O’ZBEKISTON RESPUBLIKASI OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

TERMIZ DAVLAT UNIVERSITETI

Amaliy matematika kafedrasi

«Axborot xavfsizligi»

fanidan

Ma’ruzalar matni

Bilim sohasi:	100 000	–	Gumanitar soha
Ta’lim sohasi:	110 000	–	Pedagogika
Ta’lim yo’nalishi:	5110700	–	Informatika o`qitish metodikasi

Tuzuvchilar:

I.M.Boyquziyev – TerDU “Amaliy matematika” kafedrasi o’qituvchisi

A.X.Bozorov – TerDU “Amaliy matematika” kafedrasi o’qituvchisi

TERMIZ – 2018

MUNDARIJA

KIRISH

Mazkur Ma’ruzlar matni "Axborot xavfsizligi" fanidan 5110700 – Informatika o`qitish metodikasi ta’lim yo‘nalishi talabalari uchun Fizika-matematika fakultetining "Amaliy matematika" kafedrasi professor-o’qituvchilari tomonidan ishlab chiqilgan. "Axborot xavfsizligi" fani o’quv uslubiy majmuasini yaratishda yetakchi xorijiy OTMlari o’quv dasturlariga asosiy adabiyotlardan foylalanilgan.

Fanni o'qitishdan maqsad - bo'lajak informatika o'qituvchisi fanning nazariy va amaliy jihalarini o'rganish bilan bir qatorda kompyuterdan foylananishda axborotlar havfsizligini ta'minlash va ularni himoyalash usullarni bilish va ularni amalda qo'llash ko'nikma va makalalarni shaklantirish va rivojlantirishdan iborat.

Ushbu maqsadga erishish uchun fan talabalarni nazariy bilimlar, amaliy ko'nikmalar: axborot xavfsizligi va unga tahdid soluvchi sabablar haqidagi tassavurlarini rivojlantirish, axborot tizimlari va himoyalangan axborot tizimlari haqidagi tushunlarlarni, axborot xavfsizligini ta'minlovchi standartlar va modellar haqidagi bilimlarni, axborotni himoyalash va himoyalanish usullaridan qanday foydalanish haqida bilimlarni berish vazifasini bajaradi.

Fan bo'yicha talabalarning bilim, ko'nikma va malakalariga quydagi talablar qo'yiladi: - axborot xavfsizligi va unga tahdid soluvchi sabablar, axborot tizimlari va ularning turlarini, himoyalangan axborot tizimlari,axborot xavfsizligini ta'minlovchi standartlar, axborot xavfsizligini ta'minlovchi modellar, axborotni himoyalash usulari, axborot tizimlarini xavfsizligini ta'minlovchi dasturiy va texnik vositalar, operasion tizim himoya vositalari, Elektron pochta va internetda xavfsizlik haqida **tasavvurga ega bo'Iishi;**

- axborot xavfsizligini ta'minlash va ularning oldini olish, axborot tizimlari va himoyalangan axborot tizimlarida ishlay olish, himoyalanish dasturlari va ulardan

foydalana olish,. Axborot tizimlarini xavfsizligini ta'minlovchi dasturiy va texnik vositalari bilan ishlay olish, elektron pochta va Internet tizimidan ma'lumotlar olish va yuborishda himoyalanish usullari haqidagi **bilishi va ulardan foydalana olishi*;***

- axborot xavfsizligiga taqdid soluvchi sabablarni aniqlay olish, axborot tizimlari va uiarning turlarini ajrata olish, axborot xavfsizligi standartlarini tushuntirib bera olish, Axborot xavfsizligini ta'minlovchi modellarni aniqlay olish, axborotni xavfdan himoyalanishning kriptografik metodini amalda quylay olish, antiviruslar, kriptografik paketlar, Windows operasion tizimi himoya vositalari Bilan ishlay olish va internetda xavfsizlikni ta'minlash **ko'nikmalariga ega bo'lishi kerak.**

Ushbu o’quv uslubiy qo’llanma beshta qismdan iborat bo’lib, ular sillabus, ishchi o’quv reja, namunaviy va ishchi o’quv dastur, modulni o’qitishda foydalaniladigan interfaol ta’lim metodlari, ma’ruza va amaliy mashg’ulotlar materiallaridan tashkil topgan.

I-BO'LIM. O'QUV MATERIALLAR

1-MODUL. AXBOROT XAVFSIZLIGI

1.1. MA'RUZA UCHUN MATERIALLAR

1-MAVZU: AXBOROT XAVFSIZLIGINING ASOSIY TUSHUNCHALARI

MA'RUZA MASHG'ULOTI REJASI:

1.1. Axborot xavfsizligi. Axborot xavfsizligini ta'minlash zarurati.
1.2. Axborotlarga nisbatan mavjud xavf-xatarlar asoslari va tasnifi.
1.3. Axborot tizimlarida ma'lumotlarga nisbatan xavflar.
1.4. Axborot xavfsizligining asosiy tushunchalari va uning tasnifi.

Tayanch so'z va iboralar Axborot xavfsizligi, Xavf (risk), *axborotni muhofaza etish, konsepsiya*

Axborot xavfsizligi tushunchasi

Axborot xavfsizligi - axborot soxasida shaxs, jamiyat va davlat manfaatlarining himoyalanganligi holati

Axborot xavfsizligi (AX) deganda, biz tasodifiy yoki oldindan ko'zlangan tabiiy yoki sun'iy xarakterga ega bo'lgan ta'sirlardan, qaysiki axborot subyektlariga noma'qul ziyon keltiradigan, shu jumladan infrastrukturani qo'llab quvvatlovchi axborot foydalanuvchilaridan va egalaridan axborotni himoyalanganligini tushanamiz.

Axborotni himoyalash - bu axborotni xavfsizligini ta'minlashga qaratilgan kompleks chora-tadbirlar.

Xavf (risk) tushunchasi

Kompyuter va axborot texnologiyalarning rivojlanishi katta portlash bo'ldi. Shu vaqtgacha biror bir yangi texnologiya bunday tezlik bilan insoniyat hayotiga kirib bormagan. Kompyuter texnologiyalari gen injeneriya, koinot, sun'iy intellekt kabi sohalarda yuqori imkoniyatlarni taqdim etmoqda. Lekin kompyuter texnologiyalarining boshqa zararli tomonlari ham mavjud: ular ommaviy qirg'in qurollarini, bilologik va kimyoviy qurollarni ishlab chiqishda foydalanilmoqda. Bundan tashqari kompyuter texnologiyalari moliyaviy operatsiyalarni amalga oshirishda ham qo'llanilmoqda. Kompyuter tizimlari va tarmoqlari odatda buzg'unchi, yomon maqsadli shaxslar qurboni bo'lmoqda. Bunday qastdan qilingan tahdidlardan tashqari, bilmasdan qilingan(yo'l qo'yilgan) hatti-harakatlar(xatoliklar) ham kerakli ma'lumotning yo'qolishi, buzilishiga olib kelishi mumkin[1].

Shu uchun ham kompyuter texnologiyalarining rivojlanishi bilan parallel ravishda axborot xavfsizligi ham rivojlanib bormoqda[1].

Xavf (risk) ikki qismdan iborat[1]:

1. ehtimollik
2. potensial zarar

Bugungi kunda axborot tizimlari xavfsizligi bilan bog'liq tahdirlar kelajakda sodir bo'lishi mumin bo'lgan xavflardan keladigan zararni kamaytirishga yo'naltirilgan. Kelajakda xavfdan keladigan zararning noaniqligi tufayli, to'liq xavfsizlikni (ya'ni zararni nolga yaqinlashtirish) ta'minlash juda qimmat.

[1] Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

Shuning uchun risk menejerlari xavfsizlik vositalariga ketadigan mablag‘ni minimallashtirgan holda, resurslarni taqsimlashni optimallashtirishga urinadi. Bunday jarayon odatda risklarni boshqarish deyiladi.

Xavfsizlik deb xavfdan xoli, turli hujumlar va baxtsiz hodisalar tufayli buzilishdan himoyalangan holatga aytiladi.

Risk(xavf) deb shikast yetkazilishi, yo‘qolishi ehtimolligiga aytiladi[2].

Risklarni boshqarish 3 etapdan iborat:

1. Amalga oshishi mumkin bo‘lgan risklarni aniqlash
2. Riskni minimallashtirish bo‘yicha chora-tadbirlarni tanlash va qo‘llash
3. Yuqoridagi 2 etapni tekshirish maqsadida, tajribada xavfni amalga oshirish va risk zararini baholash

Axborot, axborotni muhofaza etish **tushunchalari**

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi №439-II-sonli «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida[3]axborot va uning turlari to‘g‘risida quyidagi ta’riflar keltirilgan:

axborot - manbalari va taqdim etilish shaklidan qat’i 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[4].

Saqlash, o‘zgartirish, uzatish va ma’lum maqsadlar uchun foydalanish obekti 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, ilmiy-texniq 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[5] 1-moddasida davlat sirlari tushunchasi berilgan:

---

[2] Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

[3]Узбекистон Республикаси Олий Мажлисининг Ахборотномаси. - Т., 2003. - №1. - 2-м.

[4]Алока ва ахборотлаштириш сохасида ахборот хавфсизлиги: Атамалар ва таърифлар. Тармок стандарти: TSt 45-010:2010.

[5]Узбекистон Республикаси Олий Кенгашининг Ахборотномаси. - Т., 1993. - №5. - 232-м.

«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».

3.Axborot xavfsizligi tushunchasi, uning tashkil etuvchilari tavsifi. 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 va u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

Axborot sohasida *shaxs manfaatlari* fuqarolarning axborotdan foydalanishga doir konstitutsiyaviy huquqlarini amalga oshishida, qonunda taqiqlanmagan faoliyat bilan shug‘ullanishida hamda jismoniy, ma’naviy va intellektual rivojlanishda axborotlardan foydalanishlarida, shaxsiy xavfsizlikni ta’minlovchi axborot himoyasida namoyon bo‘ladi.

Axborot sohasida *jamiyat manfaatlari* bu sohada shaxs manfaatlarini ta’minlashda, demokratiyani mustahkamlashda, ijtimoiy huquqiy davlatni qurishda, ijtimoiy hamjihatlikni qo‘llab-quvvatlashda o‘z aksini topadi.

Axborot sohasida *davlat manfaatlari* milliy axborot infrastrukturasining rivojlanishiga sharoitlar yaratishda, axborot olish sohasida shaxs va fuqarolarning konstitutsiyaviy huquq va erkinliklarini amalga oshishida, O‘zbekistonning hududiy birligini, suverenitetini va konstitutsiyaviy tuzumining mustahkamligini, siyosiy, iqtisodiy va ijtimoiy barqarorligini ta’minlash maqsadida axborotdan foydalanishda, qonuniylik va huquq tartibotni qat’iy amalga oshishida, o‘zaro tenglik va o‘zaro manfaatdorlikdagi xalqaro hamkorlikni rivojlantirishda ifodalanadi.

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 obektlari, balki xavfsizlik sohasidagi barcha xavfsizlik obektlarining asosiy yelementlari 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 yerishishning strategik yo‘nalishlarini va ularni amalga oshirish tizimlarini o‘zida aks yettiruvchi 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.

Axborotni muhofaza qilish - axborot xavfsizligining (ma’lumotlarning butunligi, foydalana olish va zarur bo‘lganda, ma’lumotlarni kiritish, saqlash, qayta ishlash va uzatishda foydalaniluvchi axborot va uning zaxiralari konfedensialligi) muhim jihatlarini ta’minlashga yo‘naltirilgan tadbirlar majmuidir.

2-MAVZU: AXBOROT HIMOYASI VA UNING TURLARI

MA’RUZA MASHG’ULOTI REJASI:

2.1. Axborot himoyasi va uning turkumlari.

2.2. Tarmoq xavfsizligini nazorat qilishning texnik vositalari.

2.3. Avtomatlashtirilgan axborot tizimlarida ma'lumotlarga nisbatan xavflar.

2.4. Avtomatlashtirilgan axborot tizimlarida himoyalanish zaruriyati.

Tayanch so‘z va iboralar: maxfiylik, konfidentsiallik, yaxlitlik, autentifikatsiya, ishonchlilik, aniqlilik, identifikatsiyalashni nazorat qilish, qasddan buzilishlarga to’sqinlik

Axborotni himoya qilish deganda:

Axborotning jismoniy butunligini ta’minlash, shu bilan birga axborot elementlarining buzilishi, yoki yo‘q qilinishiga yo‘l qo‘ymaslik;

Axborotning butunligini saqlab qolgan holda, uni elementlarini qalbakilashtirishga (o‘zgartirishga) yo‘l qo‘ymaslik;

Axborotni tegishli huquqlarga ega bo‘lmagan shaxslar yoki jarayonlar orqali tarmoqdan ruxsat etilmagan holda olishga yo‘l quymaslik;

Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar faqat tomonlar o‘rtasida kelishilgan shartnomalar asosida qo‘llanilishiga ishonish kabilar tushuniladi

Axborotlarni himoyalashning vazifalari

Foydalanuvchanlik - bu ma’lum vaqt oralig‘ida kerakli axborot xizmatini olish imkoniyatidir. Butunlik - axborotni aktualliligi bo‘lib, uni yo‘q qilinishidan va ruxsat etilmagan o‘zgartirishlardan himoyalanganliligidir. Maxfiylik - bu axborotni ruxsat etilmagan murojaatlardan himoyalash.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

• **maxfiylik** — aniq bir axborotga fakat tegishli shaxslar doirasigina kirishi mumkinligi, ya’ni foydalanilishi qonuniy xujjatlarga muvofik cheklab qo’yilib, xujjatlashtirilganligi kafolati. Bu bandning buzilishi **o’g’irlik** yoki **axborotni oshkor qilish,** deyiladi;

• **konfidentsiallik** — inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

• **yaxlitlik** — axborot boshlang’ich ko’rinishda ekanligi, ya’ni uni saqlash va uzatishda ruxsat etilmagan o’zgarishlar qilinmaganligi kafolati; bu bandning buzilishi **axborotni soxtalashtirish** deyiladi;

• **autentifikatsiya** — axborot zaxirasi egasi deb e’lon qilingan shaxs xaqiqatan xam axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi **xabar muallifini soxtalashtirish** deyiladi;

• **apellyatsiya qilishlik** — yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo’llaniladi. Kerak bo’lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati. Yukoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin:

• **ishonchlilik** — tizim meyoriy va g’ayri tabiiy hollarda rejalashtirilganidek o’zini tutishlik kafolati;

• **aniqlilik** — xamma buyruqlarni aniq va to’liq bajarish kafolati;

• **tizimga kirishni nazorat qilish —** turli shaxs guruxlari axborot manbalariga xar xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati;

• **nazorat qilinishi** — istalgan paytda dastur majmuasining xoxlagan kismini tulik tekshirish mumkinligi kafolati;
• **identifikatsiyalashni nazorat qilish** — Hozir tizimga ulangan mijoz aniq o'zini kim deb atagan bulsa, aniq o'sha ekanligining kafolati;
• **qasddan buzilishlarga to'sqinlik** — oldindan kelishilgan me'yorlar chegarasida qasddan xato kiritilgan ma'lumotlarga nisbatan tizimning oldindan kelishilgan xolda o'zini tutishi

Axborotni himoyalashning maqsadlari quyidagilardan iborat:

- axborotning kelishuvsiz chikib ketishi, ugirlanishi, yo'qotilishi, o'zgartirilishi, soxtalashtirilishlarning oldini olish;
- shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf – xatarning oldini olish;
- axborotni yo'q qilish, o'zgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish;
- xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta'minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish;
- axborot tizimida mavjud bulgan shaxsiy ma'lumotlarning shaxsiy maxfiyligini va konfidentsialligini saklovchi fukarolarning konstitutsion xukuklarini himoyalash;
- davlat sirini, konunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saklash;
- axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chikish va kullashda sub'ektlarning xukuklarini ta'minlash.

Axborot-kommunikatsiyalar texnologiyalarining ommaviy ravishda qog`ozsiz avtomatlashtirilgan asosda boshqarilishi sababli axborot xavfsizligini ta'minlash murakkablashib va muhimlashib bormoqda. Shuning uchun ham avtomatlashtirilgan axborot tizimlarida axborotni himoyalashning yangi zamonaviy texnologiyasi paydo bo`lmoqda, DataQuest kompaniyasining ma'lumotiga ko`ra, 1996-2000 yillarda axborot himoyasi vositalarining sotuvdagi hajmi 13 mlrd. AQSh dollariga teng bo`lgan.

Axborotning zaif tomonlarini kamaytiruvchi va axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yuqolishiga to`sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi — axborotni himoyalash tizimi deyiladi.

Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo`qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalarini aniqlashlari zarur. Axborotning qimmatliligi va talab qilinadigan himoyaning ishonchliligi bir-biri bilan bevosita bog`liq.

Himoyalash tizimi uzluksiz, rejali, markazlashtirilgan, maqsadli, aniq, ishonchli, kompleksli, oson mukammallashtiriladigan va ko`rinishi tez o`zgartiriladigan bo`lishi kerak. U odatda barcha ekstremal sharoitlarda samarali bo`lishi zarur.

Axborot hajmi kichik bo`lgan tashkilotlarda axborotni himoyalashda oddiy usullarni qo`llash maqsadga muvofiq va samaralidir. Masalan, o`qiladigan qimmatbaho qog`ozlarni va Elektron hujjatlarni alohida guruhlarga ajratish va niqoblash, ushbu hujjatlar bilan ishlaydigan xodimni tayinlash va o`rgatish, binoni qo`riqlashni tashkil etish, xizmatchilarga qimmatli axborotni tarqatmaslik majburiyatini yuklash, tashqaridan keluvchilar ustidan nazorat qilish, kompyuterni himoyalashning eng oddiy usullarini qo`llash va hokazo. Odatda, himoyalashning eng oddiy usullarini qo`llash sezilarli samara beradi.

Murakkab tarkibli, ko`p sonli avtomatlashtirilgan axborot tizimi va axborot hajmi katta bo`lgan tashkilotdarda axborotni himoyalash uchun himoyalashning majmuali tizimi tashkil qilinadi. Lekin ushbu usul hamda himoyalashning oddiy usullari xizmatchilarning ishiga haddan tashqari xalaqit bermasligi kerak.

Himoya tizimining komplekslіligiga unda huquqiy, tashkiliy, muhandis-texnik va dasturiy-matematik elementlarning mavjudligi bilan erishiladi. Elementlar nisbati va ularning mazmuni tashkilotlarning axborotni himoyalash tizimining o`ziga xosligini va uning takrorlanmasligini hamda buzish qiyinligini ta'minlaydi.

Aniq tizimni ko`p turli elementlardan iborat, deb tasavvur qilish mumkin. Tizim elementlarining mazmuni nafaqat uning o`ziga xosligini, balki axborotning qimmatliligini va tizimning qiymatini hisobga olgan holda belgilangan himoya darajasini aniqlaydi.

Axborotni xuquqiy himoyalash elementi himoyalash choralarining haqli ekanligi ma'nosida tashkilot va davlatlarning o`zaro munosabatlarini yuridik mustahkamlash hamda personalning tashkilot qimmatli axborotini himoyalash tartibiga rioya qilishi va ushbu tartibning buzilishida javobgarligi tasavvur qilinadi.

Himoyalash texnologiyasi personalni tashkilotning qimmatli axborotini himoyalash qoidalariga rioya kilishga undovchi boshqarish va cheklash xarakteriga ega bo`lgan chora-tadbirlarni o`z ichiga oladi.

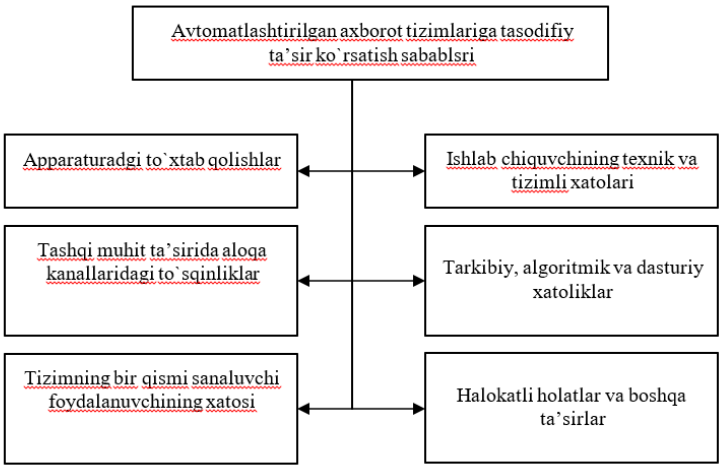
Tashkshshy himoyalash elementi boshqa barcha elementlarni yagona tizimga bog`lovchi omil bo`lib hisoblanadi. Ko`pchilik mutaxassislarning fikricha, axborotni himoyalash tizimlari tarkibida tashkiliy himoyalash 50-60 % ni tashkil qiladi. Bu hol ko`p omillarga bog`liq, jumladan, axborotni tashkiliy himoyalashning asosiy tomoni amalda himoyalashning printsipi va usullarini bajaruvchi personalni tanlash, joylashtirish va o`rgatish hisoblanadi.

Axborotni himoyalashning tashkiliy chora-tadbirlari tashkilot xavfsizligi xizmatining me'yoriy uslubiy hujjatlarida o`z aksini topadi. Shu munosabat bilan ko`p hollarla yuqorida ko`rilgan tizim elementlarining yagona nomi — axborotni tashkiliy-huquqiy himoyalash elementini ishlatadilar.

Axborotni texnik himoyalash elementi — texnik vositalar kompleksi yordamida hudud, bino va qurilmalarni qo`riqlashni tashkil qilish hamda texnik tekshirish vositalariga qarshi sust va faol kurash uchun mo`ljallangan. Texnik himoyalash vositalarining narxi baland bo`lsada, axborot tizimini himoyalashda bu element muxim ahamiyatga ega.

Axborotni himoyalashning dasturiy-matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saqlanadigan qimmatli axborotni himoyalash uchun mo`ljallangan. Kompyuter tizimi (tarmog`i)ga ziyon etkazishi mumkin bo`lgan sharoit, harakat va jarayonlar kompyuter tizimi (tarmog`i) uchun xavf-xatarlar, deb hisoblanadi.

Avtomatlashtarilgan axborot tizimlariga tasodifiy ta'sir ko`rsatish sabablari tarkibiga quyidagilar kiradi (2.1-rasm).



2.1-rasm. Avtomatlashtirilgan axborot tizimlariga tasodifiy ta'sir ko`rsatish sabablari

Ma'lumki, kompyuter tizim (tarmog`)ining asosiy komponentlari — texnik vositalar, dasturiy-matematik ta'minot va ma'lumotlardir.

Nazariy tomondan bu komponentlarga nisbatan to`rt turdagi xavflar mavjud, ya'ni uzilish, tutib qolish, o`zgartirish va soxtalahtirish.

Uzilish — tashqi harakatlar (ishlar, jarayonlar)ni bajarish uchun hozirgi shilarni vaqtincha markaziy protsessor qurilmasi yordamida to`xtatish, ularni bajargandan so`ng protsessor oldingi holatga qaytadi va to`xtatib qo`yilgan ishni davom ettiradi. Har bir uzilish tartib raqamiga ega, unga asosan markaziy protsessor qurilmasi qayta ishlash uchun qism-dasturni qidirib topadi. Protsessorlar ikki turdagi uzilishlar bilan ishlashni vujudga keltirishi mumkin: dasturiy va texnik. Biror qurilma favqulodda xizmat ko`rsatilishiga muhtoj bo`lsa, unda texnik uzilish paydo bo`ladi. Odatda bunday uzilish markaziy protsessor uchun kutilmagan hodisadir. Dasturiy uzilishlar asosiy dasturlar ichida protsessorning maxsus buyruqliari yordamida bajariladi. Dasturiy uzilishda dastur o`z-o`zini vaqtincha to`xtatib, uzilishga taalluqli jarayonni bajaradi.

Tutib olish – bu jarayon oqibatida g`arazli shaxslar dasturiy vositalar va axborotning turli magnitli tashuvchilariga kirishni yo`lga qo`yadi. Dastur va ma'lumotlardan noqonuniy nusxa olish, kompyuter tarmoqlari aloqa kanallaridan ruxsatsiz o`qishlar va hokazo harakatlar tutib olish jarayonlariga misol bo`la oladi.

O`zgartirish — ushbu jarayon yovuz niyatli shaxs nafaqat kompyuter tizimi komponentlariga (ma'lumotlar to`plamlari, dasturlar, texnik elementlari) kirishni yo`lga qo`yadi, balki ular tarkibini (ko`rinishini) o`zgartiradi. Masalan, o`zgartirish sifatida g`arazli shaxsning ma'lumotlar to`plamidagi ma'lumotlarni o`zgartirishi, yoki umuman kompyuter tizimi fayllarini o`zgartirishi, yoki qandaydir qo`shimcha noqonuniy qayta ishlashni amalga oshirish maqsadida foydalanilayotgan dasturning kodini o`zgartirishi tushuniladi.

Soxtalashtirish — bu jarayon yordamida g`arazli shaxslar tizimda hisobga olinmagan vaziyatlarni o`rganib, undagi kamchiliklarni aniqlab, keyinchalik o`ziga kerakli harakatlarni bajarish maqsadida tizimga qandaydir soxta jarayonni yoki tizim va boshqa foydalanuvchilarga soxta yozuvlarni yuboradi.

3-MAVZU: AXBOROTLARNI HIMOYALASH TA’MINOTI

MA’RUZA MASHG’ULOTI REJASI:

3.1. Tashkiliy himoyalash elementlari.

3.2. Texnik himoyalash elementlari.

3.3. Himoyani ta'minlashning texnik vositalari.

3.4. Dasturiy himoyalash elementlari.

Tayanch so‘z va iboralar: Tashkiliy himoyalash elementlari. Texnik himoyalash elementlari. Himoyani ta'minlashning texnik vositalari. Dasturiy himoyalash elementlari.

Axborot himoyasi - axborot xavfsizligini ta’minlashga karatilgan tadbirlar, uslublar va vositalar majmuasidan iborat. Shu bilan birga, axborotni to’laligi, kompyuter ashyolari va unda saqlanayotgan dasturlar hamda ma’lumotlarga ruxsatsiz kirishning oldini olish, kompyuterlardagi dasturlardan ruxsatsiz foydalanishning oldini olish kabi vazifalarni bajaradi.

Kompyuter tarmoqlarida axborotni himoyalash deb foydalanuvchilarni ruxsatsiz tarmoq, elementlari va zahiralariga egalik qilishni man etishdagi texnik, dasturiy va kriptografik usul va vositalar, hamda tashkiliy tadbirlarga aytiladi.

Tashkiliy himoyalash vositalari — bu talekommunikasiya uskunalarining yaratilishi va qo’llanishi jarayonida qabo’l qilingan tashkiliy-texnikaviy va tashkiliyxuquqiy tadbirlardir.

Axloqiy va odobiy himoyalash vositalari — bu hisoblash texnikasini rivojlanishi oqibatida paydo bo’ladigan tartib va kelishuvlardir. Ushbu tartiblar qonun darajasida bo’lmasada, uni tan olmaslik foydalanuvchilarni obro’siga ziyon yetkazishi mumkin.

Qonuniy himoyalash vositalari — bu davlat tomonidan ishlab chiqilgan xuquqiy hujjatlar sanaladi. Ular bsvosita axborotlardan foydalanish, qayta ishlash va uzatishni tartiblashtiradi va ushbu qoidalarni buzuvchilarning mas’uliyatlarini aniqlab beradi.

Axborot xavfsizligini ta’minlash. Axborot xavfsizligini ta’minlash – bu foydalanuvchining axborotlarini himoyalashga quyilgan me’yor va talablarni bajarishidir.

AXni ta’minlash muammosiga ikkita yondashuv mavjuddir: «fragmentar» va kompleksli.

«Fragmentar» yondashuv mavjud shart-sharoitlarda aniq belgilangan tahdidlarga qarshi aks ta’sir ko’rsatishga qaratilgan. Bunday yondashuvni amalga oshirishga misol sifatida kirishni boshqarishning ayrim vositalarini, ixtisoslashgan antivirusli dasturlarni keltirish mumkin.

Bunday yondashuvning afzal tomoni shundaki, bunda aniq tahdid bexato tanlab olinadi. Uning sezilarli kamchiligi esa axborotlarga ishlov berishning yagona himoyalangan muhiti yo’qligidadir.

Kompleks yondashuv AXda axborotlarga ishlov berishning himoyalangan muhi-tini yaratishga qaratilgan bo’lib, bu muhit tahdidlarga qarshi aks ta’sirning turli xil choratadbirlarini yagona kompleksga birlashtiradi. Axborotlarga ishlov berishning himoyalangan muhitini tashkil etish AXni ma’lum darajada kafolatlash imkonini beradi, bu esa kompleks yondashuvning shubhasiz afzalli-gidan dalolatdir. Bu yondashuvning kamchiliklari quyidagilardan iborat: AX foydalanuvchilarining harakat erkinligi cheklanganligi, himoya vositala-rini o’rnatish va sozlashdagi xatoliklarga yuqori darajadagi sezgirlik, boshqarish-ning murakkabligi.

Xavfsizlik siyosati ma’muriy-tashkiliy choralar, jismoniy va dasturiy-texnik vositalar yordamida amalga oshiriladi hamda himoya tizimi arxitektu-rasini belgilab beradi. Har bir muayyan tashkilot uchun xavfsizlik siyosati maxsus ishlab chiqilishi hamda undagi axborot ustida ishlashning aniq texno-logiyasi va qo’llanayotgan dasturiy, texnik vositalarga bog’liq bo’lishi kerak.

Xavfsizlik siyosati tizim obyektlariga murojaat qilish tartibini belgi-lab beruvchi kirishni boshqarish usuli bilan belgilanadi. Xavfsizlik siyosati-ning ikkita asosiy turi farqlanadi: **saylanma** va **vakolatli**.

Saylanma xavfsizlik siyosati murojaatni boshqarishning tanlanadigan usuliga asoslanadi. **Vakolatli xavfsizlik** siyosati administrator tomonidan taqdim etiladigan ko'plab ruxsat etilgan kirish munosabatlarini bildiradi. Odatda saylanma murojaat boshqaruvi xususiyatlarini tavsif etishda murojaat matrisasi asosidagi matematik modeldan foydalaniladi.

Kirish matrisasi bu shunday matrisaki, unda ustun tizim obyektiga, satr esa uning subyektiga to'g'ri keladi. Matrisaning ustun va satr kesishgan joyida subyektning obyektga ruxsat etilgan murojaat qilish turi ko'rsatiladi. Odatda obyektning subyektga «qo'yishga murojaat», «yozishga murojaat», «ijroga murojaat» va h.k. kabi turlari qo'llanadi. Kirish matrisasi kirishni boshqarish tizimlarini modellashtirishdagi eng sodda yondashuv hisoblanadi. Biroq u ancha murakkab modellar uchun asos vazifasini ham o'taydi.

Kompyuter tizimlari xavfsizligini ta'minlash choralari ularni amalga oshirish usullari bo'yicha quyidagi guruhlarga bo'linadi: huquqiy (qonunchilik); axloqiytarbiyaviy; ma'muriy;jismoniy;texnik-dasturiy.

Sanab o'tilgan AX xavfsizligi choralarini axborot himoyasi yo'lida ketma-ket qo'yilgan to'siq yoki chegaralar sifatida olib qarash mumkin. Himoya qilinayotgan axborotlarga yetib borish uchun, ketma-ket bir nechta himoya chegaralarini bosib o'tish lozim bo'ladi.

Axborotlarni himoyalashning texnik va dasturiy vositalari

Zamonaviy axborot - kommunikasiyalar texnologiyalarining yutuklari himoya uslublarining bir kator zaruriy instrumental vositalarini yaratish imkonini berdi.

Axborotlarni himoyalovchi instrumental vositalar deganda dasturlash, dasturiy - apparatli va apparatli vositalar tushuniladi. Ularning funksional tuldirilishi xavfsizlik xizmatlari oldiga kuyilgan axborotlarni himoyalash masalalarini yechishda samaralidir. Hozirgi kunda tarmoq xavfsizligini nazorat kilish texnik vositalarining juda keng spektri ishlab chikarilgan.

FUNKSIONAL VAZIFASIGA KO'RA AXBOROTLARNI MUHANDIS-TEXNIK HIMOYALASH VOSITALARI QUYIDAGI GURUHLARGA AJRATILADI:

1.Fizik vositalar. Bu vositalarga mexanik, elektromexanik, elektron, elektronoptik, radio- va radiotexnik va boshqa qurilmalar mansub bo'ladi. Bu vositalarning vazifasi axborotlarga ruxsatsiz kirishni va tajouzkorlikni boshqa mumkin bo'lgan harakatlarni oldini olishdan iborat.

Bu vositalar quyidagi vazifalarni amalga oshirish uchun qo'llaniladi:

- korxona hududini qo'riqlash va uni kuzatish uchun;
- binolarni qo'riqlash va uni nazorat qilish uchun;
- jihozlarni, mahsulotlarni, moliyaviy natijalar va axborotlarni qo'riqlash uchun;
- bino va inshoatlarni nazorat qiluvchi vositalarga kirishni himoya qilish uchun.

Barcha obyektlarni himoya qilishni fizik vositalarini uchta kategoriyaga ajratish mumkin: **ogohlantirish vositalari** (obyekt o'ralgan devorlar); **tahdidni aniqlash vositalari** (signalizasiya va kuzatish uchun o'rnatilgan televizorlari) va **tahdidni bartaraf qilish tizimlari** (o't o'chirish vositalari)

Umuman olganda bu kategoriyalarni quyidagi guruhlarga ajratish mumkin:

- qo'riqlash va qo'riqlash-o't o'chirish tizimlari;
- qo'riqlash televizorlari;
- qo'riqlash yoritgichlari;
- fizik himoyalash vositalari;
- apparat vositalari.

2. Axborotlarni himoyalashni apparat vositalari

Axborotlarni himoyalashni apparat vositalari quyidagi vazifalarni amalga oshirishga imkoniyat beradi:

- axborotni ruxsatsiz chiqib ketish kanallarini aniqlash maqsadida texnik vositalarni maxsus tekshiruvlardan o’tkazish;
- turli hil obyektlarni axborotlarni ruxsatsiz chiqib ketish kanallarini aniqlash;
- axborotni ruxsatsiz chiqib ketishi aniqlangan kanallarini lokallashtirish (ajratib olish);
- sanoat shipionaji vositalarini qidirish va aniqlash;
- konfidensial bo’lgan axborotlar va boshqa manbalarga ruxsatsiz kirishga qarshi harakatlarning konfidisial bo’lishi.

3. Dasturiy vositalar.

Axborotlarni dasturiy himoyalash – bu axborotlarni himoya qilish vazifasini amalga oshiruvchi maxsus dasturlar tizimidir. Konfidensial axborotlarning xavfsizligini ta’minlovchi dasturlari quyidagi yo’nalishlarga ajratilib ko’rsatiladi:

- axborotlarni ruxsat berilmagan kirishlardan himoyalash;
- axborotlarni nusxa olishdan himoyalash;
- axborotlarni viruslardan himoyalash;
- aloqa kanallarini dasturiyimoyalash.

Axborotlarni ruxsat berilmagan kirishlardan himoyalashni dasturiy vositalarini bajaradigan funksiyalari quyidagilardan iborat bo’ladi**:**

- obyektlar va subyektlarni identifikasiyalash;
- hisoblash resurslari va axborot resurslariga kirishga cheklovlar o’rnatish;
- axborot va dasturlar bilan bo’ladigan harakatlarni nazorat va registrasiya qilish.

2-MODUL. AXBOROTLARNI HIMOYALASH USULLARI

4-MAVZU: AXBOROTLARNI STENOGRAFIK HIMOYALASH

MA’RUZA MASHG’ULOTI REJASI:

4.1. Zamonaviy kompyuter stenografiyasi
4.2. Kompyuter stenografiyasi istiqbollari
4.3. Kompyuter stenografiyasining asosiy vazifalari
4.4. Konfidentsial axborotlarni ruxsatsiz kirishdan himoyalash

Tayanch so`zlar va iboralar: stenografiya, kodlashtirish, kriptografiya, xabar-fayl, konteyner-fayl, konteyner –orginal, konteyner-natija, kalit.

Zamonaviy kompyuter stenografiyasi

Ruxsat etilmagan kirishdan axborotni ishonchli himoyalash muammosi eng ilgaritdan mavjud va hozirgi vaqtgacha hal qilinmagan. Maxfiy xabarlarni yashirish usullari qadimdan ma’lum, inson faoliyatining bu sohasi stenografiya degan nom olgan. Bu so‘z grekcha Steganos (maxfiy, sir) va Graphy (yozuv) so‘zlaridan kelib chiqqan va «sirli yozuv» degan ma’noni bildiradi. Stenografiya usullari, ehtimol, yozuv paydo bo‘lishidan oldin paydo bo‘lgan (dastlab shartli belgi va belgilashlar qo‘llanilgan) bo‘lishi mumkin.

Axborotni himoyalash uchun kodlashtirish va kriptografiya usullari qo‘llaniladi.

Kodlashtirish deb axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoniga aytiladi.

Kriptografiya deb maxfiy xabar mazmunini shifrlash, ya’ni ma’lumotlarni maxsus algoritm bo‘yicha o‘zgartirib, shifrlangan matnni yaratish yo‘li bilan axborotga ruxsat etilmagan kirishga to‘siq quyish usuliga aytiladi.

Stenografiyaning kriptografiyadan boshqa o‘zgacha farqi ham bor. Ya’ni uning maqsadi — maxfiy xabarning mavjudligini yashirishdir. Bu ikkala usul birlashtirilishi mumkin va natijada axborotni himoyalash samaradorligini oshirish uchun ishlatilishi imkoni paydo bo‘ladi (masalan, kriptografik kalitlarni uzatish uchun).

Kompyuter texnologiyalari stenografiyaning rivojlanishi va mukammallashuviga yangi turtki berdi. Natijada axborotni himoyalash sohasida yangi yo‘nalish — kompyuter stenografiyasi paydo bo‘ldi. Global kompyuter tarmoqlari va mul’timedia sohasidagi zamonaviy progress telekommunikatsiya kanallarida ma’lumotlarni uzatish xavfsizligini ta’minlash uchun mo‘ljallangan yangi usullarni yaratishga olib keldi. Bu usullar shifrlash qurilmalarining tabiiy noaniqligidan va analogli video yoki audiosignallarning serobligidan foydalanib xabarlarni kompyuter fayllari (konteynerlar)da yashirish imkonini beradi. Shu bilan birga kriptografiyadan farqli ravishda bu usullar axborotni uzatish faktining o‘zini ham yashiradi.

K.Shennon sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi. Zamonaviy kompyuter steganografiyasida ikkita asosiy fayl turlari mavjud: yashirish uchun mo‘ljallangan xabar-fayl, va konteyner-fayl, u xabarni yashirish uchun ishlatilishi mumkin. Bunda konteynerlar ikki turda bo‘ladi: konteyner-original (yoki «bo‘sh» konteyner) - bu konteyner yashirin axborotni saqlamaydi; konteyner-natija (yoki «tuldirilgan» konteyner) - bu konteyner

yashirin axborotni saqlaydi. Kalit sifatida xabarni konteynerga kiritib qo‘yish tartibini aniqlaydigan maxfiy element tushuniladi.

Kompyuter stenografiyasi istiqbollari

Kompyuter stenografiyasi rivojlanishi tendensiyasining tahlili shuni ko‘rsatadiki, keyingi yillarda kompyuter stenografiyasi usullarini rivojlantirishga qiziqish kuchayib bormoqda. Jumladan, ma’lumki, axborot xavfsizligi muammosining dolzarbligi doim kuchayib bormoqda va axborotni himoyalashning yangi usullarini qidirishga rag‘batlantirilayapti. Boshqa tomondan, axborot-kommunikatsiyalar texnologiyalarining jadal rivojlanishi ushbu axborotni himoyalashning yangi usullarini joriy qilish imkoniyatlari bilan ta’minlayapti va albatta, bu jarayonning kuchli katalizatori bo‘lib umumfoydalaniladigan Internet kompyuter tarmogining juda kuchli rivojlanishi hisoblanadi.

Hozirgi vaqtda axborotni himoyalash eng ko‘p qo‘llanilayotgan soxa bu — kriptografik usullardir. Lekin, bu yo‘lda kompyuter viruslari, «mantiqiy bomba»lar kabi axborotiy qurollarning kriptovositalarni buzadigan ta’siriga bog‘liq ko‘p yechilmagan muammolar mavjud. Boshqa tomondan, kriptografik usullarni ishlatishda kalitlarni taqsimlash muammosi ham bugungi kunda oxirigacha yechilmay turibdi. Kompyuter steganografiyasi va kriptografiyalarining birlashtirilishi paydo bo‘lgan sharoitdan qutulishning yaxshi bir yo‘li bo‘lar edi, chunki, bu holda axborotni himoyalash usullarining zaif tomonlarini yo‘qotish mumkin.

Shunday qilib, kompyuter stenografiyasi hozirgi kunda axborot xavfsizligi bo‘yicha asosiy texnologiyalardan biri bo‘lib hisoblanadi.

Kompyuter stenografiyasining asosiy vazifalari

Zamonaviy kompyuter stenografiyasining asosiy holatlari quyidagilardan iborat:

- yashirish usullari faylning autentifikatsiyalanishligini va yaxlitligini ta’minlashi kerak;
- yovuz niyatli shaxslarga qo‘llaniluvchi steganografiya usullari to‘liq ma’lum deb faraz qilinadi;
- usullarning axborotga nisbatan xavfsizlikni ta’minlashi ochik uzataladigan faylning asosiy xossalarini stenografik almashtirishlar bilan saqlashga va boshqa shaxslarga noma’lum bo‘lgan qandaydir axborot — kalitga asoslanadi;
- agar yovuz niyatli shaxslarga xabarni ochish vaqti ma’lum bo‘lib qolgan bo‘lsa, maxfiy xabarning o‘zini chiqarib olish jarayoni murakkab hisoblash masalasi sifatida tasavvur qilinishi lozim.

Internet kompyuter tarmog‘ining axborot manbalarini tahlili quyidagi xulosaga kelishga imkon berdi, ya’ni hozirgi vaqtda stenografik tizimlar quyidagi asosiy masalalarni echishda faol ishlatilayapti:

- konfidentsial axborotni ruxsat etilmagan kirishdan himoyalash;
- monitoring va tarmoq zaxiralarini boshqarish tizimlarini engish;
- dasturiy ta’minotni niqoblash;
- intellektual egalikning ba’zi bir turlarida mualliflik huquqlarini himoyalash.

Konfidentsial axborotlarni ruxsatsiz kirishdan hamoyalash

Bu kompyuter stenografiyasini ishlatish sohasi konfidentsial axborotlarni himoyalash muammosini echishda eng samarali hisoblanadi. Masalan, tovushning eng kam ahamiyatli kichik razryadlari yashiriladigan xabarga almashtiriladi. Bunday uzgarish ko‘pchilik tomonidan tovushli xabarni eshitish paytida sezilmaydi.

Monitoring va tarmoq zaxiralarini boshqarish tizimlarini yengish

Sanoat shpionlik tizimlarining monitoring va tarmoq zaxiralarini boshqarish harakatlariga qarshi yo‘naltirilgan stenografik usullar lokal va global kompyuter tarmoqlari serverlaridan axborotning o‘tishida nazorat o‘rnatish harakatlariga qarshi turishga imkon beradi.

Dasturiy ta’minotni nikoblash

Kompyuter steganografiyasining hozirgi vaqtda ishlatiladigan boshqa bir sohasi dasturiy ta’minotni niqoblashdir. Qachonki, dasturiy ta’minotni qayd qilinmagan foydalanuvchilar tomonidan ishlatilishi o‘rinsiz bo‘lsa, u standart universal dastur mahsulotlari (masalan, matnli muharrirlar) ostida niqoblanishi yoki mul’timedia fayllari (masalan, kompyuter o‘yinlarining musiqiy ilovasi)ga yashirilishi mumkin.

Mualliflik huquqlarini himoyalash

Stenografiyadan foydalaniladigan yana bir sohalardan biri — bu mualliflik huquqlarini himoyalash hisoblanadi. Kompyuterli grafik tasvirlarga maxsus belgi qo‘yiladi va u ko‘zga ko‘rinmay qoladi. Lekin, maxsus dasturiy ta’minot bilan aniqlanadi. Bunday dastur mahsuloti allaqachon ba’zi jurnallarning kompyuter versiyalarida ishlatilayapti. Stenografiyaning ushbu yo‘nalishi nafaqat tasvirlarni, balki audio va videoaxborotni ham qayta ishlashga mo‘ljallangan. Bundan tashqari uning intellektual egaligini himoyalashni ta’minlash vazifasi ham mavjud.

Hozirgi vaqtda kompyuter stenografiyasi usullari ikki asosiy yo‘nalish bo‘yicha rivojlanmoqda:

- kompyuter formatlarining maxsus xossalarini ishlatishga asoslangan usullar;
- audio va vizual axborotlarning serobliligiga asoslangan usullar.

Stenografik dasturlar to‘grisida qisqacha ma’lumot

Windows operatsion muhitida ishlovchi dasturlar:

- Steganos for Win95 dasturi ishlatishda juda engil bo‘lib, ayni paytda fayllarni shifrlash va ularni VMR, DIV, VOS, WAV, ASCII, NTML ken-gaytmali fayllar ichiga joylashtirib yashirishda juda qudratli hisoblanadi;
- Sontraband dasturi 24-bitli VMR formatdagi grafik fayllar ichida har qanday faylni yashira olish imkoniyatiga ega.

DOS muhitida ishlovchi dasturlar:

- Jsteg dasturi ma’lumotni JRG formatli fayllar ichiga yashirish uchun mo‘ljallangan;
- FFEncode dasturi ma’lumotlarni matnli fayllar ichida yashirish imkoniyatiga ega;
- StegoDOS dasturlar paketining axborotni tasvirda yashirish imkoniyati mavjud;
- Winstorm dasturlar paketi RSX formatli fayllar ichiga xabarni shifrlab yashiradi.

OS/2 operatsion muhitida ishlovchi dasturlar:

- Texto dasturi ma’lumotlarni ingliz tilidagi matnga aylantiradi;
- Hide4PGP v1.1 dasturi VMR, WAV, VOS formatli fayllar ichiga ma’lumotlarni yashirish imkoniyatiga ega.

Macintosh kompyuterlari uchun mo‘ljallangan dasturlar:

- Raranoid dasturi ma’lumotlarni shifrlab, tovushli formatli fayl ichiga yashiradi;
- Stego dasturining RIST kengaytmali fayl ichiga ma’lumotlarni yashirish imkoniyati mavjud.

