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

Andijon davlat universiteti

Informatika kafedrasi

KOMPYUTER TARMOQLARI XAVFSIZLIGI

fanidan

MA’RUZA MATNLARI

Andijon – 2008

Ushbu ma’ruza matnlari Informatika va axborot texnologiyalari yo’nalishi magistrantlari uchun o’quv qo’llanma sifatida tavsiya etiladi.

Ma’ruza matni kiril alifbosidagi ma’ruza matnlardan olib tayyorlandi.
Tayyorlovchi: F.N.Arziqulov.

Ushbu ma’ruza matnlari «Informatika» kafedrasi yig’ilishida ko’rib chiqilgan va foydalanishga tavsiya etilgan «*26*» *avgust* 2008 y.
Bayonnoma № 1

Kafedra mudiri: F.Arzikulov

SO’Z BOSHI

Tez rivojlanib borayotgan kompyuter axborot texnologiyalari bizning kundalik xayotimizning barcha jabxalarida sezilarli uzgarishlarni olib kirmokda. Xozirda “axborot tushunchasi” sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo’lgan maxsus tovar belgisi sifatida tez-tez ishlatilmoqda. Shu bilan birga axborotning baxosi ko’p xollarda uning uzi joylashgan kompyuter tizimining baxosida bir necha yuz va ming barobarga oshib ketmoqda. Shuning uchun tamomila tabiiy xolda axborotni unga ruxsat etilmagan xolda kirishdan, qasddan uzgartirishdan, uni ug’irlashdan, yuqotishdan va boshqa jinoiy xarakterlardan ximoya qilishga kuchli zarurat tug’iladi.

Kompyuter tizimlari va tarmoqlarida axborotni ximoya ostiga olish deganda, berilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta’minlash maksadida turli vosita va usullarni qullash, choralarini ko’rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Axborotni ximoya 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 xolda, uni elementlarini qalbakilashtirishga (uzgartirishga) yo’l qo’ymaslik;
- Axborotni tegishli xuquqlarga ega bo’lmagan shaxslar yoki jarayonlar orqali tarmoqdan ruxsat etilmagan xolda olishga yo’l qo’ymaslik;
- Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar faqat tomonlar urtasida kelishilgan shartnomalar asosida qo’llanilishiga ishonish kabilar tushuniladi.

Yuqorida ta’kidlab utilganlarning barchasi asosida kompyuter tarmoqlari va tizimlarida axborot xavfsizligi muammosining dolzarbligi va muximligi kelib chiqadi. Shuning uchun xozirgi kurs Respublikamizning oliy va o’rta maxsus o’quv muassasalari o’quv rejalarida munosib o’rin egallaydi.

Ushbu kursning vazifalari:

- Talabalarda kompyuter tarmoqlari va tizimlarida axborot xavfsizligi tug’risidagi bilimlarni shakllantirish;
- Axborotni ximoya kilishning nazariy, amaliy va uslubiy asoslarini berish;
- Talabalarga kompyuter tarmoklari va tizimlarida axborot xavfsizligini ta’minlashning zamonaviy usullari va vositalarini qo’llashni amaliy jixatdan o’rgatish;

- Talabalarni axborotni ximoya qilish bo’yicha ishlab chiqarilgan turli xil dasturiy maxsulotlardan erkin foydalana olish imkonini beradigan bilimlar bilan ta’minlash;

Kursni o’zlashtirish natijasida talaba quyidagilarni bilishi shart;

- kompyuter tarmoqlari va tizimlaridagi axborot xavfsizligiga taxdid solishi kutilayotgan xavf xatarning moxiyatini va oqibatlarini tushunishi;
- kompyuter tarmoqlari va tizimlarida axborotni ximoya kilish bo’yicha qo’yiladigan asosiy talablar va asoslarni o’zlashtirish;
- kompyuter tarmoqlari va tizimlarida axborot xavfsizlagini ta’minlashda qo’llaniladigan zamonaviy usullar va vositalarni bilish;
- tizimlarda axborot butunligi va ishochligini buzuvchi viruslar va boshqa manbalar mavjudligini tizimli tekshirishni ta’minlash va ularni zararsizlashtirish buyicha choralarni ko’rish;

axborotni ximoya qilishda qo’llaniladigan zamonaviy amaliy tizimlar va dasturiy maxsulotlarni ishlata olish;

1 - MAVZU: AXBOROTLARGA NISBATAN MAVJUD XAVFSIZLIKLARNING ASOSIY TUShUNChALARI VA UNING TASNIFI

1. Axborot xavfsizligiga kiri;
2. Predmetning asosiy tushunchalari va maqsadi;
3. Axborotlarga nisbatan xavf-xatarlar tasnifi;
4. Tarmok xavfsizligini nazorat kilish vositalari

