aloqa-elektron pochta, e’lonlar elektron doskasi, onlayn mavzuli muhokamalar, chat, audioanjuman, videoanjuman, ma’lumotlar va fayllar bilan almashinish, umumiy tarmoq ilovasi va boshqalarni o‘z ichiga olgan kompyuter bilan o‘zaro aloqaqilish, «inson-mashina» muloqoti.

Interaktiv o‘quv kurslari-o‘zaro muloqot asosiga qurilgan vositalardan foydalanib tuzilgan kurslar.

Internet-yagona standart asosida faoliyat ko‘rsatuvchi jahon global kompyuter tarmog‘i.

Internet orqali o‘qitish-o‘quv-axborot manbalari va internet kompyuter tarmog‘i orqali o‘zaro bir-birlari bilan bog‘langan real vaqtdagi o‘qitish.

Internetga ulanish-internet kanallari orqali axborot resurslaridan foydalanish (ochish, qurib chiqish, nusxalash, uzatish va boshqalar) imkoniyatiga ega bo‘lgan kompyuterning ishlash tartibi.

Internet darslik-ma’lum fan bo‘yicha yagona interfeys bilan ta’minlangan, internetga joylashtirilgan, doimiy ravishda rivojlanadigan o‘quv-metodik majmua.

Internetning axborotli qismi-internet tarmog‘ida mavjud bo‘lgan turli elektron xujjat, grafiq rasm, audio, video va boshqa ko‘rinishidagi axborotlar majmui.

Internetning dasturiy ta’minoti-tarmoqqa ulangan kompyuterlar va tarmoq vositalarini yagona standart asosida ishlashi, aloqa kanallari yordamida ma’lumotlarni qidirish, qayta ishlash, saqlash hamda tarmoqda axborot xavfsizligini ta’minlash bilan bog‘liq vazifalarini amalga oshiruvchi dasturlar majmui.

Internetning texnik ta’minoti-turli rusumdagi kompyuterlar, aloqa kanallari, tarmoq texnik vositalari majmui.

Intranet-internetning ko‘pgina funksional imkoniyatlariga ega bo‘lgan tashkilot yoki ta’lim muassasasining ichki tarmog`i. Intranetga ulangan bo‘lishi ham mumkin.

Kompyuter darslik-o‘quv fani yoki uning bulimini mustaqil o‘zlashtirish imkoniyatini ta’minlaydigan dasturiy-metodik majmua. Kompyuter darsligi o‘zida oddiy darslik ma’lumotnoma, masalalar va misollar to‘plami, laboratoriya amaliyotlarining xususiyatlarini birlashtiradi.

Kontent-kursning barcha o‘quv materiallari, qo‘llanmalari, xujjatlari, vazifalari, testlar va nazorat meteriallarini qamrab oluvchi kurs mazmuni.

Kurs yakunida o‘tkaziladigan test-bilimlarni o‘zlashtirganlik darajasini baholash maqsadida kurs o‘rganilib bo‘lgandan keyin o‘tkaziladigan test sinovi.

Kursni individuallashtirish-har bir talabaning individual xususiyatlarini xisobga olgan holda o‘quv materiallarini tayyorlash jarayoni.

Kursni o‘rganish yo‘li (traektoriyasi)-kursning o‘quvchini tayyorgarlik darajasiga bog‘liq ravishda aniqlanadigan va o‘quv jarayoniga tadbiq qilinadigan modullari tuzilishi va tartibi.

Masofaviy ta’lim (MT)-ta’limni masofaviy o‘qish usul va vositalari orqali tashkil qilish shakli.

Masofaviy ta’lim markazi-ta’lim jarayonining boshqaruv, o‘quv-metodik axborot va texnik ta’minotini amalga oshiradigan alohida bo‘lim yoki vakolatxona.

Masofaviy ta’lim muassasasi-masofaviy texnologiyalar asosida o‘quv jarayonini amalga oshiradigan ta’lim muassasasi.

Masofaviy ta’lim tizimi (MTT)-masofaviy texnologiyalarni qo‘llab masofaviy ta’limni tashkil etish va amalga oshirishga jalb qilingan o‘quv-tarbiyaviy, tashkiliy, telekommunikatsiya, pedagogik va ilmiy manbalar majmuasi.

Masofaviy o‘qitish-axborot kommunikatsiya texnologiyasi (kompyuterlar, telekommunikatsiyalar, multimedia vositalari)ga asoslangan, tegishli me’yoriy xujjatlar asosida tashkillashtirilgan ta’lim shakli.