5-MAVZU: AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH

MA’RUZA MASHG’ULOTI REJASI:

5.1. Kriptografiya tushunchasi.

5.2. Kriptrografiyaning maqsadi va vazifalari.

5.3. Kriptografiyaning rivojlanish tarixi. Zamonaviy kriptografiya

5.4. Axborotlarni kriptografiyali himoyalash tamoyillari.

Tayanch so‘z va iboralar.Kriptografiya, Kriptografiyaning rivojlanish tarixi, *aloqa nazariyasi, shifrlash kaliti, simmetrik shifrlash algoritmi, asimmetrik shifrlash algoritmi.*

«Kriptografiya» atamasi dastlab «yashirish, yozuvni berkitib qo‘ymoq» ma’nosini bildirgan. Birinchi marta u yozuv paydo bo‘lgan davrlardayoq aytib o‘tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya’ni diskda saqlanadigan sonlar ko‘rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko‘rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo‘lgan har qanday axborotga nisbatan qo‘llash mumkin. Maxfiylikni ta’minlashga qaratilgan kriptografiya kengroq qo‘llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo‘llaniladigan usullarning o‘zi axborotni himoyalash bilan bog‘liq bo‘lgan ko‘p jarayonlarda ishlatilishi mumkin.

Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta’minlaydi. Masalan, to‘lov varaqlarini Elektron pochta orqali uzatishda uning o‘zgartirilishi yoki soxta yozuvlarning qushilishi mumkin. Bunday hollarda axborotning yaxlitligini ta’minlash zaruriyati paydo bo‘ladi. Umuman olganda kompyuter tarmog‘iga ruxsatsiz kirishning mutlaqo oldini olish mumkin emas, lekin ularni aniqlash mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko‘p hollarda, axborotning haqiqiyligini ta’minlash deyiladi. Kriptografiyada qo‘llaniladigan usullar ko‘p bo‘lmagan o‘zgartirishlar bilan axborotlarning haqiqiyligini ta’minlashi mumkin.

Nafaqat axborotning kompyuter tarmogidan ma’nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch hosil qilish juda muhim. Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiqlovchi turli usullar ma’lum. Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo‘lmagan protsedura. Chunki parolni qo‘lga kiritgan har qanday shaxs axborotdan foydalanishi mumkin bo‘ladi. Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish va ularni kriptografik usullar bilan himoyalash mumkin, lekin kriptografiya bundan kuchliroq parolni uzluksiz o‘zgartirish imkonini beradigan protseduralarni ham ta’minlaydi.

Kriptografiya sohasidagi oxirgi yutuqlardan biri - raqamli signatura - maxsus xossa bilan axborotni to‘ldirish yordamida yaxlitlikni ta’minlovchi usul, bunda axborot uning muallifi bergan

ochiq kalit ma’lum bo‘lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik tekshiriladigan ma’lum usullaran ko‘proq afzalliklarga ega.

Kriptografiya usullarini qo‘llashning ba’zi birlarini ko‘rib chiqamiz. Uzataladigan axborotning ma’nosini yashirish uchun ikki xil o‘zgartirishlar qo‘llaniladi: **kodlashtirish** va **shifrlash.**

Kodlashtirish uchun tez-tez ishlatiladigan iboralar to‘plamini o‘z ichiga oluvchi kitob yoki jadvallardan foydalaniladi. Bu iboralardan har biriga, ko‘p hollarda, raqamlar to‘plami bilan beriladigan ixtiyoriy tanlangan kodli so‘z to‘g‘ri keladi. Axborotni kodlash uchun xuddi shunday kitob yoki jadval talab qilinadi. Kodlashtiruvchi kitob yoki jadval ixtiyoriy kriptografik o‘zgartirishga misol bo‘ladi. Kodlashtirishning axborot texnologiyasiga mos talablar — qatorli ma’lumotlarni sonli ma’lumotlarga aylantirish va aksincha o‘zgartirishlarni bajara bilish. Kodlashtirish kitobini tezkor hamda tashqi xotira qurilmalarida amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik tizimni muvaffaqiyatli deb bo‘lmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, kodlarning yangi kitobini yaratish va uni hamma foydalanuvchilarga tarqatish zaruriyati paydo bo‘ladi.

Kriptografik o‘zgartirishning ikkinchi turi **shifrlash** o‘z ichiga — boshlang‘ich matn belgilarini anglab olish mumkin bo‘lmagan shaklga o‘zgartirish altoritmlarini qamrab oladi. O‘zgartirishlarning bu turi axborot-kommunikatsiyalar texnologiyalariga mos keladi. Bu erda algoritmni himoyalash muhim ahamiyat kasb etadi. Kriptografik kalitni qo‘llab, shifrlash algoritmining o‘zida himoyalashga bo‘lgan talablarni kamaytirish mumkin. Endi himoyalash ob’ekti sifatada faqat kalit xizmat qiladi. Agar kalitdan nusxa olingan bo‘lsa, uni Sirli (maxfiy) aloqalar sohasi **kriptologiya** deb aytiladi. Ushbu so‘z yunoncha «**kripto**» — sirli va **«logus»** — xabar ma’nosini bildiruvchi so‘zlardan iborat. Kriptologiya ikki yo‘nalish, ya’ni **kriptografiya** va **kriptotahlil**dan iborat.

Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta’minlashdan iborat.

Kriptotahlilning vazifasi esa kriptograflar tomonidan ishlab chiqilgan himoya tizimini ochishdan iborat.

Hozirgi kunda **kriptotizim**ni ikki sinfga ajratish mumkin:

• simmetriyali bir kalitlilik (maxfiy kalitli);

• asimmetriyali ikki kalitlilik (ochiq kalitli).

Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

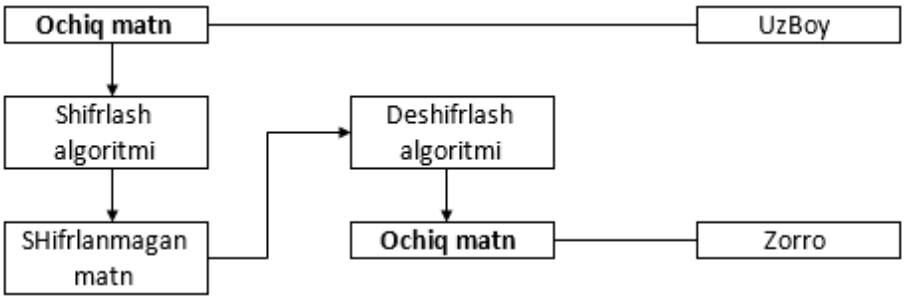
1) Axborot almashuvida ishtirok etuvchilar qanday yo‘l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?

2) Jo‘natilgan xabarning haqiqiyligini qanday aniqlasa bo‘ladi?

Ushbu muammolarning echimi ochiq kalitli tizimlarda o‘z aksini topdi.

Ochiq kalitli asimmetriyali tizimda ikkita kalit qo‘llaniladi. Biridan ikkinchisini hisoblash usullari bilan aniqlab bo‘lmaydi.

Birinchi kalit axborot jo‘natuvchi tomonidan shifrlashda ishlatilsa, ikkinchisi axborotni qabul qiluvchi tomonidan axborotni tiklashda qo‘llaniladi va u sir saqlanishi lozim.



5.1-расм. Маълумотларни шифрлаш ва дешифрлашнинг умумий схемаси

Ushbu usul bilan axborotning maxfiyligini ta’minlash mumkin. Agar birinchi kalit sirli bo‘lsa, u holda uni Elektron imzo sifatida qo‘llash mumkin va bu usul bilan axborotni autentifikatsiyalash, ya’ni axborotning yaxlitligini ta’minlash imkoni paydo bo‘ladi.

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

• foydalanuvchini autentifikatsiyalash, ya’ni kompyuter tizimi zahiralariga kirmoqchi bo‘lgan foydalanuvchini aniqlash:

• tarmoq abonentlari aloqasini o‘rnatish jarayonida ularni o‘zaro autentnfikatsiyalash.

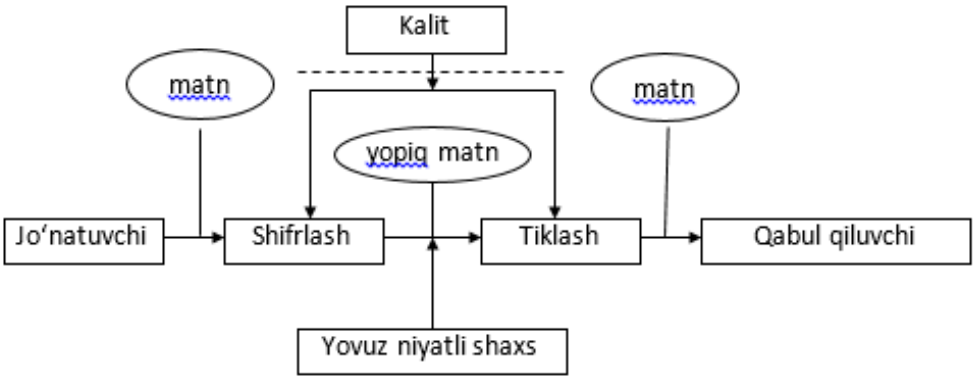
Hozirgi kunda himoyalanishi zarur bo‘lgan yo‘nalishlardan biri bu Elektron to‘lov tizimlari va Internet yordamida amalga oshiriladigan Elektron savdolardir.

Axborotlarni kriptografiyali himoyalash tamoyillari

Kriptografiya — ma’lumotlarni o‘zgartirish usullarining to‘plami bo‘lib, ma’lumotlarni himoyalash bo‘yicha quyidagi ikkita asosiy muammolarni hal qilishga yo‘naltirilgan: **maxfiylik; yaxlitlilik.**

Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o‘zgartira olmaslik haqida dalolat beradi.

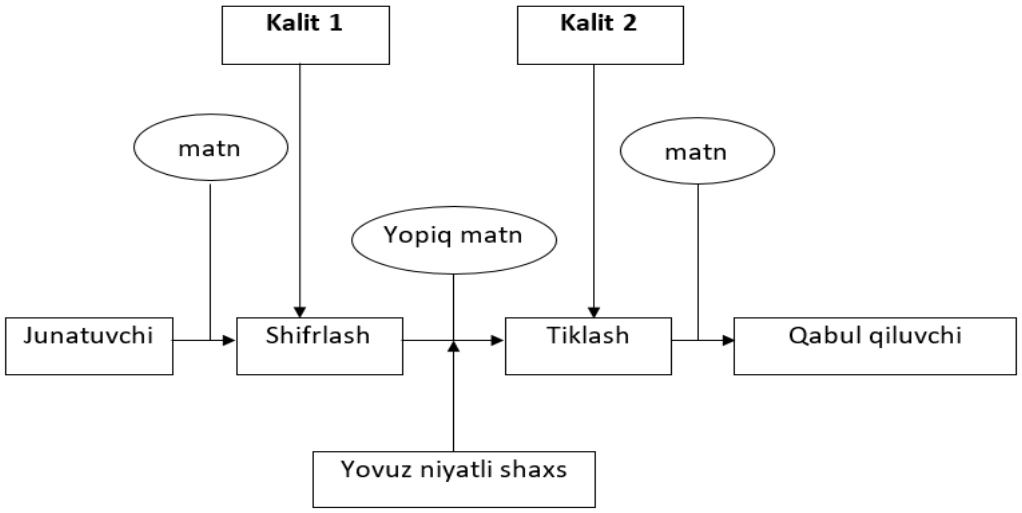
Ushbu kriptografik tizimni sxematik ravishda quyidagicha tasvirlash mumkin:



5.2-расм. Simmetrik kriptografik tizimning sxematik ko’rinishi

Bu erda kalit qandaydir himoyalangan kanal orqali junatiladi (chizmada punktir chiziklar bilan tasvirlangan). Umuman olganda, ushbu mexanizm simmetriyali bir kalitlik tizimiga taalluqlidir.

Assimmetriyali ikki kalitlik kriptografiya tizimini sxematik ravishda quyidagicha tasvirlash mumkin:



5.3-расм. Asimmetrik kriptografik tizimning sxematik ko’rinishi

Bu holda himoyalangan kanal bo‘yicha ochiq kalit jo‘natilib, maxfiy kalit jo‘natilmaydi.

YOvuz niyatli shaxslar uz maqsadlariga erisha olmasa va kriptotaxlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u holda kriptotizim **kriptomustahkam tizim de**b aytiladi.

Kriptotizimning mustaxkamligi uning kaliti bilan aniklanadi va bu kriptotahlilning asosiy qoidalaridan biri bo‘lib hisoblanadi.

Ushbu ta’rifning asosiy ma’nosi shundan iboratki, kriptotizim barchalarga ma’lum tizim hisoblanib, uning o‘zgartirilishi ko‘p vakt va mablag‘ talab qiladi, shu bois ham faqatgina kalitni o‘zgartirib turish bilan axborotni himoyalash talab qilinadi.

6-MAVZU: AXBOROTLARNI HIMOYALASHNING VOSITALARI

MA’RUZA MASHG’ULOTI REJASI:

6.1. Kompyuter ma'lumotlarini himoyalashning texnik vositalari.

6.2. Kompyuter ma'lumotlarini himoyalashning dasturiy vositalari.

6.3. Kompyuter ma'lumotlarini himoyalashning aralash vositalari.

Tayanch so‘z va iboralar. Kompyuter ma'lumotlarini himoyalashning texnik vositalari. Kompyuter ma'lumotlarini himoyalashning dasturiy vositalari. Kompyuter ma'lumotlarini himoyalashning aralash vositalari.

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.

Axborotlarni muhofaza qilishning dasturiy vositalari axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlardir. Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga etarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin.

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.

Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun «tarmoqlararo ekran» (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

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 sub’ektining unikal nomini bir qiymatli tanib olishni bildiradi. Autentifikatsiyalash esa taqdim etilgan nomni ushbu sub’ektga mosligini tasdiqlashni anglatadi (sub’ektning 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 chek-chegarasiz imkoniyatlari mavjudligi. Axborotlarni muhofaza qilishning dasturiy vositalarining kamchiliklariga quyidagilar kiradi:

– himoyalovchi dasturlarning faoliyati kompyuter tizimlari resurslaridan foydalanish hisobiga bo‘lgani uchun bu tizimlar samaradorligining susayishi;

– juda past unumdorlik (xuddi shunday vazifani bajarayotgan apparat vositalar bilan taqqoslaganda, masalan shifrlovchi qurilma);

– axborotlarni himoyalovchi ko‘pgina dasturiy vositalarning kompyuter dasturiy ta’minotiga bevosita o‘rnatilmagani (quyidagi rasmlar), bu holat qoidabuzarning ushbu dasturlarni chetlab o‘tishiga prinsipial imkoniyatlar yaratadi;

– kompyuter tizimlaridan foydalanish jarayonida axborotlarni himoyalashning dasturiy vositalarini qasddan o‘zgartirish imkoniyati.

Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga etarlicha 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 kompyuter tizimlarida tarqalish va o‘zini o‘zi ishlab chiqish xususiyatiga ega bo‘lgan kichik hajmdagi bajariluvchi dasturlar. Viruslar kompyuter tizimlarida 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 kompyuter tizimlari 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:

– kompyuter tizimlarida 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.

Tizimni qayta tiklash virus turiga, uni aniqlangan hamda zararlovchi ta’sirini boshlagan vaqtiga bog‘liq. Viruslar tizimga kirish jarayonida, o‘zini saqlaydigan joydagi ma’lumotlarni o‘chirib yuborsa hamda zararlovchi ta’siri natijasida ma’lumotlarni o‘zgartirish nazarda tutilgan bo‘lsa, zaxiraga olingan ma’lumotlarsiz yo‘qolgan ma’lumotlarni tiklab bo‘lmaydi. Viruslarga qarshi kurashda aniq bir ketma-ketlik va kombinatsiyada qo‘llaniluvchi, viruslarga qarshi kurashish usullarini hosil qiluvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi. Kompyuter tizimining xavfsiz ishlashining asosiy shartlaridan biri, amalda sinovdan o‘tkazilgan va o‘zining yuqori samara berishini ko‘rsatgan bir qator qoidalarga 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 echib olinuvchi tashuvchilarda saqlash kerak. Agar bunday nusxalar echib 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 echib olinadigan axborot tashuvchilardan va yangi fayllardan foydalanilganda ehtiyotkorlikka rioya qilish. YAngi echib 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 echiladigan 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.

Kompyuter tarmog‘idan foydalanish bosqichlarida tizimdagi axborotlarning butunligi va ulardan foydalanish huquqi quyidagilar orqali ta’minlanadi:

– kompyuter tizimlarida mavjud axborotlarning butunligi;

– kompyuter tizimlarining 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.

Axborotning butunligi va foydalanishga qulayligi apparat vositalar zaxirasini yaratish, foydalanuvchilarning xato harakatlarini blokirovka qilish, kompyuter tizimlarining ishonchli elementlaridan va barqaror ishlovchi tizimlardan foydalanish yo‘li bilan amalga oshiriladi. Tizim elementlarini qasddan ortiqcha ishlatish tahdidlari bartaraf etiladi. Buning uchun bajariladigan dasturlarga buyurtmalarni kelib tushish intensivligini o‘lchash mexanizmlaridan va bunday buyurtmalarni berishni cheklash yoki blokirovka qilish mexanizmlaridan foydalaniladi. Bunday hollarda ma’lumotlarni uzatish yoki dasturlarni bajartirishga bo‘lgan buyurtmalar oqimining birdaniga keskin oshib ketishini aniqlash imkoni ham oldindan nazarda tutilgan bo‘lishi kerak. Kompyuter tarmog‘ida axborotlarning butunligi va foydalanishga qulayligini ta’minlashning asosiy shartlaridan biri ularning zaxiralarini hosil qilishdan iborat. Axborotlar zaxirasini yaratish strategiyasi axborotning muhimligini, kompyuter tizimlarining uzluksiz ishlashiga bo‘lgan talablarni, ma’lumotlarni tiklashdagi qiyinchiliklarni hisobga olgan holda tanlanadi. Himoyalangan kompyuter tizimlarida faqatgina ruxsat etilgan dasturiy ta’minotdan foydalanilishi lozim. Foydalanishiga rasman ruxsat etilgan dasturlarning ro‘yxati, ularning butunligini nazorat qilishning usullari va davriyligi kompyuter tizimlarini 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.

7-MAVZU: SIMMETRIYALI KRIPTOTIZIM ASOSLARI
MA'RUZA MASHG'ULOTI REJASI:

7.1. Simmetrik shifrlash algoritmlari.

7.2. Trisemuss va Pleyferning bigrammali shifri.

7.3. Uinstonning 'ikkililangan kvadrat' shifri

7.4. Zamonaviy simmetrik shiflash algoritmlari

Tayanch so'z va iboralar: *Shifrlovchi jadvallar,* Trisemuss shifri, Pleyfer shifri, ikkililangan kvadrat, bigramma haqida tushuncha, AES, DES, Gost 28147-89.

Simmetrik shifrlash algoritmlari- 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.

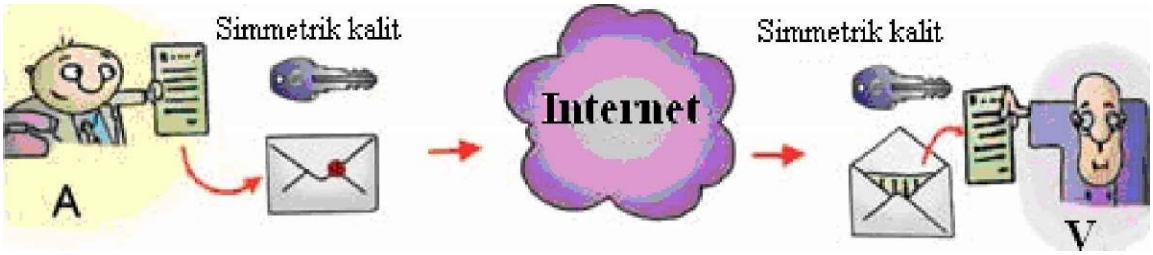
Shifrlashning simmetrik algoritmlari ikki turda bo'ladi. Ulardan biri ochiq matnga bitlar bo'yicha ishlov beradi. Ular *potokli algoritmlar* yoki *potokli shifrlar* deb nomlanadi. Ikkinchisida esa, ochiq matn bir necha bitdan iborat bo'lgan bloklarga bo'linadi. Bunday algoritmlar *blokli algoritmlar* 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.



7.1-rasm. 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.

Kriptosistemada simmetrik kriptografiya ishlatiladi. Xabar jo‘natuvchi va qabul qiluvchi incryption va decryption ikkita bir xil namunali kalit ishlatadi. Kalitlarning ikkita vazifasi bor. Bular incryption va decryptionni ko‘zatish yoki boshqarish bo‘lishi mumkin.

Simmetrik kalitlar maxfiy kalitlar ham deyiladi. Chunki bular foydalanuvchi tomonidan maxfiy va himoyalangan bo‘lishiga asoslangan. Agar buzib kiruvchi kalitlarga ega bo‘lganida u xabarni deshifrlay olardi. Simmetrik incryption kaliti ma’lumot almashuvchi har bir juft foydalanuvchi ikkita bir xil namunali kalitga ega bo‘lishi kerak. Bu shuni bildiradiki, A va B ma’lumot almashishni xoxlasa ularning ikkalasi ham ikkita bir xil kalitga ega bo‘lishi shart. Agar A- B va C bilan ham shu usulda muloqat qilmoqchi bo‘lsa, ularning barida ikkita bir xil kalit bo‘lishi kerak.Bu qisqa vaqt ichida yuzlab do‘stlar bilan muloqat qila olish imkoniyatini kamaytiradi. Kerakli odamga zarur kalitlarni saqlash qiyin vazifa to‘g‘diradi[6].

Agar 10 ta odam bir-biri bilan maxfiy muloqat qilmoqchi bo‘lsa, ularning har biri 45 tadan kalitga ixtiyoj sezadi. Agar bu 100 ta odamni tashkil qilsa, bu ko‘rsatkich 4950 taga yetadi. Bu raqamlarni quyidagi formula bilan topish mumkin[1].

$$N= n *(n-1)/2.$$

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

Trisemussning shifrlash jadvallari. 1508 yil Germaniyalik abbat Iogan Trisemuss

“Poligrafiya” deb nomlanuvchi kitobni yozdi. Bu kitobda birinchi marta taxminiy tartibda alfavit bilan to`ldiruvchi shifrlash jadvallarini qo`llashni tizimli tushuntirib berdi. Bunday shifrni olish uchun alfavit harflarini va kalitli so`zni (yoki iborani) yozish uchun jadvallar qo`llanilgan. Jadvalga qator bo`yicha kalitli so`z kiritiladi, bunda takrorlanuvchi harflar tashlab yuboriladi. So`ngra bu jadval tartib bo`yichaи alfavitning kiritilmagan harflari bilan to`ldiriladi. Kalitli so`z yoki iborani eslab qolish osonligi tufayli bunday yondashuv shifrlash va qayta ochish jarayonini soddalashtirar edi. [15] Bu shifrlashni misolda ko`rib o`tsak. Lotin alifbosi uchun jadval hajmini 6x5 deb olamiz. Kalitli so`z sifatida esa ANZURA so`zini olamiz. Agar kalitli so`zda harflar takrorlansa, navbatdagi takrorlanuvchi harf tashlab yuborilganligi uchun kalit so`z ANZUR ko`rinishni oladi. Kalitli so`z ANZUR ning harflarini jadvalning birinchi qatori, birinchi yacheykasidan boshlab joylashtirishni boshlaymiz.

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

[6] Shon Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

Agar birinchi qator to`lsa, harflarni ikkinchi qatordan boshlab joylashtirishni davom ettiramiz. Kalit so`z kiritilgach, alfavit harflarini boshdan boshlab jadvalga joylashtirishni boshlaymiz. Agar alfavit harfi kalit so`zda mavjud bo`lsa, u tashlab yuboriladi va navbatdagi harfni joylashtirish davom ettiriladi. Qator to`lgach navbatdagi qatordan joylashtirish boshlanadi. Shifrlashda bu jadvaldan ochiq matnni navbatdagi harfi topiladi va shu ustundagi pastda joylashgan harf shifrmatn harfi sifatida yoziladi. Agar matn harfi eng pastki qatorda bo`lsa, shifr matn uchun shu ustunning eng yuqorigi harfi olinadi.

Masalan, shu jadval yordamida quyidagi xabarni shifrlasak:

BIZ BIR JAMOAMIZ

Quyidagi shifr matnini olamiz:

WPE WPG ECVWCVPE

Bu shifr matni deshifrlash uchun jadvaldan shifr matnni navbatdagi harfi topiladi va shu ustundagi yuqorida joylashgan harf matn harfi sifatida yoziladi. Agar matn harfi eng yuqori qatorda bo`lsa, matn uchun shu ustunning eng quyi harfi olinadi.

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

Matn deshifrlansa:

BIZ BIR JAMOAMIZ

Bunday shifrlash jadvallari ko`p grammali deyiladi, chunki shifrlash bir harfdan bajariladi. Trisemuss shifrlash jadvallari ikki harfdan shifrlay olishini birinchilardan bo`lib bilib olgan. Bunday shifrlashlar bigrammali shifrlashlar deyiladi.

Pleyferning bigrammali shifri. Pleyfer shifri 1854 yil ixtiro qilingan bo`lib,almashtirishning eng mashhur bigrammasi hisoblanadi. U birinchi jahon urushida Buyuk Britaniyada qo`llanilgan. Pleyferning shifri asosida birlamchi xabarda taxminiy joylashagan alifbo harflari shifrlovchi jadvali yotadi. [15] Xabarni uzatuvchi va qabul qiluvchi tomonidan shifrlanadigan jadvalni eslab qolish qulayligi uchun kalitli so`z (yoki iborani) jadvalni boshlang’ich qatorlarini to`ldirishda ishlatish mumkin. Umuman olganda Pleyfer shifrlash jadvali strukturasi Trisemussning shifrlash jadvallariga o`xshash. Shuning uchun shifrlash va qayta ochish protseduralarini tushunish maqsadida Pleyfer tizimida oldin ko`rib o`tilgan Trisemuss shifrlash jadvalidan foydalanamiz:

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

Shifrlash protsedurasi quyidagi qadamlarni o`z ichiga oladi:

1. Berilgan xabar ochiq matni harflar jufti (bigramma) ga bo`linadi. Matn juft harflar sonidan iborat bo`lishi va unda ikkita bir xil harfdan bigramma bo`lmasligi kerak. Agar bu shartlar bajarilmasa, matn ba`zi orfografik xatolarga qaramasdan o`zgartiriladi.

2. Ochiq matn ketma – ket bigrammalari shifrlash jadvallari yordamida quyidagi

qoidalar bo`yicha shifr matn bigrammalariga o`tkaziladi:

a. Agar ochiq matn bigrammasining ikkala harfi ham bir qator yoki ustunga joylashmasa (masalan, yuqoridagi jadvaldagi A va F harflari singari) unda aniqlanadigan harflar jufti uchun to`rtburchak burchaklari harfi topiladi. (Bizning misolda bu AF CU harflari AF harflar juftligi CU juftida akslanadi. Shifrmatn bigrammasida harflar ketma-ketligi ochiq matn bigrammasi harflar ketma-

ketligida oynali munosabatda joylashgan bo`lishi kerak).

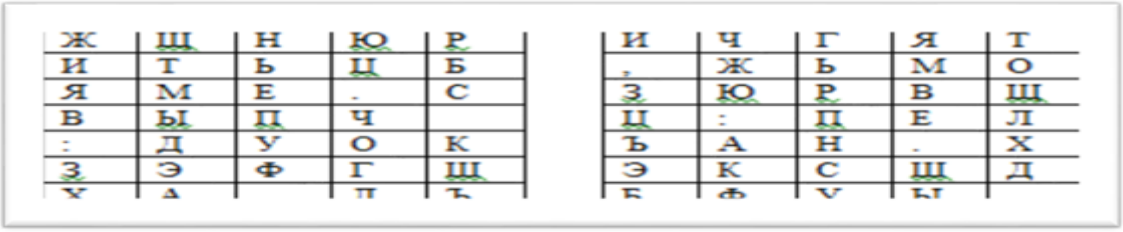
b. Agar ochiq matn bigrammalari harfi jadvalning bir ustunida joylashsa, unda shifr matn harfli deb ular tagida joylashgan harflar olinadi. (Masalan, NJ bigrammasi DQ shifr matnni beradi). Agar bunda ochiq matn harfi quyi qatorda joylashgan bo`lsa, unda shifrmatn uchun shu ustunning yuqori qatori harfi olinadi. (Masalan, IZ bigramma OX shifrmatn bigrammasini beradi).

c. Agar ochiq matnning bigrammasi ikkala harfi bitta qatorda joylashgan bo`lsa, unda shifrmatn harflari sifatida ulardan o`ngda joylashgan harflar olinadi. (Masalan, CV bigramasi UW shifr matn bigrammasini beradi). Agar bunda ochiq matn harfi eng o`ng ustunda joylashgan bo`lsa, shifr uchun shu qatorning chap ustuni harfi olinadi. (masalan, UP bigrammasi TA shifrmatn bigrammasini beradi). Ochishda ya`ni deshifrlashda harakatlar teskari tartibda omalga oshiriladi. Shuni ta`kidlash lozimki, bigrammalar bo`yicha shifrlash shifrlar chidamligini tezkor oshiradi.

Uinstonning ‘ikkililangan kvadrat’ shifri

1854 yil angliyalik Charl’z Uinston bigrammalarni shifrlashning yangi metodini o`ylab topdi va shu tariqa kriptografiya rivojiga o`z hissasini qo`shdi. U polibian shifrga o`xshash bo`lgani uchun ‘ikkilangan kvadrat’ deb nomlanadi. Uinston shifri kriptografiya tarixida yangi bosqichni ochib berdi. Polibian shifridan farqli ravishda ‘ikkilangan kvadrat’ shifrlash usulida ikkita jadvaldan foydalanilgan. Bu jadvallar gorizontal joylashgan bo`lib, shifrlash Pleyfor shifri singari bigrammalar bo`yicha shifrlanadi. Murakkab bo`lmagan modifikatsiyalar orqali qo`lda shifrlash juda qulay bo`lib, kriptografiyada ishonchli yangi kriptografik tizimini dunyoga keltirdi. Bu usul

juda ishonchli bo`lgani uchun undan Germaniyada hattoki ikkinchi jahon urushida ham foydalanilgan. [15] Axborotni shifrlash uchun kirill alfaviti harflari ixtiyoriy joylashgan ikkita jadval olingan.



Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	Щ	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
У	А		П	Ъ

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	Щ	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Shifrlash uchun matn harflarini juft-juft qilib bo`laklarga, ya`ni bigrammalarga bo`lingan. Har bir bigramma alohida shifrlangan. Har bir juft bo`lakning birinchi harfi uchun chap tomondagi birinchi jadvaldan, ikkinchi harf uchun esa o`ng tomondagi ikkinchi jadvaldan foydalanilgan. Shifrlashda juft bo`lakning birinchi harfini chap jadvaldan, ikkinchi harfini esa o`ng jadvaldan olingan. Shifrmatn harflarini olish uchun matn birinchi harfni chap jadvaldan, ikkinchisini esa o`ng jadvaldan topiladi, so`ngra shu harflar burchaklari bo`lgan xayolan to`rtburchak tuziladiki, burchaklarda tursin. Bu to`rtburchakning boshqa burchaklaridagi harflar shifr bigrammani ifodalashadi. Aytaylik, berilgan matnning ИЛ bigrammasi shifrlansin. И harfi birinchi, chap jadvalning 1-ustun va 2-qatorida joylashgan. Л harfi jadvalning 5-ustun va 4-qatorida joylashgan. Bu to`rtburchak 2 va 4 qatorlardan hamda chap jadvalning 1- va o`ng jadvalning 5-ustunidan tuzilgan.

Shunday qilib, shifrmatn bigrammasiga o`ng jadval 5-ustun va 2-qatorida joylashgan O harfi va chap jadval 1-ustun va 4-qatordagi B harflari kiradi. Shunday qilib berilgan matnning ИЛ bigrammasi uchun OB shifrmatn bigrammasini olamiz.

Agar bigrammaning ikkala harfi ham bir qatorda joylashgan bo`lsa, unda shifrmatn harflari ham shu qatordan olinadi. Shifrmatn bigrammasi birinchi harfi chap jadvaldan xabar bigrammasi ikkinchi harfi ustuniga mos bo`lgan harf olinadi. Ikkinchisi esa o`ng jadvaldan xabar bigrammasi birinchi harfi joylashgan ustunga mos harfi olinadi. Shuning uchun TO bigrammasi ЖБ shifrmatn bigrammasiga aylanadi. Xuddi shu tariqa xabar bigrammalari shifrlanadi. Misol. Quyida berilgan xabarni shifrlang:

УИНСТОННИНГ ИККИЛАНГАН КВАДРАТ ШИФРИ

AMALIY MATEMATIKA VA INFORMATIKA

Berilgan xabarni bigrammalarga bo`lamiz (Probel uchun _ belgi qo`yamiz):

УИ НС ТО НН ИН Г_ ИК КИ ЛА НГ АН _К ВА ДР АТ _Ш ИФ РИ

AM AL IY-M AT EM AT IK A- VA –I NF OR MA TI KA

Berilgan xabarga Uitstonning ‘ikkilangan kvadrat’ shifrini qo`llasak quyidagi bigrammali shifrmatnni olamiz.

ЪН ГФ ЖБ ГУ Ь: ДЛ ЖЗ ЪР ФО ГН УД :Ш :: НМ Щ_ ХЖ ТЖ

Bigrammali shifrmatnni birlashtirsak quyidagi oddiy i shifrmatnni olamiz:

ЪНГФЖБГУЬ:ДЛЖЗЪРФОГНУД:Ш::НМЩ_ХЖТЖ

Ochishda ya`ni deshifrlashda harakatlar teskari tartibda omalga oshiriladi. Uitstonning “ikkililan kvadrat” shifrini kirill alfaviti uchun qo`llasak tanlangan jadval yacheykalari soni 35 ta bo`lishi kerak. Chunki unda nuqta, vergul va ikki nuqta singari tinish belgilar ham kiritilgan. Yozuv qatori 30 tadan kam bo`lmasligа kerak, shunda uni ochish uchun juda kata qiyinchiliklar tugdiradi. ‘Ikkilangan kvadrat’ usuli shifrlanishi juda chidamli va qo`llashda sodda shifrlash hisoblanadi.

Keng tarqalgan shifrlash algoritmlari. Axborotni kriptografik himoyalash standartlari, xesh funksiya.

AYES [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‘llanilmoqda7.

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[7].

DES -algoritmi qo‘llashining asosiy sohalari:

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

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

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

tijorat xabarlarni elektron almashinuvida (xaridor, sotuvchi va bank xodimi o‘rtasida

[7] Shon Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

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.

8-MAVZU: ASIMMETRIK KRIPTOTIZIMLAR
MA'RUZA MASHG'ULOTI REJASI:

8.1. Asimmetrik kriptotizimlar va ularning qo'llanilishi.

8.2. Asimmetrik shifrlash algoritmlari.

8.3. Elektron raqamli imzo.

Tayanch so'z va iboralar U. Diffi va M.Ye. Xellman, RSA, EL-Gamal, elektron raqamli imzo

Shifrlash kaliti hamma uchun malum bo'lib, deshifrlash kaliti maxfiy bo'lgan shifrlash tizimlari asimmetrik kriptotizimlar deb atalib, bunday ochik kalitli kriptotizim birinchi marta 1976 yilda U. Diffi va M.Ye. Xellmanning «Kriptografiyada yangi yo'nalish» [1] deb nomlangan maqolasida e'lon qilindi. Bu maqola shu sohadagi ochiq ilmiy ishlarning rivojini juda yuqori pog'onaga ko'tarilishiga sabab bo'ldi. Ular o'zlarining ushbu ishida, maxfiy aloqa tizimlarida ma'lumotlarni shifrlash va deshifrlashda maxfiy kalitning tizim foydalanuvchilari orasida maxsus muhofazalangan aloqa tarmoqlari orqali uzatilishi va qabul qilinishiga hojat bo'lmaydigan ilmiy-amaliy uslub asoslarini yaratib, bugungi kunda ham rivojlanib va dolzarblashib borayotgan *ochiq (maxfiy bo'lmagan) kalitli kriptografiya davrini* boshlab berdi.

Assimmetrik kriptotizimlar matematikaning quyidagi uchta asosiy masalalarining yechilishlarini murakkabligiga asoslangandir[2- 5]:

1. Yetarli darajada katta bo'lgan butun sonni tub ko'paytuvchilarga ajratish.
2. Chekli maydonda diskret logarifmlash.
3. Chekli maydonda chiziqli algebraik tenglamalar sistemasining ildizlarini hisoblash.

Bu keltirilgan har bir masalaning yechilishi bugungi kun hisoblash qurilmalari imkoniyatlaridan to'la foydalanilganda ham murakkab va qiyin bo'lgan yoki umuman yechib bo'lmasligi nazariy jihatdan isbotlangan masalalarga olib keladi.

Mazkur metodik qo'llanmaning maqsadidan kelib chiqib, klassik asimmetrik kriptotizimlar qatoriga kiruvchi:

- **RSA**;
- **EL-Gamal;**
- **Vilyams;**
- **Rabin;**
- **Polig-Xellman;**
- **Mak-Elis**

ochiq kalitli shifrlash algoritmlari, ular asosidagi matematik elementlar va RSA, EL-Gamal elektron raqamli imzo algoritmlari haqida fikr yuritilib, konkret masalalarga qo'llab ko'rsatiladi.

Shu maqsadda avvalo yuqorida keltirilgan algoritmlar bilan bog'liq bo'lgan zarur matematik tushuncha va muhim xossalar haqida to'xtalib o'tamiz.

Asimmetrik kriptotizimlarning asosiy tashkil etuvchi elementlaridan biri yetarlicha katta (150 va undan ortiq xonali) tub sonlardan foydalanishidir.Biz bunday kriptotizimlarda malumotlarni shifrlash va deshifrlash jarayonini amalga oshirish algoritmlarini amaliy qo'llanishlarini taminlash uchun katta razryadli sonlarni tub yoki tub emasligini aniqlab olish usullarini bilishimiz muhim hisoblanadi.

Assimetrik kalitli kriptotizimlarda ma'lumot almashishda ikkita kalitdan foydalaniladi. Ikki har xil assimetrik kalitlar matematik bog'langan. Ularning biri xabarni shifrlash uchun xizmat qilsa,

ikkinchisi esa deshifrlash uchum xizmat qiladi. Ular o‘z navbatida foydalanuvchining ochiq va yopiq kaliti deb ataladi. Ochiq kalit hammaga, yopiq kalit esa foydalanuvchining o‘ziga ma’lum bo‘ladi. Ochiq kalitlar hammaga bir xil yo‘naltirilgan bo‘ladi. Muloqot qiluvchilar uchun doim yaroqli bo‘ladi[8].

Agar kimdir boshqa foydalanuvchining ochiq kalitini topib olsa ham yopiq kalitni topolmasligi kerak. Bu foydalanuvchining ochiq kalitini topgan buzuvchiga matematik usul yordamida uning yopiq kalitini topib bo‘lmasligini bildiradi. Lekin yopiq kalit topilsa, bu katta muommoga sabab bo‘ladi. Shuning uchun kalit egasi o‘z yopiq kalitini har xil uskunalardan saqlash kerak[1].

Agar A foydalanuvchi ma’lumotlarni o‘zining yopiq kaliti bilan shifrlab jo‘natsa, qabul qiluvchi ma’lumotni deshifrlash uchun A foydalanuvchining ochiq kalitiga ega bo‘lishi kerak. Qabul qiluvchi A foydalanuvchining xabarini deshifrlay olishi va o‘ziga shifrlangan holda qaytara olishi kerak. Assimetrik kalitli shifrlash texnologiyasi ishlayotganda bir xil kalit bilan shifrlash va deshifrlash mumkin emas[1].

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. Tabiiyki, Internetda xavfsiz muloqot qilish uchun shifrlash, korrespondentlarning shaxsan uchrashishlari shart bo‘lmagan holatda ma’noga ega. Muammo maxfiy kalitni uzatishda yuzaga keladi. Haqiqatda, agar jo‘natuvchi Ali qabul qiluvchi Valiga kalitni shifrlamasdan uzatsa, kalitni tutib olishlari mumkin. Agar kalit shifrlangan ko‘rinishda jo‘natilsa, unda qabul qiluvchi Vali uni ocha olmaydi. Bir nechta korrespondentlar bilan yozishmalar olib borish uchun, har bir qabul qiluvchi uchun alohida kalitlar bo‘lishi lozim, bu esa noqulaylikni tug‘diradi. 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

Keng tarqalgan shifrlash algoritmlari. Axborotni kriptografik himoyalash standartlari, xesh funksiya.

AYES [encryption standard (AES))] - AQShda ma’lumotlarni shifrlash standarti bo‘lib, simmetrik shifrtizimlarda foydalanish uchun qo‘llanadi. Blok o‘lchami 128 bit, kalit uzunligi 128,

[8] Shon Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

192 yoki 256 bitdan iborat bo‘lgan bazaviy blokli shifrlash algoritmiga asoslagan. 2002-yildan beri amalda qo‘llanilmoqda[9].

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[10].

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 Yeydelman 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 funksiya[10]. 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 xesh- funksiya 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, xesh- funksiyalar 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.

5.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

[9] Shon Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

[10] Ахборот-коммуникация технологиялари изоҳли луғати (иккинчи нашр). - Т., 2010.

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.

3-MODUL. TARMOQ, INTERNET TIZIMI VA ELEKTRON POCHTADA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI

9-MAVZU: Tarmoq himoyasini tashkil etish:
MA'RUZA MASHG'ULOTI REJASI:

9.1. Kompyuter tormoklarining zaif qismlari.

9.2. Tarmoq himoyasini tashkil kilish asoslari.

9.3. Kompyuter telefoniyasidagi himoyalash usullari.

9.4. Kompyuter tarmoqlarida himoyani ta'minlash usullari.

9.5. EHM himoyasini ta'minlashning texnik vositalari.

9.6. Kompyuter tarmoqlarida ma'lumotlarni himoyalashning asosiy yo'nalishlari

Tayanch so'z va iboralar LAN, WAN, Tarmoq himoyasini tashkil kilish, kompyuterlar telefoniyasi.

1. Kompyuter tormoklarining zaif qismlari.

Hozirgi vaktda lokal hisoblash tarmoqari (LAN) va global hisoblash tarmoqlari (WAN) orasidagi farklar yukolib bormokda. Masalan, Netware 4x yoki Vines 4.11. operatsion tizimlari LANning faoliyatini hududiy darajasiga chikarmokda. Bu esa, ya'ni LAN imkoniyatlarining ortishi, ma'lumotlarni himoyalash usullarini yanada takomillashtirishni talab kilmokda.

Himoyalash vositalarini tashkil etishda kuyidagilarni e'tiborga olish lozim:

• tizim bilan alokada bulgan sub'ektlar sonining kupligi, kupgina hollarda esa ba'zi bir foydalanuvchilarning nazoratda bulmasligi;

• foydalanuvchiga zarur bulgan ma'lumotlarning tarmoqda mavjudligi:

• tarmoqlarda turli firmalar ishlab chikargan shaxsiy kompyuterlarning ishlatilishi;

• tarmoq tizimida turli dasturlarning ishlatish imkoniyati;

• tarmoq elementlari turli mamlakatlarda joylashganligi sababli, bu davlatlarga tortilgan aloka kabellarining uzunligi va ularni tulik, nazorat kilishning kariyb mumkin emasligi;

• axborot zaxiralaridan bir vaktning uzida bir kancha foydalanuvchilarning foydalanishi;

• tarmoqqa bir qancha tizimlarning qo'shilishi;

• tarmoqning yengilgina kengayishi, ya'ni tizim chegarasining noanikligi va unda ishlovchilarning kim ekanligining noma'lumligi;

• hujum nuktalarining kupligi;

• tizimga kirishni nazorat kilishning kiyinligi.

Tarmoqni himoyalash zarurligi kuyidagi hollardan kelib chikadi:

• boshka foydalanuvchilar massivlarini ukish;

• kompyuter xotirasida kolib ketgan ma'lumotlarni ukish

himoya choralarini aylanib utib, ma'lumot tashuvchilarni usxalash;

• foydalanuvchi sifatida yashirincha ishlash;

• dasturiy tutgichlarni ishlatish;

• dasturlash tillarining kamchiliklaridan foylalanish; • himoya vositalarini bilib turib ishdan chikarish

• kompyuter viruslarini kiritish va ishlatish.

Tarmoq, muxofazasini tashkil etishda kuyidagilarni e'tiborga olish lozim: · muxofaza tizimining nazorati;

· fayllarga kirishning nazorati;

· tarmoqda ma’lumot uzatishning nazorati; · axborot zaxiralariga kirishning nazorati;
· tarmoq bilan ulangan boshka tapmoklapga ma’lumot tarkalishining nazorati

Tarmoq himoyasini tashkil kilish asoslari

Maxfiy axborotni kayta ishlash uchun kerakli tekshiruvdan utgan kompyuterlarni ishlatish lozim buladi. Muxofaza vositalarining funksional tulik bulishi muxim hisoblanadi. Bunda tizim administratorining ishi va olib borayotgan nazorat katta axamiyatta egadir. Masalan, foydalanuvchilarning tez-tez parollarni almashtirib turishlari va parollarning juda uzunligi ularni aniklashni kiyinlashtiradi. Shuning uchun xam yangi foydalanuvchini kayd etishni cheklash (masalan, fakat ish vaktida yoki fakat ishlayotgan korxonasida) muximdir. Foydalanuvchining xakikiyligini tekshirish uchun teskari aloka kilib turish lozim (masalan, modem yordamida). Axborot zaxiralariga kirish xukukini chegaralash mexanizmini ishlatish va uning ta’sirini LAN ob’ektlariga tulaligicha utkazish mumkin.

Tarmoq, elementlari urtasida utkazilayottan ma’lumotlarni muxofaza etish uchun kuyidagi choralarni kurish kerak:

• ma’lumotlarni aniklab olishga yul kuymaslik;
• axborot almashishni taxlil kilishga yul kuymaslik;
• xabarlarni uzgartirishga yul kuymaslik;
• yashirincha ulanishga yul kuymaslik va bu hollarni tezda aniklash.

Ma’lumotlarni tarmoqda uzatish paytida kriptografik himoyalash usullaridan foydalaniladi, Kayd etish jurnaliga ruxsat etilmagan kirishlar amalga oshirilganligi xakida ma’lumotlar yozilib turilishi kerak. Bu jurnalga kirishni chegaralash xam himoya vositalari yordamida amalga oshirilishi lozim.

Kompyuter tarmogida nazoratni olib borish murakkabligining asosiy sababi — dasturiy ta’minot ustidan nazorat olib borishning murakkabligidir. Bundan tashkari kompyuter viruslarining kupligi xam tarmoqda nazoratni olib borishni kiyinlashtiradi.

Hozirgi vakttacha muxofazalash dasturiy ta’minoti xilma-xil bulsa xam, operatsion tizimlar zaruriy muxofazaning kerakli darajasini ta’minlamas edi. Netware 4.1, Windows NT operatsion tizimlari yetarli darajada muxofazani ta’minlay olishi mumkin.