Axborot xavfsizligiga kirish

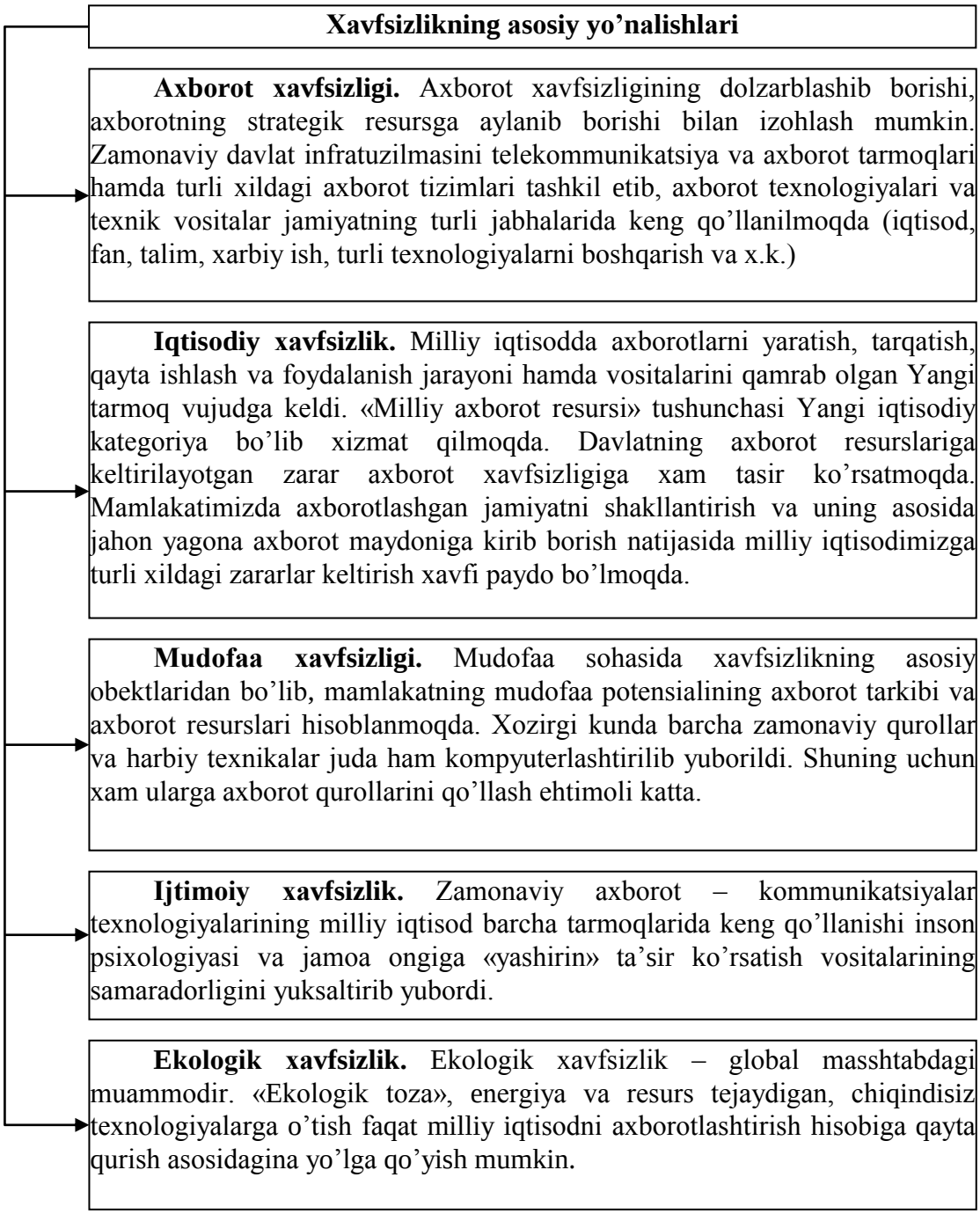
Mamlakatimiz milliy iqtisodining hech bir tarmog'i samarali va mo''tadil tashkil qilingan axborot infratuzilmasisiz faoliyat ko'rsatishi mumkin emas. Hozirgi kunda milliy axborot resurslari xar bir davlatning iqtisodiy va xarbiy salohiyatini tashkil qiluvchi omillaridan biri bo'lib xizmat kilmokda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot – kommunikatsiyalar texnologiyalarini qo'llash kengayadi. Turli xildagi axborotlar xududiy joylashishidan qat'iy nazar bizning kundalik hayotimizga Internet halqaro kompyuter tarmog'i orqali kirib keldi. Axborotlashgan jamiyat shu kompyuter tarmog'i orqali tezlik bilan shakllanib bormokda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo'qolib bormokda. Jahon kompyuter tarmog'i davlat boshqaruvini tubdan o'zgartirmoqda, ya'ni davlat axborotlarning tarqalishi mexanizmini boshqara olmay qolmoqda. Shuning uchun xam mavjud axborotlarga noqonuniy kirish, ulardan foydalanish va yo'qotish kabi muammolar dolzarb bo'lib qoldi. Bularning bari shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib kelmoqda. Davlatning axborot xavfsizligini ta'minlash muammosi milliy xavfsizlikni ta'minlashning asosiy va ajralmas qismi bo'lib, axborot himoyasi esa davlatning birlamchi masalalariga aylanmoqda.

Hozirgi kunda xavfsizlikning bir qancha yo'nalishlarini qayd etish mumkin. (1- rasm)

Predmetning asosiy tushunchalari va maqsadi

Axborotning muximlik darajasi qadim zamonlardan ma'lum. Shuning uchun xam qadimda axborotni himoyalash uchun turli xil usullar qo'llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o'qiy olmagan. Asrlar davomida bu san'at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o'n yil oldin hamma narsa tubdan o'zgardi, ya'ni axborot o'z qiymatiga ega bo'ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o'g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug'iladi.

Axborotni qayta ishlash sanoatining paydo bo’lishi axborotni himoyalash sanoatining paydo bo’lishiga olib keladi.



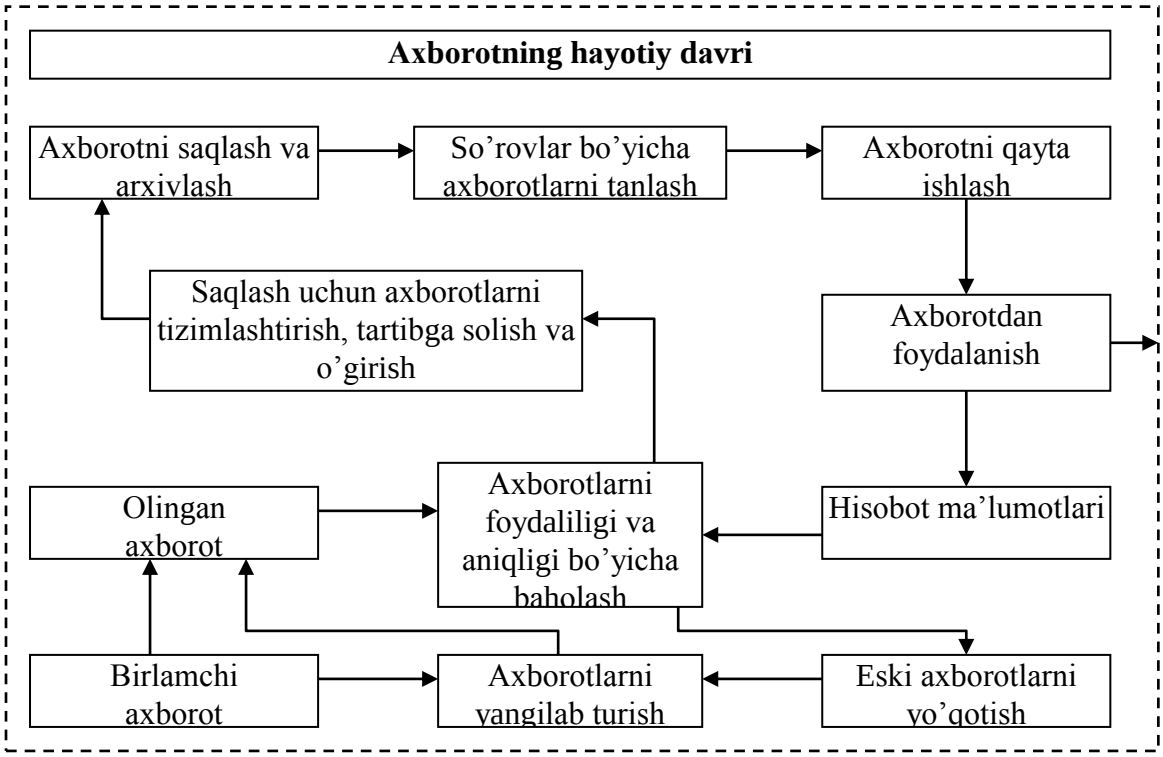
1-rasm.

Avtomatlashtirilgan axborot tizimlarida axborotlar o’zining hayotiy davriga ega bo’ladi. Bu davr uni yaratish, undan foydalanish va kerak bo’lmaganda yo’qotishdan iboratdir (2-rasm).

Axborotlar xayotiy davrining xar bir bosqichida ularning himoyalanganlik darajasi turlicha baholanadi.

Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muxim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning

mulki huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshqa moddiy hamda nomoddiy zararlar keltirishi mumkin bo'lgan turli kirishlar va o'g'irlashlardan himoyalashdir.



2-rasm

Axborot xavfsizligi deb, ma'lumotlarni yo'qotish va o'zgartirishga yo'naltirilgan tabiiy yoki sun'iy xossali tasodifiy va qasddan ta'sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va xujjatlarni o'g'irlash yoki nusxa olishdan iborat bo'lsa, hozirgi paytdagi xavf esa kompyuter ma'lumotlari to'plami, elektron ma'lumotlar, elektron massivlardan ularning egasidan ruxsat so'ramasdan foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta'minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta'minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar etkazmokchi bo'lgan nohuquqiy muomaladan xar qanday x**ujjatlashtirilgan,** ya'ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo'yilgan xolda moddiy jismda qayd etilgan **axborot** ximoyalanishi kerak.