Masofaviy o‘qitishning axborot-ta’lim muhiti-ma’lumot, axborot resurslari, o‘zaro aloqa bayonnomalari, dasturiy va tashkiliy-metodik ta’minotlarni uzatish majmui bo‘lib, foydalanuvchilarni ta’lim extiyojlarini qanoatlantirishga mo‘ljallangan.

Masofaviy o‘qitishning dasturiy ta’minoti-masofaviy o‘qitishni ta’minlovchi dasturiy vositalar va platformalar.

Masofaviy o‘qitishning texnik vositalari-masofaviy o`qitishning axborot-ta’lim muhitida o‘quv materiallarni taqdim etish uchun foydalaniladigan texnik ta’minoti.

Masofaviy o‘qitishning o‘quv-metodik ta’minoti-masofaviy o`qitishni didaktik va psixologik talablari asosida shakllantirilgan axborot-ta’lim resurslari, ularni boshqarish tizimi, masofaviy o ‘qitish metodlari, testlar va tavsiyalar majmui.

Ma’lumotlar bazasi-real ob’ekt va uning qismlari haqidagi tizimlashgan ma’lumotlar to‘plami.

Ma’lumotlar banki-ma’lumotlarni yigish, saqlash, izlash va qayta ishlashni ta’minlaydigan axborot, texnik dasturiy va tashkiliy vositalar majmui.

Metodik ta’minot-kursni o‘rganishga qaratilgan turli axborot tashuvchilardagi o‘quv materiallar, metodik tavsiyalar va maslaxatlar.

Muloqot vositalari-telekommunikatsiya (internet) orqali muloqotni ta’minlash vositalari.

Multimedia-axborotni (matn, rasm, animatsiya, audio, video) ifodalashning ko‘p imkoniyatli taqdim etil ishi.

Multimediali darsliklar-multimedia texnologiyasi yordamida axborot-ta’lim resurslaridan foydalanish imkoniyatlarini kengaytiruvchi darslik.

Oraliq test sinov-ta’lim jarayonida bilimlarni nazorat qilish shakli.

OOOK- Ommaviy ochiq onlayn kurslar

Pedagogik axborot texnologiyalari-kompyuter, tarmoq texnologiyasi va didaktik vositalarni foydalanishga asoslangan texnologiyalar.

Provayder (provider)-kompyuterlarning tarmoqqa ulanish va axborot almashishini tashkil qiladigan tashkilot.

Sayt-grafika va multimediya elementlari joylashtirilgan gipermediya xujjatlari ko‘rinishidagi mantiqan butun axborot.

Server (server)-ma’lumotlarni o‘zida saqlovchi, foydalanuvchilarga xizmat ko‘rsatuvchi, tarmoqdagi printer, tashqi xotira, ma’lumotlar ombori kabi resurslardan foydalanishni boshqaruvchi kompyuter.

Server-axborot-ta’lim resurslarini tarmoqda joylashtirish va uni tarqatish uchun mo‘ljallangan kompyuter qurilmalari majmui.

Sun’iy intellekt (artificalintelligence)-inson intellektining ba’zi xususiyatlarini o‘zida mujassamlashtirgan avtomatik va avtomatlashtirilgan tizimlar majmausi.

Ta’lim jarayonini masofaviy o‘qitish texnologiyasi-zamonaviy axborot va kommunikatsiya texnologiyalaridan foydalanib o‘quv jarayonini masofadan turib ta’minlaydigan o‘qitish usuli va vositalari hamda o‘quv jarayonlarini boshqarish majmui.

Ta’lim maqsadi-tizimlashtirilgan bilim, ko‘nikma va malakalarni o‘zlashtirish, faollik va mustaqillikni rivojlantirish, butun dunyo qarashni shakllantirish va rivojlantirish.

Ta’limning kompyuter texnologiyasi-kompyuter texnikasi, kommunikatsiya vositalari, shuningdek axborotlarni ifodalash, uzatish va yig`ish, bilish faoliyatini nazorat qilish va boshqarishni tashkil etish bo‘yicha o`qituvchining vazifalarini modellashtiruvchi interaktiv dasturiy mahsulotlar asosida pedagogik sharoitini yaratishning metod, shakl va vositalari majmui.

Teleanjuman-turli geografik joyllashtirilgan ikki va ko‘proq foydalanuvchilar guruhlarini o‘qitish maqsadida tv-texnologiyalari orqali axborotlar almashinish shakli.

Tizim (system)-yagona maqsad yo‘lida bir vaqtning o‘zida ham yaxlit, ham o‘zaro bog‘langan tarzda faoliyat ko‘rsatadigan bir necha turdagi elementlar majmuasi.