Kompyuter telefoniyasidagi himoyalash usullari

Elektron kommunikatsiyalarning zamonaviy texnologiyalari keyingi paytlarda ishbilarmonlarga aloka kanallari buyicha axborotning turlicha kurinishlari (masalan: faks, video, kompyuterli, nutkli axborotlar)ni uzatishda kupgina imkoniyatlar yaratib bermokda.

Zamonaviy ofis bugungi kunda aloka vositalari va tashkiliy texnika bilan xaddan tashkari tuldirib yuborilgan va ularga telefon, faks, avtojavob apparati, modem, skaner, shaxsiy kompyuter va x.k. kiradi. Zamonaviy texnika uchun axborot-kommunikatsiyalar texnologiyasi — **kompyuterlar telefoniyasi** rivojlanishi bilan katta turtki berildi.

Bor-yugi un yil ilgari sotuvga CANON firmasining narxi 6000 AKSh dollari bulgan «Navigator» nomli maxsuloti chikarilgan edi va u birinchi tizimlardan hisoblanadi

Kompyuter tslefoniyasi un yil ichida juda tez sur’atlar bilan rivojlandi. Hozirgi paytda sotuvda mavjud bulgan «PC Phone» (Export Industries Ltd, Israel) maxsulotining narxi bor-yugi 1000 Germaniya markasi turadi. «Powertine-II» (Talking Technology, USA)ning narxi esa 800 AQSh dollari turadi. Keyingi paytlarda kompyuter telefoniyasi yo’nalishida 70% apparat vositalarini Dialogue (USA) firmasi ishlab chikarmokda.

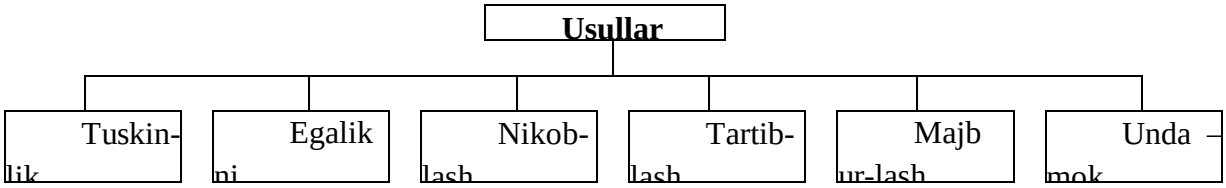
Kompyuter telefoniyasida axborotlarning xavfsizligini ta’minlash katta axamiyatga ega. Masalan, telefon xakerlarining Skotland-Yard ATSiga kirib 1,5 mln, AKSh dollari mikdorida zarar keltirishganligi xavfsizlikning zarurligini isbotlaydi.

Kompyuter telefoniyasida kullanilayotgan nutkini aniklovchi texnologiya telefon kiluvchining ovozidan tanib olish uchun axamiyatga egadir. Kompyuter telefoniyasining himoyasini yetarli darajada ta’minlash uchun Pretty Good Privacy Inc. firmasining PC Phone 1.0 dasturiy paket ishlab chikarilgan. U kompyuter telefoniyasi orkali uzatilayottan axborotlarni himoyalash uchun axborotlarni rakamli kurinishga utkazadi va kabul paytida esa dasturiy-texnik vositalar yordamida kayta ishlaydi. Zamonaviy kompyuter telefoniyasi vositatarining shifrlash tezliga xam juda yukoridir, xato kilish extimoli esa juda kichikdir (taxminan $10^{-8} – 10^{-12}$).

Kompyuter tarmoqlarida himoyani ta’minlash usullari

Kompyuter tarmoqlarida axborotni himoyalash deb foydalanuvchilarni ruxsatsiz tarmoq, elementlari va zaxiralariga egalik kilishni man etishdagi texnik, dasturiy va kriptografik usul va vositalar, xamda tashkiliy tadbirlarga aytiladi.

Bevosita telekommunikatsiya kanallarida axborot xavfsizligini ta’minlash usul va vositalarini kuyidagicha tasniflash mumkin



Yukorida keltirilgan usullarni kuyidagicha ta’riflash kabul kilingan.

Tuskinlik apparatlarga, malumot tashuvchilarga va boshkalarga kirishga fizikaviy usullar bilan **karshilik kursatish** deb aytiladi.

Egalikni boshkarish — tizim zaxiralari bilan ishlashni tartibga solish usulidir. Ushbu usul kuyidagi funksiyalardan iborat:

- tizimning xar bir ob’ektini, elementini ndentifikatsiyalash, masalan, foydalanuvchilarni;
- identifikatsiya buyicha ob’ektni yoki sub’ektni xakikiy, asl ekanligini aniklash;
- vakolatlarni tekshirish, ya’ni tanlangan ish tartibi buyicha (reglament) xafga kunini, kunlik soatni, talab kilinadigan zaxiralarni kullash mumkinligini tekshirish;
- kabul kilingan reglament buyicha ishlash sharoitlarini yaratish va ishlashga ruxsat berish;
- himoyalangan zaxiralarga kilingan murojaatlarni kayd kilish;
- ruxsatsiz xarakatlarga javob berish, masalan, signal berish, uchirib kuyish surovnomani bajarishdan voz kechish va boshkalar.

Nikoblash – ma’lumotlarni ukib olishni kiyinlashtirish maksadida ularni kriptografiya orkali kodlash.

Tartiblash — ma’lumotlar bilan ishlashda shunday shart-sharoitlar yaratiladiki, ruxsatsiz tizimga kirib olish extimoli kamaytiriladi.

Majburlash – kabul kilingan koidalarga asosan ma’lumotlarni kayta ishlash, aks xolda foydalanuvchilar moddiy, ma’muriy va jinoiy jazolanadilar.

Undamok — axlokiy va odobiy koidalarga binoan kabul kilingan tartiblarni bajarishga yunaltirilgan.

Yukorida keltirilgan usullarni amalga oshirishda kuyidagicha tasniflangan vositalarni tadbik etishadi.

Rasmiy vositalar — shaxslarni ishtirokisiz axborotlarni himoyalash funksiyalarini bajaradigan vositalardir

Norasmiy vositilar — bevosita shaxslarni faoliyati yoki uning faoliyatini aniklab beruvchi reglamentlardir.

Texnikavny vositalar sifatida elektr, elektromexanik va elektron kurilmalar tushuniladi. Texnikaviy vositalar uz navbatida, fizikaviy va apparatli bulishi mumkin.

Apparat-texnik vositalari deb telekommunikatsiya kurilmalariga kiritilgan yoki u bilan interfeys orkali ulangan kurilmalarga aytiladi. Masalan, ma'lumotlarni nazorat kilishning juftlik chizmasi, ya'ni junatiladigan ma'lumot yulda buzib talkin etilishini aniklashda kullaniladigan nazorat bulib, avtomatik ravishda ish sonining juftligini (nazorat razryadi bilan birgalikda) tekshiradi.

Fizikaviy texnik vositalar — bu avtonom xolda ishlaydigan kurilma va tizimlardir. Masalan, oddiy eshik kulflari, derazada urnatilgan temir panjaralar, kuriklash elektr uskunalari fizikaviy texnik vositalarga kiradi.

Dasturiy vositalar – bu axborotlarni himoyalash funksiyalarini bajarish uchun muljallangan maxsus dasturiy ta'minotdir. Axborotlarni himoyalashda birinchi navbatda eng keng kullanilgan dasturiy vositalar Hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parol tizimini keltirish mumkin.

Tashkiliy himoyalash vositalari — bu talekommunikatsiya uskunalarining yaratilishi va kullanishi jarayonida kabul kilingan tashkiliy-texnikaviy va tashkiliy-xukukiy tadbirlardir. Bunga bevosita misol sifatida kuyidagi jarayonlarni keltirish mumkin: binolarning kurilishi, tizimni loyixalash, kurilmalarni urnatish, tekshirish va ishga tushirish.

Axlokiy va odobiy himoyalash vositalari — bu hisoblash texnikasini rivojlanishi okibatida paydo buladigan tartib va kelishuvlardir. Ushbu tartiblar konun darajasida bulmasada, uni tan olmaslik foydalanuvchilarni obrusiga ziyon yetkazishi mumkin.

Konuniy himoyalash vositalari — bu davlat tomonidan ishlab chikilgan xukukiy xujjatlar sanaladi. Ular bsvosita axborotlardan foydalanish, kayta ishlash va uzatishni tartiblashtiradi va ushbu koidalarni buzuvchilarning mas'uliyatlarini aniklab beradi.

Masalan, Uzbekiston Respublikasi Markaziy banki tomonidan ishlab chikilgan koidalarida axborotni himoyalash guruzlarini tashkil kilish, ularning vakolatlari, majburiyatlari va javobgarliklari anik yoritib berilgan.

Xavfsizlikni taminlash usullari va vositalarining rivojlanishini uch boskichga ajratish mumkin: 1) dasturiy vositalarni rivojlantirish; 2) barcha yo'nalishlar buyicha rivojlanishi; 3) ushbu boskichda kuyidagi yo'nalishlar buyicha rivojlanishlar kuzatilmokda:

- himoyalash funksiyalarini apparatli amalga oshirish;
- bir necha himoyalash funksiyalarini kamrab olgan vositalarni yaratish; -

algoritm va texnikaviy vositalarni umumlashtirish va standartlash.

Bevosita tarmoq buyicha uzatiladigan ma'lumotlarni himoyalash maksadida kuyidagi tadbirlarni bajarish lozim buladi:

- uzatiladigan ma'lumotlarni ochib ukishdan saklanish;
- uzatiladigan ma'lumotlarni taxtil kiliщdan saklanish;
- uzatiladigan ma'lumotlarni uzgartirishga yul kuymaslik va uzgartirishga urinishlarni aniklash;
- ma'lumotlarni uzatish maksadida kullaniladigan dasturiy uzilishlarni aniklashga yul kuymaslik;

- firibgar ulanishlarning oldini olish.

Ushbu tadbirlarni amalga oshirishda asosan kriptografik usullar kullaniladi.

EXM himoyasini ta’minlashning texnik vositalari

Kompyuter orkali sodir etidadigan jinoyatlar okibatida fakatgina AKSh xar yili 100 mlrd. dollar zarar kuradi. Urtacha xar bir jinoyatda 430 ming dollar ugirlanadi va jinoyatchini kidirib topish extimoli 0,004% ni tashkil etadi.

Mutaxassislarning fikricha ushbu jinoyatlarni 80%i bevosita korxonada ishlaydigan xodimlar tomonidan amalga oshiriladi.

Sodir etiladigan jinoyatlarning taxlili kuyidagi xulosalarni beradi:

kupgina hisoblash tarmoqlarida foydalanuvchi istalgan ishchi urindan tarmoqda ulanib faoliyat kursatishi mumkin. Natijada jinoyatchi bajargan ishlarni kaysi kompyuterdan amalga oshirilganini aniklash kiyin buladi.

• ugirlash natijasida xech nima yukolmaydi, shu bois kupincha jinoiy ish yuritilmaydi; • ma’lumotlarga nisbatan mulkchilik xususiyati yukligi;

• ma’lumotlarni kayta ishlash jarayonida yul kuyilgan xatolik uz vaktida kuzatilmaydi va tuzatilmaydi, natijada kelgusida sodir buladigan xatolarning oldini olib bulmaydi;

• sodir etiladigan kompyuter jinoyatlari uz vaktida e’lon kilinmaydi, buning sababi hisoblash tarmoqlarida kamchiliklar mavjudligini boshka xodimlardan yashirish hisoblanadi.

Ushbu kamchiliklarni bartaraf kilishda va kompyuter jinoyatlarini kamaytirishda kuyidagi chora-tadbirlarni utkazish kerak buladi:

• personal masuliyatini oshirish:

• ishga kabul kilinadigan xodimlarni tekshiruvdan utkazish; • muxim vazifani bajaruvchi xodimlarni almashtirib turish;

• parol va foydalanuvchilarni kayd kilishni yaxshi yulga kuyish; • ma’lumotlarga egalik kiilishni cheklash;

• ma’lumotlarni shifrlash.

Axborot-kommunikatsiyalar texnologiyalarining rivojlanishi okibatida kupgina axborotni himoyalash instrumental vositalari ishlab chikilgan. Ular dasturiy, dasturiy-texnik va texnik vositalardir.

Hozirgi kunda tarmoq xavfsizligini ta’minlash maksadida ishlab chikilgan texnikaviy vositalarni kuyidagicha tasniflash mumkin:

Fizikaviy himoyalash vositalari — maxsus elektron kurilmalar yordamida ma’lumotlarga egalik kilishni takiklash vositalaridir.

Mantikiy himoyalash — dasturiy vositalar bilan ma’lumotlarga egalik kilishni takiklash uchun kullaniladi.

Tarmoqlararo ekranlar va shlyuzlar — tizimga keladigan xamda undan chikadigan ma’lumotlarni ma’lum hujumlar bilan tekshirib boradi va protokollashtiradi.

Xavfsizlikni auditlash tizimlari — joriy etilgan operatsion tizimdan urnatilgan parametrlarni zaifligini kidirishda kullaniladigan tizimdir.

Real vaktda ishlaydigan xavfsizlik tizimi — doimiy ravishda tarmoqning xavfsizligini taxlillash va auditlashni ta’minlaydi.

Stoxastik testlarni tashkillashtirish vositalari — axborot tizimlarining sifati va ishonchliligini tekshirishda kullaniladigan vositadir.

Anik yunaltirilgan testlar — axborot-kommunikatsiyalar texnologiyalarining sifati va ishonchliligini tekshirishda kullaniladi.

Xavflarni imitatsiya kilish — axborot tizimlariga nisbatan xavflar yaratiladi va himoyaning samaradorligi aniklanadi.

Statistik taxlilgichlar — dasturlarning tuzilish tarkibidagi kamchiliklarni aniklash, dasturlar kodida aniklanmagan kirish va chikish nuktalarini topish, dasturdagi uzgaruvchilarni tugri aniklanganligini va kuzda tutilmagan ishlarni bajaruvchi kism dasturlarini aniklashda foydalaniladi.

Dinamik taxlilgichlar — bajariladigan dasturlarni kuzatib borish va tizimda sodir buladigan uzgarishlarni aniklashda kullaniladi.

Tarmoqning zaifligini aniklash — tarmoq zaxiralariga sun'iy hujumlarni tashkil kilish bilan mavjud zaifliklarni aniklashda kullaniladi.

Misol sifitida kuyidagi vositalarni keltirish mumkin:

• Dallas Lock for Administrator — mavjud elektron Proximity uskunasi asosida yaratilgan dasturiy-texnik vosita bulib, bevosita ma'lumotlarga ruxsatsiz kirishni nazorat kilishda kullaniladi

Security Administrator Tool for ANALYZING Networks (SATAN) — dasturiy ta'minot bulib, bevosita tarmoqning zaif tomonlarini aniklaydi va ularni bartaraf etish yullarini kursatib beradi. Ushbu yo'nalish buyicha bir necha dasturlar ishlab chikilgan, masalan: Internet Security Scanner, Net Scanner, Internet Scanner va boshkalar.

• NBS tizimi — dasturiy-texnik vosita bulib, aloka kanallaridagi ma'lumotlarni himoyalashda kullaniladi;

• Free Space Communication System — tarmoqda ma'lumotlarning xar xil nurlar orkali, masalan lazerli nurlar orkali almashuvini ta'minlaydi;

• SDS tizimi — ushbu dasturiy tizim ma'lumotlarini nazorat kiladi va kaydnomada aks ettiradi. Asosiy vazifasi ma'lumotlarni uzatish vositalariga ruxsatsiz kirishni nazorat kilishdir;

• Timekey — dasturiy-texnik uskunadir, bevosita EXMning parallel portiga urnatiladi va dasturlarni belgilangan vaktda keng kullalilishini takiklaydi;

• IDX — dasturiy-texnik vosita, foydalanuvchining barmok, izlarini «ukib olish» va uni taxlil kiluvchi texnikalardan iborat bulib, yukori sifatli axborot xavfsizligini ta'minlaydi. Barmok izlarini ukib olish va xotirada saklash uchun 1 minutgacha, uni takkoslash uchun esa 6 sekundgacha vakt talab kilinadi.

Kompyuter tarmoqlarida ma'lumotlarni himoyalashning asosiy yo'nalishlari Axborotlarni himoyalashning mavjud usul va vositalari xamda kompyuter tarmoqlari kanallaridagi alokaning xavfsizligini ta'minlash texnologiyasi evolyutsiyasini solishtirish shuni kursatmokdaki, bu texnologiya rivojlanishining birinchi boskichida dasturiy vositalar afzal topildi va rivojlanishga ega buldi, ikkinchi boskichida himoyaning xamma asosiy usullari va vositalari intensiv rivojlanishi bilan xarakterlandi, uchinchi boskichida esa kuyidagi tendensiyalar ravshan bulmokda:

- axborotlarni himoyalash asosiy funksiyalarining texnik jihatdan amalga oshirilishi;
- bir nechta xavfsizlik funksiyalarini bajaruvchi himoyalashning birgalikdagi vositalarini yaratish:
- algoritm va texnik vositalarni unifikatsiya kilish va standartlashtirish.

Kompyuter tarmoqlarida xavfsizlikni taminlashda hujumlar yukori darajada malakaga ega bulgan mutaxassislar tomonidan amalga oshirilishini doim esda tutish lozim. Bunda ularning xarakat modellaridan doimo ustun turuvchi modellar yaratish talab etiladi. Bundan tashkari, avtomatlashtirilgan axborot tizimlarida personal eng ta'sirchan kismlardan biridir. Shuning uchun,

yovuz niyatli shaxsga axborot tizimi personalidan foydalana olmaslik chora-tadbirlarini o’tkazib turish ham katta ahamiyatga ega

10-MAVZU: INTERNET TARMOG'I HIMOYASINI TASHKIL ETISH

MA'RUZA MASHG'ULOTI REJASI:

10.1. Axborot xavfsizligi muammosi
10.2. Fakt va raqamlar
10.3. Axborot xavfsizligini ta'minlash yo'nalishlari
10.4. Amaliy tavsiyalar

Tayanch so'z va iboralar FedCIRC, NIST, Axborot o'g'irlash.

Axborot xavfsizligi muammosi

Internet texnologiyalarining yaratilishi turli manbalardan tez va oson yo'l bilan axborot olish imkoniyatlarini hamma uchun-oddiy fuqarodan tortib yirik tashkilotlargacha misli ko'rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta'lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib-saqlay boshladilar. Bu muhit avvalgi fizikaviy saqlashga nisbatan katta qulayliklar tug'diradi: saqlash juda ixcham, uzatish esa bir onda yuz beradi va tarmoq orqali boy ma'lumotlar bazalariga murojaat qilish imkoniyatlari juda keng. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko'payishiga olib keldi. Biznes qator tijorat sohalarida bugun axborotni o'zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo'lgan axborot haqida gap borganda o'ta ijobiy hodisa. Lekin pinhona(konfidentsial) va maxfiy axborot oqimlari uchun Internet texnologiyalari qulayliklar bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi:

- Axborot o'g'irlash
- Axborot mazmunini buzib qo'yish, egasidan iznsiz o'zgartirib qo'yish
- Tarmoqqa va serverlarga o'g'rincha suqulib kirish

Tarmoqqa tajovuz qilish: avval qo'lga kiritilgan transaktsiya(amallarning yaxlit ketma-ketligi)larni qayta yuborish, "xizmatdan yo axborotga daxldorlikdan bo'yin tovlash" , jo'natmalarni ruxsat berilmagan yo'l orqali yo'naltirish.

Axborot xavfsizligini ta'minlash quyidagi uch asosiy muammoni yechishni nazarda tutadi. Bular:

- **Pinhonalik(Confidentiality)**
- **Butunlik(Integrity)**
- **Qobillik(Availability)**

2. Fakt va raqamlar.

AQSH dagi kompyuter xavfsizligi instituti va FBR tomonidan kompyuter jinoyatlari bo'yicha 1999 yilda o'tkazilgan so'rov natijalariga ko'ra so'rovda qatnashgan tashkilotlarning 57 foyizi Internet bilan ulanish joyi "ko'pincha tajovuzlar tashkil etiladigan joy" deb, 30 foyizi ularning tarmog'iga suqulib kirish yuz berganini, 26 foyizi esa tajovuz vaqtida pinhona axborotni o'g'irlash sodir bo'lganini ma'lum qilishgan. ***AQSH kompyuter jinoyatlariga qarshi kurash Federal markazi*** - FedCIRC ma'lumotlariga ko'ra 1998 yilda 1100000 kompyuterli 130000 ga yaqin davlat tarmoqlari tajovuzga duchor bo'lgan.

"Kompyuter tajovuzi" deganda kishilar tomonidan kompyuterga beruxsat kirish uchun maxsus dasturni ishga tushirishni nazarda tutiladi. Bunday tajovuzlarni tashkil etish shakllari har xil. Ular quyidagi turlarga bo'linadi

• Kompyuterga olisdan kirish: Internet yoki Internetga kimligini bildirmay kirishga imkon beruvchi dasturlar

• O'zi ishlab turgan kompyuterga kirish: kompyuterga kimligini bildirmay kirish dasturlari asosida.

• Kompyuterni olisdan turib ishlatmay qo'yish: Internet (yo tarmoq) orqali olisdan kompyuterga ulanib, uning yoki uni ayrim dasturlarining ishlashini to'xtatib qo'yuvchi dasturlar asosida(ishlatib yuborish uchun kompyuterni qayta ishga solish yetarli).

• O'zi ishlab turgan kompyuterni ishlatmay qo'yish: ishlatmay qo'yuvchi dasturlar vositasida.

• Tarmoq skanerlari: tarmoqda ishlayotgan kompyuter va dasturlardan qay biri tajovuzga chidamsizligini aniqlash maqsadida tarmoq haqiqatda axborot yig'uvchi dasturlar vositasida.

• Dasturlarning tajovuzga bo'sh joylarini topish: Internetdagi kompyuterlarning katta guruhlari orasidan tajovuzga bardoshsizlarini izlab qarab chiquvchi dasturlar vositasida.

• Parol ochish: parollar fayllaridan oson topiladigan parollarni izlovchi dasturlar vositasida.

• Tarmoq tahlilchilari (snifferlar): tarmoq trafikini tinglovchi dasturlar vositasida. Ularda foydalanuvchilarning nomlarini, parollarini, kredit kartalari nomerlarini trafikdan avtomatik tarzda ajratib olish imkoniyati mavjud.

Eng ko'p yuz beradigan tajovuzlar quyidagi statistikaga ega:

1998 yili NIST tomonidan o'tkazilgan 237 kompyuter tajovuzining tahlili **Internetda e'lon qilingan**:

• 29 % tajovuzlar Windows muhitida yuz bergan.

Saboq: Faqat Unixgina xatarli emas ekan.

• 20% tajovuzlarda tajovuz qilganlar olisdan turib tarmoq elementlari(marshrutlovchilar, kommutatorlar, xostlar, printerlari brandmauer) gacha yetib borganlar.

Saboq: xostlarga olisdan turib bildirmay kirish bot-bot yuz beradi.

• **5% tajovuzlar marshrutlovchilarga va brandmauerlarga qarshi muvaffaqiyatli bo'lgan.**

Saboq: Internet tarmoq infrastrukturasi tashkil etuvchilarining kompyuter tajovuzlariga bardoshi yetarli emas.

• 4% tajovuzlarda Internetda tajovuzga bardoshi bo'sh xostlarni topish uchun uyushtirilgan.

Saboq: Tizim administratorlarining o'zlari o'z xostlarini muntazam skanerlab turganlari ma'qul.

• 3% tajovuzlar web-saytlar tomonidan o'z foydalanuvchilariga qarshi uyushtirilgan.

Saboq WWWda axborot izlash xavfsiz emas.

Internetda 1999 y. mart oyida eng ommaviy bo'lgan kompyuter tajovuzlari . Sendmail(eng eski dastur), ICQ(murakkab "Sizni izlayman"dasturi, undan 26 millionga yaqin kishi foydalanadi), Smurf(ping- paketlar bilan ishlaydigan dastur), Teardrop(xatolarga sezgir dastur), IMAP(pochta dasturi), Back Orifice(troyan ot, Windows 95/98ni olisdan boshqarish uchun), Netbus(Back Orifice ga o'xshash), WinNuke (Windows 95ni to'la to'xtatib qo'yaoladi)i Nmap(skanerlovchi dastur) bilan bo'lgan.

WinNuke, Papa Smurf i Teardrop dasturlari vositasida niyati buzuq kimsalar sizning kompyuteringizga tajovuz qilib ziyon yetkazishlari mumkin.

3. Axborot xavfsizligini ta'minlash yo'nalishlari

NIST 7498-2 xalqaro standarti asosiy xavfsizlik xizmatlarini belgilaydi. Uning vazifasiga ochiq tizimlar aloqasi modelining xavfsizlik yo’nalishlarini aniqlash kiradi. Bular:

• Autentifikatsiya. Kompyuter yo tarmoq foydalanuvchisining shaxsini tekshirish;

- Kirishni boshqarish(Access control). Kompyuter tarmog‘idan foydalanuvchining ruxsat etilgan kirishini tekshirish va ta’minlash;
- Ma’lumotlar butunligi. Ma’lumotlar massivi mazmunini tasodifiy yo qasddan beruxsat usullar bilan o‘zgartirishlarga nisbatan tekshirish;
- Axborot pinhonaligi. Axborot mazmunini iznsiz oshkor bo‘lishdan himoyalash
- Inkor eta olinmaslik(Neoproverjimost). Ma’lumotlar massivini jo‘natuvchi tomonidan uni jo‘natganligini yoki oluvchi tomonidan uni olganligini tan olishdan bo‘yin tovlashining oldini olish.

Ko‘plab qo‘shimcha xizmatlar (audit, kirishni ta’minlash) va qo‘llab-quvvatlash xizmatlari (kalitlarni boshqarish, xavfsizlikni ta’minlash, tarmoqni boshqarish) mazkur asosiy xavfsizlik tizimini to‘ldirishga xizmat qiladi. Web tugunining to‘la xavfsizlik tizimi barcha yuqorida keltirilgan xavfsizlik yo’nalishlarini qamrab olgan bo’lishi shart. Bunda tegishli xavfsizlik vositalari (mexanizmlari) dasturiy mahsulotlar tarkibiga kiritilgan bo‘lishi lozim.

Autentifikatsiyalashni takomillashtirish qayta ishlatiladigan parollarga xos kamchiliklarni bartaraf etishni, shu maqsadda bir martagina ishlatiladigan parol tizimidan tortib identifikatsiyalashning yuqori texnologik biometrik tizimlarigacha qo‘llashni nazarda tutadi. Foydalanuvchilar o‘zlari bilan olib yuradigan predmetlar, masalan, maxsus kartochkalar, maxsus jeton yoki disketa ancha arzon ham xavfsiz. Noyob, modul kodi himoyalangan dastur moduli ham bu maqsadlarda qulay.

Oshkor kalitlar infratuzilmasi ham Web – tugun xavfsizligining ajralmas qismi. Autentifikatsiya, ma’lumot butunligi va axborot pinhonaligi(konfidentsialligi)ni ta’minlash uchun ishlatiladigan taqsimlashga n tizim(odamlar, kompyuterlar), Ochiq kalit infrastrukturali (sertifikat nashrchisi) elektron sertifikatni e’lon qiladi.

Unda foydalanuvchi identifikatori, uning ochiq kaliti, xavfsizlik tizimi uchun qandaydir qo‘shimcha axborot va sertifikat nashr etuvchisining raqamli imzosi bor.

Ideal variantda bu tizim Yer yuzining har qanday ikki nuqtasidagi foydalanuvchi uchun sertifikatlar zanjirini tuzib beradi. Bu zanjircha kimgadir maxfiy xatni imzolash, hisob bo‘yicha pul o‘tkazish yoki elektron kontrakt tuzish uchun, boshqa kishi uchun – hujjat manbaini va imzolovchi shaxsning aslini tekshirib bilish imkonini beradi. NIST bir necha boshqa tashkilotlar bilan bu yo‘nalishda ish olib bormoqda.

Internetga ulangan tarmoqlar xakerlarning tajovuzi tufayli ochiq muloqotga xalal bersa xam brandmauerlar o‘rnatib oldilar.

PGP ga o‘xshash mukammal dasturlar bo‘lmaganda ochiq tarmoq bo‘lishi ham mumkin bo‘lmas edi.

4. Amaliy tavsiyalar

Tarmoqni kompyuter tajovuzlaridan himoyalash doimiy va o'z-o'zidan yechilmaydigan masaladir. Lekin qator oddiy himoya vositalari yordamida tarmoqqa suqulib kirishlarning ko'pchiligini oldini olish mumkin. Masalan yaxshi konfiguratsiyalangan tarmoqlararo ekran va harbir ish stantsiyalari(kompyuterlar)da o'rnatilgan virusga qarshi dasturlar ko'pchilik kompyuter tajovuzlarini barbod etadi.

Quyida **Internetni himoyalash bo'yicha 14 amaliy tavsiya bayon etilgan**.

1. **Xavfsizlik siyosati lo'nda va aniq qo'yilishi lozim**. Internet tarmog‘i xavfsizligi bo‘yicha yorqin va sobit qadamlik bilan qo‘yilisini ta'minlaydigan qoidalar va amallar bo’lishi lozim. Tarmoq xavfsizligi tizimi uning eng bo'sh joyi qanchalik kuchli himoyalangan bo'lsa shu qadar kuchlidir. Agar bir tashkilot doirasida turli xavfsizlik siyosatlariga ega bo'lgan bir necha tarmoq mavjud bo'lsa bir tarmoq boshqa tarmoqning yomon xavfsizligi tufayli obro'sini yo'qotishi mumkin.

Tashkilotlar shunday xavfsizlik siyosatini qabul qilishlari lozimki, kutilgan himoya darajasi hamma yerda bir xil amalga oshsin. Siyosatning eng ahamiyatli tomoni brandmauerlar orqali o'tkaziladigan trafiklarga yagona talab ishlab chiqilishidir. Shuningdek siyosat tarmoqda qaysi himoya vositalari (masalan, tajovuzlarni payqash vositalarimi yoki qaltis joylar skanerlarimi)va ular qanaqa ishlatilishi lozimligini belgilashi, yagona xavfsizlik darajasiga erishish uchun kompyuterlarning har xil turlari uchun standart xavfsiz konfiguratsiyalar belgilanishi shart.

2. **Brandmauer (Tarmoqlararo ekran, inglizcha-firewalls,) qo'llash lozim.** Bu tashkilotning eng asosiy himoya vositasidir. Tarmoqqa kiruvchi, undan chiquvchi trafik(axborot oqimi)ni nazorat qiladi. U trafikning biror turini to'sib qo'yishi yo tekshirib turishi mumkin. Yaxshi konfiguratsiyalangan bradmauer kompyuter tajovuzlarining ko'pchiligini qaytarishi mumkin. brandmauerlar, intellektual kartalar va boshqa texnikaviy-dasturiy himoya vositalaridan oqilona foydalanish lozim.

3. **Brandmauer va WWW-serverlarni ularning ishini to'xtatib qo'yish tahdidlariga qarshi bardoshliligini testdan o'tkazib turish lozim.** Internetda kompyuterning ishini to'xtatib qo'yishga yo'naltirilgan tajovuzlar tarqalgan. Tajovuzkorlar doimo WWW-saytlarni ishdan chiqaradilar, kompyuterlarni ortiq vazifalar bilan yuklab qo'yadilar yoki tarmoqlarni ma'nosiz paketlar bilan to'ldirib tashlaydilar. Bu turdagi tajovuzlar juda jiddiy bo'lishi mumkin, ayniqsa tajovuzkor davomli tajovuzlarni uyushtirish darajasida aqlli bo'lsa. Chunki buning manbaini topib bo'lmaydi. Xavfsizligi haqida qayg'iruvchi tarmoqlar bunday tajovuzlardan ko'riladigan zararni chamalab ko'rish uchun o'zlariga o'zlari tajovuzlarni uyushtirishlari mumkin. Bunday tahlillarni faqat katta tajribaga ega tizim administratorlari yoki maxsus maslahatchilar o'tkazishi maqsadga muvofiq.

4. **Kriptotizimlardan keng foydalanish lozim.** Tajovuzkorlar ko'pincha tarmoqqa uning ahamiyatga molik joylaridan o'tuvchi trafigini tinglash orqali trafikdan foydalanuvchilarni va ularning parollarini ajratib olish yordamida suqulib kiradilar. Shuning uchun olisdagi mashinalar bilan bog'lanishlar parol bilan himoyalanganda shifrlanishi shart. Bu ayniqsa, bog'lanish I**nternet kanallari orqali amalga oshirilganda yoki ahamiyatli server bilan bog'lanilganda zarur.** TCP/IP (eng mashhuri SSH) trafigini shifrlash uchun tijoratli va bepul dasturlar mavjud. Bulardan foydalanish tajovuzlarning oldini oladi. Internet muhit bilan birlashgan Internetda axborot oqimini va resurslarni eng ishonchli himoyalash vositasi–nosimmetrik va simmetrik kriptotizimlardan birgalikda foydalanishdir.

5. **Kompyuterlarni xavfsizlik nuqtai-nazaridan savodxonlarcha konfiguratsiyalash kerak**. Kompyuterda amal tizimlari yangitdan o'rnatilganda ko'pincha tajovuzlarga qaltis bo'ladilar.Buning sababi amal tizimi dastlab o'rnatilganda barcha tarmoq vositalaridan foydalanishga ruhsat beriladi va ulardan to'g'ri foydalaniladi deb bo'lmaydi. Bu tajovuzkor uchun mashinaga tajovuz uyushtirishda ko'p usullardan foydalanishga yo'l ochadi. Shuning uchun barcha zarur bo'lmagan tarmoq vositalari kompyuterdan uzib qo'yilishi lozim.

6. **Dasturiy ta'minotga tuzatishlarni operativ kiritishni tartibga solish(Patching).** Kompaniyalar bot-bot o'z dasturlarida topilgan xatolarni yo'qotish uchun tuzatishlar kiritib boradilar. Agar bu xatolar tuzatilmasa tajovuzkor undan foydalanib dasturingizga va u orqali kompyuteringizga tajovuz uyushtirishi mumkin. Tizim administratorlari avvalo o'zlarining eng zarur tizimlaridagi dasturlarga tuzatishlarni o'rnatib zarur xostlarni himoyalashlari zarur. Chunki tuzatishlar tez-tez yuzaga kelib turadi va ularni barcha kompyuterlarda o'rnatib chiqishga ulgurmay qolish mumkin. Odatda tuzatishlar faqat dastur ishlab chiqargan korxonadangina olinishi shart. Internet-tarmoq xavfsizligida uchratilgan **defektlarni albatta tuzatish.** Shuning bilan birga quyida keltirilgan boshqa himoya vositalaridan ham foydalanishlari zarur.

7. **Tajovuzni payqash vositalari (Intrusion Detection)dan foydalanish lozim**. Tajovuzni payqash tizimlari tajovuzlarni operativ payqab aniqlaydilar. Tarmoq ichkarisidan bo'ladigan tajovuzlarni payqash uchun ular brandmauer orqasiga qo'yiladi, branmauerga bo'ladigan tajovuzlarni aniqlash uchun esa- uning oldiga o'rnatiladi. Bunday vositalar turli imkoniyatlarga ega. Quyidagi saytdan bu xaqda qo'shimcha ma'lumotlar olish mumkin. http://www.icsa.net/services/consortia/intrusion/educational_material.shtml

8. **Viruslar va "troyan ot" dasturlarini o'z vaqtida payqashga intilish kerak**. Harqanday tarmoqning xavfsizligi uchun virusga qarshi dasturlar himoyaning ajralmas qismidir. Ular kompyuter ishini nazorat qilib zarar keltiruvchi dasturlarni topib beradilar. Ular tufayli yuzaga keladigan yagona muammo shundaki, himoya maksimal samara berishi uchun ular tarmoqning barcha kompyuterlariga o'rnatilgan bo'lishlari va muntazam yangilanib turilishlari shart. Buning uchun ko'p vaqt ketadi, lekin aks holda vosita kutilgan samarani bermaydi. Kompyuterdan foydalanuvchilarga buni qanday amalga oshirishni o'rgatib qo'yish kerak, ammo faqat ularga bu ishni to'la topshirib qo'ymaslik zarur. Virusga qarshi dasturlar bilan bir qatorda pochta serverida elektron xatlarga ilovalarni skanerlash ham lozim. Bu yo'l bilan foydalanuvchilar kompyuteriga yetib borishi mumkin bo'lgan viruslarning yo'li to'siladi.

9. **Bardoshi bo'sh joylarni skanerlab turish lozim.** Bunday skanerlovchi dasturlar aniq biror turdagi tajovuzlarga qaltis (bardoshi bo'sh)kompyuterlarni topish uchun tarmoqni skanerlaydi. Ular qaltis joylar haqida kattagina ma'lumotlar bazasiga ega bo'lib, undan u yo boshqa kompyuterda qaltis joy bor-yo'qligini topishda foydalaniladi. Tijoratli va bepul skanerlar mavjud. Tizim administratorlari davriy tarzda bunday dasturlarni o'zlarining tarmoqlariga nisbatan o'z vaqtida bardoshi bo'sh kompyuterlarni o'zlari topib tegishli chora ko'rib qo'yishlari lozim. Alohida qurilmalarni himoyasidagi zaif bo‘g‘inlarni payqab olish uchun qaltislik darajasini baholash lozim.

10. **Tarmoq topologiyasini aniqlash va port skanerlarini ishga solib turish lozim.** Bunday dasturlar tarmoq qanday tuzilganligi, unda qanaqa kompyuterlar ishlashi, har bir mashinada qanday xizmatlar bajarilishii haqida to'la manzarani ochib beradi. Hujumkorlar bu dasturlarni qaltis kompyuterlar va dasturlarni aniqlash uchun ishga soladilar. Tarmoq administratorlari ham bunday dasturdan ularning tarmoqlarida qanday dasturlar qaysi kompyuterlarda ishlayotganini aniqlashtirish uchun foydalanadilar. Noto'g'ri konfiguratsiyalangan kompyuterlarni topib ularga tuzatishlar kiritish uchun bu yaxshi vositadir.

11. **Parol ochuvchilar (Password Crackers)ni ishlatib turish lozim.** Xakerlar ko'pincha parollar bilan shifrlangan fayllarni o'g‘irlash uchun kompyuterlarning bardoshi bo'sh joylaridan foydalanishga intiladilar**.** So'ngra parol ochuvchi maxsus dasturlarni ishga soladilar va ular orqali shu shifrlangan fayllardagi bardoshi bo'sh parollarni topib oladilar. Bunday parol qo'lga kirishi bilan kompyuterga odatdagi foydalanuvchi kabi kompyuterga va tarmoqqa bildirmay kirishning turli usullaridan foydalanadilar. Garchi bu vosita niyati buzuq kimsalar tomonidan ishlatilsa ham bu tizim administratori uchun ham foydalidir. Tizim administratorlari davriy tarzda bunday dasturlarni o'zlarining shifrlangan fayllariga nisbatan o'z vaqtida bardoshi bo'sh parollarni o'zlari topib tegishli chora ko'rib qo'yishlari lozim.

12. **Jangovor muloqot o'rnatuvchilar(war dialer)ga nisbatan ziyrak bo'lish lozim.** Foydalanuvchilar ko'pincha tashkilot tarmog'i himoyasi vositalarini chetlab o'tib o'z kompyuterlariga keladigan telefon qo'ng'iroqlari qabul qilib olishga ruxsat beradilar. Ular ba'zan Ishdan qaytish oldidan modemni ulab kompyuterni uydan turib modem orqali unga ulanib tarmoqdan foydalanishni ko'zlab o'z dasturlarini shunga sozlab ketadilar. Tajovuzkorlar jangovar muloqot

o'rnatuvchi dasturlardan foydalanib ko'plab telefon nomerlariga qo'ng'iroq qilib ko'radilar va shu tariqa chetdan modem orqali kirishga yo'l qoldirgan bunday tarmoqlarga suqulib kirib tajovuz uyushtiradilar. Foydalanuvchilar ko'pincha o'z kompyuterlarini o'zlari konfiguratsiyalashlari tufayli bunday kompyuterlar tajovuzlardan yomon himoyalangan bo'ladilar va tarmoqqa tajovuz qilishga yana bitta imkoniyat tug'diradilar. Tizim administratorlari jangovor muloqot o'rnatuvchilardan muntazam suratda foydalanib o'z foydalanuvchilarining telefon raqamlarini tekshirib turishlari va unga mos qilib konfiguratsiyalangan kompyuterlarni o'z vaqtida topib chorasini ko'rishlari lozim. Tijoratli va bepul tarqaltiladigan jangovor muloqot o'rnatuvchi dasturlar mavjud.

13. **Xavfsizlikka oid tavsiyalar (security advisories)dan o'z vaqtida xabordor bo'lib, ularga amal qilish lozim.** Xavfsizlikka oid tavsiyalar – kompyuter jinoyatlariga qarshi kurash guruhlari va dastur ishlab chiqaruvchilar tomonidan yaqin orada payqalgan dasturning qaltis joylari haqida e'lon qilinadigan ogohlantirishlar. Tavsiyalar juda foydali bo'lib, o'qish uchun juda kam vaqt oladi va payqab qolingan qaltis joylar tufayli yuzaga kelishi mumkin bo'lgan eng jiddiy xavf-xatarlardan ogoh etadi. Ular xavf-xatarni ifodalab uning oldini olish uchun maslahatlar beradi. Ularni qator joylardan olish mumkin. Ikkita eng foydali bo'lgan tavsiyalar kompyuter jinoyatlariga qarshi kurash guruhi e'lon qilib turadigan tavsiyalar bo'lib CIAC va CERT saytlaridan olish mumkin.

14. **Xavfsizlik bilan bog'liq hodisalarni tekshirish guruhi muntazam faoliyat olib borishi lozim**. Har qanday tarmoqda ham xavfsizlik billan bog'liq hodisalar sodir bo'lib turadi(yolg'on trevoga bo'lsa ham). Tashkilot xizmatchilari avvaldan u yo bu holda nima qilishni bilishlari shart. Qaysi hollarda huquqiy-himoya organlariga murojaat qilish kerak, qaysi hollarda kompyuter jinoyatlariga qarshi kurash guruhini chaqirish va qaysi hollarda tarmoqni Internetdan uzib qo'yish kerak va ahamiyatli serverning qulfi buzilganda nima qilish kerak. CERT AQSH doirasida bu borada maslahatlar beradi. FedCIRC AQSH jamoat va davlat tashkilotlariga maslahatlar berish uchun mas'uldir. Harbir davlatda bunday maslahat olish joylari bo'lishi maqsadga muvofiqdir.

Kompyuter tajovuzlariga oid qo'shimcha ma'lumotlar tajovuz uyushtirish mo'ljallangan ayrim dasturlarga bag'ishlangan quyidagi maqola dan topilishi mumkin.

Kompyuter xavfsizligi bo'yicha umumiy axborot quyidagi manzillardan olinishi mumkin:

- NIST Computer Security Resource Clearinghouse
- Federal Computer Incident Response Capability
- Center for Education and Research in Information Assurance and Security
- Carnegie Mellon Emergency Response Team

Bugungi kunda axborot xavfsizligini ta'minlashda an'anaviy qo'llanilib kelingan yondoshuvlar va vositalar yetarli bo'lmay qoldi. Bunday sharoitda axborot himoyasining eng ishonchli va sinalgan usuli bo'lgan kriptografiyaning ahamiyati yanada oshdi. Quyida Internet va Internetda axborot himoyasining kriptologiya yo'nalishi haqida batafsil to'xtalamiz.

11-MAVZU: ELEKTRON POCHTANI HIMOYASINI TASHKIL ETISH

MA’RUZA MASHG’ULOTI REJASI:

11.1. Elektron pochtadan foydalanish
11.2. E-mail asoslari
11.3. E-maildagi mavjud muammolar
11.4. Elektron pochtada mavjud xavflar
11.5. Elektron pochtani himoyalash

Tayanch so‘z va iboralar USENET, SMTP, POP, IMAP, MIME.

Elektron pochtadan foydalanish

Elektron pochta yoki E-mail hozirgi kunda Internetdan foydalanish jarayonining eng mashxur kasmi hisoblanadi. E-mail orqali dunyo buyicha istalgan joyga bir zumning uzida xat yuborish yoki kabul qilish hamda yozilgan xatlarni faqatgina bir kishiga emas, balki manzillar ruyxati buyicha junatish imkoniyati mavjud. E-mail orqali munozaralar o‘tkazish imkoniyati mavjud va bu yunalishda USENET serveri kul keladi.

Ko‘pgina korxonalar uz faoliyatida bevosita E-mail tizimidan foydalanishadi. Demak, korxona va tashkilotlar raxbarlari ma’lum bir choratadbirlar orqali uz xodimlarini E-mail bilan ishlash, undan okilona foydalanishga urgatishi lozim. Ushbu jarayonning asosiy maqsadi muhim hujjatlar bilan ishlashni tugri yulga kuyish hisoblanadi.

Bu erda quyidagi yunalishlar buyicha takliflarni e’tiborga olish zarur:

- E-mail tizimidan tashkilot faoliyati maqsadlarida foydalanish;
- shaxsiy maqsadda foydalanish;
- maxfiy axborotlarni saqlash va ularga kirish:
- Elektron xatlarni saqlash va ularni boshqarish.

E-mail asoslari

Internetda asosiy pochta protokollariga quyidagilar kiradi:

- SMTP (Simple Mail Transfer Protocol);
- POP (Post Office Protocol);
- IMAP (Internet Mail Access Protocol);
- MIME (Multi purpose Internet Mail Extensions).

Bular bilan birma-bir tanishib chikamiz:

SMTP — ushbu protokol asosida server boshqa tizimlardan xatlarni kabul kiladi va ularni foydalanuvchining pochta kutisida saklaydi. Pochta serveriga interaktiv kirish huquqiga ega bo‘lgan foydalanuvchilar uz kompyuterlaridan bevosita xatlarni ukiy oladilar. Boshqa tizimdagi foydalanuvchilar esa uz xatlarini ROR-3 va IMAP protokollari orqali o‘qib olishlari mumkin;

POP — eng keng tarkalgan protokol bo‘lib, serverdagi xatlarni, boshqa serverlardan kabul kilingan bulsa-da, bevosita foydalanuvchi tomonidan o‘qib olinishiga imkoniyat yaratadi. Foydalanuvchilar barcha xatlarni yoki hozirgacha ukilmagan xatlarni kurishi mumkin. Hozirgi kunda POP ning 3-versiyasi ishlab

chikilgan bo‘lib va autentifikatsiyalash usullari bilan boyitilgan;

IMAP — yangi va shu bois ham keng tarkalmagan protokol sanaladi.

Ushbu protokol quyidagi imkoniyatlarga ega:

• pochta kutilarini yaratish, uchirish va nomini uzgartirish;
• yangi xatlarning kelishi;
• xatlarni tezkor uchirish;
• xatlarni kidirish; • xatlarni tanlab olish.