Axborot xavfsizligi nuktai 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 kilishlik** — etarlicha 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 xollarda rejalashtirilganidek o'zini tutishlik kafolati;

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

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

• **nazorat kilinishi** — istalgan paytda dastur majmuasining xoxlagan kismini tulik tekshirish mumkinligi kafolati;

• **identifikatsiyalashni nazorat kilish** — xozir tizimga ulangan mijoz aniq o'zini kim deb atagan bo'lsa, aniq o'sha ekanligining kafolati;

• q**asddan buzilishlarga to'sqinlik** — oldindan kelishilgan me'yorlar chegarasida qasddan xato kiritilgan ma'lumotlarga nisbatan tizimning oldindan kelishilgan xolda o'zini tutishi.

Axborotni ximoyalashning maqsadlari quyidagilardan iborat:

- axborotning kelishuvsiz chikib ketishi, o'g'irlanishi, yo'qotilishi, o'zgartirilishi, soxtalashtirilishlarning oldini olish;

- shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf – xatarning oldini olish;

- axborotni yo'q qilish, o'zgartirish, soxtalashtirish, nusxa ko'chirish, to'siqlash bo'yicha ruxsat etilmagan xarakatlarning oldini olish;

- xujjatlashtirilgan axborotning miqdori sifatida xuquqiy tartibini ta'minlovchi, axborot zaxirasi va axborot tizimiga xar qanday noqonuniy aralashuvlarning ko'rinishlarining oldini olish;

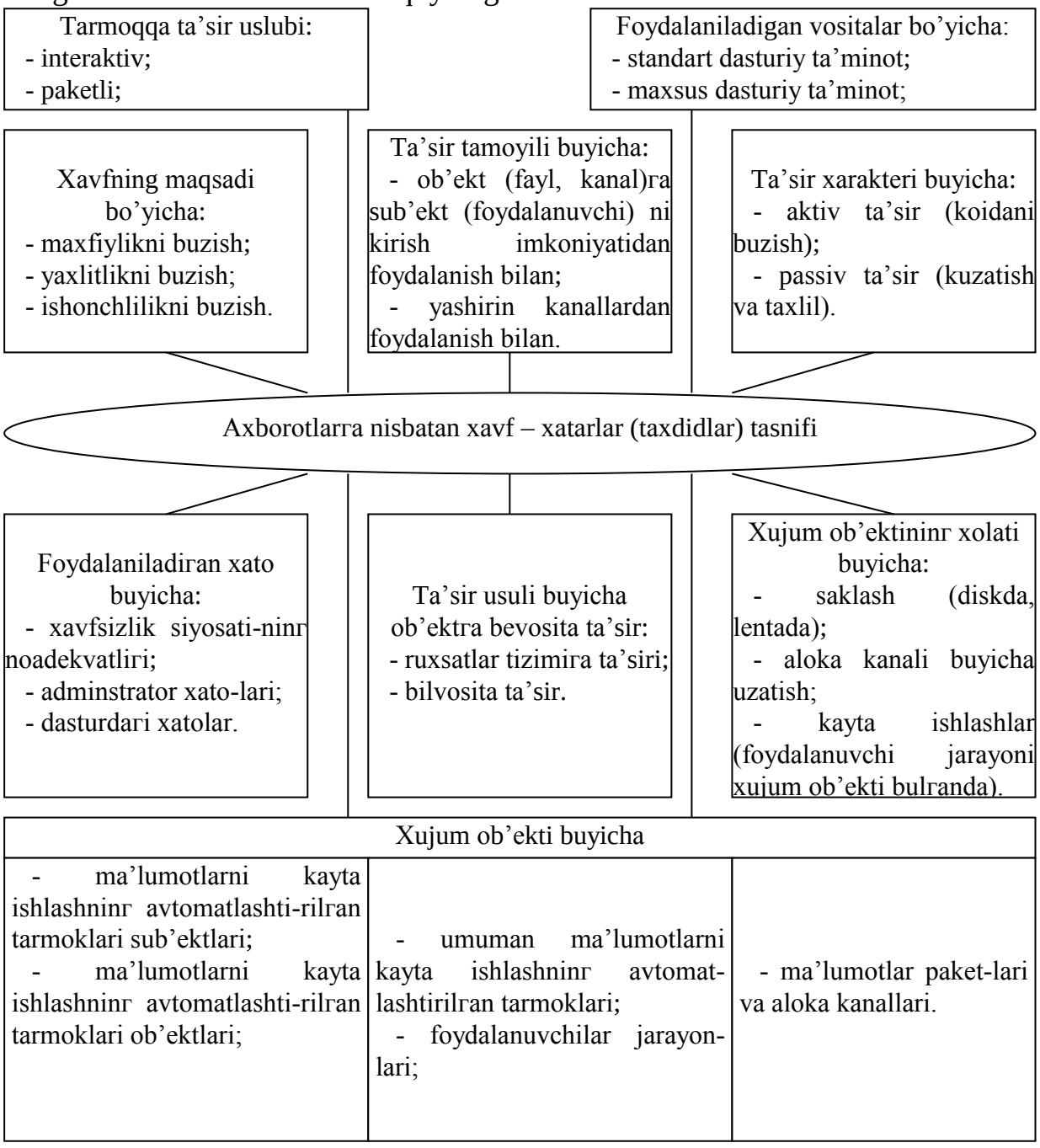
- axborot tizimida mavjud bo'lgan shaxsiy ma'lumotlarning shaxsiy maxfiyligini va konfidentsialligini saqlovchi fuqarolarning konstitutsion xuquqlarini ximoyalash;

- davlat sirini, qonunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saqlash;

- axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chiqish va qo'llashda sub'ektlarning xuquqlarini ta'minlash.

Axborotlarga nisbatan xavf-xatarlar tasnifi

Ilmiy va Amaliy tekshirishlar natijalarini umumlashtirish natijasida axborotlarga nisbatan xavf xatarlarni quyidagicha tasniflash mumkin.



Xavfsizlik siyosatining eng asosiy vazifalaridan biri ximoya tizimida potentsial xavfli joylarni kidirib topish va ularni bartaraf etish xisoblanadi.

Tekshirishlar shuni kursatadiki, tarmokdagi eng katta xavflar — bu ruxsatsiz kirishga muljallangan maxsus dasturlar, kompyuter viruslari va dasturning ichiga joylashtirilgan maxsus kodlar bulib, ular kompyuter tarmoklarining barcha ob’ektlari uchun katta xavf tugdiradi.

Tarmok xavfsizligini nazorat kilish vositalari

Zamonaviy axborot - kommunikatsiyalar texnologiyalarining yutuklari ximoya uslublarining bir kator zaruriy instrumental vositalarini yaratish imkonini berdi.

Axborotlarni ximoyalovchi instrumental vositalar deganda dasturlash, dasturiy - apparatli va apparatli vositalar tushuniladi. Ularning funktsional tuldirilishi xavfsizlik xizmatlari oldiga kuyilgan axborotlarni ximoyalash masalalarini echishda samaralidir. Xozirgi kunda tarmok xavfsizligini nazorat kilish texnik vositalarining juda keng spektri ishlab chikarilgan.