Tuyutor-auditoriya va auditoriyadan tashqari mashg‘ulotlarning alohida turlarini o‘tkazib, o‘quvchilarning mustaqil ishlashlariga rahbarlik qiladigan,

o‘quvchilar tomonidan o‘quv rejasini bajarganliklari hamda o‘quv materialini o‘zlashtirganliklarini nazorat qiluvchi o‘qituvchi - maslahatchi.

O‘qitishning virtual muhiti-ta’lim jarayonining barcha ishtirokchilari orasida interaktiv aloqani ta’minlaydigan maxsus o‘zaroaloqador va doimiy yangilanib turiladigan o‘qitish vositalarining majmuasini tashkil etuvchi ochiq tizim.

O‘quv materiallarni saqlash texnologiyalari-o‘quv materiallarini axborot tashuvchilarda: chop etilgan mahsulot, audio va videokasetalar, disketalar, disklar, ftp va www- serverlarda saqlash vosita va metodlari majmui.

Foydalanuvchi interfeysi-foydalanuvchini tizim yoki tarmoq bilan o‘zaro ta’sirini aniqlaydigan shakl.

Foydalanuvchilarni qayd etish-axborot-ta’lim resurslariga kirish huquqini olish uchun foydalanuvchi xaqidagi ma’lumotlarni kiritish jarayoni.

Chat - axborot almashish real vaqtda olib boriladigan internetdagi muloqot.

Ekspert tizimlar-xulosa chiqarish qoida va mexanizmlari yig‘indisiga ega bo‘lganbilimlar omborini o‘z ichiga olgan sun’iy intellekt tizimi.

Elektron aloqa-axborot tarmoqlari orqali foydalanuvchilarga xatlarni etkazishni ta’minlashning muhim tarmoqli ko‘rinishi.

Elektron aloqa-kompyutertarmoqlari orqali foydalanuvchilarga ma’lumotlarni etkazib berish.

Elektron aloqa (electronicmail)-kompyuter tarmog‘ida ma’lumotlarni saqlash va ularni foydalanuvchilar orasida o‘zaro almashishini ta’minlaydigan tizim. Internetda telefon tarmog‘i orqali foydalanuvchilar orasida ma’lumot almashish imkonini beradi, ma’lumot matn yoki fayl ko‘rinishida bo‘lishi mumkin.

Elektron darslik-kompyuter texnologiyalariga asoslangan o‘qitish metodlaridan foydalanishga mo‘ljallangan o‘qitish vositasi.

Elektron jadval-nomlangan satr va ustun ko‘rinishidagi tartiblangan va turli tipdagi axborotlarni qayta ishlaydigan dastur.

Elektron kutubxona-elektron axborot-ta’lim resurslari majmuasi.

Elektron pochta-kompyutertarmoqlari asosida foydalanuvchilar o‘rtasida elektron shakldagi matn, tasvir, ovoz, video vaboshqa axborotlarni uzatuvchi va qabulqiluvchi vosita.

Elektron o‘quv qo‘llanma-bu davlat ta’lim standartining mutaxassislik va yo‘nalishlar bo‘yicha fanlarning alohida muhimroq bo‘limlari bo‘yicha tayyorlangan elektron nashrlar, namunaviy va ishchi rejalar, shuningdek mashqlar va masalalar to‘plamlari, xarita va sxemalar albomlari, tuzilma atlaslari, fanlar bo‘yicha xrestomatiyalar, diplom loyihasi bo‘yicha ko‘rsatmalar, ma’lumotnomalar aks etgan elektron manbadir.

Elektron universitetlar-bu Internetdan foydalangan xolda ta’limning yangi texnologiya va shakli.

Keys-texnologiya-masofaviy o‘qitishni tashkil qilishning shunday uslubiki, masofaviy ta’limda matnli, audiovizual vamultimediali (keys) o‘quv uslubiy materiallar majmuasi qo‘llanishga asoslanadi.

MUNDARIJA

СОДЕРЖАНИЕ

CONTENTS

S.A. Tishlikov., A.N. Qudratov., J.D.Saidov., D.D.Doniyorov. Axborot xavfsizligi. O‘quv- uslubiy qo‘llanma. Guliston, 2023. – 167 bet.

S.A.Tishlikov
A.N. Qudratov
J.D. Saidov
D.I. Doniyorov

AXBOROT XAVFSIZLIGI

O‘quv- uslubiy qo‘llanma texnikumlar
va akademik litseylar uchun

Guliston 2023 y