IMAR sayohatda bo‘lgan foydalanuvchilar uchun POPga nisbatan qulay bo‘lib hisoblanadi;

MIME — Internet pochtasining ko‘p maqsadli kengaytmasi suzlari kiskartmasi bo‘lib, u xatlarning formatini aniqlash imkonini beradi, ya’ni:

• matnlarni har xil kodlashtirishda junatish;
• har xil formatdagi nomatn axborotlarni junatish;
• xabarning bir necha qismdan iborat bo‘lishi;
• xat sarlavhasida har xil kodlashtirishdagi ma’lumotni joylashtirish.

Ushbu protokol rakamli Elektron imzo va ma’lumotlarni shifrlash vositalaridan iborat bo‘lib, bundan tashkari uning yordamida pochta orqali bajariluvchi fayllarni ham junatish mumkin. Natijada, fayllar bilan birga viruslarni ham tarkatish imkoniyati tugiladi.

E-maildagi mavjud muammolar

Elektron pochta bilan ishlash jarayonida quyidagi xatolarga yul kuyish mumkin:

• xatni tasodifan junatish;
• xatning notugri manzil buyicha junatilishi;
• xatlar arxivining keskin oshib ketishi okibatida tizimning ishdan chikishi;
• yangiliklarga notugri obuna bo‘lish;
• xatni tarkatish ruyxatida xatoga yul kuyish.

Agar tashkilotning pochta tizimi bevosita Internetga ulangan bulsa, yul kuyilgan xatolar okibati keskin oshib ketadi.

Ushbu xatolarning oldini olish usullarining ba’zi birlari quyidagilar:

- foydalanuvchilarni ukitish;
- Elektron pochta dasturlarini tugri konfiguratsiyalash;
- Internetdagi protokollarga tulik amal qiluvchi dasturlarni qo‘llash.

Bundan tashkari Elektron pochtaning shaxsiy maqsadda ishlatilishi tashkilot raxbariyati uchun ba’zi bir muammolarni keltirib chikarishi mumkin, chunki Email manzilida tashkilot nomlari aks ettirilgan bo‘lishi extimoldan holi emas. Natijada, shaxs junatayotgan xat tashkilot nomidan deb kabul kilinishi mumkin. SHu bois, telefonlar kabi E-maildan shaxsiy ishlar uchun foydalanishni cheklab kuyish zarur buladi. Albatta, buni joriy qilish qiyin masala.

Elektron pochtada mavjud xavflar

Elektron pochta bilan ishlash jarayonida quyidagi xavflar mavjud:

1. **Junatuvchining kalbaki manzili.** Kabul kilingan xatni E-mail manzili anikligiga tulik ishonch xosil qilish qiyin, chunki xat junatuvchi uz manzilini kalbakilashtirishi mumkin.
2. **Xatni qo’lga kiritish**. Elektron xat va uning sarlavxasi uzgartirilmasdan, shifrlanmasdan junatiladi. SHu bois, uni yulda kulga kiritish va mazmunini uzgartirishi mumkin.
3. **Pochta «bomba»si.** Pochga tizimiga ko‘plab Elektron xatlar junatiladi, natijada tizim ishdan chikadi. Pochta serverining ishdan chikish holatlari quyidagilardir:

• disk tulib qoladi va keyingi xatlar qabul kilinmaydi. Agar disk tizimli bulsa, u holda tizim tamomila ishdan chikishi mumkin;

• kirishdagi navbatda turgan xatlar sonining oshib ketishi natijasida keyingi xatlar umuman navbatga kuyilmaydi;

• olinadigan xatlarning maksimal sonini uzgartirish natijasida keyingi xatlar kabul kilinmaydi yoki uchiriladi;

• foydalanuvchiga ajratilgan diskning tuldirilishi natijasida keyingi xatlar kabul kilinmaydi va diskni tozalab bulmaydi.

4. «Qorqinchli» (noxush) xat. Internet orqali olinadigan Elektron xatlarning umuman noma'lum shaxslar tomonidan junatilishi va bu xatda foydalanuvchilarning shaxsiyatiga teguvchi suzlar bo'lishi mumkin.

Elektron pochtani himoyalash

Yuqorida keltirilgan xavflarga nisbatan quyidagi himoyalanish usullari ishlab chikilgan:

- kalbaki manzildan himoyalanish, bu holda shifrlangan Elektron imzolarni qo'llash taklif kilinadi;

- xatni qo'ga kiritishdan himoyalanish, bu holda xabarni yoki junatish kanalini shifrlash taklif kilinadi.

Ushbu himoyalash usullari bevosita qolgan xavflarning ulushini kamaytiradi.

12-MAVZU: BOG'LANISHNI NAZORAT QILISH TIZIMLARI, METODOLOGIYA

MA'RUZA MASHG'ULOTI REJASI:

12.1. Eng maqbul bo'lgan (optimal) ulanish

12.2. Tarmoqlarni nazorat qilish va tahlil qilish tizimlari

12.3. Virtuallashgan muhitlarning nazorat qilinishi

Tayanch so'z va iboralar NetFlow, SPAN-porti, Phantom Virtualization Tap.

Bugungi kunda ko'pchilik korxona va tashkilotlarning faoliyatidagi muvaffaqiyatlar g'oyat katta darajada ular tomonidan foydalanadigan tarmoq xizmatlari hamda qo'llanmalari ishining ishonchliligi va sifatiga bog'liq, bularga o'z navbatida ushbu xizmatlar hamda qo'llanmalarning trafigini uzatayotgan tarmoq infratuzilmalarining holati va parametrlari nihoyat darajada ta'sir etadi. Tarmoqni monitoring qilish, shuningdek tarmoq xizmatlari va qo'llanmalarining samaradorligi bo'yicha hal qiluvchi parametrlarini (KPI) nazorat qilish foydalanuvchilarga ko'rsatilayotgan xizmatlarning sifatini talab etiladigan darajada saqlab turish uchun ularning ishidagi muammolarni tezroq aniqlash va bartaraf qilishga yordam berishadi.

Eng maqbul bo'lgan (optimal) ulanish

Tarmoq hamda tarmoq xizmatlari va qo'llanmalarining ishini nazorat qilish tarmoq trafigini egallash va tahlil qilishni nazarda tutadi. Bu nafaqat tarmoqdagi muammolarni aniqlash (diagnostika qilish) maqsadida, balki jiddiy ravishda muhim bo'lgan xizmatlar va qo'llanmalarning ishini maqbullashtirish (optimallashtirish) uchun ham, shuningdek Tezkor-qidiruv tadbirlarning funktsiyalarini ta'minlash uchun texnik vositalari tizimi (SORM) doirasida axborot xavfsizligiga oid tahdidlarni aniqlab topish va tarmoq orqali uzatilayotgan ma'lumotlarni qonuniy (legal) ravishda tutib olishni (qo'lga tushirishni) amalga oshirish maqsadida qilinadi.

AT (axborot texnologiyalari) mutaxassislari har xil monitoring qilish vositalaridan, shu jumladan bayonnomalarni tahlil qiladigan asboblardan (analizatorlardan), RMON naysimon asboblaridan (zondlaridan), NetFlow to'plab ta'minlovchilaridan (kollektorlaridan), IDS / IPS tizimlaridan va tarmoq trafigining katta hajmlarini yozib olishga imkoniyati mavjud bo'lgan server maslaklari (platformalari) negizidagi sinov vositalaridan (probniklardan) foydalanishadi («Korporativ tarmoqni tahlil qilish, monitoring qilish va aniqlash (diagnostika qilish)» bo'limini qarang). Nazorat qilinishi kerak bo'lgan tarmoq trafigini egallash maqsadida ularni tarmoqqa ulash uchun hammasidan ko'ra monitoring qilish vositalarining maxsus tarmoqlantirgichidan (tarmoqni shoxobchalarga bo'lintiruvchi asbobdan) yoki shunday tarmoqlantirgichning funktsiyalariga ega bo'lgan uzib-ulagichlaridan (kommutatorlaridan) foydalangani afzalroq. Ethernet uzib-ulagichining ortiqcha yuklanib ketganligi va nuqsoni bo'lgan (defektli) paketlarni o'tkazmayotgan bo'lishi

mumkin SPAN-portidan farqli ravishda, tarmoq kanalining uzilgan joyiga ulanayotgan tarmoqlantirgich mazkur kanal bo'yicha uzatilayotgan butun trafikning (hammasini!), uning yuklanganligi darajasiga bog'liq bo'lmagan holda, nazorat qilinishi imkoniyatini yaratadi. Tarmoqlantirgich nazorat qilinayotgan kanalning ishiga hech qanday ta'sir ko'rsatmaydi va uning ishonchliligini pasaytirmaydi, chunki elektr energiyasi bilan ta'minlashda to'xtalish sodir bo'lganda, mis liniyasiga nisbatan tarmoqlantirgich nazorat qilinayotgan trafik uchun shaffof bo'lib qolayveradi, optik-tolali tarmoqlantirgich esa — sust (passiv) moslama bo'lib, uni umuman elektr energiyasi bilan ta'minlash ehtiyoji yo'q. Bundan tashqari, tarmoqlantirgich orqali ulangan monitoring qilish vositasi IP-manziliga muhtoj bo'lmaganligi sababli, u tarmoqdan alohida ajratib olingan (izolyatsiya qilingan) bo'ladi, va buning natijasida uni xakerlar hujumlariga duchor bo'lishi ehtimoli sezilarli darajada kamaytiriladi.

Sotuvda mis yoki optik-tolali liniyalari uchun ma'lumotlarni uzatish bo'yicha qo'llab-quvvatlaydigan maksimal darajadagi tezligi har xil — 10 Mbit/s dan 100 Gbit/s gacha bo'lgan tarmoqlantirgichlarning juda keng assortimenti mavjud. Jumladan, odatdagi tarmoqlantirgichlardan tashqari regeneratsiya qiladigan tarmoqlantirgichlar ishlab chiqariladi va ulardan xuddi o'sha trafikning o'zginasini bir vaqtning o'zida bir nechta monitoring qilish vositalari yordami bilan nazorat qilish zaruriyati bo'lganda foydalaniladi. Bunday qurilma tarmoqlantirilgan trafikni bir vaqtning o'zida o'zining bir nechta monitoring qilish portlari orqali chiqaradi. Agarda nazorat qilinishi zarur bo'lgan tarmoq kanallarining soni mavjud bo'lgan monitoring qilish vositalarining sonidan oshib ketsa, agregatsiya qiladigan tarmoqlantirgichdan foydalanish mumkin, u bir nechta nazorat qilinayotgan kanallardan bo'lgan trafikni birlashtiradi va umumlashtirilgan oqimni o'zining bitta yoki bir nechta monitoring qilish portlari orqali chiqaradi. Lekin ushbu oqimning tezligi monitoring qilish vositasi portining o'tkazish qobiliyatidan oshib ketishi mumkin, hamda bunday vaziyatda paketlarning yo'l qo'yib bo'lmaydigan yo'qotilishiga olib keladi. Bunga yo'l qo'ymaslikning usullaridan bittasi — yetarli darajadagi katta buferga ega bo'lgan agregatsiya qiladigan tarmoqlantirgichning modelini tanlash.

Shuningdek monitoring qilish vositasi tezroq bo'lgan tarmoq kanaliga ulanganida (misol uchun, agar 10-Gigabitli tarmoqlantirgich yordami bilan 1 GE portli tahlil qiladigan asbob (analizator) 10 GE liniyasiga ulanilsa), u ortiqcha yuklanib ketishi mumkin. Monitoring qilish vositalariga yuklanganlikni pasaytirish uchun tarmoqlantirilgan trafikni dastlabki ravishda filtrlashdan keng foydalaniladi, shunda mazkur vosita faqat unga o'zining asosiy (masalan, tarmoqqa qilingan hujumlarni aniqlab topish bilan bog'liq bo'lgan) vazifalarini amalga oshirishi uchun kerak bo'lgan ma'lumotlarni oladi. Shuningdek yuklanganlikni muvozanatga keltirish funktsiyasi mavjud bo'lgan qurilma yordami bilan yuqori tezlikdagi trafikni bir nechta monitoring qilish vositalari o'rtasida deyarli teng-baravar taqsimlash mumkin. Bu holatda ko'pincha uzatilayotgan paketlarning oqimlari

butunligicha saqlangan bo'lishi muhimdir, ya'ni xuddi o'sha oqimning o'zginasiga tegishli bo'lgan barcha paketlar xuddi o'sha monitoring qilish vositasining o'zginasiga (yuklanganlikni muvozanatga keltirishga ega bo'lgan vositalar guruhida) kelib tushishi zarur. Trafikni filtrlash va yuklanganlikni muvozanatga keltirish yanada yuqori tezlikdagi tarmoq texnologiyalari joriy qilinganida mavjud bo'lgan monitoring qilish vositalariga sarflangan investitsiyalarni himoyalash imkoniyatini yaratadi. Trafikni agregatsiya va regeneratsiya qilish, filtrlash hamda yuklanganligini muvozanatga keltirish funktsiyalari monitoring qilish vositalarining uzib-ulagichlarida (kommutatorlarida) va ularga bo'lgan yuklanganlikni muvozanatga keltiruvchi asboblarda mavjud. Shunday qilib, agarda monitoring qilish vositalarini tez-tez bitta kanaldan boshqa kanalga o'zgartirish zaruriyati bo'lib turganda va / yoki trafikni filtrlash hamda yuklanganligini muvozanatga keltirish funktsiyalari kerak bo'lganda, ushbu vositalarni tarmoqlantirgichlarga yoki SPAN-portlariga to'g'ridan-to'g'ri emas, balki tegishli uzib-ulagichlar orqali ulash kerak.

Tarmoq kanalining uzilgan joyiga (inline) ulanayotgan monitoring qilish vositasidan (masalan, IPS dan) foydalanish zaruriyati bo'lganligida, aylanib o'tadigan (bypass) uzib-ulagichni (kommutatorni) ishga solish kerak. Agar mazkur vosita qandaydir sabablarga ko'ra ishlamay qolsa, aylanib o'tadigan uzib-ulagich trafikni uni aylanib o'tgan holda yo'naltiradi, hamda bu bilan jiddiy ravishda muhim bo'lgan xizmatlar va qo'llanmalardan erkin foydalanish holatini saqlab qoladi (foydalanuvchilar uchun). Sotuvda odatdagi tarmoqlantirgichlar va aylanib o'tadigan uzib-ulagichlar bilan bir qatorda, mazkur qurilmalarning har xil aqliy (intellektual) turlari mavjud bo'lib, ular maxsus monitoring qilish moslamasini ulamagan holda RMON statistikasini ko'zdan kechirish imkoniyatini yaratadi. RMON ni qo'llab-quvvatlash imkoniyati monitoring qilish vositalarining uzib-ulagichlarida ham mavjud.

Net Optics kompaniyasi Director oilasiga mansub bo'lgan tarmoqlantirgichlarning, aylanib o'tadigan uzib-ulagichlarning, shuningdek monitoring qilish vositalari uzib-ulagichlarining hamda xBalancer yuklanganlikni muvozanatga keltiruvchi samarali moslamaning keng assortimentini ishlab chiqaradi. Director qurilmalari nazorat qilinishi kerak bo'lgan trafikni ularga ulangan monitoring qilish vositalari bo'yicha uzib-ulashadi, agregatsiya qilishadi, regeneratsiya qilishadi, filtrlashadi va bir me'yorda taqsimlashadi. Mazkur oilaning eng aqlli (intellektual) a'zolari oqimlarning butunligi saqlangan holda yuklanganlikni o'zgaradigan (dinamik ravishda) muvozanatga keltirilishini hamda DPI funktsiyasidan foydalangan holda trafikning dastlabki ravishda filtrlanishini ta'minlashadi. Director uzib-ulagichlaridan farqli ravishda, xBalancer moslamasi inline- monitoring qilish vositalariga yuklanganlikni bir me'yorda (shuningdek oqimlarning butunligi saqlangan holda) taqsimlash imkoniyatiga ega. Nazorat qilinayotgan tarmoqda o'rnatilgan o'zining ko'p sonli mahsulotlarining markazlashgan holda boshqarilishini amalga oshirish uchun, Net Optics kompaniyasi Indigo Pro boshqaruv maslagini (platformasini) taklif qiladi.

Virtuallashgan muhitlarning nazorat qilinishi

Oxirgi yillarda AT (axborot texnologiyalari) tizimlarining ishlashi samarasini va ularning moslashuvchanligini oshiradigan, hamda xarajatlarni kamaytiradigan virtuallashgan tarmoq muhitlarining keng qamrovli ommalashtirilishi ro'y berdi. Lekin xuddi o'sha gipervizorning o'zginasida virtual mashinalari orasida uzatilayotgan trafikning odatdagi jismoniy monitoring qilish vositalari yordami bilan egallanishi va tahlil qilinishi imkoniyati mavjud emas. Ushbu trafikning nazorat qilinmasligi korxonaning axborot xavfsizligiga nisbatan tahdid yaratadi va tarmoqdagi to'xtalishlar aniqlanishini (diagnostika qilinishini) qiyinlashtiradi.

Mazkur muammoning yechimi sifatida Net Optics kompaniyasi o'zi ishlab chiqaradigan hamda trafikni virtuallashgan hisoblash muhitlarda nazorat qilish uchun mo'ljallangan Phantom Virtualization Tap (virtual tarmoqlantirgich) dasturiy ta'minotidan (DT) foydalanishni taklif qiladi. Mazkur dasturiy yechimning gipervizor o'zagining ichiga o'rnatiladigan Phantom Monitor tarkibiy qismi virtual uzib-ulagich (kommutator) orqali virtual mashinalari orasida uzatilayotgan butun trafikni (hammasini) tutib olish (qo'lga tushirish), tutib olinayotgan (qo'lga tushirilayotgan) paketlarni aqliy (intellektual) filtrlash, hamda nazorat qilinishi kerak bo'lgan ma'lumotlarni monitoring qilish vositalariga yuborish imkoniyatlariga ega. Bundan tashqari mazkur tarkibiy qism tutib olingan (qo'lga tushirilgan) trafikni an'anaviy jismoniy monitoring qilish vositalari yordami bilan nazorat qilish uchun jismoniy tarmoq portiga yuborish imkoniyatiga ega.

Phantom Virtualization Tap yechimi virtual mashinalarning ishiga xalaqit bermaydi va ularning hech qanday turlanishini (ko'rinishining o'zgartirilishini) talab qilmaydi. Mazkur yechimning ikkinchi asosiy dasturiy tarkibiy qismi — Phantom Manager — trafik to'g'risidagi ma'lumotni yig'ish va berish, shuningdek nazorat qilinayotgan xostlarda ishlaydigan ko'p sonli virtual tarmoqlantirgichlarni boshqarishga mo'ljallangan. Virtual muhitlarning ishlashi to'g'risidagi statistika ma'lumoti ikkinchi va uchinchi pog'onalarda beriladi (uzatilgan paketlarning soni, yuklanganlik va boshqalari). Albatta, virtuallashgan muhitni monitoring qilish uchun virtual uzib-ulagichning SPAN-portlari yordami bilan undan trafikni chiqarish imkoniyati mavjud, lekin bu maqsadda mazkur uzib-ulagich unumdorligining yarmigacha sarf qilinadi. Aksincha, Phantom Virtualization Tap virtual tarmoqlantirgich virtual uzib-ulagichni yuklantirmaydi, hamda uning o'tkazish qobiliyati o'zgarmagan holda qoladi.

Phantom Virtualization Tap yechimi eng ko'p uchraydigan virtuallashtirish maslaklariga (platformalariga): VMware vSphere ESX / ESXi Server 4.x / 5.x; Microsoft Hyper-V 8.x; Citrix Xen Server 5.6.x; Redhat KVM 2.6.32 va Oracle VM 3.0 mos (to'g'ri keladi). Bu yechim virtual muhitlarning xavfsizligini va ishining ishonchliligini, hamda ularning me'yoriy talablarga javob berishini ta'minlashga yordam beradi.

Monitoring qilishga oldindan tayyorgarlik ko'rish kerak

Tarmoqni monitoring qilish bo'yicha ko'p pog'onali tizimda nazorat qilinayotgan tarmoqda o'rnatilgan hamda unga turli-tuman monitoring qilish vositalarining oson va qulay ravishda ulanishini ta'minlab kelayotgan har xil tarmoqlantirgichlar, aylanib o'tadigan uzib-ulagichlar (kommutatorlar) va monitoring qilish vositalarining uzib-ulagichlari erkin foydalanish pog'onasini tashkil qilishadi (rasmga qarang), Net Optics kompaniyasida uni Monitoring Access Platform (MAP) deb ham atashadi. Mazkur maslak (platforma) nazorat qilinishi kerak bo'lgan trafikni monitoring qilish vositalariga (har xil turdagi sinov vositalariga (probniklarga)) uzatadi, ular o'z navbatida tarmoqning, tarmoq xizmatlari va qo'llanmalarining ishlashi to'g'risidagi ma'lumotlar bilan yuqori pog'onadagi monitoring qilish va boshqarish dasturiy vositalarini ta'minlashadi.

Net Optics kompaniyasi MAP ning amalga oshirilishini kelgusidagi tarmoqning tarkibiy qismi sifatida oldindan rejalashtirishni hamda uni yaratish jarayonida MAP qurilmalarini boshqa tarmoq asbob-uskunalari bilan birga o'rnashtirishni (installyatsiya qilishni) tavsiya qiladi. MAP tarmoqdagi muammolar paydo bo'lishidan avval yaratilishi maqsadga muvofiqdir.

MAP me'morchiligida (arxitekturasida) erkin foydalanish, taqsimlanish va tarmoq o'zagi pog'onalarida, shuningdek korxonaning serverlari joylashgan ma'lumotlar bilan ishlash markazida (MIM) jiddiy ravishda muhim bo'lgan tarmoq kanallarining trafigini monitoring qilish imkoniyatlarini ko'zda tutish zarur. Ma'lumotlar bilan ishlash markazida (MIM) va tarmoq o'zagida ko'pgina yuqori tezlikdagi liniyalar to'planganligi sababli, u yerlarda Director oilasiga mansub bo'lgan ko'p portli kanallarni agregatsiya qiladigan asboblarni va uzib-ulagichlarni (kommutatorlarni) o'rnatish tavsiya qilinadi. Virtuallashgan muhitlarni nazorat qilish uchun ma'lumotlar bilan ishlash markazidagi (MIM) serverlarda Phantom Virtualization Tap virtual tarmoqlantirgichlarni ishga solish maqsadga muvofiq.

13-MAVZU: TELEKOMMUNIKATSIYALAR VA TARMOQ XAVFSIZLIGI

MA’RUZA MASHG’ULOTI REJASI:

13.1. Muloqot etalon modeli
13.2. Lokal tarmoqni boshqarish arxitekturasi

Tayanch so‘z va iboralar ISO, OSI, axborot uzatish uchun kabellar, kabellarni ulash uchun razemlar, moslovchi terminatorlar, tarmoq adapterlari, repiterlar, transiverlar, konsentratorlar, ko’priklar, yo’naltirgichlar (marshrutizatorlar), shlyuzlar.

Kompyuterlarni tarmoqqa ulash jarayonida juda ko’p operatsiylarni amalga oshiriladi , ya’ni kompyuterdan kompyuterga axborotlarni uzatilishi to’liq ta’minlanadi. Qandaydir ilovalar bilan ish olib borayotgan foydalanuvchiga nima qanday amalga oshirilayotganining farqi yo’q albatta. Uning uchun faqat boshqa ilovaga ega bo’lish yoki tarmoqda joylashgan boshqa kompyuter resurslariga ega bo’lish mavjuddir xolos. Aslida esa hamma uzatilayotgan axborot ko’p ishlov berish bosqichlaridan o’tib boradi. Avalambor u bloklarga ajratilib har biri aloxida boshqarish axboroti bilan ta’minlanadi. Xosil bo’lgan bloklar paket sifatida jihozlanadi, bu paketlar kodlashtiriladi, shundan so’ng elktr signallari yoki yorug’lik signali yordamida

Tanlangan ega bo’lish usulida tarmoq orqali uzatiladi, ya’ni qabul qilingan paketni qaytatdan bloklangan axborotlari tiklanib, bloklar axborotlar ko’rinishida ulanadi va shundan so’nggina boshqa ilovaga foydalanish uchun tayyor bo’ladi. Bu albatta bo’ladigan jarayonni ancha soddalashtirib bayon qilinishi. Aytib o’tilgan ishlarning bir qismi albatta dasturlar yordamida amalga oshirilsa, boshqa qismi esa qurilmalar ishtirokida bajariladi.

Butun sanab o’tilgan va bajarilishi lozim bo’lgan muolajalarni(процедуры) bir-biri bilan muloqot qiluvchi bosqich va bosqich ostiga bo’lihni aynan tarmoq modellari bajarishi lozimdir. Bu modellar tarmoq tarkibidagi abonentlar o’rtasidagi muloqotni va turli tarmoqlar o’rtasidagi turli bosqichdagi muloqotni to’g’ri tashkil qilish imkoiyatini yaratadilar. Xozirgi vaqtda eng ko’p ishlatiladigan va tanilgan OSI (Open System Interconnection) ochiq sitemada axborot almashinuvini etalon modeli. Bu holtda “ochiq sistema” atamasi o’zi bilan ulanmagan, ya’ni boshqa qandaydir sistemalar bilan aloqa qilih imkoniyati mavjud sistema tushiniladi (yopiq sistemaga nisbatan).

Muloqot etalon modeli

Xalqaro standartlar tashkiloti ISO (International Standards Organization) tomonidan 1984-yili OSI modeli taqdim qilingan. Shundan beri hamma tarmoq mahsulotlarini ishlab chiqaruvchilar tomonidan foydalanib kelinmoqda. Har qanday universal model singari, OSI modeli ham ancha qo’pol. Tez o’zgarishlarni bajarishi qiyin, shuning uchun turli formalar taklif qiladigan real tarmoq vositalari qabul qilingan vazifalarni taqsimlashga juda ham rioya qilmaydilar.

Lekin OSI modeli bilan tanishish tarmoqda ro’y berayotgan jarayonni yaxshi tushunishga yordam beradi. Hamma tarmoqda bajariladigan vazifalar(funksiyalar) modelda 7 ta bosqichga bo’lingan(1-rasm). Yuqori o’rindagi bosqichlar ancha murakkab bo’lib, global masalalarni bajaradilar. Buning uchun pasdagi bosqichlarni o’z maqsadlari uchun ishlatib ularni boshqaradilar. Pastda joylashgan bosqichlar maqsadi – yuqori bosqichga xizmat ko’rsatish, yuqori joylashgan bosqichlar uchun ko’rsatiladigan bu xizmatning mayda qismlarining bajarilish tartibi muhim emas.

Pastda joylashgan bosqichlar ancha sodda, ancha aniq vazifalarni bajaradilar. Ideal holda har bir bosqich o'zidan tepadagi va pastdagi bosqich bilan muloqot qiladi. Yuqori bosqich ayni vaqtda ilovaga ishlayotgan, amaliy masalaga to'g'ri kelsa, pastgi bosqich esa signalni aloqa kanali orqali uzatishga to'g'ri keladi. 1-rasmda keltirilgan bosqichlar vazifasi tarmoq abonentlarining har biri tomonidan bajariladi.

Bir abonentdagi har bir bosqich Sunday ishlaydiki u boshqa abonentning xuddi shu bosqichi bilan aloqasi bordek, ya'ni tarmoq abonentlarining bir xil nomli bosqichlari o'rtasida virtual mavjud. Bir tarmoq abonentlari o'rtasidagi real aloqa faqat eng past birinchi bosqichda mavjud (jismoniy bosqich). Axborot uzatayotgan abonentda axborot barcha bosqichlardan yuqoridan boshlab pastgi bosqichda tugaydi. Qabul qilayotgan abonentda esa qabul qilingan axborot teskari yo'nalishda, pastki bosqichdan boshlab yuqori bosqichga harakat qiladi.

Hamma bosqich vazifalarini ko'rib chiqamiz.

Amaliy bosqich (Application, прикладный уровень) yoki ilovalar bosqichi, u quyidagi xizmatlarni amalga oshiradi : foydalanuvchining ilovasini shaxsan tasdiqlaydi, masalan, fayllar uzatishning dasturiy vositalari axborot bazasiga ega bo'lish, elektron pochta vositalari, serverda qayd qilish xizmati. Bu bosqich qolgan 6 ta bosqichni boshqaradi.

Prezitentatsiya bosqichi(Presentation, презентативый уровень) axborotni tanishtirish bosqichi, bu bosqichda axborotni aniqlanadi va axborot formatini ko'rinish sintaksisini tarmoqqa qulay ravishda o'zgartiradi, ya'ni tarjimon vazifasini bajaradi. Shu yerda axborot shifrlanadi va deshifrlanadi, lozim bo'lgan taqdirda ularni zichlashtiradi.

Aloqa o'tkazish vaqtini boshqarish bosqichi (Session, сеансовый уровень) aloqa o'tkazish vaqtini boshqaradi(ya'ni aloqani o'rnatadi, tasdiqlaydi va tamomlaydi). Bu bosqichda abonentlarni mantiqiy nomlarini tanish, ularga ega bo'lish huquqini nazorat qilish vazifalari ham bajariladi.

Transport bosqichi (Transport) paketni xatosiz va yo'qotmasdan, kerakli ketma-ketlikda yetkazib berishni amalga oshiradi. Shu yerda yana uzatilayotgan uzatilayotgan axborotlarni paketga joylash uchun bloklarga taqsimlanadi va qabul qilingan axborotlarni qayta tiklanadi.

Tarmoq bosqichi (Network, сетевой уровень) bu bosich paketlarni manzillash, mantiqiy nomlarni jismoniy tarqmoq manziliga o'zgartirish, teskariga ham va shuningdek paketni kerakli abonentga jo'natish yo'nalishini tanlashga (agarda tarmoqda bir nechta abonent bo'lsa) javobgar.

Kanal bosqichi yoki uzatish yo'lini boshqarish bosqichi (data link), bu bosqich standard ko'rishdagi paket tuzishga va boshlash hamda tamom bo'lishni boshqarish maydonini paket tarkibiga joylashishiga javobgardir. Shu yerda yana tarmoqqa ega bo'lishni uzatishdagi xatoliklar aniqlanadi va yana qabul qilish qurilmasiga xato uzatilgan paketlarni qaytatdan uzatishni boshqarish amalga oshiriladi.

Jismoniy bosqich (Physical, физический уровень) – bu modelni eng quyi bosqichi bo'lib, uzatilayotgan axborotni signal kattaligiga kodlashtiradi, uzatish muhitiga qabul qilishni va teskari kodlashni amalga oshirishga javob beradi. Shu yerda yana ulanish moslamalariga, razemlarga, elektr bo'yicha moslashtirish va yerga ulanish hamda to'siqlardan himoya qilish va hokazolarga talablar aniqlanadi.

Modelni quyi ikki bosqichning (1 va 2) vazifasini odatda qurilmalar bajaradi (2-bosqich vazifasini bir qismini tarmoq adapterining dasturiy drayveri bajaradi). Aynan shu bosqichlarda tarmoq topologiyasi, uzatish tezligi, axborot almashishni boshqarish usuli va paket formati

(o'lchami), tarmoq turiga to'g'ri ta'luqli ko'rsakichlar aniqlanadi (Ethernet, Token-Ring, FDDI). Yuqori bosqichlar to'g'ridan-to'g'ri biror aniq qurilma bilan ishlamaydi, vaholangki 3,4 va 5 bosqichlar qurilma xususiyatlarini hisobga olishlari mumkin. 6 va 7 bosqichlar umuman qurilmalarga hech qanday aloqasi yo'q. Tarmoq qurilmalaridan birini boshqa birorta qurilma bilan o'zgartirganda ham ular buni hech vaqt sezmaydilar.

2-bosqich (kanal bosqichi) ikkita bosqich ostiga ajratiladi:

-Yuqori bosqich osti (LLC – Logical Link Control, верхний подуровень) – bu bosqich osti mantiqiy ulashni amalga oshiradi, ya'ni virtual aloqa kanalini o'rnatadi (uning vazifasini bir qismini tarmoq adapterlarining drayver dasturi bajaradi).

-Quyi bosqich osti (MAC – Media Access Control, нижний подуровень) – bu bosqich osti aloqa uzatish muhiti (aloqa kanali) bilan to'g'ridan-to'g'ri ega bo'lishni amalga oshiradi. U tarmoq qurilmasi bilan to'g'ri bog'langan.

OSI modelidan tashqari, 1980-yili fevral oyida qabul qilingan (802 soni yil va oyidan kelib chiqqan) IEEE Project 802 modeli ham mavjud. Bu modelni OSI modelini aniqlashtirilgan, rivojlantirilgan modeli deb qarash mumkin.

Bu model aniqlashtirgan standartlar (802-spesifikatsiya) o'n ikki toifaga bo'linib, ularning har biriga nomer berilgan. Ular quyidagilar :

* 802-1 – tarmoqlarni birlashtirish.
* 802-2 – mantiqiy aloqani boshqarish.
* 802-3 – "shina" topologiyali CSSA/CD ega bo'lish usuli mahalliy hisoblash tarmoq va Ethernet.
* 802-4 – "shina" topologiyali lokal tarmoq, markerli ega bo'lish.
* 802-5 – "halqa" toplogiyali lokal tarmoq, markerli ega bo'lish.
* 802-6 – shahar tarmog'I (Metropolitan Area Network, MAN).
* 802-7 – keng miqyosda aloqa olib boorish texnologiyasi (широковещательная технология).
* 802-8 – optotolali texnologiya.
* 802-9 – tovushni va axborotlarni uzatish imkoniyati bor integral tarmoq.
* 802-10 – tarmoq xavfsizligi.
* 802-11 – simsiz tarmoq.
* 802-12 – "yulduz" topologiyali markazni boshqarishga ega mahalliy tarmoq (100 VG-Any LAN).

802-3, 802-4, 802-5, 802-12 standartlar OSI model etalonning ikkinchi (kanal) bosqichiga qarashli MAC bosqich osti tarkibiga to'g'ri keladi. Qolgan 802-spesifikatsiyalar tarmoqning umumiy masalalarini hal qiladilar.

Lokal tarmoqni boshqarish arxitekturasi

Mahallliy hisoblash tarmoq qurilmalari abonentlar o'rtasidagi real aloqani ta'minlab beradilar. Tarmoqni loyihalashtirish bosqichida qurilmalarni tanlash juda katta ahamiyatga ega, chunki qurilmalarni narxi umumiy tarmoq narxining katta qismini tashkil qiladi. Aloqa qurilmalarini o'zgartirish esa, nafaqat qo'shimcha mablag'ni talab qiladi, yana qiyin ish hajmini oshishga ham sabab bo'ladi. Mahalliy tarmoq qurilmalariga quyidagilar kiradi:

- axborot uzatish uchun kabellar;
- kabellarni ulash uchun razemlar;
- moslovchi terminatorlar;
- tarmoq adapterlari;

- repiterlar;
- transiverlar;
- konsentratorlar;
- ko’priklar ;
- yo’naltirgichlar (marshrutizatorlar);
- shlyuzlar.

Ularni ba’zilarini ko’rib chiqamiz.

Tarmoq adapterlarini turli adabiyotlarda yana kontroller, karta, plata, interfeyslar, NIC (Network Interface Card) nomlari bilan ham ataydilar. Bu qurilmalar mahalliy tarmoqning asosiy qismi, ularsiz tarmoq hosil qilish mumkin emas. Tarmoq adapterlarining vazifasi – kompyuterni (yoki boshqa abonentni) tarmoq bilan ulash, yana qabul qilingan qoidalarga rioya qilgan holda kompyuter bilan aloqa kanali o’rtasida axborot almashinuvini ta’minlashdir. Aynan shu qurilmalar OSI modelining quyi bosqichlari bajarishi kerak bo’lgan vazifalarni amalga oshiradi. Odatda tarmoq adapterlari plata ko’rinishida ishlab chiqariladi va kompyuterni sistema magistrallarini kengaytirish uchun qoldirilgan razemga o’rnatiladi (odatda ISA yoki PCI). Tarmoq adapter platasida ham odatda bitta yoki bir nechta tashqi razemlar bo’lib, ularga tarmoq kabellari ulanadi.

Tarmoq adapterlarining hamma vazifalari ikkiga bo’linadi : magistral va tarmoq. Magistral vazifalari adapter bilan kompyuterning sistema shinasi o’rtasidagi almashinuvni amalga oshirish (ya’ni o’zining magistral manzilini tanish, kompyuterga axborot uzatish va kompyuterdan axborot qabul qilish, kompyuter uchun uzilish signalini hosil qilish va hokazolar) kiradi. Tarmoq vazifalari esa adapterlarni tarmoq bilan muloqotini bilan ta’minlashdir.

Kompyuter tarkibida adapter platasini ravon ishlashi uchun uning asosiy ko’rsatkichlarini to’g’ri o’rnatish kerak :

v kiritish-chiqarish portining asos manzilini (ya’ni manzil maydonining boshlanish manzilini, u orqali kompyuter adapter bilan muloqot qiladi) ;

v foydalaniladigan uzilish nomeri (ya’ni taqiqlash yo’lining nomeri, u orqali kompyuterga adapter o’zi bilan axborot almashinuvi zarurligi haqida xabar beradi) ;

v bufer hamda yuklanuvchi xoriralarning asos manzili (ya’ni adapter tarkibiga kiruvchi kompyuter aynan shu xotira bilan muloqot qilishi uchun).

Bu ko’rsatkichlarni foydalanuvchi tomonidan adapterdagi ulash moslamasi (jamer) yordamida tanlab o’rnatish mumkin, lekin plata beriladigan maxsus adapterni initsializatsiyalovchi dastur yordamida ham o’rnatish mumkin. Hamma ko’rsatkichlarni (manzil va uzilish nomeri) tanlashda e’tibor berish kerakki, ular kompyuterning boshqa qurilmalarida o’rnatilib band bo’lgan ko’rsatkichlaridan farq qilishi kerak. Hozirgi zamon tarmoq adapterlarida ko’pincha Plug-and-Play tartibi qo’llaniladi, ya’ni ko’rsatkichlarni foydalanuvchi tomonidan o’rnatilishining (sozlashning) hojati yo’q, ularda sozlash kompyuter elektr manbayiga ulanganda avtomatik ravishda amalga oshiriladi.

Adapterning asosiy tarmoq vazifalariga quyidagilar kiradi :

v kompyuter va mahalliy tarmoq kabelini galvanik ajratish (buning uchun odatda signalni impuls transformatori orqali uzatiladi) ;

v mantiqy signallarni tarmoq signallariga va aksiga o’zgartirish ;

v tarmoq signallarini kodlash va dekodirlash ;

v qabul qilinayotgan paketlardan aynan shu abonentga manzillashtirilgan paketlarni tanlab qabul qilish ;

v parallel kodni ketma-ket kodga axborot uztilishda o'zgartirish va axborot qabul qilishda aksiga o'zgartirsh ;

v adapterning bufer xotirasiga uzatilayotgan va qabul qilinayotgan axborotlarni yozish ;

v qabul qilingan axborot almashinuvini boshqarish usulida tarmoqqa ega bo'lishni tashkil qilish ;

v axborotlarni qabul qilish va uzatishda paketlarning nazorat bitlari yig'indisini hisoblash.

Odatda hamma tarmoq vazifalari maxsus katta integral sxemalar yordamida amalga oshirilganligi uchun adapter platasining o'lchami kichik va narxi arzondir.

Agarda tarmoq adapteri bir necha turdagi kabellar bilan ishlay olsa, u holda yana bir sozlanishi lozim bo'lgan ko'rsatkich qo'shiladi (kabel turini tanlash). Masalan, adapter platasida u yoki bu turdagi kabelga ulash uchun moslama (перемычка) bo'lishi mukin.

Adapterdan boshqa hamma mahalliy tarmoq qurilmalari yordamchi qurilmalar bo'lib, ko'pincha ularsiz ham ishni tashkil qilish mumkin.

Transiverlar yoki uzatish va qabul qilish qurilmalari (Transmitter-Receiver, приемопередатчики), ular adapter bilan tarmoq kabeli o'rtasidagi axborotni uzatish uchun xizmat qiladilar yoki tarmoqning ikki qismlari (segment) o'rtasidagi axborot uzatishni amalga oshiradilar. Transiver signalni kuchaytirish, signal qiymatlarini o'zgartirish yoki signal ko'rinishini o'zgartirish (masalan elektr signalni yorug'lik signaliga va teskarisiga) ishlarini bajaradi. Ko'pincha adapter platasiga o'rnatigan qabul qilish va uzatish qurilmasini transiver deb ham yuritiladi.

Repiterlar yoki qaytaruvchi (repeater, повторитель) qurilmasi transiverga nisbatan ancha oddiy vazifani bajaradi. U faqat susaygan signalni qayta tiklab avvalgi, ya'ni uzatilgan vaqtdagi ko'rinishga (amplitudasi va ko'rinishini) keltiradi. Signalni qayta tiklashning asosiy maqsadi, tarmoq uzunligini oshirishdan iborat. Lekin repiterlar ko'pincha boshqa vazifalarni ham bajaradilar, masalan, tarmoqqa ulanadigan qismlarni galvanik ajratish. Repiterlar va transiverlar hech mahal o'zidan o'tayotgan axborotga hech qanday ishlov bermaydilar.

Yo'naltirgichlar – har bir paket uchun qulay uzatish yo'lini tanlab, uzatuvchi qurilma. Buning uchun tarmoqning eng ko'p yuklangan qismlarini va buzilgan qismlarini aylanib o'tishi kerak. Ular odatda murakkab shoxlamali tarmoqda ishlatiladi, bu holda alohida olingan abonentlar o'rtasida bir necha aloqa yo'li mavjud bo'lishi mumkin.

14-MAVZU: XAVFSIZLIKNI AMALIY BOSHQARISH

MA’RUZA MASHG’ULOTI REJASI:

14.1. Tarmoq xavfsizligiga tahdidlarning turlari

14.2. Tarmoq orqali ma’lumot almashish mobaynida yuborilayotgan axborotni eshitish va o‘zgartirishga qarshi samarali natija beruvchi texnologiyalar

Tayanch so‘z va iboralar Eavesdropping, Denial-of-service, Port scanning, IPSec, IDC, VPN.

Tashkilot tarmog'i doirasida xavfsizlikni global boshqarish siyosati. Lokal xavfsizlik siyosatini shakllantirish. Lokal xavfsizlik siyosatini barcha axborot himoyalovchi qurilmalargacha olib borish.

Mamlakatimiz siyosatining ustuvor yo‘nalishlariga kiritilgan kompyuter va axborot texnologiyalari, telekomunikatsiya, ma’lumotlarni uzatish tarmoqlari, Internet xizmatlaridan foydalanish rivojlanmoqda va modernizatsiyalashmoqda. Jamiyatimizning barcha sohalariga kundalik hayotimizga zamonaviy axborot texnologiyalarini keng joriy etish istiqboldagi maqsadlarimizga erishishni ta’minlaydi. Har bir soha faoliyatida Internet tarmog‘idan foydalanish ish unumdorligini oshirmoqda.

Aynan tarmoqdan foydalangan holda tezkor ma’lumot almashish vaqtdan yutish imkonini beradi. Xususan, yurtimizda Elektron hukumat tizimi shakllantirilishi va uning zamirida davlat boshqaruv organlari hamda aholi o‘rtasidagi o‘zaro aloqaning mustahkamlanishini tashkil etish tarmoqdan foydalangan holda amalga oshadi. Tarmoqdan samarali foydalanish demokratik axborotlashgan jamiyatni shakllantirishni ta’minlaydi. Bunday jamiyatda, axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha tezkor natijaga ega bo‘linadi.

Biroq tarmoqqa noqonuniy kirish, axborotlardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Ish faoliyatini tarmoq bilan bog‘lagan korxona, tashkilotlar hamda davlat idoralari ma’lumot almashish uchun tarmoqqa bog‘lanishidan oldin tarmoq xavfsizligiga jiddiy e’tibor qara-tishi kerak. Tarmoq xavfsizligi uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotni ishonchli tizimli tarzda ta’minlash maqsadida turli vositalar va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirish orqali amalga oshiriladi. Tarmoq xavsizligini ta’minlash maqsadida qo‘llanilgan vosita xavf-xatarni tezda aniqlashi va unga nisbatan qarshi chora ko‘rishi kerak. Tarmoq xavfsizligiga tahdidlarning ko‘p turlari bor, biroq ular bir necha toifalarga bo‘linadi:

- axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (Eavesdropping);
- xizmat ko‘rsatishdan voz kechish; (Denial-of-service)
- portlarni tekshirish (Port scanning).

Axborotni uzatish jarayonida, eshitish va o‘zgartirish hujumi bilan telefon aloqa liniyalari, internet orqali tezkor xabar almashish, videokonferensiya va faks jo‘natmalari orqali amalga oshiriladigan axborot almashinuvida foydalanuvchilarga sezdirmagan holatda axborotlarni tinglash, o‘zgartirish hamda to‘sib qo‘yish mumkin. Bir qancha tarmoqni tahlillovchi protokollar orqali bu hujumni amalga oshirish mumkin. Hujumni amalga oshiruvchi dasturiy ta’minotlar orqali CODEC (video yoki ovozli analog signalni raqamli signalga aylantirib berish va aksincha) standartidagi raqamli tovushni osonlik bilan yuqori sifatli, ammo katta hajmni egallaydigan ovozli fayllar (WAV)ga aylantirib beradi. Odatda bu hujumning amalga oshirilish jarayoni foydalanuvchiga umuman sezilmaydi. Tizim ortiqcha zo‘riqishlarsiz va shovqinsiz belgilangan amallarni bajaraveradi.

Axborotning o‘g‘irlanishi haqida mutlaqo shubha tug‘ilmaydi. Faqatgina oldindan ushbu tahdid haqida ma’lumotga ega bo‘lgan va yuborilayotgan axborotning o‘z qiymatini saqlab qolishini xohlovchilar maxsus tarmoq xafvsizlik choralarini qo‘llash natijasida himoyalangan tarmoq orqali ma’lumot almashish imkoniyatiga ega bo‘ladilar. Tarmoq orqali ma’lumot almashish mobaynida yuborilayotgan axborotni eshitish va o‘zgartirishga qarshi bir necha samarali natija beruvchi texnologiyalar mavjud:

- IPSec (Internet protocol security) protokoli;
- VPN (Virtual Private Network) virtual xususiy tarmoq;
- IDS (Intrusion Detection System) ruxsatsiz kirishlarni aniqlash tizimi.

Ipsec (Internet protocol security) bu xavfsizlik protokollari hamda shifrlash algoritmlaridan foydalangan holda tarmoq orqali xavfsiz ma’lumot almashish imkonini beradi. Bu maxsus standart orqali tarmoqdagi kompyuterlarning o‘zaro aloqasida dastur va ma’lumotlar hamda qurilmaviy vositalar bir-biriga mos kelishini ta’minlaydi. Ipsec protokoli tarmoq orqali uzatilayotgan axborotning sirliligini, ya’ni faqatgina yubo-ruvchi va qabul qiluvchiga tushunarli bo‘lishini, axborotning sofligini hamda paketlarni autentifikatsiyalashni amalga oshiradi. Zamonaviy axborot texnologiyalarni qo‘llash har bir tashkilotning rivojlanishi uchun zaruriy vosita bo‘lib qoldi, Ipsec protokoli esa aynan quyidagilar uchun samarali himoyani ta’minlaydi:

- bosh ofis va filiallarni global tarmoq bilan bog‘laganda;
- uzoq masofadan turib, korxonani internet orqali boshqarishda;
- homiylar bilan bog‘langan tarmoqni himoyalashda;
- elektron tijoratning xavfsizlik darajasini yuksaltirishda.