2 – MAVZU: AVTOMATLAShTIRILGAN AXBOROT TIZIMLARIDA MA'LUMOTLARGA NISBATAN XAVFLAR

1. Avtomatlashtirilgan axborot tizimlarida ximoyalash zaruriyati;
2. Axborotni ximoyalash tizimi;
3. Tashkilotlardagi axborotlarni ximoyalash;
4. Ximoyalash tizimining komplekskliligi;
5. Axborotlarni tashkiliy himoyalash elementlari;
6. Axborot tizimlarida ma'lumotlarga nasbatan xavf-xatarlar.

Avtomatlashtirilgan axborot tizimlarida ximoyalash zaruriyati

Axborot - kommunikatsiyalar texnologiyalarining ommaviy ravishda kog'ozsiz avtomatlashtirilgan asosda boshkarilishi sababli axborot xavfsizligini ta'minlash murakkablashib va muximlashib bormokda. Shuning uchun xam avtomatlashtirilgan axborot tizimlarida axborotni ximoyalashning yangi zamonaviy texnologiyasi paydo bulmokda. DataQuest kompaniyasining ma'lumotiga kura, 1996—2000 yillarda axborot ximoyasi vositalarining sotuvdagi xajmi 13 mlrd. AKSh dollariga teng bulgan.

Axborotni ximoyalash tizimi

Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chikib ketishiga va yukatilishiga tuskinlik kiluvchi tashkiliy, texnik, dasturiy, texnologik va boshka vosita, usul va choralarning kompleksi — **axborotni ximoyalash tizimi** deyiladi.

Axborot egalari xamda vakolatli davlat organlari shaxsan axborotning kimmatliligi, uning yukotilishidan keladigan zarar va ximoyalash mexanizmining narxidan kelib chikkan xolda axborotni ximoyalashning zaruriy darajasi xamda tizimning turini, ximoyalash usullar va vositalarini aniklashlari zarur. Axborotning kimmatliligi va talab kilinadigan ximoyaning ishonchliligi bir-biri bilan bevosita boglik.

Ximoyalash tizimi uzluksiz, rejali, markazlashtirilgan, maksadli, anik, ishonchli, kompleksli, oson mukammallashtiriladigan va kurinishi tez

uzgartiriladigan bulishi kerak. U odatda barcha ekstremal sharoitlarda samarali bulishi zarur.

Tashkilotlardagi axborotlarni ximoyalash

Axborot xajmi kichik bulgan tashkilotlarda axborotlarni ximoyalashda oddiy usullarni kullash maksadga muvofik va samaralidir. Masalan, ukiladigan kimmatboxo kogozlarni va elektron xujjatlarni aloxida guruxlarga ajratish va nikoblash, ushbu xujjatlar bilan ishlaydigan xodimni tayinlash va urgatish, binoni kuriklashni tashkil etish, xizmatchilarga kimmatli axborotlarni tarkatmaslik majburiyatini yuklash, tashkaridan keluvchilar ustidan nazorat kilish, kompyuterni ximoyalashning eng oddiy usullarini kullash va xokazo. Odatda, ximoyalashning eng oddiy usullarini kullash sezilarli samara beradi.

Murakkab tarkibli, kup sonli avtomatlashtirilgan axborot tizimi va axborot xajmi katga bulgan tashkilotlarda axborotni ximoyalash uchun ximoyalashning majmuali tizimi tashkil kilinadi. Lekin ushbu usul xamda ximoyalashning oddiy usullari xizmatchilarning ishiga xaddan tashkari xalakit bermasligi kerak.

Ximoyalash tizimining kompleksliligi

Himoya tizimining kompleksliligiga unda xukukiy, 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 uziga xosligini, balki axborotning qimmatliligini va tizimning qiymatini hisobga olgan holda belgilangan himoya darajasini aniqlaydi.

Axborotni huquqiy himoyalash elementi himoyalash choralarining haqli ekanligi ma’nosida tashkilot va davlatlarning uzaro munosabatlarini yuridik mustahkamlash xamla personalning tashkilot qimmatli axborotini himoyalash tartibiga rioya qilishi va ushbu tartibni buzilishida javobgarligi tasavvur qilinadi.

Axborotlarni tashkiliy himoyalash elementlari

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

Tashkiliy himoyalash elementi boshka barcha elementlarni yagona tizimga bog’lovchi omil bo’lib hisoblanadi. Ko’pchilik mutaxassislarning fikricha, axborotlarni himoyalash tizimlari tarkibida tashkiliy himoyalash 50—60 % ni tashkil qiladi. Bu hol ko’p omillarga bog’liq, jumladan, axborotlarni tashkiliy himoyalashning asosiy tomoni amalda ximoyalashning printsipi va usullarini bajaruvchi personalni tanlash, joylashtirish va urgatish hisoblanadi.

Axbortlarni himoyalashning tashkiliy chora – tadbirlari tashkilot xavfsizligi xizmatining me’yoriy uslubiy hujjatlarida uz aksini topadi. Shu munosabat bilan

ko’p hollarda yuqorida ko’rilgan tizim element-larining yagana nomi — axborotni tashkiliy - huquqiy himoyalash elementini ishlatadilar.

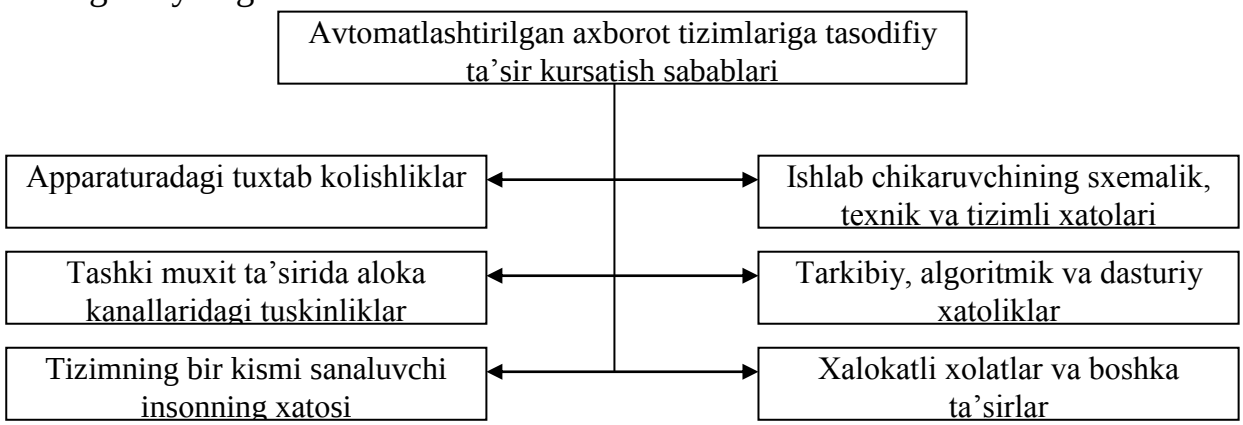
Axborotlarni muhandis – texiik himoyalash elementi — texnik vositalar kompleksi yordamida hudud, bino va qurilmalarni quriqlashni tashkil qilish hamda texnik tekshirish vositalariga karshi sust va faol kurash uchun muljallangan. Texnik himoyalash vositalarining narxi baland bo’lsada, axborot tizimini himoyalashda bu element muhim ahamiyatga ega.

Axborotni himoyalashning dasturiy – matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saqlanadigan qimmatli axborotlarni himoyalash uchun mo’ljallangan.

Axborot tizimlarida ma’lumotlarga nasbatan xavf-xatarlar

Kompyuter tizimi (tarmogi)ga ziyon etkazishi mumkin bo’lgan sharoit, xarakat va jarayonlar **kompyuter tizimi (tarmogi)** uchun xavf - xatarlar, deb hisoblanadi.

Avtomatlashtirilgan axborot tizimlariga tasodifiy ta’sir kursatish sabablari tarkibiga kuyidagilar kiradi.



Ma’lumki, kompyuter tizim (tarmog’)ining asosiy komponentlari — texnik vositalari, 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 soxtalashtirish:**

— uzilish — qandaydir tashqi harakatlar (ishlar, jarayonlar)ni bajarish uchun hozirgi ishlarni vaqtincha markaziy protsessor qurilmasi yordamida tuxtatishdir, ularni bajargandan so’ng protsessor oldingi holatga qaytadi va to’xtatib quyilgan 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 uzilishlar paydo bo’ladi. Odatda bunday uzilish markaziy protsessor uchun kutilmagan hodisadir. Dasturiy uzilishlar asosiy dasturlar ichida protsessorning maxsus buyruqlari yordamida bajariladi. Dasturiy uzilishda dastur o’z – o’zini vaktincha to’xtatib, uzilishga taalluqli jarayonni bajaradi.

— tutib olish — jarayoni oqibatida g’arazli shaxslar dasturiy vositalar va axborotlarning turli magnitli tashuvchilariga kirishni qulga kiritadi. Dastur va ma’lumotlardan noqonuniy nusxa olish, kompyuter tarmoklari aloqa kanallaridan nomualliflik 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 tuplamlari, dasturlar, texnik elementlari) kirishni qulga kiritadi, balki ular bilan manipulyatsiya (o’zgartirish, ko’rinishini o’zgartirish) ham kiladi. Masalan, o’zgartirish sifatida g’arazli shaxsning ma’lumotlar to’plamidagi ma’lumotlarni o’zgartirishi, yoki umuman kopyuter tizimi fayllarini o’zgartirishi, yoki kandaydir qo’shimcha noqonuniy kayta ishlashni amalga oshirish maksadida foydalanilayotgan dasturning kodini o’zgartirishi tushunilali;

— soxtalashtirish — xam jarayon sanalib, uning yordamida g’arazli shaxslar tizimda hisobga olinmagan vaziyatlarni o’rganib, undagi kamchiliklarni aniklab, keyinchalik o’ziga kerakli harakatlarni bajarish maqsadida tizimga qandaydir soxta jarayonni yoki tizim va boshqa foydalanuvchilarga soxta yozuvlarni yuboradi.

3 – MAVZU: VIRUS VA ANTIVIRUSLAR TASNIFI

1. Virus va uning turlari;

2. Kompyuter viruslaridan axborotlarga ruxsatsiz kirish va ulardan foydalanishni tashkil etish;

3. Antivirus dasturlari;

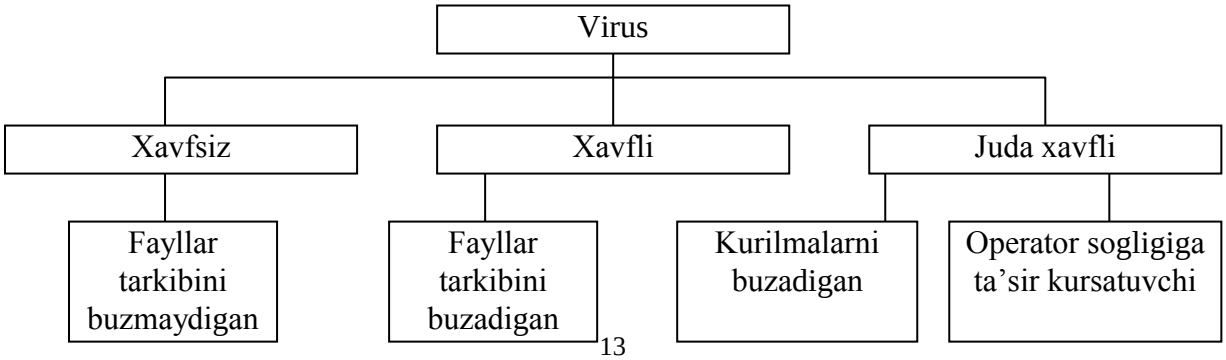
4. Viruslarga qarshi chora-tadbirlar.

Virus va uning turlari

Hozirgi kunda kompyuter viruslari g’arazli maqsadlarda ishlatiluvchi turli xil dasturlarni olib kelib tatbiq etishda eng samarali vositalardan biri hisoblanadi. Kompyuter viruslarini **dasturli viruslar** deb atash tugriroq bo’ladi.

Dasturli virus deb avtonom ravishda ishlash, boshqa dastur tarkibiga o’z – o’zidan qushiluvchi, ishga kodir va kompyuter tarmoqlari va alohida kompyuterlarda uz – uzidan tarkalish xususiyatiga ega bulgan dasturga aytiladi.

Viruslar bilan zararlangan dasturlar **virus tashuvchi** yoki **zararlangan dasturlar** deyiladi.



Zararlangan disk – bu ishga tushirish sektorida virus dastur joylashib olgan diskdir.

Xozirgi paytda kompyuterlar uchun kupgina nokulayliklar tugdirayotgan xar xil turlardagi kompyuter viruslari keng tarkalgan. Shuning uchun xam ulardan saklanish usullarini ishlab chikish muxim masalalardan biri xisoblanadi. Xozirgi vaktda 65000 dan kup bulgan virus dasturlari borligi aniklangan. Bu viruslarning katta guruxini komp'yuterning ish bajarish tartibini buzmaydigan, ya'ni «ta'sirchan bulmagan» viruslar guruxi tashkil etadidi.

Viruslarning boshka guruxiga kompyuterning ish tartibini buzuvchi viruslar kiradi. Bu viruslarni kuyidagi turlarga bulish mumkin: **xavfsiz viruslar** (fayllar tarkibini buzmaydigan), **xavfli viruslar** (fayllar tarkibini buzuvchi) xamda **juda xavfli viruslar** (kompyuter kurilmalarini buzuvchi va operator sogligiga ta'sir etuvchi). Bu kabi viruslar odatda professional dasturchilar tomonidan tuziladi.

Kompyuter virusi – bu maxsus yozilgan dastur bulib, boshka dasturlar tarkibiga yoziladi, ya'ni zararlaydi va kompyuterlarda uzining garazli maksadlarini amalga oshiradi.

Kompyuter virusi orkali zararlanish okibatida kompyuterlarda kuyidagi uzgarishlar paydo buladi:

• ayrim dasturlar ishlamaydi yoki xato ishlay boshlaydi;

• bajariluvchi faylning xajmi va uning yaratilgan vakti uzgaradi;

• ekranda anglab bulmaydigan belgilar, turli xil tasvir va tovushlar paydo buladi;

• kompyuterning ishlashi sekinlashadi va tezkor xotiradagi bush joy xajmi kamayadi;

• disk yoki diskdagi bir necha fayllar zararlanadi (ba'zi xollarda disk va fayllarni tiklab bulmaydi):

• vinchester orkali kompyuterning ishga tushishi yukoladi.