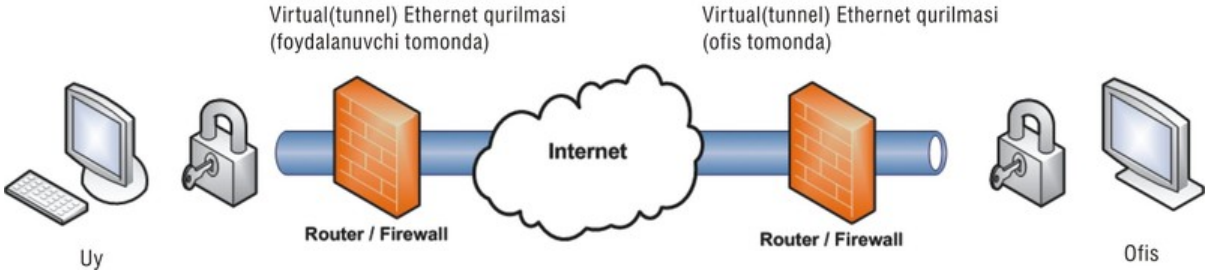
VPN (Virtual Private Network) virtual xususiy tarmoq sifatida ta’riflanadi. Bu texnologiya foydalanuvchilar o‘rtasida barcha ma’lumotlarni almashish boshqa tarmoq doirasida ichki tarmoqni shakllantirishga asoslangan, ishonchli himoyani ta’minlashga qaratilgan. VPN uchun tarmoq asosi sifatida Internetdan foydalaniladi.

VPN texnologiyasining afzalligi. Lokal tarmoqlarni umumiy VPN tarmog‘iga birlashtirish orqali kam xarajatli va yuqori darajali himoyalangan tunelni qurish mumkin. Bunday tarmoqni yaratish uchun sizga har bir tarmoq qismining bitta kompyuteriga filiallar o‘rtasida ma’lumot almashishiga xizmat qiluvchi maxsus VPN shlyuz o‘rnatish kerak. Har bir bo‘limda axborot almashishi oddiy usulda amalga oshiriladi. Agar VPN tarmog‘ining boshqa qismiga ma’lumot jo‘natish kerak bo‘lsa, bu holda barcha ma’lumotlar shlyuzga jo‘natiladi. O‘z navbatida, shlyuz ma’lumotlarni qayta ishlashni amalga oshiradi, ishonchli algoritm asosida shifrlaydi va Internet tarmog‘i orqali boshqa filialdagi shlyuzga jo‘natadi. Belgilangan nuqtada ma’lumotlar qayta deshifrlanadi va oxirgi kompyuterga oddiy usulda uzatiladi. Bularning barchasi foydalanuvchi uchun umuman sezilmas darajada amalga oshadi hamda lokal tarmoqda ishlashdan hech qanday farq qilmaydi. Eavesdropping hujumidan foydalanib, tinglangan axborot tushunarsiz bo‘ladi.

Bundan tashqari, VPN alohida kompyuterni tashkilotning lokal tarmog‘iga qo‘shishning ajoyib usuli hisoblanadi. Tasavvur qilamiz, xizmat safariga noutbukingiz bilan chiqqansiz, o‘z tarmog‘ingizga ulanish yoki u yerdan biror-bir ma’lumotni olish zaruriyati paydo bo‘ldi. Maxsus dastur yordamida VPN shlyuz bilan bog‘lanishingiz mumkin va ofisda joylashgan har bir ishchi kabi faoliyat olib borishigiz mumkin. Bu nafaqat qulay, balki arzondir.

VPN ishlash tamoyili. VPN tarmog‘ini tashkil etish uchun yangi qurilmalar va dasturiy ta’minotdan tashqari ikkita asosiy qismga ham ega bo‘lish lozim: ma’lumot uzatish protokoli va uning himoyasi bo‘yicha vositalar.

Ruxsatsiz kirishni aniqlash tizimi (IDS) yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi. Ruxsatsiz kirishlarni aniqlash tizimlari deyarli chorak asrlik tarixga ega. Ruxsatsiz kirishlarni aniqlash tizimlarining ilk modellari va prototiplari kompyuter tizimlarining audit ma'lumotlarini tahlillashdan foydalangan. Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.



14.1-rasm. Ruxsatsiz kirishlarni aniqlash tizimi modeli

IDS tizimlari arxitekturasi tarkibiga quyidagilar kiradi:

- himoyalangan tizimlar xavfsizligi bilan bog‘liq holatlarni yig‘ib tahlillovchi sensor qism tizimi;
- sensorlar ma'lumotlariga ko‘ra shubhali harakatlar va hujumlarni aniqlashga mo‘ljallangan tahlillovchi qism tizimi;
- tahlil natijalari va dastlabki holatlar haqidagi ma'lumotlarni yig‘ishni ta'minlaydigan omborxona;
- IDS tizimini konfiguratsiyalashga imkon beruvchi, IDS va himoyalangan tizim holatini kuzatuvchi, tahlil qism tizimlari aniqlagan mojarolarni kuzatuvchi boshqaruv konsoli.

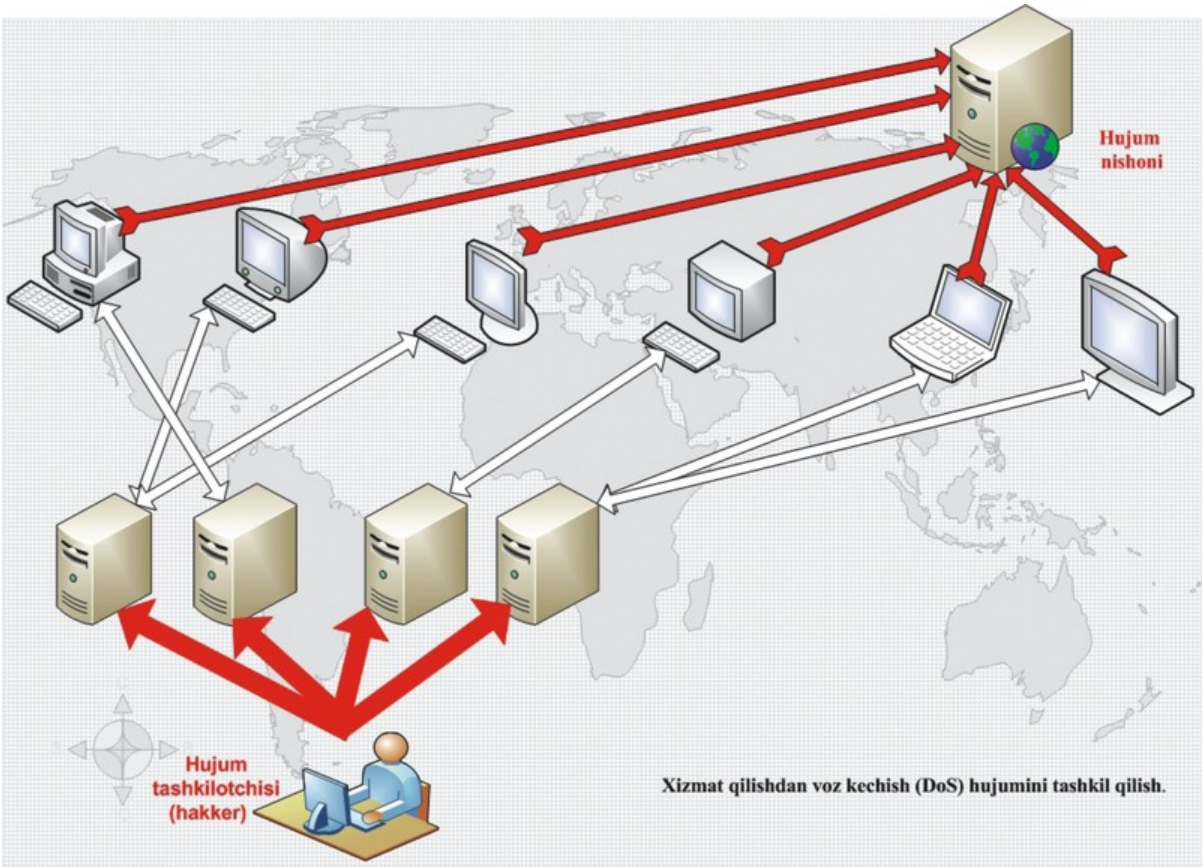
Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (NIDS) ishlash tamoyili quyidagicha:

1. tarmoqqa kirish huquqiga ega bo‘lgan trafiklarni tekshiradi;
2. zararli va ruxsatga ega bo‘lmagan paketlarga cheklov qo‘yadi.

Sanab o‘tilgan xavfsizlik bosqichlarini qo‘llagan holda Eavesdropping tahdidiga qarshi samarali tarzda himoyalanish mumkin.

DOS (Denial-of-service) tarmoq hujumning bu turi xizmat qilishdan voz kechish hujumi deb nomlanadi. Bunda hujum qiluvchi legal foydalanuvchilarning tizim yoki xizmatdan foydalanishiga to‘sqinlik qilishga urinadi. Tez-tez bu hujumlar infratuzilma resurslarini xizmatga ruxsat so‘rovlari bilan to‘lib toshishi orqali amalga oshiriladi. Bunday hujumlar alohida xostga yo‘naltirilgani kabi butun tarmoqqa ham yo‘naltirilishi mumkin. Hujumni amalga oshirishdan oldin obyekt to‘liq o‘rganilib chiqiladi, ya'ni tarmoq hujumlariga qarshi qo‘llanilgan himoya vositalarining zaifligi yoki kamchliklari, qanday operatsion tizim o‘rnatilgan va obyekt ish faoliyatining eng yuqori bo‘lgan vaqti. Quyidagilarni aniqlab va tekshirish natijalariga asoslanib, maxsus dastur yoziladi. Keyingi bosqichda esa yaratilgan dastur katta mavqega ega bo‘lgan serverlarga yuboriladi. Serverlar o‘z bazasidagi ro‘yxatdan o‘tgan foydalanuvchilarga yuboradi. Dasturni qabul qilgan foydalanuvchi ishonchli server tomonidan yuborilganligini bilib yoki bilmay dasturni o‘rnatadi. Aynan shu holat minglab hattoki, millionlab kompyuterlarda sodir bo‘lishi mumkin. Dastur belgilangan vaqtda barcha

kompyuterlarda faollashadi va to‘xtovsiz ravishda hujum qilinishi mo‘ljallangan obyektning serveriga so‘rovlar yuboradi. Server tinimsiz kelayotgan so‘rovlarga javob berish bilan ovora bo‘lib, asosiy ish faoliyatini yurgiza olmaydi. Server xizmat qilishdan voz kechib qoladi.



14.2-rasm-Xizmat qilishdan voz kechish hujumini tashkil qilish modeli

Xizmat qilishdan voz kechish hujumidan himoyalanishning eng samarali yo‘llari quyidagilar:

- tarmoqlararo ekranlar texnologiyasi (Firewall);
- IPsec protokoli.

Tarmoqlararo ekran ichki va tashqi perimetrlarning birinchi himoya qurilmasi hisoblanadi. Tarmoqlararo ekran axborot-kommunikatsiya texnologiya (AKT)larida kiruvchi va chiquvchi ma’lumotlarni boshqaradi va ma’lumotlarni filtrlash orqali AKT himoyasini ta’minlaydi, belgilangan mezonlar asosida axborot tekshiruvini amalga oshirib, paketlarning tizimga kirishiga qaror qabul qiladi. Tarmoqlararo ekran tarmoqdan o‘tuvchi barcha paketlarni ko‘radi va ikkala (kirish, chiqish) yo‘nalishi bo‘yicha paketlarni belgilangan qoidalar asosida tekshirib, ularga ruxsat berish yoki bermaslikni hal qiladi. Shuningdek, tarmoqlararo ekran ikki tarmoq orasidagi himoyani amalga oshiradi, ya’ni himoyalanayotgan tarmoqni ochiq tashqi tarmoqdan himoyalaydi. Himoya vositasining quyida sanab o‘tilgan qulayliklari, ayniqsa, paketlarni filtrlash funksiyasi DOS hujumiga qarshi himoyalanishning samarali vositasidir. Paket filtrlari quyidagilarni nazorat qiladi:

- fizik interfeys, paket qayerdan keladi;
- manbaning IP-manzili;
- qabul qiluvchining IP-manzili;
- manba va qabul qiluvchi transport portlari.

Tarmoqlararo ekran ba’zi bir kamchiliklari tufayli Dos hujumidan to‘laqonli himoyani ta’minlab bera olmaydi:

• loyihalashdagi xatoliklar yoki kamchiliklar — tarmoqlararo ekranlarning har xil texnologiyalari himoyalana-yotgan tarmoqqa bo‘ladigan barcha suqilib kirish yo‘llarini qamrab olmaydi;

• amalga oshirish kamchiliklari — har bir tarmoqlararo ekran murakkab dasturiy (dasturiy-apparat) majmua ko‘rinishida ekan, u xatoliklarga ega. Bundan tashqari, dasturiy amalga oshirish sifatini aniqlash imkonini beradigan va tarmoqlararo ekranda barcha spetsifikatsiyalangan xususiyatlar amalga oshirilganligiga ishonch hosil qiladigan sinov o‘tkazishning umumiy metodologiyasi mavjud emas;

• qo‘llashdagi (ekspluatatsiyadagi) kamchiliklar — tarmoqlararo ekranlarni boshqarish, ularni xavfsizlik siyosati asosida konfiguratsiyalash juda murakkab hisoblanadi va ko‘pgina vaziyatlarda tarmoqlararo ekranlarni noto‘g‘ri konfiguratsiyalash hollari uchrab turadi. Sanab o‘tilgan kamchiliklarni IPsec protokolidan foydalangan holda bartaraf etish mumkin. Yuqoridagilarni umumlashtirib, tarmoqlararo ekranlar va IPsec protokolidan to‘g‘ri foydalanish orqali DOS hujumidan yetarlicha himoyaga ega bo‘lish mumkin.

Port scanning hujum turi odatda tarmoq xizmatini ko‘rsatuvchi kompyuterlarga nisbatan ko‘p qo‘llanadi. Tarmoq xavfsizligini ta’minlash uchun ko‘proq virtual portlarga e’tibor qaratishimiz kerak. Chunki portlar ma’lumotlarni kanal orqali tashuvchi vositadir. Kompyuterda 65 536ta standart portlar mavjud. Kompyuter portlarini majoziy ma’noda uyning eshigi yoki derazasiga o‘xshatish mumkin. Portlarni tekshirish hujumi esa o‘g‘rilar uyga kirishdan oldin eshik va derazalarni ochiq yoki yopiqligini bilishiga o‘xshaydi. Agar deraza ochiqligini o‘g‘ri payqasa, uyga kirish oson bo‘ladi. Hakker hujum qilayotgan vaqtda port ochiq yoki foydalanilmayotganligi haqida ma’lumot olishi uchun Portlarni tekshirish hujumidan foydalanadi.

Bir vaqtda barcha portlarni tahlil qilish maqsadida xabar yuboriladi, natijada real vaqt davomida foydalanuvchi kompyuterning qaysi portini ishlatayotgani aniqlanadi, bu esa kompyuterning nozik nuqtasi hisob-lanadi. Aynan ma’lum bo‘lgan port raqami orqali foydalanuvchi qanday xizmatni ishlatayotganini aniq aytish mumkin. Masalan, tahlil natijasida quyidagi port raqamlari aniqlangan bo‘lsin, aynan shu raqamlar orqali foydalanilayotgan xizmat nomini aniqlash mumkin

• Port #21: FTP (File Transfer Protocol) fayl almashish protokoli;

• Port #35: Xususiy printer server;

• Port #80: HTTP traffic (Hypertext Transfer [Transport] Protocol) gipermatn almashish protokoli;

• Port #110: POP3 (Post Office Protocol 3) E-mail portokoli.

Hujum turlari	Himoya vositalari
Axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (*Eavesdropping*)	IPSec (*Internet protocol security*) protokoli. VPN (*Virtual Private Network*) virtual xususiy tarmoq IDS (*Intrusion Detection System*) ruxsatsiz kirishlarni aniqlash tizimi
Xizmat ko‘rsatishdan voz kechish (*Denial-of-service*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*) IPSec (*Internet protocol security*) protokoli.
Portlarni tekshirish (*Port scanning*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*)

14.3-rasm. Hujum turlari va himoyalanish vositalari

Portlarni tekshirish hujumiga qarshi samarali himoya yechimi tarmoqlararo ekran texnologiyasidan unumli foydalanish kutilgan natija beradi. Barcha portlarni bir vaqtda tekshirish

haqidagi kelgan so‘rovlarga nisbatan tarmoqlararo ekranga maxsus qoida joriy etish yo‘li bilan hujumni bartaraf etish mumkin.

15-MAVZU: AXBOROT JINOYATINI ANIQLASH UCHUN HUQUQIY QONUNCHILIK BAZASI

MA’RUZA MASHG’ULOTI REJASI:

15.1. Axborot jinoyatini aniqlash sohasida xorij tajribasi
15.2. Axborot jinoyatini aniqlash uchun huquqiy qonunchilik bazasi

Tayanch so‘z va iboralar: umumiy ob’ekt, maxsus ob’ekt, turdosh ob’ekt, bevosita ob’ekt.

Hozirgi ijtimoiy taraqqiyot voqeliklari, texnologik jarayonlarning elektron vositalar bilan boshqarish usullariga o‘tilishi, EHM yordamida amalga oshiriladigan aktlarga yuridik kuch berilishi ushbu jarayonlardan axborot texnologiyalari sohasida jinoyatlar sodir etish uchun foydalanishga ham shart-sharoit yaratdi. Telekommunikatsiya tarmoqlarining tarkibiy qismlari ishiga, ular muhitida ishlovchi kompyuter dasturlariga g‘ayriqonuniy aralashish, kompyuter axborotini qonunga xilof ravishda modifikatsiyalashtirish va yo‘q qilib yuborish davlat infratuzilmasining nihoyatda muhim elementlari ishini buzishi mumkin hamda ko‘plab odamlarning halok bo‘lishi, katta miqdorda mulkiy zarar yetkazilishi yoki boshqa ijtimoiy xavfli oqibatlarning kelib chiqishi xavfini tug‘diradi.

Xorijda tarmoq texnologiyalari rivojlanishining boshlang‘ich bosqichida, iqtisodiyotning axborot texnologiyalariga unchalik bog‘liq emasligi tufayli, virusli va boshqa turdagi kompyuter hujumlaridan yyetkaziladigan zarar unchalik katta emas edi. Hozirgi vaqtda bunday hujumlar soni borgan sari ko‘payib borayotgan, ularni avtomatlashtirish mexanizmlari yaratilayotgan, fuqarolar, tijoratchilar, davlat hokimiyati organlari axborotdan foydalanish va uni ayirboshlashning elektron vositalariga juda bog‘liq bo‘lib qolgan sharoitda axborot tizimlariga hujumlarning amalga oshirilishidan ko‘rilayotgan zarar ulkan summalarni tashkil etmoqda.

Kompyuter texnologiyalari sohasidagi jinoyatlarning ko‘payishi, ularning yuqori darajadagi ijtimoiy xavfliligi mazkur jinoyatlardan muhofaza qilish choralarini (avvalo kompyuter texnologiyalarining o‘zini qo‘riqlash orqali) ishlab chiqishni taqozo etdi. Olimlar tadqiqotlarining ko‘rsatishicha, bunday muhofaza vositalarning 60 % huquqiy vositalarga, 20 % kriptografik va 20 % dasturiy, apparatga oid hamda boshqa jismoniy, tashkiliy vositalarga to‘g‘ri keladi.

1965 yilda AQSHda axborot texnologiyalari xavfsizligini ta’minlashga qaratilgan va 1973 yilda Shvetsiyada kompyuterni suiiste’mol qilganlik uchun jinoiy javobgarlik to‘g‘risidagi dastlabki qonunlar hamda 1994 yilda BMT tomonidan kompyuterlardan foydalanish bilan bog‘liq jinoyatlarning oldini olish va ularga qarshi kurash bo‘yicha yo‘riqnoma qabul qilindi.

O‘zbekistonda axborot texnologiyalari sohasidagi munosabatlarni qonun hujjatlari bilan tartibga solish va muhofaza qilish masalasi o‘tgan asrning 90 – yillari boshlarida hal etila boshlangan. Bunday kechikish muayyan darajada mamlakatimizda EHM rivojlanishining darajasi pastligi bilan bog‘liq edi.

1994 yil 6 mayda O‘zbekiston Respublikasining «Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma’lumotlar bazalarining huquqiy himoyasi to‘g‘risida»gi qonuni qabul qilindi. Unga keyinchalik O‘zbekiston Respublikasining 2002 yil 5 aprel va 8 avgustdagi qonunlari bilan o‘zgartish va qo‘shimchalar kiritildi. Mazkur qonunda ma’muriy va jinoiy javobgarlik haqida so‘z yuritilgan (15-modda) va mualliflik huquqlarini buzganlik uchun javobgarlik nazarda tutilgan. O‘zbekiston Respublikasining «Axborot erkinligi printsiplari va kafolatlari to‘g‘risida»gi 2002 yil 12 dekabr hamda «Axborotlashtirish to‘g‘risida»gi 2003 yil 11 dekabr qonunlarining qabul qilinishi axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash bo‘yicha qonun hujjatlarining asosini

tashkil etadi. Ularda jinoyatlarni to‘g‘ri kvalifikatsiya qilish va aybdor shaxslarni jinoiy javobgarlikka tortish uchun printsipial ahamiyatga ega bo‘lgan ko‘plab huquqiy va texnikaviy terminlarga ta’riflar berilgan.

Axborot texnologiyalari sohasidagi jinoyatlar nafaqat intellektual mulk daxlsizligini buzish, balki fuqarolarning shaxsiy hayoti haqidagi ma’lumotlarni oshkor etish, bevosita zarar va olinmagan foyda ko‘rinishida mulkiy zarar yetkazilishi, firma obro‘sining to‘kilishi, korxona, muassasa va tashkilotlar huquqiy faoliyatini buzishning har xil turlari va boshqalardir.

Yuqoridagilardan kelib chiqqan holda ta’kidlash mumkinki ushbu turdagi jinoyatlar axborot texnologiyalaridan qonuniy, xavfsiz foydalanishni ta’minlovchi munosabatlarga tajovuz qiladi.

Jinoyat ob’ektining to‘rt bo‘g‘inli tuzilishga ega ekanligi haqidagi nazariyaga asoslanadigan bo‘lsak, axborot texnologiyalaridan g‘ayriqonuniy foydalanish bilan bog‘liq jinoiy tajovuzning **umumiy ob’ektini** jinoyat qonuni bilan muhofaza etiladigan barcha ijtimoiy munosabatlar majmui, **maxsus ob’ektini** jamoat xavfsizligi va jamoat tartibi, **turdosh ob’ektini** axborot texnologiyalaridan qonuniy va xavfsiz foydalanish borasidagi ijtimoiy munosabatlar majmui tashkil qiladi. **Bevosita ob’ekti** esa muayyan moddaning nomi va dispozitsiyasidan kelib chiqib aniqlanadi. Aksariyat hollarda axborot texnologiyalari sohasidagi jinoyatning asosiy tarkibi ob’ektining ushbu turi muqobil tarzda ifodalangan, og‘irlashtiruvchi tarkiblarda ularning soni, tabiiyki, ko‘paytirilgan.

Umumiy, maxsus, turdosh va bevosita ob’ektlarning ajratilishi ob’ektiv ravishda ular qamrab oladigan jinoiy-huquqiy qo‘riqlash ob’ekti bo‘lmish ijtimoiy munosabatlarning butun hajmini aks ettiradi va O‘zbekiston Respublikasi Jinoyat kodeksining hozirgi tuzilishiga muvofiq keladi[11].

Axborot texnologiyalari sohasidagi jinoyatlarning ob’ekti nimadan iborat, degan masala hanuzgacha bahsli bo‘lib kelmoqda. Jumladan, yuridik adabiyotlarda ushbu turdagi jinoyatlarning ob’ekti va predmeti xususida har xil fikrlar bor. Masalan, V. V. Krilov ushbu jinoyatlarning ob’ektini EHM ma’lumotlari tashkil qiladi, deb hisoblaydi[12]. L. Chichko esa ob’ekt deganda EHM axborotini[13], V. B. Vexov esa mashina axborotini[14] tushunishni ta’kidlagan. Axborot jinoyat ob’ekti bo‘lishi mumkin degan qarash tarafdorlari fikricha axborot, shu jumladan, kompyuter axboroti jamiyat uchun yaratilgan qulaylikdir, shu sababli ular noqonuniy yo‘q qilinganida yoki modifikatsiyalashtirilganida zarar ko‘rilishi ayni haqiqatdir. Ammo kompyuter axboroti (masalan, sir saqlanadigan ma’lumotlar) qonunga xilof tarzda nusxa ko‘chirilishi va ular to‘sib qo‘yilishi mumkin. Bunda axborot o‘zi aslo zarar ko‘rmaydi. Vaholanki, jinoyat ob’ekti doimo jinoiy qilmishdan zarar ko‘radi, aks holda, jinoyat tarkibi mavjud bo‘lmaydi. Xo‘sh, jinoyat nimada namoyon bo‘ladi? Yuqoridagi ikki holatda nima yuz beradi? Unda nima va qanday zarar ko‘radi?

Birinchi holda axborot qonuniy egasining undan monopol foydalanish munosabatlariga, ikkinchi holda esa bevosita qonuniy va xavfsiz foydalanish munosabatlariga zarar yetadi. Binobarin, kompyuter axboroti o‘z-o‘zicha har doim ham zarar ko‘rmaydi, ammo barcha hollarda undan foydalanish munosabatlari buziladi degan xulosaga kelish mumkin.

Jinoiy-huquqiy tushunishda kompyuter axboroti axborot texnologiyalari sohasidagi jinoyatlarning predmeti hisoblanadi. Masalan bunday holatlar Jinoyat kodeksi 278^1, 278^2, 278^4 va 278^6-moddalarining dispozitsiyalarida to‘g‘ridan-to‘g‘ri ko‘rsatilgan. Boshqa hollarda esa

---

[11] Qarang: Таджиханов Б.У. Уголовно-правовые меры борьбы с терроризмом / Отв. ред. докт. юрид. наук А.С. Якубов. – Т.:, 2003. – С.4–20; Наумов А.В. Российское уголовное право. Общая часть. – М., 1999. –162–163.

[12] Qarang: Крылов В. Информационные преступления – новый криминологический объект // Российская юстиция. – 1997. – № 7 – С.22 – 23.

[13] Qarang: Чичко Л. Компьютерные хищения // Российская юстиция. – 1996. – №5. – С.45.

[14] Qarang: Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М., 1996. –С.163.

predmetning aniqlanishi jinoyat tarkibi boshqa elementlarining aniqlanishi bilan bog‘langan (Jinoyat kodeksining 278^3 va 278^5-moddalari).

O‘zbekiston Respublikasining «Axborot erkinligi printsiplari va kafolatlari to‘g‘risida»gi qonunning 3-moddasiga muvofiq, axborot deganda, taqdim etilish shaklidan qat’i nazar, shaxslar, narsalar, faktlar, hodisalar, voqea va jarayonlar to‘g‘risidagi ma’lumotlar tushuniladi. Jinoyat kodeksi Maxsus qismining axborot texnologiyalari sohasidagi jinoyatlarga oid bobining xususiyati shundaki, unda axborotning alohida turi – kompyuter axboroti haqida so‘z boradi.

Kompyuter axboroti EHM yordamida ishlov beriladigan va foydalaniladigan hamda shaxslar, narsalar, faktlar, hodisalar, voqealar va jarayonlar to‘g‘risidagi ma’lumotlarga, shuningdek undan foydalanish rejimi (qoidalari)ni belgilagan mulkdorning identifikatsion atributlariga ega EHM dasturlari va ma’lumotlar bazalaridir. EHM dasturlari va ma’lumotlar bazalari ham jinoiy-huquqiy muhofaza etilishi kerak. Shu o‘rinda EHM dasturlarining xususiyatlarini keltirib o‘tish lozim. Ular bir jihatdan, axborotga ta’sir ko‘rsatish vositasi bo‘lsa, boshqa jihatdan komandalar va ma’lumotlar majmuidan iborat axborotdir. Ya’ni ularga muayyan ikki tomonlamalik xos. Bu esa EHM dasturini axborot turlaridan biri sifatida talqin etish uchun asos bo‘ladi. O‘zbekiston Respublikasining «Elektron hisoblashmashinalari uchun yaratilgan dasturlar va ma’lumotlar bazalarining huquqiy himoyasi to‘g‘risida»gi qonunining 1-moddasida EHM dasturlariga quyidagicha ta’rif berilgan: «EHM dasturi – muayyan natija olish maqsadida EHM va boshqa kompyuter qurilmalarining ishlashi uchun mo‘ljallangan ma’lumotlar va komandalar majmuini namoyon etishning ob’ektiv shakli. EHM dasturi deganda, uni ishlab chiqish davomida olingan tayyorgarlik materiallari hamda ushbu dastur yuzaga keltiradigan audiovizual tasvirlar ham nazarda tutiladi».

Xo‘sh, ma’lumotlar bazasi deganda nima tushuniladi? Yuqoridagi qonunga ko‘ra, «ma’lumotlar bazasi – ma’lumotlar majmuini taqdim etish va tashkil qilishning, ushbu ma’lumotlar EHM yordamida topiladigan va ishlov beriladigan tarzda tartibga solingan ma’lumotlarning ob’ektiv shakli (masalan: moddalar, hisob-kitoblar)».

Ma’lumki, kompyuter axboroti mashina tashuvchisida, EHMda, EHM tizimida, EHM tarmog‘ida bo‘lishi mumkin.

Mashina tashuvchisi – kompyuter axborotini doimiy saqlash va tashish uchun mo‘ljallangan qurilmalar.

EHM mikroprotsessorni o‘z ichiga oladigan sistema bloki, klaviatura (EHMga bosma simvol yozuvlarni kiritishga imkon beruvchi qurilma) va monitor (turli ma’lumotlarni aks ettiruvchi qurilma) kabilardan iboratdir.

Kompyuterning sistema blokiga turli qo‘shimcha qurilmalar ulanishi mumkin. Ular EHMning funktsional imkoniyatlarini kengaytirish uchun mo‘ljallangan. Bunday qurilmalarga printer, skaner, modem kabilar kiradi. EHM tizimini kompyuterning o‘zi va barcha atrofidagi qurilmalar tashkil etadi.

EHM tarmog‘i bir qancha kompyuterlarning birlashmasidan iborat bo‘lib, maxsus kabellar yordamida hosil qilinadi.

Yuridik adabiyotlarda ba’zan shunday axborot texnologiyalari bilan bog‘liq jinoyatlarga oid jumboqli savollar ham uchraydi. Masalan, EHMdan o‘zga ob’ektga qarshi boshqa g‘ayriqonuniy tajovuz sodir etish maqsadida foydalanilganda, kompyuter axboroti mazkur jinoyatning faqat predmetimi yoki vositasi ham bo‘lishi mumkinmi? Bunga rossiyalik olim A. V. Sorokin shunday javob beradi: «Axborot ham boshqa jinoyatlarni sodir etishda vosita hisoblanadi deb qabul qilish

«kompyuter jinoyatlari» tushunchasining doirasini haddan tashqari kengaytirishda hamda qonun chiqaruvchi organning ham, huquqni qo‘llovchining ham ishini murakkablashtiradi»[15].

Texnik nuqtai nazardan, kompyuter axboroti haqiqatan ham kompyuter tizimi doirasidagi harakat (jinoiy harakat bo‘lishi shart emas) vositasi hisoblanadi, lekin bunda uni EHMning o‘zidan ajratmasligimiz kerak. Soddaroq aytganda, axborot kompyuterdan alohida emas, faqat u bilan birgalikdagina texnik va yuridik jihatdan vosita bo‘ladi. Shu bois, EHM vositasida amalga oshirilgan jinoyatlarni kvalifikatsiya qilishda masalani tugagan deb ham hisoblash mumkin. Buning uchun EHMni apparat va dasturiy ta’minot kompleksi sifatida idrok etish mumkin. Qalbaki plastik kartochka yordamida xarid uchun haq to‘langanda yoki bankdagi bir hisob raqamdan boshqasiga pul mablag‘i g‘ayriqonuniy yoki haq to‘lanmay o‘tkazilganda esa qilmish muayyan shakldagi talon-torojlik deb baholanishi lozim.

Axborot texnologiyalari sohasidagi jinoyatlar tarkiblarining **ob’ektiv tomoni** aksariyat hollarda moddiy tarkib sifatida ifodalanadi. Shu bois nafaqat ijtimoiy xavfli qilmishning sodir etilishi, balki ijtimoiy xavfli oqibatlarning yuz berishi, shuningdek qilmish bilan yuz bergan oqibat o‘rtasidagi sababiy aloqa aniqlanishi ham nazarda tutiladi. Jinoyatlarning alohida tarkiblari (JK 278^3 va 278^6-moddalar) qonunda formal tarkib sifatida ifodalangan. Ularning tugash payti sifatida, oqibatlari qachon yuz berishidan qat’i nazar, harakat yoki harakatsizlikning sodir etilish vaqti ko‘rsatilgan. Ijtimoiy xavfli qilmishlarning o‘zi esa mazkur jinoyatlarga tatbiqan harakatlar shaklida namoyon bo‘ladi va ba’zan harakatsizlik bo‘lishi mumkin. Bir holatda jinoyat tarkibi ob’ektiv tomonining bunday belgisi, jinoyatni sodir etish usuli sifatida, asosiy va og‘irlashtiruvchi holatlarga ega tarkiblarining majburiy belgisi sifatida ifodalanadi. Qolgan hollarda jinoyat tarkibi, shuningdek sodir etilish joyi, vaqti, quroli, vositalari, vaziyati sud tomonidan aybni yengillashtiruvchi yoki og‘irlashtiruvchi holatlar sifatida inobatga olinishi mumkin.

Axborot texnologiyalari sohasidagi jinoyatlar turli EHM, apparat vositalari, periferiya (atrof) qurilmalari va aloqa liniyalaridan foydalanilgan holda sodir etiladi. Bu, o‘z navbatida, jinoyatning sodir etilish joyi haqidagi masalaning qo‘yilishiga sabab bo‘ladi. Dunyoning deyarli barcha mamlakatlaridagi vakillarni birlashtirgan jahon axborot tarmog‘i (INTERNET)ning yaratilishi qilmishni zararli oqibatlar kelib chiqadigan joydan uzoqda sodir etishga ham imkon beradi. Bunday hollarda rossiyalik tadqiqotchilar YU. I. Lyapunov va A. V. Pushkin, jinoyat sodir etish joyi deganda, oqibatlar yuz beradigan joyning qayerda ekanligidan qat’i nazar, qilmish (harakat yoki harakatsizlik) sodir etilgan davlatning hududini tushunadilar. Masalani bunday hal etishda ushbu mualliflar Rossiya Federatsiyasi Jinoyat kodeksining 9-moddasi 2-qismida, oqibatlari qachon yuz berishidan qat’i nazar, qilmish sodir etilgan vaqt jinoyat sodir etish vaqti deb topilishiga asoslanadilar[16]. Biroq, yuqoridagi qoidaga zaruriy aniqliklar kiritmay turib, uni O‘zbekiston Respublikasi jinoyat qonuni hujjatlariga qabul qilish mumkin emas, chunki u O‘zbekiston Respublikasi Jinoyat kodeksining 13-moddasi 1-qismiga ziddir. Ushbu moddaga muvofiq jinoyatning sodir etilish vaqti qanday (formal yoki moddiy tarkibli) jinoyat sodir etilganligiga qarab aniqlanadi belgilangan. Formal tarkibli jinoyatning sodir etilish vaqti deb ijtimoiy xavfli qilmish amalga oshirilgan vaqtni, moddiy tarkibli jinoyatning sodir etilish vaqti deb esa jinoyat qonunida nazarda tutilgan jinoiy oqibatlarning yuz berish vaqtini tan olish lozim[17]. Binobarin, axborot texnologiyalari sohasidagi formal tarkibli jinoyatlarning sodir etilish joyi – ijtimoiy xavfli qilmish sodir etilgan davlat hududi, moddiy tarkibli jinoyatning sodir etilish joyi esa

[15] Qarang: Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Ресурс Интернет: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

[16] Qarang: Уголовное право. Особенная часть. – М.,1998. – С.546.

[17] Qarang: Уголовное право. Общая часть / А.С.Якубов, Р. Кабулов и др. – Т., 2005. – С. 112-119.

oqibatlar yuz bergan (axborot yo‘q qilib yuborilgan, modifikatsiyalashtirilgan, to‘sib qo‘yilgan, nusxa ko‘chirilgan) mamlakat hududi hisoblanadi.

Axborot texnologiyalari sohasidagi jinoyatlarning **sub’ektiv tomoni** aybning to‘g‘ri yoki egri ko‘rinishidagi qasd shakli bilan tavsiflanadi. Faqatgina bitta jinoyat, ya’ni axborotlashtirish qoidalarini buzganlik uchun javobgarlikni belgilovchi JK 278^1-moddasidagi jinoyat ham qasddan, ham ehtiyotsizlik tufayli sodir etilishi mumkin.

Qonun chiqaruvchi tomonidan ikkita jinoyat uchun, JK 278^3 va 278^6 – moddalarida jinoyat sub’ektiv tomonining zaruriy belgisi sifatida *maqsad* belgilangan. Boshqa holatlarda motiv va maqsad jinoyatlarning zaruriy belgisi sifatida ko‘rsatilmagan, lekin ularning belgilanishi jazoni individuallashtirish uchun katta ahamiyat kasb etadi. Ushbu jinoyatlar g‘arazdan, bezorilik maqsadida, o‘ch olish niyatida, “sport manfaatlari uchun”, shuningdek, siyosiy va boshqa manfaatlar motivida sodir etilishi mumkin. Mazkur turdagi jinoyatlar ustunlikka intilish, zavq olish hohishi, boshqa jinoyatlarni yashirish kabi maqsadlarda sodir etilishi mumkin.

Axborot texnologiyalari sohasidagi jinoyatlarning **sub’ekti** aqli raso, 16 yoshga to‘lgan, axborotlarni qo‘riqlash majburiyatiga ega yoki kompyuter axborotlariga qonunga xilof ravishda kirgan shaxslar hisoblanadi.

Psixofiziologik tavsif nuqtai nazaridan, ular ijodkor shaxs, mutaxassis, texnik chaqiruvga tavakkal bora oluvchilar. Hozirgi kunda yirik kompaniyalar tajribali xakerlarni axborot va kompyuter tizimlariga himoya tizimini yaratish maqsadida ishga olishga harakat qilmoqdalar.

Ekspert tadqiqot materiallaridan xulosa qilish mumkinki, jinoyat sodir etish vaqtida 20 yoshga yyetmaganlar 33%, 20 – 40 yoshdagilar 54 %, 40 yoshdan oshganlar 13 %ni tashkil etgan. O‘tkazilgan tadqiqot natijalari xakerlarni 13 yoshdan 20 yoshgacha bo‘lgan o‘smirlar tashkil qiladi degan taxminlarni inkor etadi.

Kompyuter texnologiyalaridan foydalanish sohasidagi jinoyatlarni erkaklar besh martagacha ko‘p sodir etishadi. Bunday jinoyatlar sub’ektining ko‘pchiligi oliy yoki tugallanmagan oliy texnik ma’lumotlilar (53,7%), qolganlari esa oliy ma’lumotlilar, shuningdek tugallanmagan oliy ma’lumotlilar (19,2%) hisoblanishadi.

So‘ngi vaqtlarda ularning safida ayollarning ulushi ortib bormoqda. Bu aksariyat hollarda ayollar tomonidan (kotiba, hisobchi, iqtisodchi, menedjer, g‘aznachi, nazoratchi kabilar) kompyuter asbob-uskunalari bilan bog‘liq ko‘pgina ish joylari, mutaxassisliklar va mansablarning egallanishi bilan bog‘liqdir.

Kriminologik tadqiqotlarning guvohlik berishicha, jinoyatchilarning 52% ini kompyuter axbortlarini ishlab chiqish sohasida maxsus tayyorgarlik ko‘rganlar; 97% ini kundalik ish faoliyatida kompyuter tizimi va axborot texnologiyalaridan foydalanuvchi davlat tashkiloti va muassasalarining xodimlari; 30%ini kompyuter vositalari texnikalarining ekspluatatsiya qilishga bevosita munosabatda bo‘lgan huquqbuzarlar tashkil etadi[18].

Xulosa tariqasida aytish mumkinki, axborot texnologiyalari sohasidagi jinoyatlarni sodir etuvchi shaxslarning doirasi nisbatan keng. Tadqiqot natijalaridan ko‘rinib turibdiki, jinoyat sub’ektlari jamiyatning turli qatlam vakillaridan, 16 dan 60 yoshgacha, tayyorgarlik darajasi esa – tajribasizlardan tortib, mutaxassislargacha yoki kompyuter texnikasi sohasida minimal bilimga ega bo‘lgan barcha yoshdagi shaxslar bo‘lishi mumkin.

[18] Qarang.: Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. – М., 1997. – С. 40-44; Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. – Красноярск, 202. – С, 8 – 14; 62-64.

Ob’ektiv va sub’ektiv belgilarning tahlilidan kelib chiqib, mazkur jinoyatlarga quyidagicha ta’rif berish mumkin: *kompyuter axborotlaridan huquqiy va xavfsiz foydalanishdagi ijtimoiy munosabatlarga zarar yyetkazish yoxud zarar yyetkazish xavfini keltirib chiqaruvchi, aybli, jinoiy jazoga sazovor ijtimoiy xavfli qilmish axborot texnologiyalari sohasidagi jinoyatlar* deyiladi.

Axborot texnologiyalari sohasidagi jinoyatlarning ijtimoiy xavfliligi quyidagi holatlarda sezilarli darajada oshadi: a) bir guruh shaxslar tomonidan oldindan til biriktirib; b) takroran va xavfli retsidivist tomonidan; v) uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab; g) juda ko‘p miqdorda zarar yyetkazgan holda sodir etilgan bo‘lsa.

Bunday zaruriy belgilar JK 278^1-moddasida ko‘rsatilgan jinoyat tarkibidan tashqari axborot texnologiyalari sohasidagi jinoyatlarning barcha turining “a” va “b” bandlarida mavjud. Jinoyatning uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilishi JK 278^2, 278^3, 278^6-moddalari ikkinchi qismining kvalifikatsiyaga oid belgisi hisoblanadi. Juda ko‘p miqdorda zarar yyetkazilishiga sabab bo‘lish JK 278^1, 278^4, 278^6-moddalari ikkinchi qismining kvalifikatsiyaga oid belgisi hisoblanadi.

JK 29-moddasi 3-qismiga muvofiq, jinoyatda ikki yoki undan ortiq shaxs birgalikda jinoyat sodir etish uchun oldindan til biriktirgan bo‘lsa jinoyat bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilgan deyiladi. Axborot texnologiyalari sohasidagi jinoyatlarda jinoyat sodir etishga kelishuv (jinoyatning ob’ektiv tomoni belgilarini bajarishdan oldin yoxud to‘satdan paydo bo‘lgan qasd natijasida, bevosita bajarishdan oldin bo‘lishini bildiradi.

Birgalikda bajaruvchilik yoki ishtirokchilikda oldindan til biriktirish deganda tor ma’noda, jinoyat sodir etishdagi vazifalarning taqsimlanishi (bajaruvchi, yordamchi, dalolatchi, tashkilotchi), shuningdek guruhning barcha ishtirokchilari sub’ekt belgilariga ega bo‘lgan holda jinoyat sodir etishga birgalikda qasd qilganligi tushuniladi.

Agar guruh tarkibida bitta ishtirokchi jinoyat sub’ekti bo‘lsa-yu, qolganlari voyaga yetmaganligi uchun sub’ekt sanalmasa, oldindan til biriktirgan guruh mavjud emas deb hisoblanadi. Bunday holatda yagona sub’ekt axborot texnologiyalari sohasidagi jinoyatlarni sodir etganligi uchun, shuningdek u 18 yoshga to‘lmaganlarni jinoyat sodir etishga undagan bo‘lsa, voyaga yetmaganlarni g‘ayriijtimoiy hatti-harakatlarga jalb qilganligi uchun (JK 127-moddasi 3-qismi) jinoyatlar majmui bo‘yicha javobgarlikka tortiladi.

Shu o‘rinda ta’kidlab o‘tish lozimki, jinoyat sub’ekti hisoblangan shaxs javobgarlik yoshiga yetmagan shaxsni jinoyat sodir etishga majburlab, unda o‘zi ishtirok etmagan bo‘lsa, u javobgarlik yoshiga yetmagan shaxsdan qurol sifatida foydalanganligi uchun o‘sha jinoyatning bajaruvchisi sifatida javobgarlikka tortiladi. JK 32-modda 1-qismiga muvofiq, takroran jinoyat sodir etish deganda, JK Maxsus qismining aynan bir moddasi, qismi yoki Kodeksda alohida ko‘rsatilgan hollarda turli moddalarda nazarda tutilgan ikki yoki undan ortiq jinoyatlarni shaxs turli vaqtlarda sodir etganligi, ammo ularning birortasi uchun ham sudlanmaganligi tushuniladi.

Shu bilan birga oldin sodir etgan jinoyati tugallangan yoki yo‘qligi, bajaruvchi yoki ishtirokchilikning boshqa turi sifatida jinoyat sodir etganligi ahamiyat kasb etmaydi. Axborot texnologiyalari sohasidagi jinoyatlarda takroriylik ikki yoki undan ortiq bir–biriga o‘xshash jinoyatlardan tashkil topadi.

Bu esa takroran jinoyat sodir etish agarda xuddi shunday (bir-biriga o‘xshash) ijtimoiy xavfli tajovuz sodir etganligini anglatadi. Misol uchun, kompyuter sabotaji agar shaxs tomonidan ikkinchi marotaba sodir etilgan va birinchi qilmishida JK 278^5-moddasi 1-qismidagi jinoyat alomatlari mavjud bo‘lib, javobgarlikka tortilmagan bo‘lsa (JK 278^5-moddasi 2-qismi “b” bandi), unda takroran sodir etilgan hisoblanadi. Tahlil qilinayotgan zaruriy belgi qancha va qanday ko‘rinishda jinoyat sodir

etilganligidan qat'i nazar inobatga olinadi. Asosiysi, oldingi sodir etgan o‘xshash jinoyati JK 64-moddasi bo‘yicha o‘zining huquqiy ahamiyatini saqlab turgan bo‘lishi lozim.

JK 34-moddasi 2-qismiga muvofiq, xavfli retsidivist deganda, ilgari hukm qilingan jinoyatiga o‘xshash jinoyat sodir etgan shaxsning qasddan yangi jinoyat sodir etishi tushuniladi. Axborot texnologiyalari sohasidagi jinoyatlarni xavfli retsidivist tomonidan sodir etilgan deb kvalifikatsiya qilish uchun huquqni qo‘llovchi organlar aybdorga ushbu belgini hisobga olgan holda ayblov taqdim qilishga majburdirlar. Shaxs ilgari JK 278^2-moddasi 1–qismida ko‘rsatilgan komp'yuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanganligi uchun sudlanib, yangidan shunga o‘xshash jinoyat sodir etsa, JK 278^2-moddasi 2-qismi "b" bandi bo‘yicha (xavfli retsidivist sifatida) javobgarlikka tortilishi lozim.

Ta'kidlash joizki, mazkur jinoyatlarni kvalifikatsiya qilishda zaruriy belgilarni hisobga olishning asosiy sharti sifatida, jazoni ijro etish muddatining (JK 69-moddasi) o‘tib ketmaganligi yoki qonunda belgilangan tartibda sudlanganlik holatining tugallanmaganligi yoki olib tashlanmaganligi yohud shaxsning ilgari sodir etilgan o‘xshash jinoyati uchun sudlanganligi to‘g‘risidagi faktlar hisoblanadi.

Uyushgan guruh deganda, ikki yoki undan ortiq shaxsning birgalikda jinoiy faoliyat olib borish uchun oldindan bir guruhga birlashishi tushuniladi (JK 29-moddasi 4-qismi).

Guruh jinoiy faoliyatining uzoqqa cho‘zilganligi, tarkibning o‘zgarmasligi, aloqalarining mustahkamligi, lider (boshqaruvchi, tashkilotchi) orqali boshqa yaqin guruhlar bilan faoliyat sohasi bo‘limida guruh ishtirokchilari orasidagi rollar va vazifalarining ierarxik taqsimlanganligi (vertikal va gorizontal bo‘yicha), jinoiy faoliyatni rejalashtirishda qattiq ichki intizom jinoiy guruhning uyushganligi deb tavsiflanadi[19].

Sanab o‘tilgan belgilar u yoki bu munosiblikdagi belgilar mazkur turdagi jinoiy ko‘rinishlarga taalluqli bo‘lib, har qanday uyushgan guruhlarda o‘zlarini ko‘p yoki kam darajada namoyon qiladi. Bundan tashqari, guruhni uyushgan deb hisoblash uchun guruhning kompyuter axborotlarini noqonuniy va xavfsiz foydalanish sohasida jinoiy faoliyatni olib borish maqsadida tashkil etilganligini aniqlash zarur.

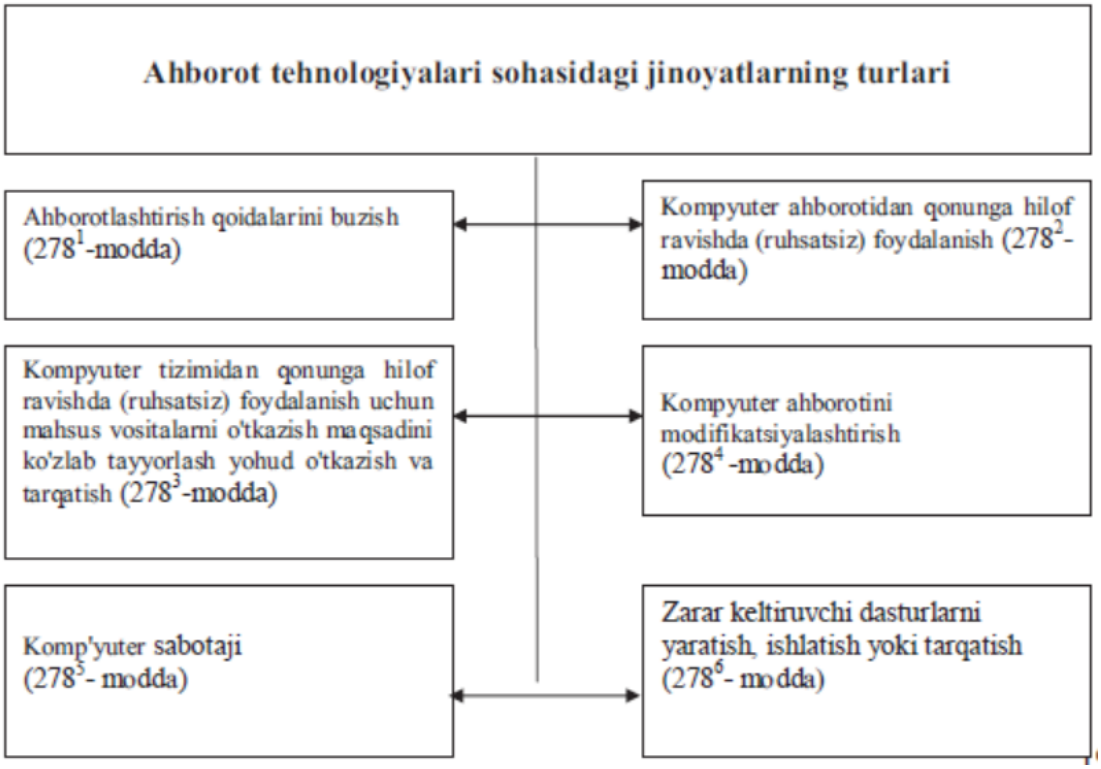
JK 278^3 va 278^6-moddalari 2-qismi "g" bandlarida uyushgan guruhni tashkil etgan yoki unga rahbarlik qilgan, shuningdek guruhning jinoyat sodir etishida qatnashgan shaxslarning jinoiy javobgarliklari asoslari, shartlari va hajmi, JK 30-moddasi 2–qismida esa guruhdagi ishtirokchilik to‘g‘risida so‘z boradi. Bu kabi holatlarda, ma'lum bir jinoyat sodir etishda qanday rolni bajarganligidan qat'i nazar, uyushgan guruhning barcha a'zolari bajaruvchi sifatida (JK 28-moddasiga havola qilmasdan) javobgarlikka tortiladilar. Yuqorida ta'kidlangan JK Maxsus qism moddalaridagi kvalifikatsiya etish belgilari sifatida jinoyatning uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilishi belgilanganligi sababli og‘irlashtiruvchi holat sanaladi. Ularga ko‘ra, jazo uyushgan guruh a'zosi bo‘lmagan, lekin jinoyat sodir etishda uyushgan guruh tarkibida bir marotaba qatnashgan yoki uyushgan guruh manfaatlarini ko‘zlab, o‘z tashabbusi bilan yoxud uyushgan guruh buyrug‘i bilan jinoyatni mustaqil sodir etgan aybdor shaxslarga ham qo‘llaniladi.

JK 278^1-moddasi 2-qismi, 278^4-moddasi 2-qismi "a" bandi va 278^6-moddasi 2-qismi "a" bandlarida zaruriy belgi sifatida nazarda tutilgan juda ko‘p miqdordagi zarar eng kam oylik ish haqining uch yuz baravariga va undan ko‘pga teng hisoblanadi. Bunday holatda "zarar" tushunchasi nafaqat to‘g‘ridan-to‘g‘ri yetkazilgan zarar, balki boy berilgan foyda ham hisoblanadi. Alohida

[19] Qarang: Соттиев И.А. Уюшган жиноятчиликка қарши курашишнинг ҳуқуқий воситалари: Ўқув қўлланма – Т, 2005. – 30-43 б.

ta’kidlash lozimki, jinoyat sodir etilishi natijasida shaxs amalda juda ko‘p miqdordagi zarardan kamroq zarar yetkazgan, lekin aybdorning qasdi aynan shunday zarar yetkazilishiga yo‘naltirilgan bo‘lsa, mazkur jinoyat suiqasd qilish kabi kvalifikatsiya qilinadi.

O‘zbekiston Respublikasining jinoyat qonunchiligida axborot texnologiyalari sohasiga taalluqli oltita asosiy va kvalifikatsiyaga oid tarkiblarga ega jinoyatlar uchun javobgarliklar belgilangan. Ular quyidagi rasmda aks ettirilgan.



15.1-rasm. Axborot texnologiyalari soahsidagi jinoyatlar

16-MAVZU: JISMONIY XAVFSIZLIK

MA’RUZA MASHG’ULOTI REJASI:

16.1. Axborot manbalarini fizik ximoyalash tizimi
16.2. Axborotni injener ximoyalash

Tayanch so‘z va iboralar: Ob’ektlarni injener himoyalash va texnik qo‘riqlash, Axborot manbalarini fizik ximoyalash tizimi, Avtonom qo‘riqlash tizimi.

Axborot manbalarini fizik ximoyalash tizimi niyati buzuqning ximoyalanuvchi axborot manbalariga suqilib kirishini oldini oluvchi hamda tabiiy ofatdan, avvalo yong‘indan, ogoxlantiruvchi vositalarni o‘z ichiga oladi.

Injener konstruksiyalar taxdid manbalarini axborot manbalari tomon xarakati (tarqalishi) yo‘lida ushlab qoluvchi to‘siqlarni yaratadi.

Axborotga taxdidlarning turlari va ro‘y berishi vaqtining noaniqligi, axborotni himoyalovchi vositalarining ko‘p sonliligi va turli – tumanligi, favqulot vaziyatlardagi vaqtning tanqisligi *axborotni fizik himoyalash vositalarini boshqarishga* yuqori talablar qo‘yadi.

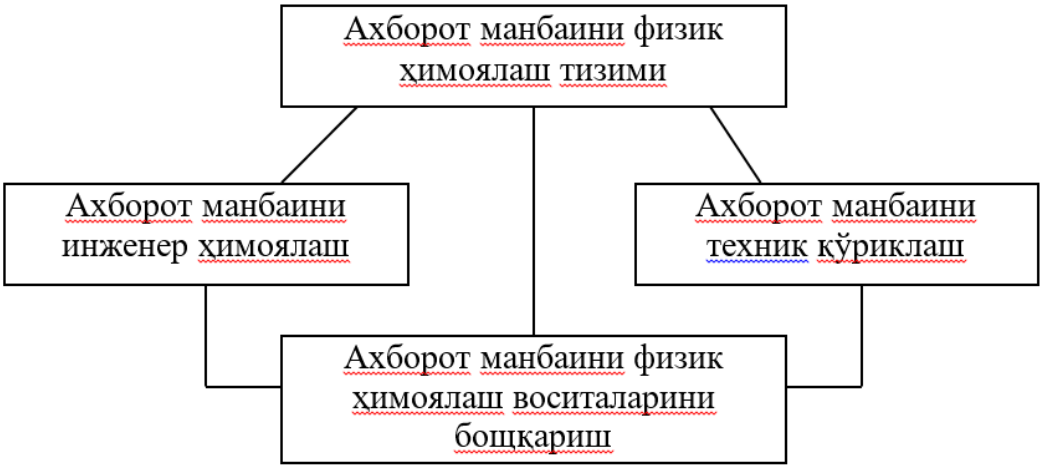
Boshqarish qo‘yidagilarni ta’minlashi lozim:

- axborotni himoyalashning umumiy prinsiplarini amalga oshirish;
- axborotni fizik himoyalash tizimini va uni sirqib chiqishidan himoyalash tizimini yagona doirada ishlashini muvofiqlashtirish;
- axborotni himoyalash bo‘yicha operativ qaror qabul qilish;
- himoya choralarining samaradorligini nazoratlash.

Fizik himoyalash tizimini boshqarish bo‘yicha me’yoriy xujjatlar axborotni himoyalash bo‘yicha yo‘riqnomalarda o‘z aksini topgan. Ammo yo‘riqnomalarda barcha vaziyatlarni hisobga olish mumkin emas. Fizik himoyalash tizimining vositalari vaqt tanqisligi sharoitida notipik vaziyatlar sodir bo‘lganida to‘g‘ri xulosa qabul qilinishini ta’minlashi lozim.

Fizik ximoyalash tizimining tarkibi turli – tuman: oddiy qulfli yog‘och eshikdan to qo‘riqlashning avtomatlashtirilgan tizimigacha. Fizik ximoyalash tizimning umumlashtirilgan sxemasi 7-rasmda keltirilgan.

Ob’ektlarni injener himoyalash va texnik qo‘riqlash zaruriyati statistika orqali tasdiqlanadi, ya’ni suqilib kirishlarning 50% dan ko‘prog‘i xodimlar va mijozlar tomonidan erkin foydalaniladigan ob’ektlarga amalga oshirilsa, faqat 5 % kuchli qo‘riqlash rejimli ob’ektlarga amalga oshiriladi.



16.1-rasm. Axborot manbaini fizik himoyalash tizimining strukturasi

Axborotni injener ximoyalashni quyidagilar ta’minlaydi:

- niyati buzuqning va tabiiy ofatning axborot manbalariga (yoki qimmatbaho narsalarga) qarab harakat qilishi mumkin bo‘lgan yo‘ldagi tabiiy va sun’iy to‘siqlar;
- foydalanishni nazoratlovchi va boshqaruvchi tizimlarning to‘suvchi qurilmalari.

Tabiiy to‘siqlarga tashkilot xududida yoki yonidagi yurish qiyin bo‘lgan joylar (zovurlar, jarlar, qoyalar, daryolar, quyuq o‘rmon va changalzor) taalluqli bo‘lib, ulardan chegaralar mustaxkamligini kuchaytirishda foydalanish maqsadga muvofiq hisoblanadi.

Sun’iy to‘siqlar odamlar tomonidan yaratilib, tabiiy to‘siqlardan konstruksiyasi va niyati buzuq ta’siriga barqarorligi bilan jiddiy farqlanadi. Ularga turli devorlar, qavatlararo pollar, shiplar, bino derazalari va h. taalluqli.

Derazalar mexanik ta’sirga bardosh oyna va metall panjaralar yordamida mustaxkamlanadi.

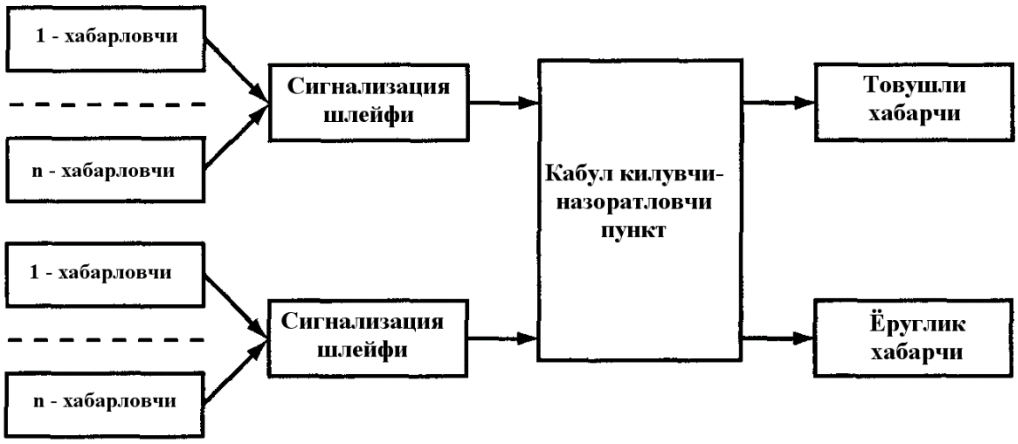
Himoyaning oxirgi chegaralarini metall shkaflar, seyflar tashkil etadi. Shu sababli ularning mexanik mustaxkamligiga yuqori talablar qo‘yiladi.

Metall shkaflar maxfiylik grifi yuqori bo‘lmagan hujjatlarni, qimmatbaho narsalarni, katta bo‘lmagan pul mablag‘ini saqlashga mo‘ljallangan. Shkaflarning ishonchliligi faqat metalning pishiqligiga va qulflarning maxfiyligiga bog‘liq.

16.2 - rasmda ob’ektlarni qo‘riqlovchi texnik vositalar kompleksining namunaviy strukturasi keltirilgan. Qo‘riqlaydigan *xabarlovchi* (datchik) texnik qurilma bo‘lib, u unga niyati buzuq tomonidan mexanik kuch va maydon ta’sir qilganida trevoga signalini shakllantiradi.

Signalizatsiya shleyfi elektr zanjirni hosil qilib, datchiklar va qabul qiluvchi - nazoratlovchi asboblarning elektr bog‘lanishini ta’minlaydi.

Qabul qiluvchi – nazoratlovchi punkt datchiklardan keladigan signallarni qabul qilish va ishlashga, qo‘riqlash xodimlarini tovush va yorug‘lik signali yordamida trevoga signallari kelganligi, datchiklar va shleyflar ishlashidagi nosozliklar xususida xabardor qilishga mo‘ljallangan.



16.2-rasm. Ob’ektlarni qo‘riklovchi texnik vositalar kompleksining namunaviy strukturasi

Hozirda *televizion kuzatuv tizimi* keng qo‘llanilmoqda. Bu tizim tarkibiga tungi vaqtda qo‘riqlanuvchi hududda kerakli yoritilganlik darajasini ta’minlovchi navbatchi yorituvchi vositalari ham kiradi.

Avtonom qo‘riqlash tizimining ekspluatatsiyasi katta sarf -xarajatlarni talab etadi. Shu sababli markazlashtirilgan qo‘riqlash tizimlari keng qo‘llaniladi. Ushbu tizimda niyati buzuqlarni neytrallashtirish masalasi bir necha tashkilotlar uchun umumiy hisoblanadi.

Markazlashtirilgan qo‘riqlashga misol tariqasida omonat bank filiallarini, kichik firmalarni, xususiy uylarni, dala hovlilarni, xonadonlarni qo‘riqlashni ko‘rsatish mumkin.

17-MAVZU: MILLIY XAVFSIZLIK TUSHUNCHASI

MA’RUZA MASHG’ULOTI REJASI:

17.1. Axborot xavfsizligining milliy xavfsizlik tizimidagi o‘rni
17.2. Axborot xavfsizligining zamonaviy konsepsiyasi

Tayanch so‘z va iboralar: milliy manfaatlar, inson va uning huquqlari, milliy xavfsizlik muammosi.

Axborot xavfsizligining milliy xavfsizlik tizimidagi o‘rni. XXI asrda shaxs, jamiyat va davlat taraqqiyotida axborot resurslari va texnologiya-larining rolini ortishi natijasida O‘zbekiston Respublikasida 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 obyektlari, shu bilan birga jami xavfsizlik sohalaridagi xavfsizlik obyektlarining asosiy elementlaridir;

– axborot yondashuvidan asosiy ilmiy-amaliy usul sifatida foydala-nish 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 cham-barchas 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 mav-qeini belgilaydi. Axborot sohasidagi O‘zbekistonning milliy manfaatlarini,
ularga erishishining strategik yo‘nalishlarini va ularni amalga oshirish tizimlarini o‘zida aks ettiruvchi maqsadlar yaxlitligi davlat axborot siyo-satini anglatadi. Shu bilan birga davlat axborot siyosati mamlakatning tashqi va ichki siyosatining asosiy tashkil etuvchisi hisoblanadi va jamiyat-ning 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‘riq-lash ma’nosida);

– kompyuter xavfsizligi yoki ma’lumotlar xavfsizligi – kompyuter tarmoqlarida ma’lumotlarning saqlanishini, foydalanishga ruxsat etilganli-gini va konfedensialligini ta’minlovchi apparat va dasturiy vositalar to‘plami, axborotdan mualliflashtirilmagan 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 himoyalanganli;

– 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.

Xavfsizlik siyosati – xavfsizlik obyektlari 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.

O‘zbekiston Respublikasi Prezidentining 2015-yilning 4-fevral kuni e’lon qilingan “O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligini tashkil etish to‘g‘risida”gi Farmoniga ko‘ra “Axborot xavfsizligini ta’minlash va kommunikatsiya tarmoqlari, dasturiy mahsulotlar, axborot tizimlari va resurslarini himoya qilishning zamonaviy texnologiyalarini tatbiq etish chora-tadbirlarini amalga oshirish, axborot resurslarini himoya qilish bo‘yicha texnik infra-tuzilmani yanada rivojlantirish” ustuvor vazifalardan biri sifatida qayd etilgan.

Axborot xavfsizligi deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan qilingan ta’sirlardan axborot va uni qo‘llab-quvvatlab turuvchi infratuzilmaning himoyalanganligi tushuniladi. Bunday ta’sirlar axborot munosabatlariga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni ta’minlovchi infratuzilmaga jiddiy zarar yetkazishi mumkin.

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida axborot xavfsizligi *axborot borasidagi xavfsizlik* deb belgilangan va u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

18-MAVZU: AXBOROT URUSHI

MA’RUZA MASHG’ULOTI REJASI:

18.1. Axborot xuruji
18.2. Axborot xurujiga qarshi kurash

Tayanch so‘z va iboralar: Axborot xuruji, axborot «urushi», milliy xavfsizlik muammosi.

Axborot xurujini ta’bir joiz bo’lsa, axborot «urushi» deyish mumkindir. U odam bolasini ne-ne musibat va ko’ylarga solmaydi, deysiz! ONG ta’sir doirasida uning girdobiga tushgach, aniqrog’i mag’lub bo’lgach hammadan ham men zo’rman, hech kimdan qo’rqmayman, deydi. Hatto o’limdan ham!

Odam bolasi ozgina ma’naviyat, ma’rifatdan bahra olsa yuragiga pokiza ruh kiradi, qalbi yumshaydi, mehri tovlanadi, mehribonlashib qoladi… Bu ONG g’olib bo’ldi degani. Unga internetning mingta, millionta «yomon» xabarining qizig’i yo’q, alg’ov-dalg’ov o’yinlari esa bir pul.

Birinchi Prezidentimiz Islom Karimov o’zining «Yuksak ma’naviyat — yengilmas kuch» asarida shunday yozadi: «Biz farzandlarimizni ona Vatanga muhabbat, boy tariximizga, ota-bobolarimizning muqaddas diniga sadoqat ruhida tarbiyalash uchun, ta’bir joiz bo’lsa avvalo ularning qalbi va ongida mafkuraviy immunitetni kuchaytirishimiz zarur. Toki yoshlarimiz milliy o’zligini, shu bilan birga, dunyoni chuqur anglaydigan, zamon bilan barobar qadam tashlaydigan insonlar bo’lib yetishsin. Ana shunda johil aqidaparastlarning «da’vati» ham, axloq-odob tushunchalarini rad etadigan, biz uchun mutlaqo begona g’oyalar ham ularga o’z ta’sirini o’tkaza olmaydi».

Internetdan ba’zi axborotlarni o’qib yoqa ushlaysan, taajjubga tushasan. Axir, hech qachon ilon bol, asalari zahar to’plamaydi-ku?!

Nima emish, avstraliyalik 73 yashar Uill o’zining kasal mushugiga uylanibdi…

Nima emish, norvegiyalik bir odam o’zini zombilarcha tutib, yo’lovchilarga tashlanibdi…

Nima emish, Fransiyada bir jinsli nikohlar soni ortib bormokda…

Nima emish, falon davlatda aka o’z singlisi bilan turmush quribdi…

«Axborot – mo’jiza, joziba, falsafa». O’zbekiston jahon tillari universiteti xalqaro jurnalis-tika fakulteti o’qituvchisi, filologiya fanlari doktori, professor Xurshid Do’stmuxammedovning ushbu kitobi shunday so’zlar bilan boshlanadi: «Odamlar hayotida, umuman dunyoda yuz berayotgan barcha o’zgarishlar, yangilanishlarning sababchisi axborot!

Axborot nima, uning xis-lati, hikmati, mo’’jizalari nimalarda namoyon bo’lmoqda? Bugun yo ertaga u inson yoki insoniyat boshiga yana ne kunlarni solishi mumkin? Bashariyatni qay ko’chalarga boshlab ketish ehtimoli ko’proq?».

Mana bu savollar har bir uyg’oq qalbga, kelajakka, ma’naviyatmizga, ma’rifatimizga, qadriyatimizga berilgan savoldir. Javobni esa o’zimizdan, yuragimizdan qidiraylik.

O’sha kitobdan olingan fikr-mulohazalarni Sizga ilindik: «Tezroq! Ko’proq! Unumliroq! shiori boshqarmoqda insoniyatni».

«Bizni axborot, axborot oqimining shiddati shu ko’yga solmoqda…».

«Anglanmagan behalo-vatlik, besamar besaranjomlik qurbonlari asrimikan «axborot asri»?…»

«Inson qayoqqa borayottanini biladi…».

Hayotiy hikmat, falsafa va donishmandlik xamirturushidan iborat bu hayot chizgilari, shunday atash lozim bo’lsa, o’z-o’zidan yaralmagan, shunchaki qog’ozga tushib qolmagan.

Ustoz, Sizga tasanno!

Bugun axborot xuruji kirib bormagan hududning o’zi qolmadi. Istaysizmi yo’qmi, xohlaysizmi-yo’qmi bu shubha yoki gumon emas. Yo alhazar, «O’rgimchak to’ri» dunyoni egallab bo’ldi! Dod deysizmi, faryod deysizmi, iloj qancha?!

Eng dahshatlisini aytaylik, bugungi yosh avlodning 90 foizi internet tarmog’ining «quli». Yoshlar xohlagan o’yinini o’ynaydi, shunga odatlanib qolgan, xumorini shundan bosadi, shundan o’zgacha «zavq” oladi… Holbuki, ayni paytda internet tarmog’ida o’z joniga qasd qilishni targ’ib qiluvchi 9 mingdan ziyod, erotik mazmundagi 4 mingdan ziyod sayt-lar mavjud. Tarmoqdagi 49 foiz o’yinlar zo’ravonlik va yovuzlikni, 42 foizi bolalar va o’smirlar onlayn tizimi orqali tarqaladigan pornografiya «illat»larini targ’ib qilishga qaratilgan bo’lsa… Zero, xalqaro ekspertlar dunyo miqyosida 38 foiz bolalar zo’ravonlik ruhidagi sayt-larni, 28 foiz bolalar esa millatchilik harakteridagi veb-sahifalarni muntazam ravishda tomosha qilib borishlarini ta’kidlashmoqda.

Yoshlar ma’naviyatiga internet tarmoqlarining salbiy ta’siri haqida qancha ko’p yozilyapti, shuncha ko’p aytilyapti, ammo baribir bu holat kamaymayapti. Kompyuterga mukkasidan ketib ongini zaharlab, umrini, ayniqsa yoshligini xazon qilayotgan ayrim yoshlar borligidan ko’z yumib bo’lmaydi. Aytaverish, tergayverish kerak. Ota-ona aytsa, maktabda aytilsa, kollej, litsey yoki oliy o’quv yurtlarida aytilsa, aytilaversa, dashnom berilaversa, tanqid qilinaversa oxiri bo’ldi, bas, deb har qanday yosh bu yo’ldan qaytadi. Agar lozim deb topilsa, maktab yoki kollejlarda haftasiga bir-ikki soatdan «Axborot xavfsizligi» yoki «Axborot» degan darslar kiritilsa, maqsadga muvofiq bo’larmidi!

Tib ilmining sultoni Abu Ali Ibn Sino bejiz mana bu satrlarni yozmagan: «Bola xulqini maromida saqlashga alohida e’tibor berish kerak, bunga bolani qattiq g’azablanish, qo’rqish, uyqusizlikdan saqlash orqali erishiladi. G’azab kuchni qizdiradi, qayg’u kuchni ozdiradi, hafalik beg’amlikka moyil qiladi. Xulqning mo’’tadilligi natijasida ham nafs, ham badan sog’lom bo’ladi».

Internet axborot xuruji, axborot to’foni, axborot olami, axborot «urushi»ga o’t qo’yib yubordi, desak mubolag’a bo’lmas. Bu urushga bas keladigan, uni yengadigan faqat bir kuch bor bu ma’naviyat, bu ma’rifat, bu e’tiqod, bu ishonch… Biz uni «Xamsa», «O’tkan kunlar», «Sarob», «Yulduzli tunlar», «Ikki eshik orasi», «Jimjitlik», «Dunyoning ishlari», «Farg’ona tong otguncha»… durdona asarlardan axtarmog’imiz, izlamog’imiz kerak. Qo’limizga kitob olib o’qisakgina, internetga nisbatan qalbimizga, yuragimizga vujudimiz orqali yetib boradi.

— Internet degani barchani o’ziga tortgan, — deydi O’zbekiston Musulmonlar idorasi raisining o’rinbosari Shayx Abdulaziz Mansurov. — Yaxshi, ezgulik yo’lida undan foydalansangiz nur ustiga nur. Ammo…

Yaqinda Abu Nasr Farobiyning bir kitobini turkchadan o’zbekchaga o’girishibdi. O’zimizda, yurtimizda bu kitob yo’q. Turkchasi esa to’g’ri, risoladagidek chiqmaydi. Bu kitobni menga tahrir qilib berish uchun olib kelishibdi. Arabchasini topib kelinglar, dedim. Shunda internetdan tavakkal qilib axtarsam, arabchasi chiqib turibdi-ku! Bu endi internetning haqiqiy foydasi, ahamiyati!

Ammo… Internetdan chet elning vahshiy, zo’ravonlik, fohisha kinolariga mukkasidan ketadigan, yoshlar ongini zaharlaydigan, o’zgartirib yuboradigan, Islom diniga rahna soladigan holatlar yo’q, deb hech kim kafolat bera olmaydi?

— Bugungi kunda ko’plab bolalar Internetga tob’elik kasalligiga chalinib qolmoqdalar, -deydi FarDU katta o’qituvchisi Mavjudaxon Uralova. — Farzandingiz internetdan chiqqandan so’ng uning kayfiyatidagi o’zgarishlarni kuzating, unda tajanglik, betoqatlik, toliqish, ishtahasizlik kabi holatlarni kuzatsangiz bu bolangizda Internetga tob’elik kasalligi rivojlanayotganligidan darak beradi.

— Muammo yetarli, — deydi professor X.Do’stmuxam- medov, — uni hal qiluvchi, har qanday masala yechimini topguvchi kuch ham yetarli. U o’zimiz! U jahon tajribalari, ilg’or an’analar! U o’zimizning azaliy qadriyatlarimiz! U bebaho mustaqilligimiz!

Taraqqiyot shiddati, shosh-qaloqlik sindromi insoniyatni qayerlarga olib boradi? Ro'shnolikkami, ezgulik yo razolatgami? Insoniyat o'zi yaratgan, erishgan va erishayotgan taraqqiyot cho'qqilaridan ag'darilib tushmasligi epini topa biladimi? Eng dahshatlisi, bu vazifa uning ixtiyoridan chiqib ketmaydimi. Bordi-yu ixtiyoridan, imkonidan chiqib ketsa, najot nimada?

Yana ma'rifat, ma'naviyat, madaniyat va axloq-odobda!

— Dunyoda inson ongi uchun kurash avj olmoqda, -deydi filologiya fanlari nomzodi, professor Fayzulla Mo'minov. Bunday sharoitda O'zbekiston fuqarolarining tarixan boy ichki dunyosini, umuminsoniy va milliy qadriyatlar uyg'unligi bilan boyitilgan hayotiy pozitsiyasini, mustaqillik g'oyalari bilan ma'naviyatini asrash dolzarb muammoga aylanmoqda.

— Sir emaski, «Facebook», «Odnoklassniki», «lnstagramm», «Twitter», «Whatsapp» kabi ijtimoiy tarmoqlar tish-tirnog'i bilan yoshlar ongini zaharlashga, qalbini ishg'ol etishga intilmoqda, — deydi Toshkent moliya instituti «Ustoz va murabbiylar» kengashi raisi Nuriddin Ochilov. — Achchiq bo'lsa-da, aytish lozimki o'zlarining bo'sh vaqtlarini kutubxona, kasb-hunar ustaxonalari-yu, sport zallarida o'tkazish o'rniga internetdagi zararli ma'lumotlarga bilib — bilmay qiziqib qolgan yoshlar ekstremistik, missionerlik guruhlari va «siyosiy tashkilotlar» tomonidan tarqatilayotgan axborotlar ta'siriga tushib qolmaslikpariga kim kafolat beradi?

Bular hammaning vazifasi va muammosi.

Bular ongli mavjudotning tashvishi, og'riq nuqtasi.

O'zbekistonda xizmat ko'rsatgan madaniyat hodimi Qutlibeka Rahimboyevaning ajoyib bir so'zi bor:

«Biz aytishni biladigan xalqmiz». Zero, o'qishni, yozishni, eshitishni, ko'rishni, mulohaza qilishni ham joyiga qo'yadigan xalqmiz. Ayniqsa yoshlarimiz nimani o'qishni, nimani yozishni, nimani eshitishni, nimani ko'rishni, nimani o'ziga olishni to'g'ri tanlay va ajrata olsalar kifoya.

Yoshlarga oid davlat siyosati – doimo amalda. Bizning O'zbekistonimizda yoshlarni informatsion xurujlardan asrash borasida qat'iy kurash siyosati – doimo kun tartibida.

Yoshlar bizning davlatimizda doimo g'amxo'rlikda, qo'llab-quvvatlashda, asrab-avaylashda. Ular davlatimiz himoyasida, yuksak ishonchda.

Zero, hozirgi vaqtda mamlakatimiz aholisining 32 foizini yoki 10 millionini 30 yoshgacha bo'lgan yoshlarimiz tashkil etadi. O'zbekiston Respublikasining Prezidenti Shavkat Mirziyoyev o'z ma'ruzasida yoshlarimizga katta ishonch bildirib, quyidagi fikrlarni bildiradi:

«Biz yoshlarga doir davlat siyosatini hech og'ishmasdan, qat'iyat bilan davom ettiramiz. Nafaqat davom ettiramiz, balki bu siyosatni eng ustuvor vazifamiz sifatida bugun zamon talab qilayotgan yuksak darajaga ko'taramiz.

Yoshlarimizning mustaqil fikrlaydigan, yuksak intellektual va ma'naviy salohiyatga ega bo'lib, dunyo miqyosida o'z tengdoshlariga hech qaysi sohada bo'sh kelmaydigan insonlar bo'lib kamol topishi, baxtli bo'lishi uchun davlatimiz va jamiyatimizning bor kuch va imkoniyatlarini safarbar etamiz.»

Yoshlar, yoshlar va yana yoshlar… Ular ertamiz, kelajagimiz. Ozod va obod Vatanni, mustaqil yurtimizni ular qo'liga ishonib topshiraylik.

19-MAVZU: AXBOROT XAVFSIZLIGI SOHASIDA XALQARO VA MILLIY ME'YORIY-HUQUQIY BAZA

MA'RUZA MASHG'ULOTI REJASI:

19.1. Axborot xavfsizligi sohasiga oid halqaro standartlar
19.2. Axborot xavfsizligi sohasiga oid milliy standartlar
19.3. Axborot xavfsizligi sohasiga oid me'yoriy xujjatlar

Tayanch iboralar: *Huquqiy ta'minot, qonun, aktlar, standart, jarayonli yondashuv, boshqarish tizimi, xavflarini baholash, xavfsizlikni ta'minlash usullari, risklarini boshqarish, O'z DSt, ISO/IEC, milliy standartlar, GOST 28147-89.*

1. Axborot xavfsizligi sohasiga oid halqaro standartlar

Axborot xavfsizligining huquqiy ta'minoti – axborotni himoyalash tizimida bajarilishi shart bo'lgan qonun chiqarish aktlar, me'yoriy - huquqiy hujjatlar, qoidalar yo'riqnomalar, qo'llanmalar majmui. Xozirda axborot xavfsizligining huquqiy ta'minoti masalasi ham amaliy, ham qonunchilik jixatidan faol o'rganib chiqilmoqda.

ISO/IEC 27001:2005 – "Axborot texnologiyalari. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar". Ushbu standart axborot xavfsizligini boshqarish tizimini (AXBT) ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat ko'rsatish va uni takomillashtirish modeli va talablaridan iborat. AXBT joriy etilishi tashkilotning strategik qarori bo'lib qolishi kerak. AXBTni ishlab chiqish va joriy etishda xavfsizlikning ehtiyojlari, maqsadlari, foydalaniladigan jarayonlari, tashkilotning ko'lami va strukturasi hisobga olinishi kerak. AXBT va uning yordamchi tizimlari vaqt o'tishi bilan o'zgaradi degan taxmin bor. Shuningdek, AXBTni kengaytirish masshtablari tashkilotning ehtiyojlariga bog'liq bo'ladi, masalan, oddiy vaziyat AXBT uchun oddiy yechimni talab qiladi. Muvofiqlikni baholash uchun ushbu standartdan ichki va tashqi tomonlar foydalanishi mumkin.

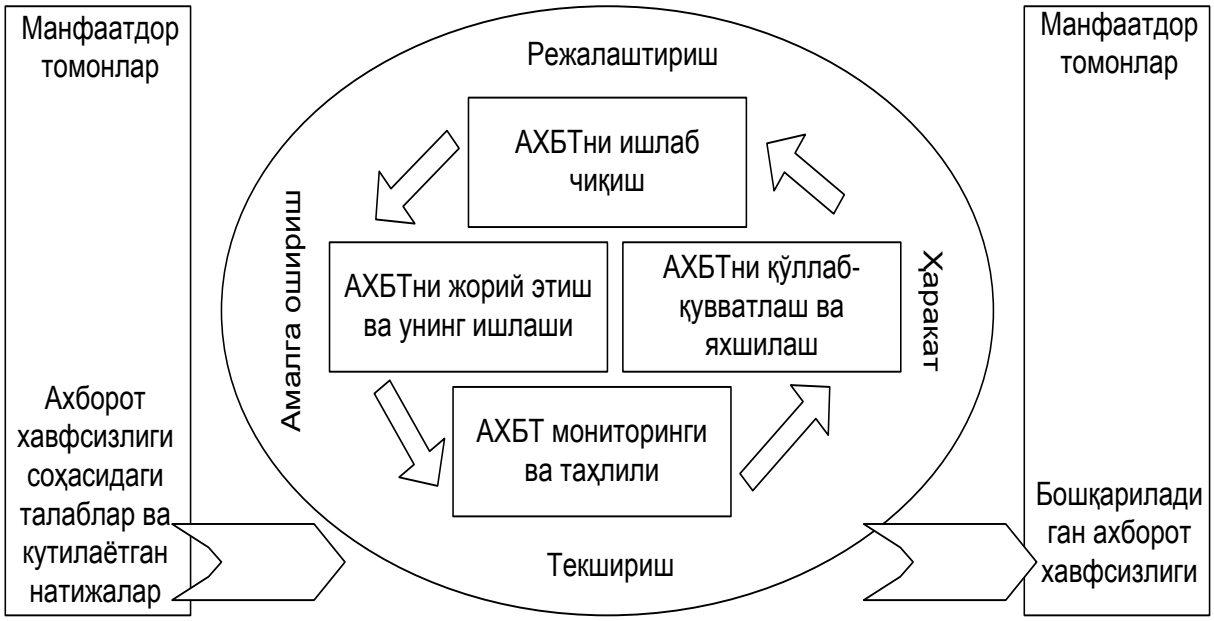
Jarayonli yondashuv. Ushbu standart tashkilot AXBTni ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat ko'rsatish va uni takomillashtirishda jarayonli yondashuvning qo'llanishiga yo'naltirilgan.

Ushbu standartda AXBT har bir jarayonini ishlab chiqishda qo'llanishi mumkin bo'lgan *rejalashtirish – amalga oshirish – tekshirish - harakat* [«Rlan-Do-Check-Act» (PDCA)] modelikeltirilgan.

Ushbu model AXBT axborot xavfsizligi talablari va manfaatdor tomonlarning kutilayotgan natijalaridan kiruvchi ma'lumotlar sifatida qanday foydalanishini va zarur xatti-harakatlar va jarayonlarni amalga oshirish natijasida e'lon qilingan talablar va kutilayotgan natijalarni qanoatlantirishidan dalolat beradigan ma'lumotlarni olishini ko'rsatadi.

1-misol. Axborot xavfsizligining buzilishi tashkilot uchun jiddiy moliyaviy yo'qotishlarning va/yoki qandaydir qiyinchiliklarning sababi bo'la olmaydi degan talab qo'yilishi mumkin.

2-misol. Qandaydir jiddiy mojaro, masalan, sayt yordamida elektron savdoni amalga oshirayotgan tashkilot saytining buzilishi natijasida yuzaga keladigan holat uchun – tashkilot buzilish oqibatlarini minimumga keltirish uchun yetarli bilim va tajribaga ega bo'lgan mutaxassislarga ega bo'lishi kerak.



19.1-rasm. AXBT jarayonlariga PDCA modelini qo‘llash.

Boshqa boshqarish tizimlari bilan moslashuv. Ushbu standart boshqa boshqaruv standartlari bilan moslashuvini yaxshilash va integratsiya qilishuchun ISO 9001:2000 va ISO 14001:2004 standartlari bilan muvofiqlashtirilgan. Kerakli tarzda loyihalashtirilgan bitta boshqaruv tizimi barcha ushbu standartlarning talablariga javob berishga qodir. 19.1-jadvalda ushbu standartning ISO 9001:2000 va ISO 14001:2004 standartlari bilan o‘zaro bog‘liqligi ko‘rsatilgan.

Ushbu standart tashkilotga amaldagi AXBTni boshqa boshqaruv tizimlarining tegishli talablari bilan moslashtirish yoki integratsiya qilish imkonini beradi.

19.1-jadval.

Rejalashtirish (AXBTni ishlab chiqish)	Tashkilotning umumiy siyosati va maqsadlarida e’lon qilingan natijalarga erishish maqsadida siyosat va maqsadlarni belgilash, xatarlarni boshqarish va axborot xavfsizligini takomillashtirish bilan bog‘liq bo‘lgan jarayonlar va protseduralarni aniqlash.
Amalga oshirish (AXBTni joriy etish va uning ishlashi)	AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashi.
Tekshirish (AXBT monitoringi va tahlili)	Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash. Natijalarning yuqori rahbariyat tomonidan tahlil qilinishi.
Harakat (AXBTni qo‘llab quvvatlash va takomillashtirish)	AXBT ichki auditlari natijalariga, rahbariyat tomonidan qilingan tahlil yoki uzluksiz takomillashtirish maqsadida boshqa manbalardan olingan ma’lumotlarga asoslangan tuzatuvchi va ogohlantiruvchi harakatlarni bajarish

ISO/IEC 27002:2005 – “Axborottexnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

Axborot - biznesning boshqa muhim aktivlari kabi qiymatga ega bo‘lgan aktiv va shunday ekan, u tegishli ravishda muhofaza qilingan bo‘lishi kerak. Bu o‘zaro aloqalar bilan doimo rivojlanayotgan amaliy ish muhitida ayniqsa muhim. Hozirgi vaqtda ushbu o‘zaro aloqalar natijasida axborot tahdidlar va zaifliklarning o‘sib borayotgan soni va turli xiliga duchor bo‘lmoqda.

Axborot xavfsizligining zarurati. Axborot va uni saqlab turuvchi jarayonlar, axborot tizimlari va tarmoq infratuzilmasi biznesning bebaho aktivlari bo‘lib hisoblanadi. Axborot xavfsiligini aniqlash, ta’minlash, saqlab turish va yaxshilash tashkilotning raqobatbardoshliligi, qadrliligi, daromadliligi, qonun hujjatlariga muvofiqligini va ishbilarmonlik obro‘sini ta’minlashda katta ahamiyatga ega.

Axborot xavfsizligi talablarini aniqlash. Tashkilot o‘zining axborot xavfsizligiga bo‘lgan talablarini quyidagi uchta muhim omilni hisobga olib aniqlashi muhim:

- biznesning global strategiyasi va tashkilotning maqsadlarini e’tiborga olib, tashkilotda olingan xavflarni baholash yordamida tashkilot aktivlariga tahdidlar aniqlanadi, tegishli aktivlarning zaifligi va tahdidlar paydo bo‘lish ehtimoli, shuningdek kelib chiqishi mumkin bo‘lgan oqibatlar baholanadi;

-tashkilot, uning savdo sheriklari, pudratchilar va xizmatlarni yetkazib beruvchilar, qoniqtirishi kerak bo‘lgan yuridik talablar, qonun hujjatlarining talablari, tartibga soluvchi va shartnomaviy talablar, shuningdek, ushbu tomonlaring ijtimoiy madaniy muhiti boshqa omil bo‘lib hisoblanadi;

-o‘zining ishlashini ta’minlash uchun tashkilot tomonidan ishlab chiqilgan prinsiplar, maqsadlar va talablarning maxsus to‘plami yana bir omil bo‘lib hisoblanadi.

Axborot xavfsizligi xavflarini baholash. Axborot xavfsizligiga qo‘yiladigan talablar xavflarni muntazam baholash yordamida aniqlanadi. Axborot xavfsizligini boshqarish bo‘yicha tadbirlarga ketgan sarf-xarajatlar axborot xavfsizligining buzilishi natijasida tashkilotga yetkazilishi mumkin bo‘lgan zarar miqdoriga mutanosib bo‘lishi lozim.

Axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlash. Axborot xavfsizligiga qo‘yiladigan talablar belgilanganidan va xavflar aniqlanganidan so‘ng xavflarni qabul qilsa bo‘ladigan darajagacha pasayishini ta’minlaydigan, axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlash va joriy etish kerak. Ushbu tadbirlar ushbu standartdan, boshqa manbalardan tanlab olinishi, shuningdek, axborot xavfsizligini boshqarish bo‘yicha tashkilotning o‘ziga xos ehtiyojlarini qondiradigan tadbirlar ishlab chiqilishi mumkin. Axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlash xavflarni qabul qilish mezonlariga, xavflarga baho berish variantlariga asoslangan tashkiliy qarorlarga va xavflarni tashkilotda qabul qilingan boshqarishga umumiy yondashishga bog‘liq. Ushbu tanlovni tengishli milliy va xalqaro qonun hujjatlari va normalar bilan muvofiqlashtirish kerak.

Axborot xavfsizligini joriy qilish uchun tayanch nuqta. Axborot xavfsizligini boshqarish bo‘yicha alohida tadbirlar axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va uni joriy qilish uchun tayanch nuqta bo‘lib xizmat qilishi mumkin. Bunday tadbirlar qonun hujjatlarining asosiy talablariga asoslanadi yoki axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida qabul qilinishi mumkin.

Qonunchilik nuqtai nazaridan axborot xavfsizligini boshqarish bo‘yicha asosiy choralar quyidagilar hisoblanadi:

- ma’lumotlarni muhofaza qilish va shaxsiy axborotning konfidensialligi;
- tashkilot hujjatlarini muhofaza qilish;
- intellektual mulkka egalik qilish huquqi.

Axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida hisoblangan axborot xavfsizligini boshqarish bo‘yicha tadbirlar quyidagilarni o‘z ichiga oladi:

- axborot xavfsizligi ciyosatini hujjatlashtirish;
- axborot xavfsizligini ta’minlash bo‘yicha majburiyatlarni taqsimlash;
- axborot xavfsizligi qoidalariga o‘qitish;
- ilovalardagi axborotga to‘g‘ri ishlov berish;
- texnik zaifliklarniboshqarishstrategiyasi;
-tashkilotninguzluksizishiniboshqarish;
-axborot xavfsizligi mojarolarini va takomillashtirishlarini boshqarish.