Viruslar asosan disklarning yuklanuvchi sektorlarini va exe, som, sys va bat kengaytmali fayllarni zararlaydi. Xozirgi kunda bular katoriga ofis dasturlari yaratadigan faylarni xam kiritish mumkin. Oddiy matnli fayllarni zararlaydigan viruslar kamdan – kam uchraydi.

Fayllar tarkibini buzmaydigan viruslar

Tezkor xotira kurilmasida kupayuvchi	Operatorni ta'sirlantiruvchi	Tarmok viruslari

Operatorni ta'sirlantiruvchi			
Kurilmalarni ishdan chikaruvchi	**Terminalda xabar chikaruvchi**	**Tovushli effektlarni xosil kiluvchi**	**Ish tartibini uzgartiruvchi**
- protsessor			- klaviatura

- xotira	- matnli	- oxang	
- MD, vinchester			- displey
- printer	- grafikli	- nutk sintezi	
- port PS-232			printer
Displey		- maxsus effektlar	
- klaviatura			- port PS-232

Kompyuterning viruslar bilan zararlanish yullari kuyidagilardir:
1. Disketlar orkali.
2. Kompyuter tarmoklari orkali.
3. Boshka yullar yuk.

Fayl tarkibini buzuvchi viruslar

Foydalanuvchining ma'lumotlari va dasturlarni buzuvchi		**Tizim ma'lumotlarini buzuvchi**		
Dasturlarni buzuvchi	Ma'lumotlarni buzuvchi	Disk soxasini buzuvchi	Formatlash	Tezkor tizim fayllarini buzuvchi
Dasturning boshlangich yozuvlarini buzuvchi	Ma'lumotlar bazalarini buzuvchi	Diskning mantikiy tarkibini buzish		
Bajariluvchi dasturlarni buzuvchi	Matnli xujjatlarni buzuvchi	Ma'lumot tashuvchilarning tarkibini buzuvchi		
Kompilyatorlarning kism dasturlar tuplamini buzuvchi	Grafik tasvirlarni buzuvchi			
	Elektron jadvalni buzuvchi			

Operator va kurilmalarga ta'sir etuvchi viruslar

Kurilmalarni buzuvchi			**Operatorga ta'sir etuvchi**	
Displeyning Lyuminafor katlamini kuydiruvchi	Kompyuterlarning mikrosxemasini ishdan chikaruvchi	Printerni ishdan chikaruvchi	MDni buzuvchi	Operator texnikasiga ta'sir etuvchi

Xozirgi paytda xazil shaklidagi viruslardan tortib to kompyuter kurilmalarini ishdan chikaruvchi viruslarning turlari mavjud.

Masalan. Win 95.CIH virusi doimiy saklash kurilmasi (Flash BIOS) mikrosxemasini buzadi. Afsuski, bu kabi viruslarni yuk kilish uchun, fakat ular uz garazli ishini bajarib bulgandan sunggina, karshi choralar ishlab chikiladi. Win 95.CIH virusiga karshi choralarni kurish imkoniyati Dr.Web dasturida mavjud.

Kompyuter viruslaridan axborotlarga ruxsatsiz kirish va ulardan foydalanishni tashkil etish

Shuni aytib utish lozimki, xozirgi paytda xar-xil turdagi axborot va dasturlarni ugirlab olish niyatida kompyuter viruslaridan foydalanish eng samarali usullardan biri xisoblanadi.

Dasturli viruslar kompyuter tizimlarining xavfsizligiga taxdid solishning eng samarali vositalaridan biridir. Shuning uchun xam dasturli viruslarning imkoniyatlarini taxlil kilish masalasi xamda bu viruslarga karshi kurashish xozirgi paytning dolzarb masalalaridan biri bulib koldi.

Viruslardan tashkari fayllar tarkibini buzuvchi **troyan dasturlari** mavjud. Virus kupincha kompyuterga sezdirmasdan kiradi. Foydalanuvchinint uzi troyan dasturini foydali dastur sifatida diskka yozadi. Ma’lum bir vakt utgandan keyin buzgunchi dastur uz ta’sirini kursatadi.

Uz-uzidan paydo buladigan viruslar mavjud emas. Virus dasturlari inson tomonidan kompyuterning dasturiy ta’minotini, uning kurilmalarini zararlash va boshka maksadlar uchun yoziladi. Viruslarning xajmi bir necha baytdan to unlab kilobaytgacha bulishi mumkin.

Troyan dasturlari foydalanuvchiga zarar keltiruvchi bulib, ular buyruklar (modullar) ketma – ketligidan tashkil topgan, omma orasida juda keng tarkalgan dasturlar (tahrirlovchilar, o’yinlar, translyatorlar) ichiga o’rnatilgan bo’lib, bir qancha hodisalar bajarilishi bilan ishga tushadigan «mantiqiy bomba» deb ataladigan dasturdir. O’z navbatida, «mantikiy bomba»ning turli ko’rinishlaridan biri «soat mexanizmli bomba» hisoblanadi.

Shuni ta’kidlab o’tish kerakki, troyan dasturlari o’z-o’zidan ko’paymasdan, kompyuter tizimi bo’yicha dasturlovchilar tomonidan tarqatiladi.

Troyan dasturlardan viruslarning farqi shundaki, viruslar kompyuter tizimlari buylab tarkatilganda, ular mustaqil ravishda hosil bo’lib, o’z ish faoliyatida dasturlarga o’z matnlarini yozgan holda ularga zarar ko’rsatadi.

Zararlangan dasturda dastur bajarilmasdan oldin virus o’zining buyruqlari bajarilishiga imkoniyat yaratib beradi. Buning uchun xam virus dasturning bosh qismida joylashadi yoki dasturning birinchi buyrugi unga yozilgan virus dasturiga shartsiz o’tish bo’lib xizmat qiladi. Boshqarilgan virus boshqa dasturlarni zararlaydi va shundan so’ng virus tashuvchi dasturga ishni topshiradi.

Virus hayoti odatda quyidagi davrlarni o’z ichiga oladi: **qullanilish, inkubatsiya, replikatsiya** (o’z-o’zidan ko’payish) va **hosil bo’lish.** Inkubatsiya davrida virus passiv bo’lib, uni izlab topish va yukotish kiyin. Hosil bulish davrida u o’z funktsiyasini bajaradi va qo’yilgan maqsadiga erishadi.

Tarkibi jihatidan virus juda oddiy bo’lib, bosh qism va bazi hollarda dumdan iborat. Virusning bosh qismi deb boshkarilishini birinchi bo’lib

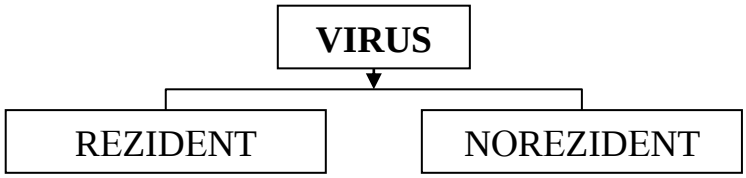
ta’minlovchi imkoniyatga ega bo’lgan dasturga aytiladi. Virusning dum qismi zararlangan dasturda bo’lib, u bosh kismidan alohida joyda joylashadi.