Muvaffaqiyatning eng muhim omillari. Tajriba shuni ko‘rsatadiki, tashkilotda axborot xavfsizligini ta’minlash bo‘yicha tadbirlarni muvaffaqiyatli joriy qilish uchun quyidagi omillar hal qiluvchi hisoblanadi:

-axborot xavfsizligi maqsadlari, siyosatlari va muolajalarining biznes maqsadlariga muvofiqligi;

-xavfsizlik tizimini joriy qilish, madadlash, monitoringini o‘tkazish va modernizatsiya qilishga yondashishning korporativ madaniyat bilan muvofiqligi;

-rahbariyat tomonidan real qo‘llab-quvvatlash va manfaatdorlik;

-xavfsizlik talablarini, xavflarni baholash va xavflarni boshqarishni aniq tushunish;

-tashkilot rahbarlari va xodimlari tomonidan axborot xavfsizligining samarali marketingini o‘tkazish, shuningdek, axborot xavfsizligining choralarini qo‘llash zaruratini tushunishni ta’minlash;

-axborot xavfsizligi siyosatiga tegishli yo‘riqnomalar, tavsiyalarni va tegishli standartlarni barcha xodimlar va subpudratchilarga berish;

-axborot xavfsizligini boshqarish bo‘yicha tadbirlarni moliyalashtirish sharti;

-o‘qitish va tayyorlashning zarur darajasini ta’minlash;

-axborot xavfsizligi mojarolarini boshqarishning samarali jarayonini tasdiqlash;

-o‘lchanadigan ko‘rsatkichlarning axborot xavfsizligini boshqarishning samaradorliligini va uni yaxshilash bo‘yicha bajaruvchilardan tushgan takliflarni baholash uchun foydalaniladigan har tomonlama va balanslangan tizimi.

Tashkilotga tegishli qo‘llanmalarni ishlab chiqish. Ushbu standart tashkilotning muayyan ehtiyojlari uchun qo‘llanmalar ishlab chiqish uchun tayanch nuqta sifatida baholanishi kerak. Ushbu standartda keltirilgan yo‘riqnomalar va tadbirlarning hammasi ham qo‘llashga yaroqli bo‘lavermaydi.

Bundan tashqari, ushbu standartga kiritilmagan qo‘shimcha choralar kerak bo‘lib qolishi mumkin. Bu holda auditorlar va biznes bo‘yicha sheriklar tomonidan o‘tkaziladigan muvofiqlik tekshiruvini yengillashtiradigan, bir vaqtda bir necha tomondan qilingan havolalarning saqlanishi foydali bo‘lishi mumkin.

O‘zDStISO/IEC 27005:2013 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborotxavfsizligi risklarini boshqarish”

Ushbu standart tashkilotda axborot xavfsizligi risklarini boshqarish bo‘yicha tavsiyalarni o‘z ichiga oladi.

Ushbu standart O‘z DSt ISO/IEC 27001 da belgilangan umumiy konsepsiyalarni qo‘llab-quvvatlaydi va risklarni boshqarish bilan bog‘liq yondashuv asosida axborot xavfsizligini aynan bir xil ta’minlashni amalga oshirish uchun mo‘ljallangan.

Ushbu standartni, to‘la tushunib yetish uchun O‘z DSt ISO/IEC 27001 va O‘z DSt ISO/IEC 27002da bayon qilingan konsepsiyalarni, modellarni, jarayonlarni va terminologiyani bilish zarur.

Ushbu standart tashkilotning axborot xavfsizligini obro‘sizlantirishi mumkin bo‘lgan risklarni boshqarishni amalga oshirishni rejalashtiradigan barcha turdagi tashkilotlar (masalan, tijorat korxonalari, davlat muassasalari, notijorat tashkilotlar) uchun qo‘llaniladi.

Ushbu standartda quyidagi standartlarga bo‘lgan havolalardan foydalanilgan:

O‘z DSt ISO/IEC 27001:2009 Axborot texnologiyalari. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar.

O‘z DSt ISO/IEC 27002:2008 Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari

O‘zDStISO/IEC 27006:2013 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlarining auditi va ularni sertifikatlashtirish organlariga qo‘yiladigan talablar”

O‘z DSt ISO/IEC 17021 - bu tashkilotlarni boshqarish tizimlarining auditini va sertifikatlashtirilishini amalga oshiradigan organlar uchun mezonlarni o‘rnatadigan standartdir. Agar bu organlar O‘z DSt ISO/IEC 27001 ga muvofiq, axborot xavfsizligini boshqarish tizimlari (AXBT)ning sertifikatlashtirilishini va auditini o‘tkazish maqsadida, O‘z DSt ISO/IEC 17021 muvofiq keladigan organlar sifatida akkreditlanadigan bo‘lsa, u holda O‘z DSt ISO/IEC 17021 ga qo‘llanma va qo‘shimcha talablar zarur. Ular ushbu standartda taqdim etilgan.

Ushbu standartning matni O‘z DSt ISO/IEC 17021 strukturasini takrorlaydi, AXBT uchun spetsifik bo‘lgan qo‘shimcha talablar va AXBTni sertifikatlashtirish uchun O‘z DSt ISO/IEC 17021 ni qo‘llash bo‘yicha qo‘llanma esa, «AX» abbreviaturasi bilan belgilanadi.

«Kerak» atamasidan ushbu standartda O‘z DSt ISO/IEC 17021 va O‘z DSt ISO/IEC 27001 talablarini aks ettirgan holda majburiy bo‘lgan shartlarni ko‘rsatish uchun foydalaniladi. «Zarur» atamasidan, garchi bu talablarni qo‘llash bo‘yicha qo‘llanma bo‘lsa ham, sertifikatlashtirish organi tomonidan qabul qilinishi ko‘zda tutiladigan shartlarni belgilash uchun foydalaniladi.

ISO/IEC 15408-1-2005 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari va vositalari. Axborot texnologiyalari xavfsizligini baholash mezonlari”

ISO/IEC 15408-2005 xalqaro standarti ISO/IEC JTC 1 «Axborot texnologiyalari» Birgalikdagi texnik qo‘mita, SC 27 «AT xavfsizligini ta’minlash metodlari va vositalari» kichik qo‘mita tomonidan tayyorlangan. ISO/IEC 15408-2005 ga o‘xshash matn «Axborot texnologiyalari xavfsizligini baholashning umumiy mezonlari» 2.3-versiya (2.3 UM deb nomlanadi) sifatida «Umumiy mezonlar» loyihasining homiy-tashkilotlari tomonidan e’lon qilingan.

Standartning ikkinchi tahriri texnik jihatdan qayta ishlashga to‘g‘ri kelgan birinchi tahrir (ISO/IEC 15408:1999)ni bekor qiladi va uni almashtiradi.

ISO/IEC 15408-2005 ga o‘xshash bo‘lgan O‘z DSt ISO/IEC 15408 «Axborot texnologiyalari - Xavfsizlikni ta’minlash metodlari va vositalari - Axborot texnologiyalari xavfsizligini baholash mezonlari» umumiy sarlavha ostidagi quyidagi qismlardan tashkil topgan:

1-qism: Kirish va umumiy model;

2-qism: Xavfsizlikka qo‘yiladigan funksional talablar;

3-qism: Xavfsizlikka qo‘yiladigan ishonch talablari.

O‘z DSt ISO/IEC 15408 xavfsizlikni mustaqil baholash natijalarini qiyoslash imkoniyatini beradi. Bunga AT mahsulotlari va tizimlarining xavfsizlik funksiyalariga va xavfsizlikni baholashda ularga qo‘llaniladigan ishonch choralariga qo‘yiladigan talablar umumiy to‘plamining taqdim etilishi bilan erishiladi.

O‘z DSt ISO/IEC 15408 AT mahsulotlari va tizimlarining xavfsizlik funksiyalari bilan ishlab chiqilishidagi kabi, shunday funksiyali tijorat mahsulotlari va tizimlarining sotib olinishida ham

qo‘llanma sifatida foydali. ATning bunday mahsuloti yoki tizimining baholanishi baholash ob’ekti (BO) deb ataladi. BundayBOga, masalan, operatsiontizimlar, hisoblashtarmoqlari, taqsimlangantizimlarvailovalarkiradi.

2. Axborot xavfsizligi sohasiga oid milliy standartlar

Ushbu bo‘limda keltirilgan standartlar zamon talablari tomonidan kelib chiqqan holda amalga oshirilgan bo‘lib, asos sifatida O‘zbekiston Respublikasining "Elektron raqamli imzo xususida"gi va "Elektron xujjat almashinuvi xususida"gi qonunlarini keltirishimiz mumkin.

Ushbu standartlar EHM tarmoqlarida, telekommunikatsiyada, alohida hisoblash komplekslari va EHMda axborotni ishlash tizimlari uchun axborotni shifrlashning umumiy algoritmini va ma’lumotlarni shifrlash qoidasini belgilaydi.

O‘z DSt 1092:2009 – “Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari”

Ushbu standart umumiy foydalanishdagi muhofazalanmagan telekommunikatsiya kanallari orqali uzatiladigan, berilgan xabar (elektron hujjat) ostiga qo‘yilgan elektron raqamli imzo (ERI)ni shakllantirish va uning haqiqiyligini tasdiqlash uchun elektron raqamli imzo algoritmi (ERIA)ni belgilaydi.

Standart elektron raqamli imzoni shakllantirish va uning haqiqiyligini tasdiqlashda turli maqsadlar uchun mo‘ljallangan axborotlarni qayta ishlash tizimlarida qo‘llash uchun mo‘ljallangan.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O‘z DSt 1047:2003 Axborot texnologiyalari. Atamalar va ta’riflar.

O‘zDSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.

O‘z DSt 1105:2009 – “Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi”

Ushbu « Ma’lumotlarni shifrlash algoritmi» (MShA) standarti elektron ma’lumotlarni muhofaza qilish uchun mo‘ljallangan kriptografik algoritmni ifodalaydi. MShA - simmetrik blokli shifr bo‘lib, axborotni shifrmatnga o‘girish va dastlabki matnga o‘girish uchun foydalaniladi. MShA 256 bit uzunlikdagi ma’lumotlar blokini shifrmatnga o‘girish va shifrmatnni dastlabki matnga o‘girish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitdan foydalanishi mumkin.

Standart, elektron hisoblash mashinalari (EHM) tarmoqlarida, alohida hisoblash komplekslari va EHMda axborotga ishlov berish tizimlarida axborotni shifrlashning yagona algoritmini o‘rnatib, ma’lumotlarni shifrlash qoidalarini belgilaydi.

Ma’lumotlarni shifrlash algoritmi dasturiy, apparat yoki apparat-dasturiy kriptografik modullarda amalga oshirish uchun mo‘ljallangan.

Tashkilotlar, korxonalar va muassasalar EHM tarmoqlarida, alohida hisoblash komplekslarida yoki EHMda saqlanuvchi va uzatiluvchi ma’lumotlarning kriptografik muhofazasini amalga oshirishda mazkur standartdan foydalanishlari mumkin.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O‘zDSt 1047:2003 Axborot texnologiyalari. Atamalar va ta’riflar.

O‘zDSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.

O‘z DSt 1106:2009 – “Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi”

Ushbu standart axborotni qayta ishlash va muhofaza qilishning kriptografik metodlarida, shu jumladan avtomatlashtirilgan tizimlarda axborot uzatish, qayta ishlash va saqlashda elektron raqamli imzo (bundan keyin - ERI) protseduralarini amalga oshirish uchun qo‘llaniladigan ikkilik simvollarining istalgan ketma-ketligi uchun xeshlash funksiyasining (bundan keyin - XF) algoritmini va hisoblash protsedurasini belgilaydi.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

GOST 28147-89 Sistemы obrabotki informatsii. Zaщita kriptograficheskaya. Algoritmы kriptograficheskogo preobrazovaniya

O‘z DSt 1047:2003 Axborot texnologiyalari. Atamalar va ta’riflar

O‘z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar

O‘z DSt 1204:2009 – “Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik modullarga xavfsizlik talablari”

Ushbu standart ochiq va simmetrik kalitli kriptografik modullarga qo‘yiladigan yagona xavfsizlik talablarini belgilaydi hamda axborotning kriptografik muhofaza qilish vositalarini loyihalash, ishlab chiqish, sotish (eltib berish) va undan foydalanish uchun mo‘ljallangan. Standart EHM, telekommunikatsiya tarmoqlari, ayrim hisoblash komplekslari yoki EHMda saqlanadigan va uzatiladigan konfidensial axborotni muhofaza qiladigan kriptografik modullarga qo‘yiladigan xavfsizlik talablarini belgilaydi.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O‘z DSt 1092:2005 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.

O‘z DSt 1105:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.

O‘z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.

3. Axborot xavfsizligi sohasiga oid me’yoriy xujjatlar

RH 45-215:2009 - Rahbariy hujjat. Ma’lumotlar uzatish tarmog‘ida axborot xavfsizligini ta’minlash to‘g‘risida Nizom. Ushbu hujjat N 100:2002 «Ma’lumotlar uzatish milliy tarmog‘ida axborot xavfsizligini ta’minlash to‘g‘risida nizom» o‘rniga amalga kiritilgan bo‘lib, ma’lumotlar uzatish tarmog‘ida (MUT) axborot xavfsizligini ta’minlash bo‘yicha asosiy maqsadlar, vazifalar, funksiyalar va tashkiliy-texnik tadbirlarni belgilaydi.

RH 45-185:2011-Rahbariy hujjat. Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi. Ushbu hujjat RH 45-185:2006 hujjati o‘rniga amalga kiritilgan bo‘lib, davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturlarini ishlab chiqish tartibini belgilaydi.

Hujjat axborot xavfsizligini ta’minlash dasturlari doirasida ishlab chiqiladigan chora-tadbirlarning maqsadlari, vazifalari, tuzilmasi va ro‘yxatiga qo‘yiladigan namunaviy talablarni belgilaydi.

RH 45-193:2007 - Rahbariy hujjat. Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi. Ushbu hujjat davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlashning namunaviy tartibini belgilaydi.

Ushbu hujjat talablari davlat organlarining saytlari uchun xosting xizmatlarini taqdim etuvchi barcha ho‘jalik yurituvchi sub’ektlar tomonidan qo‘llanilishi majburiydir.

TSt 45-010:2010 – Tarmoq standarti. Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar. Ushbu tarmoq standarti O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi davlat standartlashtirish, metrologiya va sertifikatlashtirish markazi («O‘zdavstandart») tomonidan 2002 yil 6 avgustda 112/066-son bilan ro‘yxatga olingan TSt 45.010:2002 «Otraslevoy standart. Informatsionnaya bezopasnost v sfere svyazi i informatizatsii. Terminы i opredeleniya» o‘rniga amalga kiritilgan bo‘lib, aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi.

20-MAVZU: XAVFSIZLIK MODELLARI

MA’RUZA MASHG’ULOTI REJASI:

20.1. Axborot xavfsizligini buzuvchining modeli
20.2. Xarrison-Ruzzo-Ulmanning diskretsion modeli
20.3. Bella-LaPadulaning mandatli modeli
20.4. Xavfsizlikning rolli modeli

Tayanch iboralar: ta’minot, model, kategoriya, g‘oyaviy, ishonchsiz, resurs, buzuvchi, diapazon, maqsad, nishon, xavfsizlik modellari.

1. Axborot xavfsizligini buzuvchining modeli

Bo‘lishi mumkin bo‘lgan tahdidlarni oldini olish uchun nafaqat operatsion tizimlarni, dasturiy ta’minotni himoyalash va foydalanishni nazorat qilish, balki buzuvchilar turkumini va ular foydalanadigan usullarni aniqlash lozim.

Sabablar, maqsadlar va usullarga bog‘liq holda axborot xavfsizligini buzuvchilarni to‘rtta kategoriyaga ajratish mumkin:

- sarguzasht qidiruvchilar;
- g‘oyaviy xakerlar;
- xakerlar-professionallar;
- ishonchsiz xodimlar.

Sarguzasht qidiruvchi, odatda, yosh, ko‘pincha talaba yoki yuqori sinf o‘quvchisi va unda o‘ylab qilingan xujum rejasi kamdan-kam bo‘ladi. U nishonini tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi. Bunday sarguzasht qidiruvchi muvaffaqiyatlarini fakat yaqin do‘stlari–kasbdoshlari bilan o‘rtoqlashadi.

G‘oyali xaker – bu ham sarguzasht qiduruvchi, ammo mohirroq. U o‘zining e’tiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yaxshi ko‘rgan hujum turi Web-serverning axborotini o‘zgartirishi yoki, juda kam hollarda, hujumlanuvchi resurslar ishini blokirovka qilish. Sarguzasht qidiruvchilarga nisbatan g‘oyali xakerlar muvaffaqiyatlarini kengrok auditoriyada, odatda axborotni xaker Web-uzelda yoki Usenet anjumanida joylashtirilgan holda e’lon qiladilar.

Xaker-proffesional harakatlarning aniq rejasiga ega va ma’lum resurslarni mo‘ljallaydi. Uning hujumlari yaxshi o‘ylangan va odatda bir necha bosqichda amalga oshiriladi. Avval u dastlabki axborotni yig‘adi (operatsion tizim turi, taqdim etiladigan servislar va qo‘llaniladigan himoya choralari). So‘ngra u yig‘ilgan ma’lumotlarni hisobga olgan holda hujum rejasini tuzadi va mos instrumentlarni tanlaydi (yoki hatto ishlab chiqadi). Keyin, hujumni amalga oshirib, maxfiy axborotni oladi va nihoyat harakatlarining barcha izlarini yo‘q qiladi. Bunday hujum qiluvchi professional, odatda yaxshi moliyalanadi va yakka yoki professionallar komandasida ishlashi mumkin.

Ishonchsiz xodim o‘zining harakatlari bilan sanoat josusi yetkazadigan muammoga teng muammoni tug‘diradi. Buning ustiga uning borligini aniqlash murakkabroq. Undan tashqari unga tarmoqning tashqi himoyasini emas, balki faqat, odatda unchalik qatiy bo‘lmagan tarmoqning ichki himoyasini bartaraf qilishiga to‘g‘ri keladi. Ammo, bu holda uning korporativ ma’lumotlardan ruxsatsiz foydalanishi xavfi boshqa har qanday niyati buzuq odamnikidan yuqori bo‘ladi.

20.1-rasm. Axborot xavfsizligini buzuvchining modeli

Tizimdan ruxsatsiz foydalanishga majbur etish sabablarining diapazoni yetarlicha keng: kompyuter bilan o‘ynaganidagi hayajon ko‘tarinkiligidan to jirkanch menedjer ustidan hokimlik hissiyotigacha. Bu bilan nafaqat ko‘ngil ochishni xoxlovchi havaskorlar, balki professional dasturchilar ham shug‘ullanadi. Ular parolni tanlash, faraz qilish natijasida yoki boshka xakerlar bilan almashish yo‘li orqali qo‘lga kiritadilar. Ularning bir qismi nafaqat fayllarni ko‘rib chiqadi, balki fayllarning mazmuni bilan qiziqa boshlaydi. Bu jiddiy tahdid hisoblanadi, chunki bu holda beozor sho‘xlikni yomon niyat bilan qilingan harakatdan ajratish qiyin bo‘ladi.

Yaqin vaqtgacha rahbarlardan norozi hizmatchilarning o‘z mavqelarini suiiste’mol qilgan xolda tizimni buzishlari, undan begonalarning foydalanishlariga yo‘l qo‘yishlari yoki tizimni ish holatida qarovsiz qoldirishlari tashvishlantirar edi. Bunday harakatlarga majbur etish sabablari quyidagilar:

- hayfsanga yoki rahbar tomonidan tanbehga reaksiya;
- ish vaqtidan tashqari bajarilgan ishga firma haq to‘lamaganidan norozilik;
- firmani qandaydir yangi tuzilayotgan firmaga raqib sifatida zaiflashtirish maqsadida kasos olish kabi yomon niyat.

Rahbardan norozi xodim jamoa foydalanuvchi hisoblash tizimlariga eng katta tahdidlardan birini tug‘diradi. Shuning uchun ham xakerlar bilan kurashish agentligi individual kompyuter sohiblariga jon deb xizmat ko‘rsatadilar.

2. Xarrison-Ruzzo-Ulmanning diskretsion modeli

Ma’lumki, xavfsizlik siyosati deganda axborotni ishlash jarayonini qat’iy belgilovchi umumiy tartib va qoidalar majmui tushuniladiki, ularning bajarilishi ma’lum tahdidlar to‘plamidan himoyalanishni ta’minlaydi va tizim xavfsizligining zaruriy (ba’zida yetarli) shartini tashkil etadi. Xavfsizlik siyosatining formal ifodasi xavfsizlik siyosatining modeli deb ataladi.

Himoyalangan axborot tizimlarini ishlab chiqaruvchilar xavfsizlik modelidan quyidagi hollarda foydalanishadi:

- ishlab chiqariladigan tizim xavfsizligi siyosatining formal spetsifikatsiyasini (tafsilotli ro‘yxatini) tuzishda;
- himoya vositalarini amalga oshirish mexanizmlarini belgilovchi himoyalangan tizim arxitekturasining bazaviy prinsiplarini tanlash va asoslashda;
- tizim xavfsizligini etalon model sifatida tahlillash jarayonida;
- xavfsizlik siyosatiga rioya qilishning formal isboti yo‘li bilan ishlab chiqariladigan tizim xususiyatlarini tasdiqlashda.

Iste’molchilar xavfsizlikning formal modellarini tuzish yo‘li bilan ishlab chiqaruvchilarga o‘zlarining talablarini aniq va ziddiyatli bo‘lmagan shaklda yetkazish hamda himoyalangan tizimlarning o‘zlarining ehtiyojlariga mosligini baholash imkoniyatiga ega bo‘ladilar.

Kvalifikatsiya (Malaka) bo‘yicha ekspertlar himoyalangan tizimlarda xavfsizlik siyosatining amalga oshirilish adekvatligini taxlillash mobaynida xavfsizlik modelidan etalon sifatida foydalanadilar.

Xavfsizlik modeli quyidagi bazaviy tasavvurlarga asoslangan.

1. Tizim o‘zaro harakatdagi “sub’ektlar” va “ob’ektlar” majmuasidan iborat. Ob’ektlarni intuitiv ravishda axborotli konteynerlar ko‘rinishida tasavvur etish mumkin, sub’ektlarni esa ob’ektlarga turli usullar bilan ta’sir etuvchi bajariluvchi dasturlar deb hisoblash mumkin. Tizimni bunday tasavvur etishda axborotni ishlash xavfsizligi xavfsizlik siyosati shakllantiruvchi qoidalar va cheklashlar to‘plamiga mos holda sub’ektlarning ob’ektlardan foydalanishni boshqarish masalasini yechish orqali ta’minlanadi. Agar sub’ektlar xavfsizlik siyosati qoidalarini buzish imkoniyatiga ega bo‘lmasa, tizim xavfsiz hisoblanadi. Ta’kidlash lozimki, “ob’ekt” va “sub’ekt” tushunchalarining tavsifi turli modellarda jiddiy farqlanishi mumkin.
2. Tizimdagi barcha o‘zaro harakatlar sub’ektlar va ob’ektlar orasida ma’lum xildagi munosabatlarni o‘rnatish orqali modellashtiriladi.
3. Barcha amallar o‘zaro harakat monitori yordamida nazoratlanadi va xavfsizlik siyosati qoidalariga muvofiq ma’n etiladi yoki ruxsat beriladi.
4. Xavfsizlik siyosati qoidalar ko‘rinishida beriladi, bu qoidalarga mos holda sub’ektlar va ob’ektlar orasida barcha o‘zaro harakatlar amalga oshirilishi shart. Ushbu qoidalarni buzilishiga olib keluvchi o‘zaro harakatlar foydalanishni nazoratlovchi vositalar yordamida to‘sib qo‘yiladi va amalga oshirilishi mumkin emas.
5. Sub’ektlar, ob’ektlar va ular orasidagi munosabatlar (o‘rnatilgan o‘zaro harakat) to‘plami tizim “holatini” belgilaydi. Tizimning har bir xolati modelda taklif etilgan xavfsizlik mezoniga muvofiq xavfsiz yoki taxlikali bo‘ladi.
6. Xavfsizlik modelining asosiy elementi – xavfsiz xolatidagi tizim barcha o‘rnatilgan qoida va cheklashlarga rioya qilinganida taxlikali holatga o‘tish mumkin emasligi tasdig‘ining (teoremasining) isboti.

Xarrison-Ruzzo-Ulmanning diskretsion modeli klassik (mumtoz) diskretsion model hisoblanib, sub’ektlarning ob’ektlardan foydalanishni ixtiyoriy boshqarishni va foydalanish xuquqlarining tarqalishi nazoratini amalga oshiradi.

Ushbu model doirasida axborotni ishlash sistemasi axborotdan foydalanuvchi sub’ektlar (S to‘plam), himoyalanuvchi axborotga ega bo‘lgan ob’ektlar (O to‘plam) va mos harakatlarni, (masalan o‘qish (R), yozish (W), dasturni bajarish(E)) vakolatini anglatuvchi foydalanish xuquqlarining chekli to‘plami $R = \{r_1, r_2, \dots, r_n\}$ majmui ko‘rinishida ifodalanadi.

Shunday qilib, Xarrison-Ruzzo-Ulmanning diskretsion modeli umumiy quyilishida tizim xavfsizligini kafolatlamaydi, ammo aynan ushbu model xavfsizlik siyosati modellarining butun bir sinfiga asos bo‘lib xizmat qiladiki, ular foydalanishni boshqarishda va xuquqlarni tarqalishini nazoratlashda barcha zamonaviy tizimlarda ishlatiladi.

3. Bella-LaPadulaning mandatli modeli

Foydalanishni boshqarishning mandatli modeli ko‘pgina mamlakaltlarning davlat va hukumat muassasalarida qabul qilingan maxfiy xujjat almashish qoidalariga asoslangan. Bella Lapadula siyosatining asosiy mazmuni amaliy hayotdan olingan bo‘lib, himoyalanuvchi axborotni ishlashda qatnashuvchilarga va bu axborot mavjud bo‘lgan xujjatlarga xavfsizlik satxi nomini olgan maxsus belgi, masalan “maxfiy”, “mutlaqo maxfiy” va h. kabilarni tayinlashdan iborat. Xavfsizlikning barcha satxlari o‘rnatilgan ustunlik munosabati asosida tartiblanadi, masalan, “mutlaqo maxfiy” satxi “maxfiy” satxidan yuqori yoki undan ustun turadi. Foydalanishni nazoratlash o‘zaro harakatdagi tomonlarning xavfsizlik sathlariga bog‘liq holda quyidagi ikkita oddiy qoida asosida amalga oshiriladi:

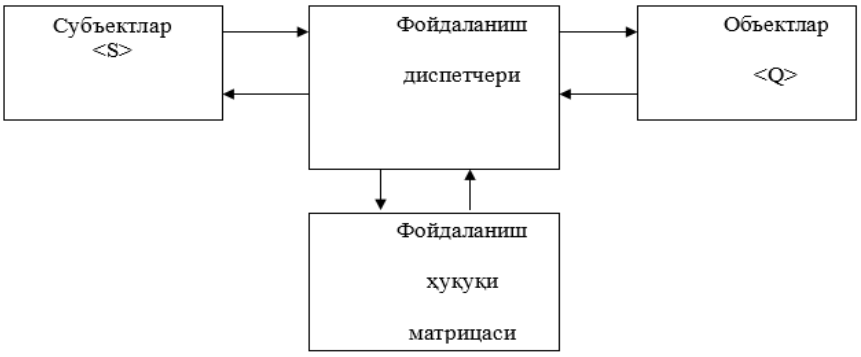
1. Vakolatli shaxs (sub’ekt) faqat xavfsizlik satxi o‘zining xavfsizlik satxidan yuqori bo‘lmagan xujjatlardan axborotni o‘qishga haqli.
2. Vakolatli shaxs (sub’ekt) xavfsizlik sathi o‘zining xavfsizlik satxidan past bo‘lmagan xujjatlarga axborot kiritishga xaqli.

Birinchi qoida yuqori satx shaxslari tomonidan ishlanadigan axborotdan past satx shaxslari tomonidan foydalanishdan himoyalashni ta’minlaydi. Ikkinchi qoida (juda muhim qoida) axborotni ishlash jarayonida yuqori satx ishtirokchilariga axborotning sirqib chiqishini (bilib yoki bilmasdan) bartaraf etadi.

Bella va La-Padula modeli. Bu modelda foydalanish huquqini cheklash vositalarini qurish maqsadida aktiv subektlar S’ va passiv ob’ektlar Q tushunchalari kiritilgan bo‘lib sub’ektlarning passiv ob’ektlardan foydalanish xuquqlari turlicha bo‘ladi. Ba’zida bu model «foydalanish huquqini cheklovchi matritsa modeli» deb yuritiladi. Ko‘pgina mavjud real vaqtli operatsion tizimlarda Bella va La-Padula modeli ishlatiladi. Bu modelda foydalanish dispetcherining ishlatilishi shart bo‘lib, himoya tizimi quyidagi uchlik orqali ifodalanadi:

$$Z=< S, Q, P >$$

Bu yerda S sub’ektlar to‘plami, Q- ob’ektlar to‘plami, P- ub’ektlarning ob’ektlardan foydalanish huquqlari to‘plami.



20.2-rasm. Bella-LaPadula modeli

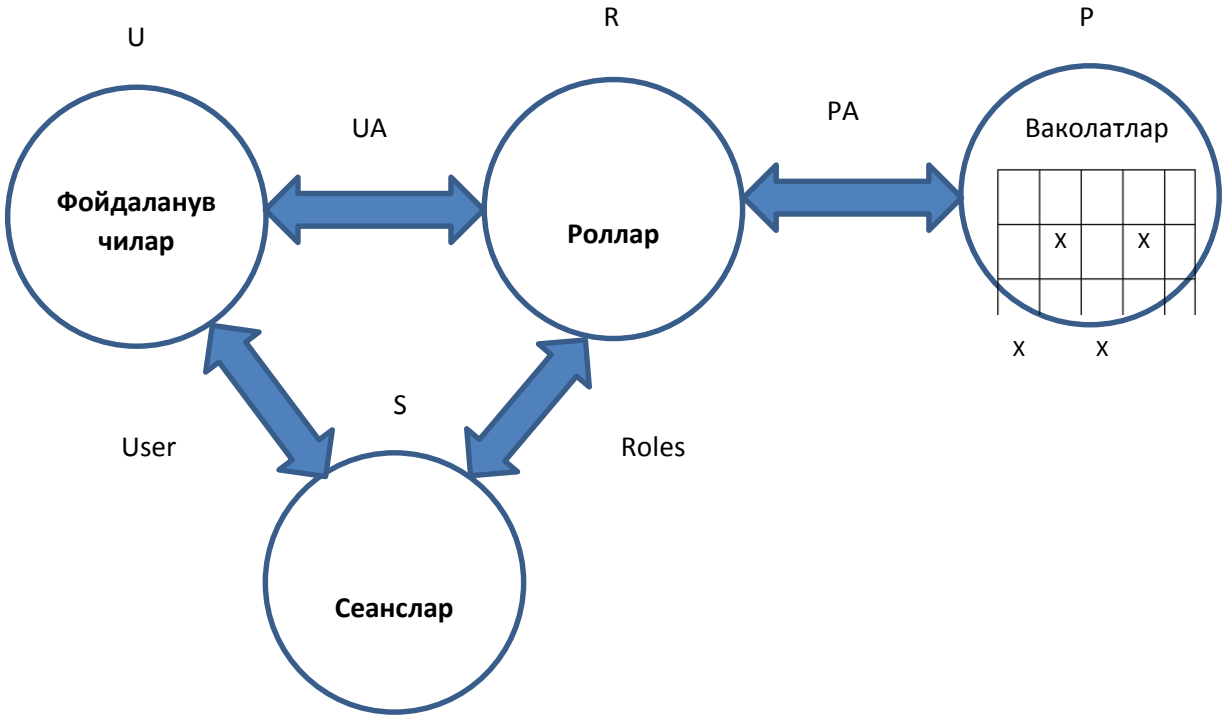
4. Xavfsizlikning rolli modeli

Rolli model xavfsizlik siyosatining mutlaqo o‘zgacha xili hisoblanidiki, bu siyosat diskretsion modelga xos foydalanishni boshqarishdagi moslanuvchanlik bilan mandatli modelga xos foydalanishni nazoratlash qoidalarining qat’iyligi orasidagi murosaga asoslangan.

Rolli modelda “sub’ekt” tushunchasi “foydalanuvchi” va “rol” tushunchalari bilan almashtiriladi. Foydalanuvchi – tizim bilan ishlovchi va ma’lum xizmat vazifalarini bajaruvchi odam. Rol – tizimda faol ishtirok etuvchi abstrakt tushuncha bo‘lib, u bilan ma’lum faoliyatni amalga oshirish uchun zarur vakolatlarining chegaralangan, mantiqiy bog‘liq to‘plami bog‘langan.

Rol siyosati keng tarqalgan, chunki bu siyosat boshqa qat’iy va rasmiy siyosatlardan farqli o‘laroq real hayotga juda yaqin. Haqiqatan, tizimda ishlovchi foydalanuvchilar shaxsiy ismidan harakat qilmay, ma’lum xizmat vazifalarni amalga oshiradi, ya’ni o‘zlarining shaxsi bilan bog‘liq bo‘lmagan qandaydir rollarni bajaradi.

Rolli siyosat ishlatilganida foydalanishni boshqarish ikki bosqichda amalga oshiriladi: birinchi bosqichda har bir rol uchun ob’ektdan foydalanish xuquqlari to‘plamidan iborat vakolatlar to‘plami ko‘rsatiladi, ikkinchi bosqichda har bir foydalanuvchiga uning qo‘lidan keladigan rollar ro‘yxati tayinlanadi. Rollarga vakolatlar eng kichik imtiyoz prinsipida tayinlanadi, ya’ni har bir foydalanuvchi o‘zining ishini bajarish uchun faqat minimal zarur vakolatlar to‘plamiga ega bo‘lishi shart. Rolli model tizimni quyidagi to‘plamlar ko‘rinishida tavsiflaydi (20.3-rasmga qaralsin):



20.3-rasm. Foydalanishni boshqarishning rolli modeli

U – foydalanuvchilar to‘plami;

R – rollar to‘plami;

P – ob’ektdan foydalanish vakolatlari to‘plami (masalan, foydalanish xuquqlari matritsasi ko‘rinishida);

S – foydalanuvchilarni tizim bilan ishlash seanslari to‘plami.

Yuqorida sanab o‘tilgan to‘plamlar uchun quyidagi munosabatlar belgilanadi:

$PA \subseteq P \times R$- har bir rolga unga berilgan vakolatlarni tayinlab, vakolatlar to‘plamini rollar to‘plamiga akslantiriladi;

Xavfsizlik siyosati modellari bo‘yicha xulosalar.

Xavfsizlikning diskretsion va mandatli siyosatlari mavjud avtomatlashtirilgan axborot tizimlarda qabul qilingan an’anaviy mexanizmlarga mos keladi. Diskretsion modellar uchun ob’ektlarga (fayllarga) xuquqlar ular tegishli bo‘lgan foydalanuvchilar tomonidan tayinlanadi, jarayon vakolatlari esa uni foydalanuvchi nomidan bajarilayotgan foydalanuvchi identifikatori orqali aniqlanadi. Mandatli model uchun ob’ektlarning xavfsizlik darajasi ularda saqlanayotgan xujjatlarning maxfiylik grifiga mos keladi, sub’ektlarning xavfsizlik darajasi esa foydalanuvchilarning “ruxsat(dopusk)” kategoriyasiga asosan aniqlanadi. Aksincha, rolli siyosat xavfizlikning tatbiqiy siyosatini akslantiradi. Shu sababli bu siyosatda aniq moslik mavjud emas. Ushbu siyosatni amalga oshirish mexanizmini tatbiqiy masala shartlari hamda rollar va vakolatlarni tayinlash metodikasiga asosan ishlab chiqish zarur.

21-MAVZU: ELEKTRON RAQAMLI IMZO

MA’RUZA MASHG’ULOTI REJASI:

21.1. Elektron raqamli imzo
22.1. Kriptografik kalitlarni boshqarish

Tayanch iboralar: *tekshirish, maxfiy, abonent, shifrlash, maxfiy kalit, matritsa, kriptografik kalit, kodlash kaliti, global tarmok.*

Elektron raqamli imzo

Elektron hujjatlarni tarmoq orqali almashishda ularni ishlash va saqlash xarajatlari kamayadi, qidirish tezlashadi. Ammo, elektron hujjat muallifini va hujjatning o‘zini autentifikatsiyalash, ya’ni muallifning haqiqiyligini va olingan elektron hujjatda o‘zgarishlarning yo‘qligini aniqlash muammosi paydo bo‘ladi.

Elektron hujjatlarni auyentifikatsiyalashdan maqsad ularni mumkin bo‘lgan jinoyatkorona harakatlardan himoyalashdir. Bunday harakatlarga quyidagilar kiradi:

- faol ushlab qolish - tarmoqqa ulangan buzg‘unchi hujjatlarni (fayllarni) ushlab qoladi va o‘zgartiradi. - maskarad – abonent S hujjatlarni abonent V ga abonent A nomidan yuboradi;
- renegatlik — abonent A abonent V ga xabar yuborgan bo‘lsada, yubormaganman deydi;
- almashtirish — abonent V hujjatni o‘zgartiradi, yoki yangisini shakillantiradi va uni abonent A dan olganman deydi;
- takrorlash - abonent A abonent V ga yuborgan hujjatni abonent S takrorlaydi.

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 bog‘liq majburiyatlaridan tonish imkoniyatini bermaydi;
- imzo chekilgan matn yaxlitligini kafolatlaydi.

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

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

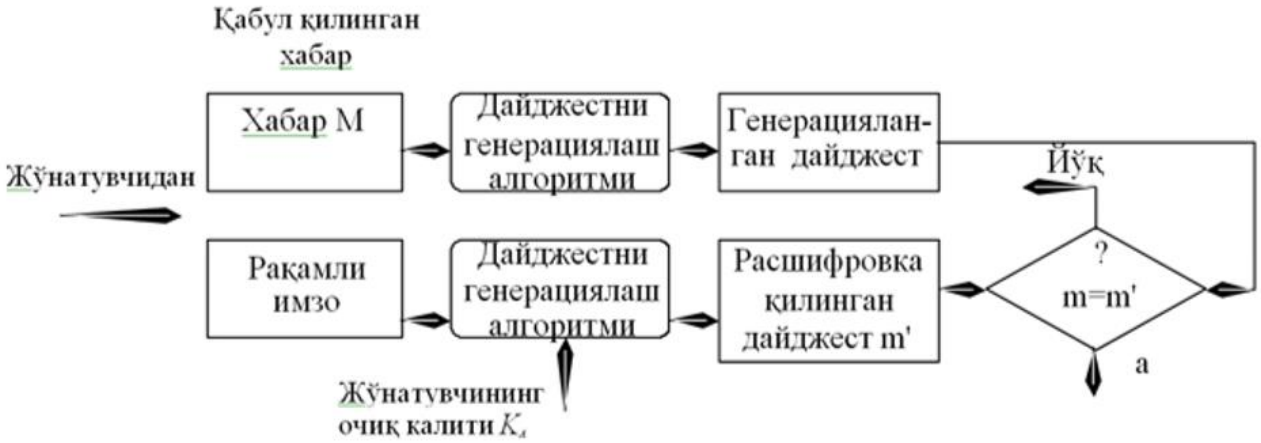
Elektron raqamli imzoni shakllantirish sxemasi

21.1-rasm. Raqamli imzoni shakllantirish muolajasi.

Ushbu muolajani tayyorlash bosqichida xabar jo‘natuvchi abonent A ikkita kalitni generatsiyalaydi: mahfiy kalit k_A. va ochiq kalit K_A. Ochiq kalit K_A uning jufti bo‘lgan maxfiy kaliti

k_A dan hisoblash orqali olinadi. Ochiq kalit K_A tarmoqning boshqa abonentlariga imzoni tekshirishda foydalanish uchun tarqatiladi.

Elektron raqamli imzoni tekshirish sxemasi



21.2-rasm. Raqamli imzoni tekshirish muolajasi.

Tarmoq abonentlari olingan xabar “M”ning raqamli imzosini ushbu xabarni jo‘natuvchining ochik kaliti $K_A$yordamida tekshirishlari mumkin.

Har 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 indentifikatori (ochiq kalit nomi);
- raqamli imzoning o‘zi.

1977 yilda AQSh da yaratilgan RSA tizimi birinchi va dunyoda mashhur elektron raqamli imzo tizimi hisoblanadi va yuqorida keltirilgan prinsiplarni amalga oshiradi. Ishonchliligining yuqoriligi va shaxsiy kompyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmli 1984 yilda El Gamal tomonidan ishlab chiqildi.

Kriptografik kalitlarni boshqarish

Kalitlarni taqsimlashga quyidagi talablar qo‘yiladi:

- taqsimlashning operativligi va aniqligi;
- taqsimlanuvchi kalitlarning konfidensialligi va yaxlitligi.

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

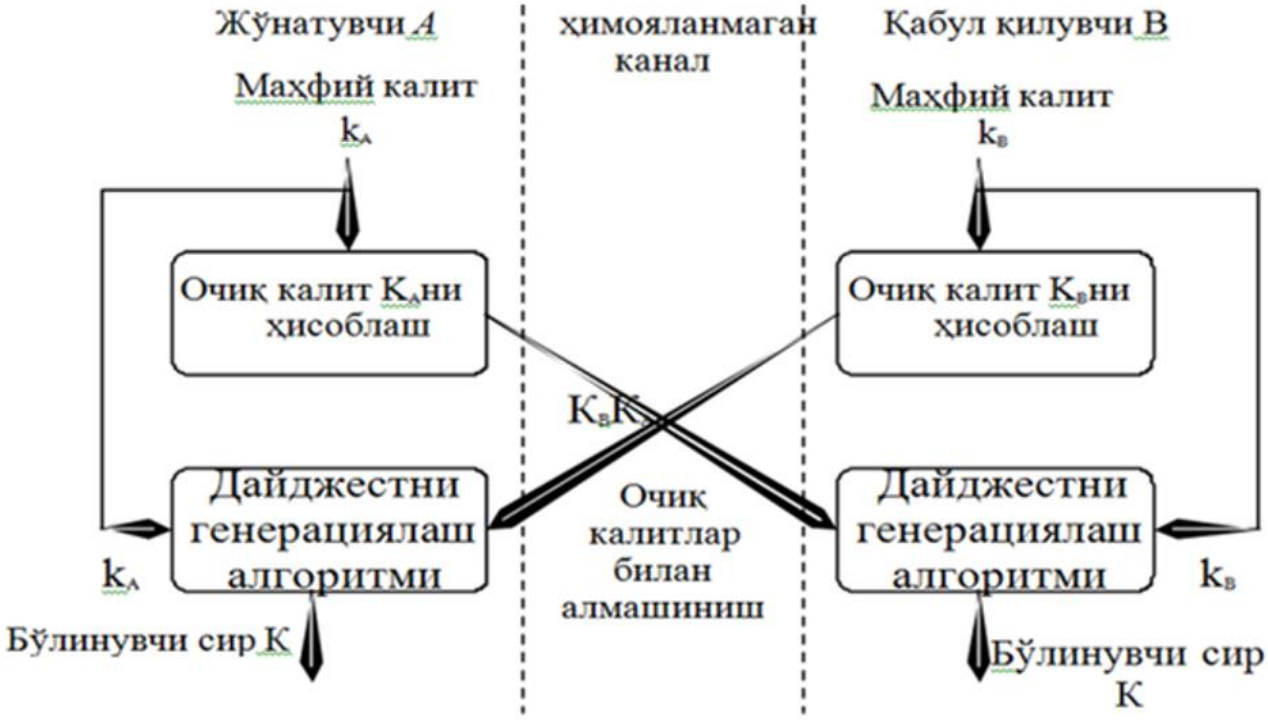
1.Kalitlarni taqsimlovchi bitta yoki bir nechta markazlardan foydalanish.

2.Tarmoq 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 bo‘lgan suiste’mollar tarmoq xavfsizligining jiddiy buzilishiga olib kelishi mumkin. Ikkinchi usuldagi muammo tarmoq sub’ektlarining haqiqiy ekanligiga ishonch hosil qilishdir.

U. Diffi va M.Xellman tomonidan kashf etilgan kalitlarni ochiq taqsimlash usuli foydalanuvchilarga kalitlarni himoyalanmagan aloqa kanallari orqali almashishga imkon beradi. Uning xavfsizligi chegaralangan sohada diskret logarifmlarni hisoblashning mushkulligiga asoslanadi.

Diffi-Xellmanning kalitlarni ochiq taqsimlash sxemasi



22.3-rasm. Diffi-Xellmanning kalitlarni ochiq taqsimlash sxemasi

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

Diffi-Xellman sxemasida axborot almashinuvida ishtirok etuvchi foydalanuvchilar A va V mustakil ravishda uzlarining maxfiy kalitlarini k_A va k_B ni generatsiyalaydilar (k_A va k_B kalitlar foydalanuvchilar A va V lar sir saklovchi tasodifiy katta butun sonlar).

- So'ngra foydalanuvchi A o'zining maxfiy kaliti k_A asosida ochik kalitni xisoblaydi:
- $K_A = g^{KA}$ *(mod N).*
- Bir vaktning o'zida foydalanuvchi *V* o'zining maxfiy kaliti k_B asosida ochik kalitni xisoblaydi:
- $K_B = g^{KB}$ *(mod N).*

Bu yerda *N* va *g* katta butun oddiy sonlar. Arifmetik amallarning moduliga keltirish orkali bajariladi. *N* va *g* sonlarni sir sakdash shart emas, chunki odatda, bu kiymatlar tarmok va tizimdan foydalanuvchilarning barchasi uchun umumiy xisoblanadi.

Sungra foydalanuvchilar A va V uzlarining ochik kalitlarini himoyalanmagan kanal orkali almashtiradilar va umumiy sessiya maxfiy kaliti Kni (bulinuvchi sirni) xisoblashda ishlatadilar: foydalanuvchi A: $K = (K_v)^{kl}$ (mod*N*) = $(g^{kB})^{kl}$ (mod*N*), foydalanuvchi V: $K' = (K_l)^{kv}$ (mod*N*) = $(g^{kA})^{kv}$ (mod*N*), bunda $K = K'$, chunki $(g^{kB})^{kl} = (g^{kA})^{kv}$ (mod*N*).

22-MAVZU: INDENTIFIKASIYA VA AUTENTIFIKASIYA

MA’RUZA MASHG’ULOTI REJASI:

22.1.Asosiy tushunchalar va turkumlanishi
22.2.Parollar asosida autentifikatsiyalash
22.3.Foydalanuvchilarni biometrik identifikatsiyalash va autentifikatsiyalash

Tayanch iboralar: *Identifikatsiya, autentifikatsiya, ma’murlash, avtorizatsiya, maskarad, takroriy, majburiy kechikish.*

Asosiy tushunchalar va turkumlanishi

Identifikatsiya (Identification) - foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan funksiyadir. 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) haqiqatdan aynan o‘zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o‘tkazishda 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 (foydalanuvchi-larning) 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) – subektga 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 konfidensialligi 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 reaksiya ko‘rsatish uchun juda muhimdir.

Ma’lumotlarni uzatish kanallarini himoyalashda sub’ektlarning o‘zaro autentifikatsiyasi, ya’ni aloqa kanallari orqali bog‘lanadigan sub’ektlar xaqiqiyligining o‘zaro tasdig‘i bajarilishi shart. Xaqiqiylikning tasdig‘i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. “Ulash” atamasi orqali tarmoqning ikkita sub’ekti o‘rtasida mantiqiy bog‘lanish tushuniladi. Ushbu muolajaning maqsadi – ulash qonuniy sub’ekt bilan amalga oshirilganligiga va barcha axborot mo‘ljallangan manzilga borishligiga ishonchni ta’minlashdir.

O‘zining xaqiqiyligining tasdiqlash uchun sub’ekt tizimga turli asoslarni ko‘rsatishi mumkin. Sub’ekt ko‘rsatadigan asoslarga bog‘liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo‘linishi mumkin:

- 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 kategoriya 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 kategoriyada kriptografik usullar va vositalar ishlatilmaydi. Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

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 ta’minlanuvchi xavfsizlik darajasi bo‘yicha ham turkumlash mumkin. Ushbu yondashishga binoan autentifikatsiya jarayonlari quyidagi turlarga bo‘linadi:

- parollar va raqamli sertifikatlardan foydalanuvchi autentifi-katsiya;

- kriptografik usullar va vositalar asosidagi qatiy autentifi-katsiya;

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

- foydalanuvchilarni biometrik autentifikatsiyasi.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o‘ziga xos masalalarni yechishga imkon beradi. Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi. Shu bilan bir qatorda ta’kidlash lozimki, nullik bilim bilan isbotlash xususiyatiga ega bo‘lgan autentifikatsiyaga qiziqish amaliy xarakterga nisbatan ko‘proq nazariy xarakterga ega. Balkim, yaqin kelajakda ulardan axborot almashinuvini himoyalashda faol foydalanishlari mumkin.

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 modifikatsiya-lash 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 odam protokolning ushbu sessiya doirasida ushlab qolingan axborotni orqaga qaytaradi.

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

- matn tanlashli xujum (chosen text attack). Niyati buzuq odam 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 misol yondashishga tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyinga o‘zaro aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko‘rsatish mumkin;

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

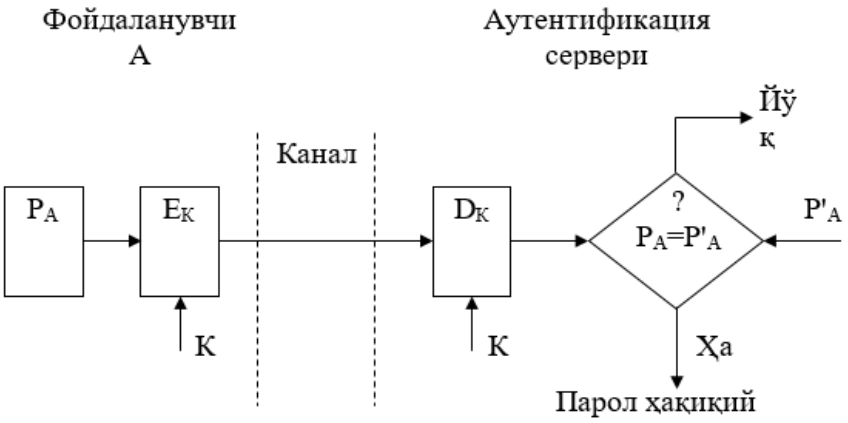
“So‘rov-javob” mexanizmi quyidagicha. Agar foydalanuvchi A foydalanuvchi V dan oladigan xabari yolg‘on emasligiga ishonch xosil qilishni istasa, u foydalanuvchi V uchun yuboradigan xabarga oldindan bilib bo‘lmaydigan element – X so‘rovini (masalan, qandaydir tasodifiy sonni) qo‘shadi. Foydalanuvchi V javob berishda bu amal ustida ma’lum amalni (masalan, qandaydir f(X) funksiyani hisoblash) bajarishi lozim. Buni oldindan bajarib bo‘lmaydi, chunki so‘rovda qanday tasodifiy son X kelishi foydalanuvchi V ga ma’lum emas. Foydalanuvchi V harakati natijasini olgan foydalanuvchi A foydalanuvchi V ning xaqiqiy ekanligiga ishonch xosil qilishi mumkin. Ushbu usulning kamchiligi - so‘rov va javob o‘rtasidagi qonuniyatni aniqlash mumkinligi.

Parollar asosida autentifikatsiyalash

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.

Paroldan foydalangan holda oddiy autentifikatsiyalash sxemasi 1–rasmda keltirilgan.

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 Ye_k va rasshifrovka qilish D_k vositalari kiritilgan.



22.1-rasm. Paroldan foydalangan holda oddiy autentifikatsiyalash

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.

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 ruyxatidagi 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 buzuq odamning 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 ruyxatidan 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 Security Dynamics kompaniyasi tomonidan ishlab chiqilgan bo‘lib, qator kompaniyalarning, xususan Cisco Systems 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 Security Dynamics 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 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.

Foydalanuvchilarni biometrik identifikatsiyalash va autentifikatsiyalash

Oxirgi vaqtda insonning fiziologik parametrlari va xarakteristikalarini, xulqining xususiyatlarini o‘lchash orqali foydalanuvchini ishonchli autentifikatsiyalashga imkon beruvchi biometrik autentifikatsiyalash keng tarqalmoqda.

Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan quyidagi afzalliklarga ega:

-biometrik alomatlarning noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqori;

- biometrik alomatlarning sog‘lom shaxsdan ajratib bo‘lmasligi;

- biometrik alomatlarni soxtalashtirishning qiyinligi.

Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik algoritmlar quyidagilar:

- barmoq izlari;

- qo‘l panjasining geometrik shakli;
- yuzning shakli va o‘lchamlari;
- ovoz xususiyatlari;
- ko‘z yoyi va to‘r pardasining naqshi.

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

- xatolik inkorlar koeffitsiyenti FRR (false-reject rate);
- xatolik tasdiqlar koeffitsiyenti FAR (false-alarm rate).

Xatolik inkor tizim qonuniy foydalanuvchi shaxsini tasdiqlamaganda paydo bo‘ladi (odatda FRR qiymati taxminan 100 dan birni tashkil etadi). Xatolik tasdiq tizim noqonuniy foydalanuvchi shaxsini tasdiqlaganida paydo bo‘ladi (odatda FAP qiymati taxminan 10000 dan birni tashkil etadi). Bu ikkala koeffitsiyent bir biri bilan bog‘liq: xatolik inkor koeffitsiyentining har biriga ma’lum xatolik tasdiq koeffitsiyenti mos keladi. Mukammal biometrik tizimda ikkala xatolikning ikkala parametri nulga teng bo‘lishi shart. Afsuski, biometrik tizim ideal emas, shu sababli nimanidur qurbon qilishga to‘g‘ri keladi. Odatda tizimli parametrlar shunday sozlanadiki, mos xatolik inkorlar koeffitsiyentini aniqlovchi xatolik tasdiqlarning istalgan koeffitsiyentiga erishiladi.

Biometrik autentifikatsiyalashning daktiloskonik tizimi

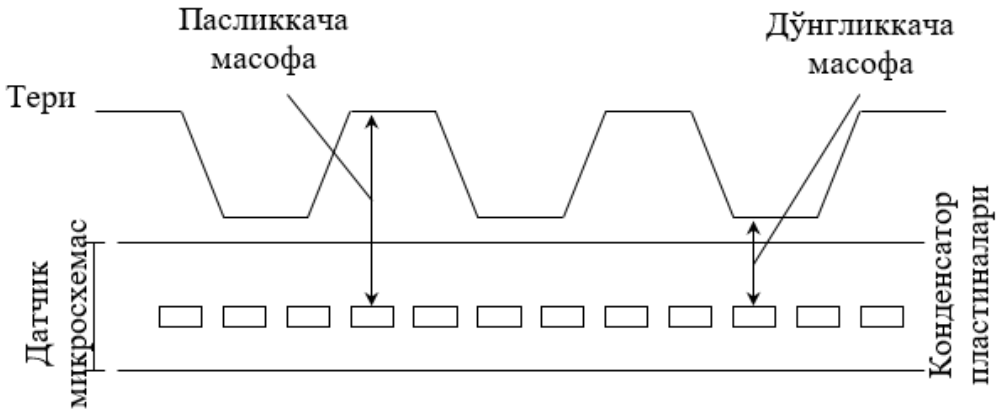
Biometrik tizimlarning aksariyati identifikatsiyalash parametri sifatida barmoq izlaridan foydalanadi (autentifikatsiyaning daktiloskopik tizimi). Bunday tizimlar sodda va qulay, autentifikatsiyalashning yuqori ishonchliligiga ega. Bunday tizimlarning keng tarqalishiga asosiy sabab barmoq izlari bo‘yicha katta ma’lumotlar ba’zasining mavjudligidir. Bunday tizimlardan dunyoda asosan politsiya, turli davlat va ba’zi bank tashkilotlari foydalanadi.

Autentifikatsiyaning daktiloskopik tizimi quyidagicha ishlaydi. Avval foydalanuvchi ro‘yxatga olinadi. Odatda, skanerda barmoqning turli xolatlarida skanerlashning bir necha varianti amalga oshiriladi. Tabiiyki, namunalar bir–biridan biroz farqlanadi va qandaydir umumlashtirilgan namuna, «pasport» shakllantirilishi talab etiladi. Natijalar autentifikatsiyaning ma’lumotlar bazasida xotirlanadi. Autentifikatsiyalashda skanerlangan barmoq izi ma’lumotlar bazasidagi «pasportlar» bilan taqqoslanadi.

Barmoq izlarining skanerlari. Barmoq izlarini skanerlovchi an’anaviy qurilmalarda asosiy element sifatida barmoqning xarakterli rasmini yozuvchi kichkina optik kamera ishlatiladi. Ammo, daktiloskopik qurilmalarni ishlab chiqaruvchilarning ko‘pchiligi integral sxema asosidagi sensorli qurilmalarga e’tibor bermoqdalar. Bunday tendensiya barmoq izlariga asoslangan autentifikatsiyalashni qo‘llashning yangi sohalarini ochadi.

Bunday texnologiyalarni ishlab chiquvchi kompaniyalar barmoq izlarini olishda turli, xususan elektrik, elektromagnit va boshqa usullarni amalga oshiruvchi vositalardan foydalanadilar.

Skanerlardan biri barmoq izi tasvirini shakllantirish maqsadida teri qismlarining sig‘im qarshiligini o‘lchaydi. Masalan, Veridicom kompaniyasining daktiloskopik qurilmasi yarim-o‘tkazgichli datchik yordamida sig‘im qarshiligini aniqlash orqali axborotni yig‘adi. Sensor ishlashining prinsipi quyidagicha: ushbu asbobga quyilgan barmoq kondensator plastinalarining biri vazifasini o‘taydi (2-rasm). Sensor sirtida joylashgan ikkinchi plastina kondensatorning 90000 sezgir plastinkali kremniy mikrosxemasidan iborat. Sezgir sig‘im datchiklari barmoq sirti do‘ngliklari va pastliklari orasidagi elektrik maydon kuchining o‘zgarishini o‘lchaydi. Natijada do‘ngliklar va pastliklargacha bo‘lgan masofa aniqlanib, barmoq izi tasviri olinadi.



22.2-rasm. Sensor ishlashining prinsipi

Integral sxema asosidagi sensorli tekshirishda AuthenTec kompaniyasida ishlatiluvchi usul aniqlikni yana ham oshirishga imkon beradi.

Qator ishlab chiqaruvchilar biometrik tizimlarni smart-kartalar va karta–kalitlar bilan kombinatsiyalaydilar.

Integral sxemalar asosidagi barmoq izlari datchiklarining kichik o‘lchamlari va yuqori bo‘lmagan narxi ularni himoya tizimi uchun ideal interfeysga aylantiradi. Ularni kalitlar uchun breloklarga o‘rnatish mumkin. Natijada foydalanuvchi kompyuterdan boshlab to kirish yo‘li, avtomobillar va bankomatlar eshiklaridan himoyali foydalanishni ta’minlaydigan universal kalitga ega bo‘ladi.

Qo‘l panjasining geometrik shakli bo‘yicha autentifikatsiyalash tizimlari. Qo‘l panjasi shaklini o‘quvchi qurilmalar barmoqlar uzunligini, qo‘l panja qalinligi va yuzasini o‘lchash orqali qo‘l panjasining hajmiy tasvirini yaratadi. Masalan, Recognition Systems kompaniyasining mahsulotlari 90 dan ortiq o‘lchamlarni amalga oshiradi. Natijada keyingi taqqoslash uchun 9-xonali namuna shakllantiriladi. Bu natija qo‘l panjasini individual skanerida yoki markazlashtirilgan ma’lumotlar bazasida saqlanishi mumkin. Qo‘l panjasini skanerlovchi qurilmalar narxining yuqoriligi va o‘lchamlarining kattaligi sababli tarmoq muhitida kamdan-kam ishlatilsada, ular qat’iy xavfsizlik rejimiga va shiddatli trafikka ega bo‘lgan hisoblash muhiti (server xonalari ham bunga kiradi) uchun qulay hisoblanadi. Ularning aniqligi yuqori va inkor koeffitsiyenti ya’ni inkor etilgan qonuniy foydalanuvchilar foizi kichik.

Yuzning tuzilishi va ovoz bo‘yicha autentifikatsiyalovchi tizimlar.

Bu tizimlar arzonligi tufayli eng foydalanuvchan hisoblanadilar, chunki aksariyat zamonaviy kompyuterlar video va audeo vositalariga ega. Bu sinf tizimlari telekommunikatsiya tarmoqlarida masofadagi foydalanuvchi sub’ektni identifikatsiyalash uchun ishlatiladi. Yuz tuzilishini skanerlash texnologiyasi boshqa biometrik texnologiyalar yaroqsiz bo‘lgan ilovalar uchun to‘g‘ri keladi. Bu holda shaxsni identifikatsiyalash va verifikatsiyalash uchun ko‘z, burun va lab xususiyatlari ishlatiladi. Yuz tuzilishini aniqlovchi qurilmalarni ishlab chiqaruvchilar foydalanuvchini identifikatsiyalashda hususiy matematik algoritmlardan foydalanadilar.

Ma’lum bo‘lishicha, ko‘pgina tashkilotlarning hodimlari yuz tuzilishini skanerlovchi qurilmalarga ishonmaydilar. Ularning fikricha kamera ularni rasmga oladi, so‘ngra suratni monitor ekraniga chiqaradi. Kameraning sifati esa past bo‘lishi mumkin. Undan tashqari yuz tuzilishini

skanerlash – biometrik autentifikatsiyalash usullari ichida yagona, tekshirishga ruxsatni talab qilmaydigan (yashiringan kamera yordamida amalga oshirilishi mumkin) usul hisoblanali.

Ta'kidlash lozimki, yuz tuzilishini aniqlash texnologiyasi yanada takomillashtirilishni talab etadi. Yuz tuzilishini aniqlovchi aksariyat algoritmlar quyosh yorug'ligi jadalligining kun bo'yicha tebranishi natijasidagi yorug'lik o'zgarishiga ta'sirchan bo'ladilar. Yuz holatining o'zgarishi ham aniqlash natijasiga ta'sir etadi. Yuz holatining 45^0 ga o'zgarishi aniqlashni samarasiz bo'lishiga olib keladi.

Ovoz bo'yicha autentifikatsiyalash tizimlari

Bu tizimlar arzonligi tufayli foydalanuvchan hisoblanadilar. Hususan ularni ko'pgina shaxsiy kompyuterlar standart komplektidagi uskuna (masalan mikrofonlar) bilan birga o'rnatish mumkin. Ovoz bo'yicha autentifikatsiyalash tizimlari har bir odamga noyob bo'lgan balandligi, modulyatsiyasi va tovush chastotasi kabi ovoz xususiyatlariga asoslanadi. Ovozni aniqlash nutqni aniqlashdan farqlanadi. Chunki nutqni aniqlovchi texnologiya abonent so'zini izoxlasa, ovozni aniqlash texnologiyasi so'zlovchining shaxsini tasdiqlaydi. So'zlovchi shaxsini tasdiqlash ba'zi chegaralanishlarga ega. Turli odamlar o'xshash ovozlar bilan gapirishi mumkin, har qanday odamning ovozi vaqt mobaynida kayfiyati, hissiyotlik holati va yoshiga bog'liq holda o'zgarishi mumkin. Uning ustiga telefon apparatlarning turli-tumanligi va telefon orqali bog'lanishlarining sifati so'zlovchi shaxsini aniqlashni qiyinlashtiradi. Shu sababli ovoz bo'yicha aniqlashni yuz tuzilishini yoki barmoq izlarini aniqlash kabi boshqa biometriklar bilan birgalikda amalga oshirish maqsadga muvofiq hisoblanadi.

Ko'z yoyi to'r pardasining shakli bo'yicha autentifikatsiyalash tizimi

Bu tizimlarni ikkita sinfga ajratish mumkin:

- ko'z yoyi rasmidan foydalanish;
- ko'z to'r pardasi qon tomirlari rasmidan foydalanish.

Odam ko'z pardasi autentifikatsiya uchun noyob ob'ekt hisoblanadi. Ko'z tubi qon tomirlarining rasmi hatto egizaklarda ham farqlanadi. Identifikatsiyalashning bu vositalaridan xavfsizlikning yuqori darajasi talab etilganida (masalan harbiy va mudofaa ob'ektlarining rejimli zonalarida) foydalaniladi.

Biometrik yondashish "kim bu kim" ekanligini aniqlash jarayonini soddalashtirishga imkon beradi. Daktiloskopik skanerlar va ovozni aniqlovchi qurilmalardan foydalanish xodimlarni tarmoqqa kirishlarida murakkab parollarni eslab qolishdan xalos etadi. Qator kompaniyalar korxona masshtabidagi bir martali autentifikatsiya SSO (Single Sign-On) ga biometrik imkoniyatlarni integratsiyalaydilar. Bunday biriktirish tarmoq ma'murlariga parollarni bir martali autentifikatsiyalash xizmatini biometrik texnologiyalar bilan almashtirishga imkon beradi. Shaxsni biometrik autentifikatsiyalashning birinchilar qatorida keng tarqalgan sohalaridan biri mobil tizimlari bo'ldi. Muammo faqat kompyuter o'g'irlanishidagi yo'qotishlarda emas, balki axborot tizimining buzilishi katta zararga olib kelishi mumkin. Undan tashqari, noutbuklar dasturiy bog'lanish (mobil kompyuterlarda saqlanuvchi parollar yordamida) orqali korporativ tarmoqdan foydalanishni tez-tez amalga oshiradi. Bu muammolarni kichik, arzon va katta energiya talab etmaydigan barmoq izlari datchiklari yechishga imkon beradi. Bu qurilmalar mos dasturiy ta'minot yordamida axborotdan foydalanishning mobil kompyuterda saqlanayotgan to'rtta satxi - ro'yxatga olish, ekranni saqlash rejimidan chiqish, yuklash va fayllarni deshifratsiyalash uchun autentifikatsiyani bajarishga imkon beradi.

Foydalanuvchini biometrik autentifikatsiyalash maxfiy kalitdan foydalanishni modul ko'rinishida shifrlashda jiddiy ahamiyatga ega bo'lishi mumkin. Bu modul axborotdan faqat xaqiqiy

xususiy kalit egasining foydalanishiga imkon beradi. So‘ngra kalit egasi o‘zining maxfiy kalitini ishlatib xususiy tarmoqlar yoki Internet orqali uzatilayotgan axborotni shifrlashi mumkin.

23-MAVZU: VIRTUAL XIMOYALANGAN TARMOQLAR

MA’RUZA MASHG’ULOTI REJASI:

23.1. VPN tushunchasi va uning turlari

23.2. VPN tarmoqlari klassifikatsiyasi

23.3. VPN tarmoq qurishning asosiy turlari

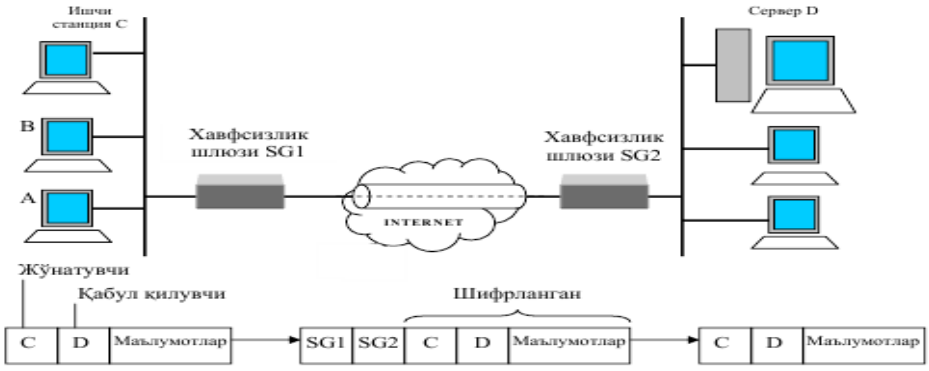
Tayanch iboralar: VPN tunneli, IpSec

Internetning hamma yerda tarqalishidan manfaat ko‘rish maqsadida tarmoq xujumlariga samarali qarshilik ko‘rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq VPN yaratish ustida ishlar olib borildi. Natijada 1990 yilning boshida virtual xususiy tarmoq VPN konsepsiyasi yaratildi. "Virtual" iborasi VPN atamasiga ikkita uzel o‘rtasidagi ulanishni vaqtincha deb ko‘rilishini ta’kidlash maqsadida kiritilgan Haqiqattan, bu ulanish doimiy, qat’iy bo‘lmay, faqat ochiq tarmoq bo‘yicha trafik o‘tganida mavjud bo‘ladi.

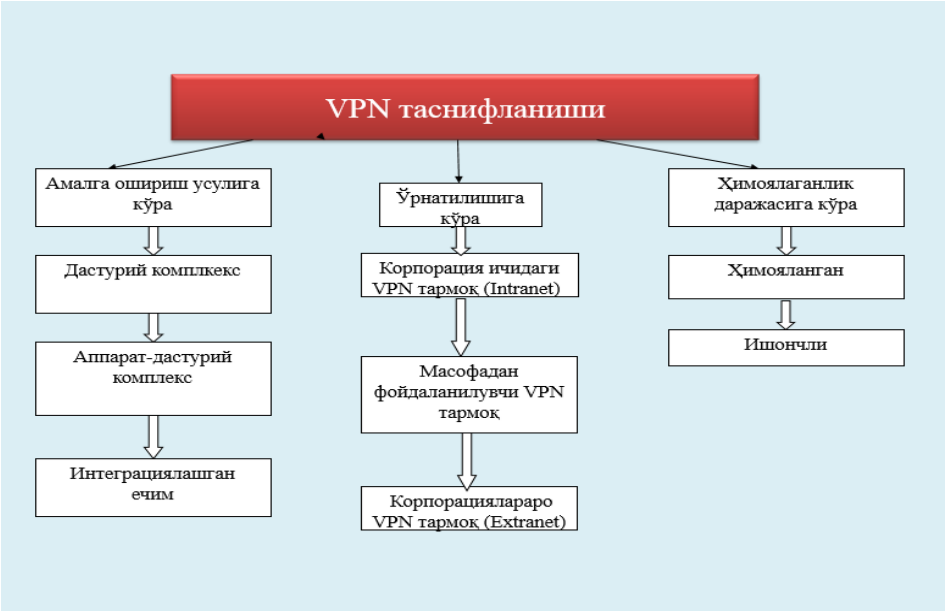
Axborotni VPN tunneli bo‘yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

- o‘zaro aloqadagi taraflarni autentifikatsiyalash;
- uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash);
- etkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish.

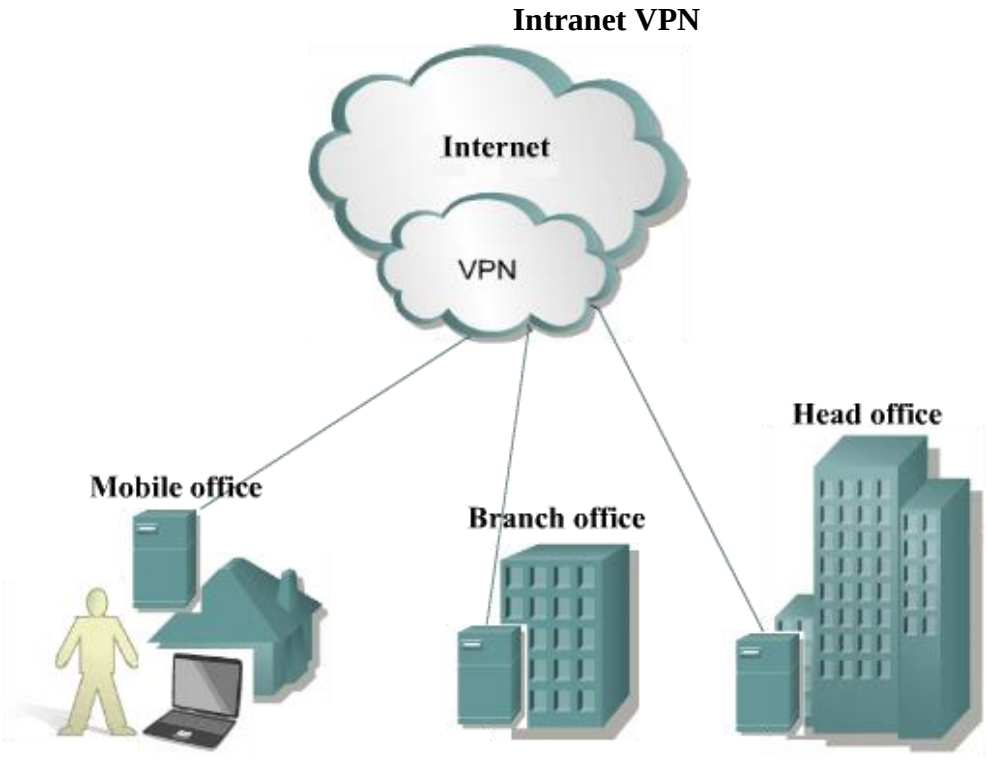
Virtual himoyalangan tunnel sxemasi



23.1-rasm. Virtual himoyalangan tunnel sxemasi



23.1-rasm. VPN tasniflanishi



23.3-rasm. Intranet VPN

Marshrutizatorlar asosidagi VPN.

VPN qurishning ushbu usuliga binoan himoyalangan kanallarni yaratishda marshrutizatorlardan foydalaniladi. Lokal tarmoqdan chiquvchi barcha axborot marshrutizator orqali o‘tganligi sababli, unga shifrlash vazifasini yuklash tabiiy. Marshrutizator asosidagi VPN asbob-uskunalariga misol tariqasida Cisco-Systems kompaniyasining qurilmalarini ko‘rsatish mumkin.

Tarmoqlararo ekranlar asosidagi VPN.

Aksariyat ishlab chiqaruvchilarning tarmoqlararo ekrani tunnellash va ma’lumotlarni shifrlash vazifalarini madadlaydi. Tarmoqlararo ekranlar asosidagi yechimga misol tariqasida Check Point Software Technologies kompaniyasining Fire Wall-1 mahsulotini ko‘rsatish mumkin. Shaxsiy

kompyuter asosidagi tarmoqlararo ekranlar faqat uzatiluvchi axborot hajmi nisbatan kichik bo‘lgan tarmoqlarda qo‘llaniladi. Ushbu usulning kamchiligi bitta ishchi o‘rniga hisoblanganda yechim narhining yuqoriligi va unumdorlikning tarmoqlararo ekran ishlaydigan apparat ta’minotiga boqliqligi.

Dasturiy ta’minot asosidagi VPN.

Dasturiy usul bo‘yicha amalga oshirilgan VPN mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan qurilmadan qolishsada, VPN-tarmoqlarni amalga oshirilishida yetarli quvvatga ega. Ta’kidlash lozimki, masofadan foydalanishda zaruriy o‘tkazish polosasiga talablar katta emas. Shu sababli, dasturiy mahsulotlarning o‘zi masofadan foydalanish uchun yetarli unumdorlikni ta’minlaydi. Dasturiy mahsulotlarning shubhasiz afzalligi—qo‘llanilishining moslanuvchanligi va qulayligi, hamda narxining nisbatan yuqori emasligi.

Ixtisoslashtirilgan apparat vositalari asosidagi VPN.

Ixtisoslashtirilgan apparat vositalari asosidagi VPNlarning eng muhim afzalligi unumdorligining yuqoriligidir. Ixtisoslashtirilgan VPN tizimlarda shifrlashning mikrosxemalarda amalga oshirilishi tezkorlikning ta’minlanishiga sabab bo‘ladi. Ixtisoslashtirilgan VPN-qurilmalar xavfsizlikning yuqori darajasini ta’minlaydi, ammo ularning narhi anchagina yuqori.

OSI modelining ish sathi bo‘yicha VPNning turkumlanishi

Kanal sathidagi VPN

OSI modelining kanal sathida ishlatiluvchi VPN vositalari uchinchi (va yuqoriroq) sathning turli xil trafigini inkapsulatsiyalashni ta’minlashga va "nuqta-nuqta" tilidagi virtual tunnellarni (marshrutizatordan marshrutizatorga yoki shaxsiy kompterdan lokal hisoblash tarmog‘ining shlyuzigacha) qurishga imkon beradi.

Tarmoq sathidagi VPN.

Tarmoq sathidagi VPN-mahsulotlar IPni IPga inkapsulyatsiyalashni bajaradi. Bu sathdagi keng tarqalgan protokollardan biri SKIP protokolidir. Ammo bu protokolni autentifikatsiyalash, tunnellash va IP-paketlarni shifrlash uchun atalgan IPSec(IPSecurity) protokoli asta-sekin surib chiqarmoqda.

Seans sathidagi VPN

Ba’zi VPNlar "kanal vositachilari" (circuit proxy) deb ataluvchi usuldan foydalanadi. Bu usul transport sathi ustida ishlaydi va har bir soket uchun alohida trafikni himoyalangan tarmoqdan umumfoydanuvchi Internet tarmog‘iga retranslyatsiyalaydi. (IP soketi TCP-ulanishning va muayyan port yoki berilgan port UDP kombinatsiyasi orqali identifikatsiyalanadi. TCP/IP stekida beshinchi-seans sathi bo‘lmaydi, ammo soketlarga mo‘ljallangan amallarni ko‘pincha seans sathi amallari deb yuritishadi.)

24-MAVZU: SIMSIZ ALOQA TIZIMLARIDA AXBOROT HIMOYASI

MA’RUZA MASHG’ULOTI REJASI:

24.1. Simsiz tarmoq konsepsiyasi va tuzilmasi
24.2. Simsiz tarmoqlar xavfsizligiga tahdidlar
24.3. Simsiz tarmoqlar xavfsizligi protokollari

Tayanch iboralar: *quvvat, global tarmoqlar, qayta uzatgich, litsenziya, telekommunikatsiya, axborotn jo‘natish, uzatishning asinxron usuli.*

Simsiz tarmoq konsepsiyasi

Simsiz tarmoqlar odamlarga simli ulanishsiz o‘zaro bog‘lanishlariga imkon beradi. Bu siljish erkinligini va uy, shahar qismlaridagi yoki dunyoning olis burchaklaridagi ilovalardan foydalanish imkonini ta’minlaydi. Simsiz tarmoqlar odamlarga o‘zlariga qulay va xohlagan joylarida elektron pochtani olishlariga yoki Web- sahifalarni ko‘zdan kechirishlariga imkon beradi. Simsiz tarmoqlarning turli xillari mavjud, ammo ularning eng muhim xususiyati bog‘lanishning kompyuter qurilmalari orasida amalga oshirilishidir. Kompyuter qurilmalariga shaxsiy raqamli yordamchilar (Personal digital assistance, PDA), noutbuklar, shaxsiy kompyuterlar, ser- verlar va printerlar taalluqli. Odatda uyali telefonlarni kompyuter qurilmalari qatoriga kiritishmaydi, ammo eng yangi telefonlar va hatto naushniklar ma’lum hisoblash imkoniyatlariga va tarmoq adapterlariga ega. Yaqin orada elektron qurilmalarning aksariyati simsiz tarmoqlarga ulanish imkoniyatini ta’minlaydi

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

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

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

Bunday tarmoq, masalan, foydalanuvchi PDA sida va uning shaxsiy kompyuterida yoki noutbukida a’lumotlarni simsiz sinxronlashni ta’minlashi mumkin. Xuddi shu tariqa printer bilan simsiz ulanish ta’minlanadi. Kompyuterni tashqi qurilmalar bilan ulovchi simlar chi-galliklarining yo‘qolishi yetarlicha jiddiy afzallik bo‘lib, buning evazi-ga tashqi qurilmalarning boshlang‘ich o‘rnatilishi va keyingi, zaruriyattug‘ilganda, joyining o‘zgartirilishi anchagina osonlashadi

Simsiz lokal tarmoqlar ofislarning ichida va tashqarisida, ish - lab chiqarish binolarida uzatishlarning yuqori xarakteristikalarini ta’minlaydi. Bunday tarmoqlardan foydalanuvchilar odatda noutbuklarni, shaxsiy kompyuterlarni va katta resurslarni talab etuvchi ilovalarni bajarishga qodir protsessorli va katta ekranli ***PDA*** larni ishlatishadi. Xizmatchi tarmoq xizmatlaridan majlislar zalida yoki binoning boshqa xonalarida bo‘la turib foydalanashi mumkin. Bu xizmatchiga o‘z vazifala- rini samarali bajarishga imkon beradi. Simsiz lokal tarmoqlar uzatish- ning 54Mbit/sgacha tezligida barcha ofis yoki maishiy ilovalar talablari- ni qondirish imkoniga ega. Xarakteristikalari, komponentlari, narxi va bajaradigan amallari bo‘yicha bunday tarmoqlar Ethernet xilidagi an’ana-viy simli lokal tarmoqlariga o‘xshash.

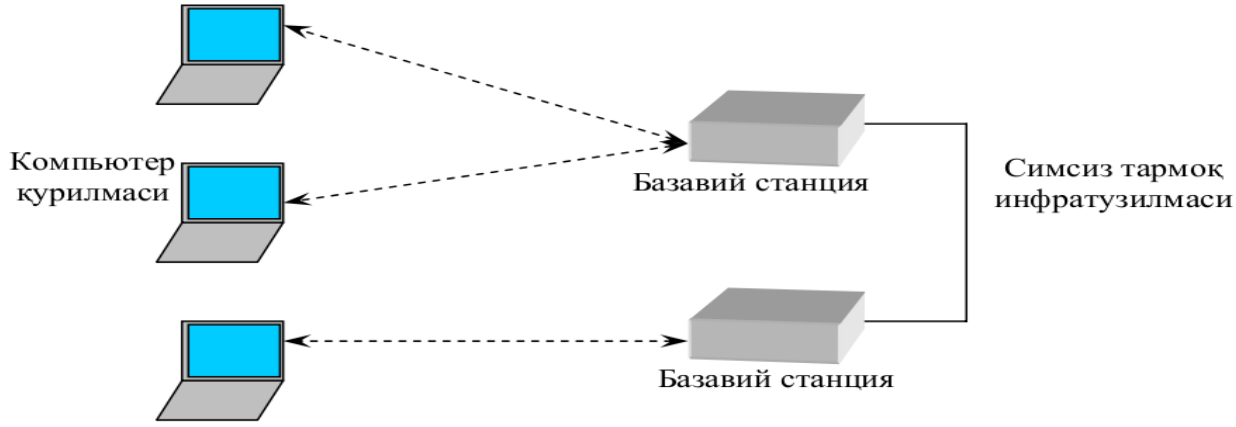
Simsiz regional tarmoqlar yuzasi bo‘yicha shaxarga teng bo‘lgan xu-dudga xizmat qiladi. Aksariyat xollarda ilovalarni bajarishda belgilan-gan ulanish talab etiladi, ba’zida esa mobillik zarur bo‘ladi. Masalan, kasalxonada bunday tarmoq asosiy bino va masofadagi klinikalar orasida ma’lumotlarni uzatishni ta’minlaydi. Yoki energetik kompaniya bunday tarmoqdan shaxar masshtabida foydalanib, turli tumanlardan beriladigan ish naryadlaridan foydalanishini ta’minlaydi. Natijada, simsiz regional tarmoqlar mavjud tarmoq infratuzilmalarini bir yerga to‘playdi yoki mo- bil foydalanuvchilarga mavjud tarmoq infratuzilmalari bilan ulanishni o‘rnatishga imkon beradi.

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

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

Simsiz global tarmoqlar mobil ilovalarning, ulardan mamlakat yoki hatto kontinent masshtabida foydalanishni ta’minlash bilan ishla-nishini ta’minlaydi. Iqtisodiy mulohazalarga tayangan holda, telekommu-nikatsiya kompaniyalari ko‘pgina foydalanuvchilar uchun uzoq masofadan ula-nishni ta’minlovchi simsiz global tarmoqning nisbatan qimmat infratu-zilmasini yaratadilar. Bunday yechimning xarajati barcha foydalanuvchilar o‘rtasida taqsimlanadi, natijada abonent to‘lovi unchalik yuqori bo‘lmaydi.

Simsiz tarmoq tuzilmasi



24.1-rasm. Simsiz tarmoq tuzilmasi

Foydalanuvchilar. Simsiz tarmoq foydalanuvchiga xizmat qilishligi sababali, foydalanuvchiga simsiz tarmoqning muhim qismi sifatida qarash mumkin. Foydalanuvchi simsiz tarmoqdan foydalanish jarayonini boshlay-di va uning o‘zi tugallaydi. Shu sababli unga "oxirgi foydalanuvchi" ata-masi joiz hisoblanadi. Odatda, foydalanuvchi simsiz tarmoq bilan o‘zaro aloqani ta’minlash bilan bir qatorda, muayyan ilovalar bilan bog‘liq boshqa vazifalarni bajaruvchi *kompyuter qurilmalari (computer device)* bilan ish ko‘radi.

Simsiz tarmoqlar xavfsizligiga tahdidlar

Simsiz texnologiyadan foydalanilib juda katta afzalliklarga eri- shish mumkin. Bu texnologiya foydalanuvchilarga aloqani yo‘qotmasdan be- malol harakatlanish xissiyotini bersa, tarmoq yaratuvchilariga bog‘lanishlarni tashkil etish uchun katta imkoniyatlarni yaratadi. Undan tashqari tarmoqdan foydalanish uchun ko‘pgina yangi qurilmalarni paydo bo‘lishiga imkon beradi. Ammo

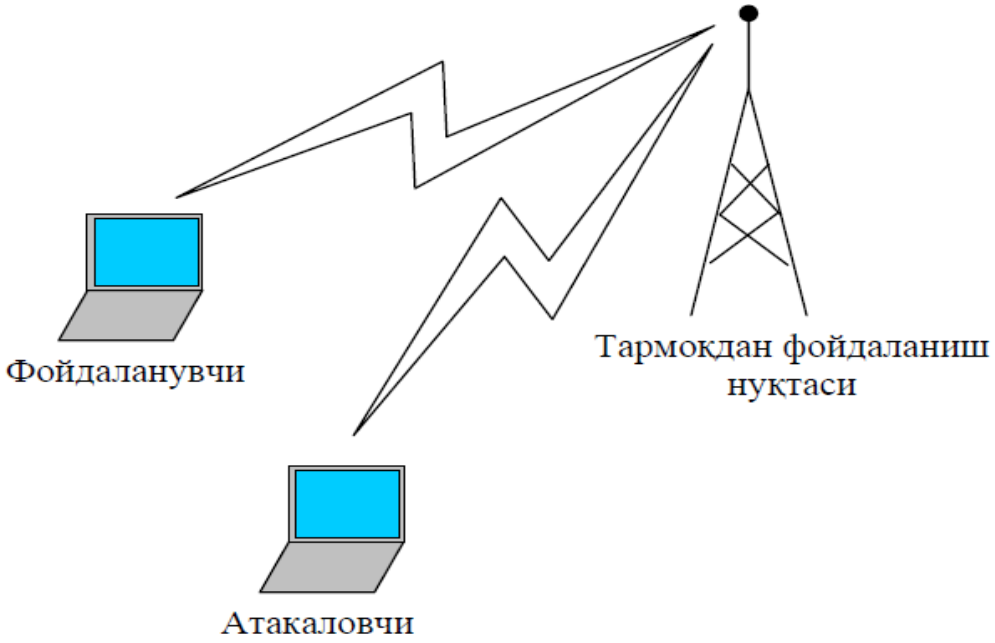
simsiz texnologiya oddiy simli tarmoqlarga qaraganda o‘zida ko‘proq tahdidlarni eltadi. Xavfsiz simsiz ilovani yaratish uchun simsiz "xujumlar" o‘tuvchi bo‘lishi mumkin bo‘lgan barcha yo‘nalishlarni aniqlash lozim. Afsuski, ilovalar hech qachon butun- lay xavfsiz bo‘lmaydi, ammo simsiz texnologiyalardagi xavf-xatarni sin-chiklab o‘rganish har xolda himoyalanish darajasini oshishiga yordam beradi. Demak, mumkin bo‘lgan tahdidlarni taxlillab, tarmoqni shunday qurish lo-zimki, xujumlarga xalaqit berish va nostandart "xujumlar"dan himoyalanishga tayyor turish imkoni bo‘lsin.

Nazoratlanmaydigan xudud

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

Yashirincha eshitish

Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda eng tarqalgan muammo anonim xujumlarning mumkinligi.



24.2-rasm. Yashirincha eshitish

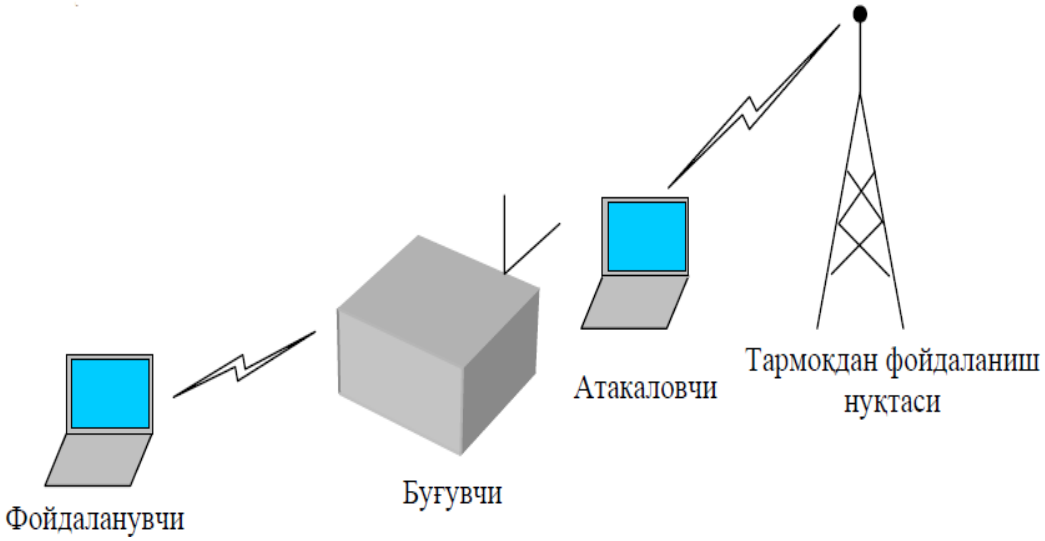
Bo‘g‘ish. Tarmoqlarda bo‘ ish atayin yoki atayin bo‘lmagan interferensiyaning aloqa kanalidagi jo‘natuvchi va qabul qiluvchi imkoniyatidan oshganida sodir bo‘ladi. Natijada bu kanal ishdan chiqariladi. Xujum qiluvchi bo‘ ishning turli usullaridan foydalanishi mumkin.

Xizmat ko‘rsatishdan voz kechish. DoS (Denial of Service — xizmat ko‘rsatishdan voz kechish) xilidagi xujum tarmoqni butunlay ishdan chiqarishi mumkin. Butun tarmoqda, jumladan bazaviy stansiyalarda va mijoz terminallarida, shunday kuchli interferensiya paydo bo‘ladiki, stansiyalhar bir-birlari bilan bog‘lana olmaydilar. Bu xujum ma’lum doiradagi barcha kommunikatsiyani o‘chiradi. Simsiztarmoqqa bo‘ladigan DoS xujumni oldini olish yoki tuxtatish qiyin. Simsiz tarmoq texnologiyalarining aksariyati litsenziyalanmagan chastotalardan foydalanadi, demak, bir qancha elektron qurilmalardan interferensiya bo‘lishi mumkin.

Mijozlarni bo‘g‘ish

Mijoz stansiyasini bo‘g‘ish firibgarga o‘zini bo‘g‘ilgan mijoz o‘rniga qo‘yishiga imkon beradi (24.3-rasm). Mijoz ulanishni amalga oshira olmasin degan maqsadda unga xizmat ko‘rsatishdan voz

kechish uchun ham bu ishdan foydalaniladi. Juda mohirlik bilan qilingan xujumlar niyati buzuq odam stansiyasini bazaviy stansiyaga ulash maqsadida mavjud ulanishni uzadi.



24.3-rasm. Mijoz stansiyasini bo‘g‘ish

WLTS protokoli. SSL/TLSga asoslangan WLTS protokoli WAP (Wireless Application Protocol – cimsiz ilovalar protokoli) qurilmalarida, masalan, uyali telefonlarda va cho‘ntak kompyuterlarida ishlatiladi. SSL va WLTS bir - biridan transport sathi bilan farqlanadi. SSL yo‘qolgan paketlarni qayta uzatishda yoki nostandart pa- ketlarni uzatishda TCP ishiga ishonadi. WLTSdan foydalanuvchi WAP qurilmalari o‘z funksiyalarini bajarishida TCPni qo‘llay olmaydilar, chunki faqat UDP (user Datagram Protocol) bo‘yicha ishlaydilar. UDP pro- tokoli esa ulanishga mo‘ljallanmagan, shu sababli bu funksiyalar WLTSga kiritilishi lozim.

802.1x protokoli. Bu protokolning asosiy vazifasi - autentifika- tsiyalashdir; ba’zi hollarda protokoldan shifrlovchi kalitlarni o‘rnatishda foydalanish mumkin. Ulanish o‘rnatilganidan so‘ng undan faqat 802.1x. trafigi o‘tadi, ya’ni DHCP (Dynamic Host Configuration Protocol - xostlar- ni dinamik konfiguratsiyalash protokoli), IP va h. kabi protokollarga ruxsat berilmaydi. Extensible Authentification Protocol (EAP) (RFC 2284) foydalanuvchilarni autentifikatsiyalashda ishlatiladi.