Kompyuter viruslari xarakterlariga nisbatan **norezident, rezident, butli, gibridli va paketli viruslar**ga ajratiladi.

Faylli **norezident viruslar** to’liqligicha bajarilayotgan faylda joylashadi, shuning uchun ham u faqat virus tashuvchi dastur faollashgandan so’ng ishga tushadi va bajarilgandan so’ng tezkor xotirada saqlanmaydi.

Rezident virus norezident virusdan farqliroq tezkor xotirada saqlanadi.

Rezident viruslarning yana bir ko’rinishi **but viruslar** bo’lib, bu virusning vazifasi vinchester va egiluvchan magnitli disklarning yuklovchi sektorini ishdan chiqarishdan iborat. But viruslarning boshi diskning yuklovchi but sektorida va dumi disklarning ixtiyoriy boshka sektorlarida joylashgan bo’ladi.



Paketli virusning bosh qismi paketli faylda joylashgan bo’lib, u operatsion tizim topshiriqlaridan iborat.

Gibridli viruslarning boshi paketli faylda joylashadi. Bu virus xam faylli, ham but sektorli bo’ladi.

Tarmoqli viruslar kompyuter tarmoklarida tarqalishga moslashtirilgan, ya’ni tarmoqli viruslar deb axborot almashishda tarqaladigan viruslarga aytiladi.

Viruslarning turlari:

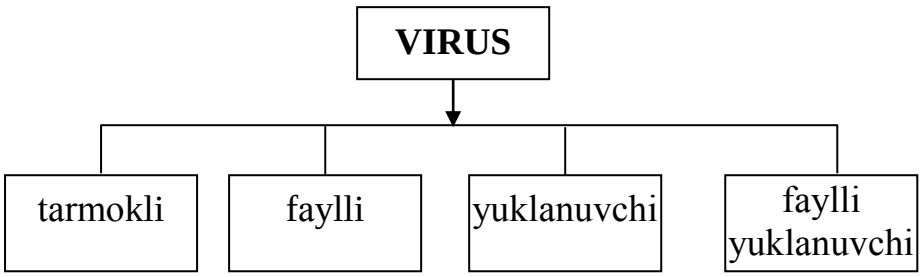
1) **fayl viruslari.** Bu viruslar *som, exe* kabi turli fayllarni zararlaydi;

2) **yuklovchi viruslar.** Kompyuterni yuklovchi dasturlarni zararlaydi;

3) **drayverlarni zararlovchi viruslar.** Operatsion tizimdagi sonfig.sys faylni zararlaydi. Bu kompyuterning ishlamasligiga sabab bo’ladi;

4) **DIR viruslari.** FAT tarkibini zararlaydi;

5) **stels-viruslari.** Bu viruslar o’zining tarkibini uzgartirib, tasodifiy kod o’zgarishi bo’yicha tarqaladi. Uni aniklash juda qiyin, chunki fayllarning o’zlari o’zgarmaydi;



6) **Windows viruslari.** Windows operatsion tizimidagi dasturlarni zararlaydi.

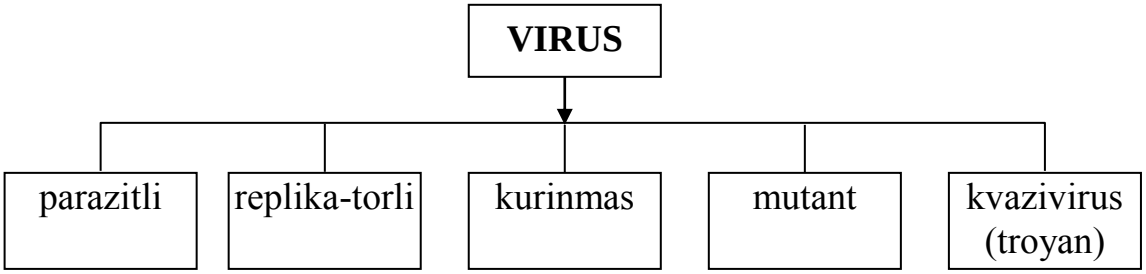
Misol sifatida quyidagilarni keltirish mumkin:

1) Eng xavfli viruslardan biri Internet orqali tarqatilgan «Chernobil» virusi bo’lib, u 26 aprelda tarkatilgan va har oyning 26-kunida komp’yuterlarni zararlashi mumkin.

2) I LOVE YOU virusi Filippindan 2000 yil 4 mayda E-mail orkali tarqatilgan. U bugun jahon buyicha 45 mln. kompyuterni zararlagan va ishdan chikargan. Moddiy zarar 10 mlrd. AQSh dollarini tashkil kilgan.

3) 2003 yil mart oyida Shvetsiyadan zlektron pochta orkali GANDA virusi tarqatilgan va u butun dunyoda minglab kompyuterlarni zararlagan. Bu virusni tarqatgan shaxs hozir qulga olingan va u 4 yil kamoq jazosiga hukm etilishi mumkin.

Asoslangan algoritmlar buyicha dasturli viruslarni kuyidagicha tasniflash mumkin.



Parazitli virus — fayllarning tarkibini va diskning sektorini uzgartiruvchi virus. Bu virus oddiy viruslar turkumidan bo’lib, osonlik bilan aniqlanadi va o’chirib tashlanadi.

Replikatorli virus — «chuvalchang» deb nomlanadi, kompyuter tarmoqlari bo’yicha tarqalib, komlyuterlarning tarmoqdagi manzilini aniqlaydi va u erda o’zining nusxasini qoldiradi.

Kurinmas virus — stels-virus deb nom olib, zararlangan fayllarga va sektorlarga operatsion tizim tomonidan murojaat qilinsa, avtomatik ravishda zararlangan qismlar o’rniga diskning toza qismini taqdim etadi. Natijada ushbu viruslarni aniqlash va tozalash juda katta qiyinchiliklarga olib keladi.

Mutant virus — shifrlash va deshifrlash algoritmlaridan iborat bo’lib, natijada virus nusxalari umuman bir-biriga o’xshamaydi. Ushbu viruslarni aniqlash juda qiyin muammo.

Kvazivirus virus — «Troyan» dasturlari, deb nom olgan bo’lib, ushbu viruslar ko’payish xususiyatiga ega bo’lmasa-da, «foydali» qism-dastur xisobida bo’lib, antivirus dasturlar tomonidan aniqlanmaydi. Shu bois ham ular o’zlarida mukammallashtirilgan algoritmlarni to’siqsiz bajarib, qo’yilgan maqsadlariga erishishlari mumkin.

Antivirus dasturlari

Hozirgi vaqtda viruslarni yo’qotish uchun ko’pgina usullar ishlab chiqilgan va bu usullar bilan ishlaydigan dasturlarni **antiviruslar** deb atashadi. Antiviruslarni, kullanish usuliga ko’ra, quyidagilarga ajratishimiz mumkin: ***detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar.***

Detektorlar — virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo'yicha tezkor xotira va fayllarni ko'rish natijasida ma'lum viruslarni topadi va xabar beradi. Yangi viruslarni aniqlab olmasligi detektorlarning kamchiligi xisoblanadi.

Faglar — yoki doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oldingi xolatiga kaytaradi.

Vaktsinalar — yuqoridagilardan farqli ravishda himoyalanayotgan dasturga urnatiladi. Natijada dastur zararlangan deb hisoblanib, virus tomonidan o'zgartirilmaydi. Faqatgina ma'lum viruslarga nisbatan vaktsina qilinishi uning kamchiligi hisoblanadi. Shu bois xam, ushbu antivirus dasturlari keng tarqalmagan.

Privivka — fayllarda xuddi virus zararlagandek iz qoldiradi. Buning natijasida viruslar «privivka qilingan» faylga yopishmaydi.

Filtrlar — quriqlovchi dasturlar kurinishida bo'lib, rezident holatda ishlab turadi va viruslarga xos jarayonlar bajarilganda, bu haqda foydalanuvchiga xabar beradi.

Revizorlar — eng ishonchli himoyalovchi vosita bo'lib, diskning birinchi holatini xotirasida saqlab, undagi keyingi o'zgarishlarni doimiy ravishda nazorat qilib boradi.

Detektor dasturlar kompyuter xotirasidan, fayllardan viruslarni qidiradi va aniqlangan viruslar xaqida xabar beradi.

Doktor dasturlari nafaqat virus bilan kasallangan fayllarni topadi, balki ularni davolab, dastlabki holatiga qaytaradi. Bunday dasturlarga Aidstest, Doctor Web dasturlarini misol kilib keltirish mumkin. Yangi viruslarning to'xtovsiz paydo bo'lib turishini hisobga olib, doktor dasturlarini ham yangi versiyalari bilan almashtirib turish lozim.

Filtr dasturlar kompyuter ishlash jarayonida viruslarga xos bo'lgan shubhali harakatlarni topish uchun ishlatiladi.

Bu xarakatlar kuyidagicha bo'lishi mumkin:

- fayllar atributlarining o'zgarishi;
- disklarga doimiy manzillarda ma'lumotlarni yozish;
- diskning ishga yuklovchi sektorlariga ma'lumotlarni yozib yuborish.

Tekshiruvchi (revizor) dasturlari virusdan ximoyalanishning eng ishonchli vositasi bo'lib, kompyuter zararlanmagan holatidagi dasturlar, kataloglar va diskning tizim maydoni holatini xotirada saklab, doimiy ravishda yoki foydalanuvchi ixtiyori bilan kompyuterning joriy va boshlangach holatlarini bir-biri bilan solishtiradi. Bunga ADINF dasturini misol qilib keltirish mumkin.

Viruslarga qarshi chora-tadbirlar

Kompyuterni viruslar bilan zararlanishidan saklash va axborotlarni ishonchli saqlash uchun quyidagi qoidalarga amal qilish lozim:

- kompyuterni zamonaviy antivirus dasturlar bilan ta'minlash;
- disketalarni ishlatishdan oldin har doim virusga qarshi tekshirish;

- qimmatli axborotlarning nusxasini har doim arxiv fayl ko’rinishida saqlash.

Kompyuter viruslariga karshi kurashning quyidagi turlari mavjud:

- viruslar kompyuterga kirib buzgan fayllarni o’z holiga qaytaruvchi dasturlarning mavjudligi;
- kompyuterga parol bilan kirish, disk yurituvchilarning yopiq turishi;
- disklarni yozishdan ximoyalash;
- litsenzion dasturiy ta’minotlardan foydalanish va o’g’irlangan dasturlarni qo’llamaslik;
- kompyuterga kiritalayotgan dasturlarning viruslarning mavjudligini tekshirish;
- antivirus dasturlaridan keng foydalanish;
- davriy ravishda kompyuterlarni antivirus dasturlari yordamida viruslarga qarshi tekshirish.

Antivirus dasturlaridan DrWeb, Adinf, AVP, VootCHK va Norton Antivirus, Kaspersky Security kabilar keng foylalaniladi.

4 – MAVZU: AXBOROTLARNI STENOGRAFIK XIMOYALASh USULLARI

1. Zamonaviy kompyuter stenografiyasi;
2. Kompyuter stenografiyasi istikbollari;
3. Kompyuter stenografiyasining asosiy vazifalari;
4. Konfidentsial axborotlarni ruxsatsiz kirishdan hamoyalash.

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 qullanilgan) bo’lishi mumkin.

Axborotni himoyalash uchun **kodlashtirish** va **kriptografiya** usullari qo’llaniladi.

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

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

Stenografiyaning krintografiyadan boshqa o’zgacha farqi ham bor. Ya’ni uning maqsadi — maxfiy xabarning mavjudligini yashirishdir. Bu ikkala usul birlashtirilishi mumkin va natijada axborotni ximoyalash 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 stenogryafiya**si paydo bo’ldi.

Global kompyuter tarmoqlari va multimedia soxasidagi 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 kuyish tartibini aniklaydigan maxfiy element tushuniladi.

Kompyuter stenografiyasi istikbollari

Kompyuter stenografiyasi rivojlanishi tendentsiyasining 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. Boshka tomondan, axborot-kommunikatsiyalar texnologiyalarining jadal rivojlanishi ushbu axborotni ximoyalashning 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 qullanilayotgan soxa bu — kriptografik usullardir. Lekin, bu yo’lda kompyuter viruslari, «mantiqiy bomba»lar kabi axborotiy qurollarning kriptovositalarni buzadigan ta’siriga bog’liq ko’p echilmagan muammolar mavjud. Boshka tomondan, kriptografik usullarni ishlatishda kalitlarni taqsimlash muammosi ham bugungi kunda oxirigacha echilmay turibdi. Kompyuter steganografiyasi va kriptografiyalarining birlashtirilishi paydo bo’lgan sharoitdan qutulishning yaxshi bir yo’li bular 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 malum 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 chikarib olish jarayoni murakkab xisoblash 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 nikoblash;
- intellektual egalikning ba’zi bir turlarida mualliflik huquqlarini himoyalash.

Konfidentsial axborotlarni ruxsatsiz kirishdan hamoyalash

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

Monitoring va tarmok zaxiralarini boshqarish tizimlarini engish

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

Dasturiy ta’minotni nikoblash

Kompyuter steganografiyasining xozirgi vaqtda ishlatiladigan boshka bir sohasi dasturiy ta’minotni niqoblashdir. Qachonki, dasturiy ta’minotni kayd qilinmagan foydalanuvchilar tomonidan ishlatilishi o’rinsiz bo’lsa, u standart universal dastur mahsulotlari (masalan, matnli muxarrirlar) ostida niqoblanishi yoki multimedia 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 quyiladi va u kuzga ko'rinmay qatadi. Lekin, maxsus dasturiy ta'minot bilan aniqlanadi. Bunday dastur mahsuloti allakachon ba'zi jurnallarning kompyuter versiyalarida ishlatilayapti. Stenografiyaning ushbu yo'nalishi nafakat tasvirlarni, balki audio va videoaxborotni ham qayta ishlashga muljallangan. Bundan tashkari uning intellektual egaligini himoyalashni ta'minlash vazifasi ham mavjud.

Hozirgi vaqtda kompyuter stenografiyasi usullari ikki asosiy yo'nalish buyicha rivojlanmokda:

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

Stenografik dasturlar to'grisida kisqacha malumot

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 kudratli xisoblanadi;

• Sontraband dasturi 24-bitli VMR formatdagi grafik fayllar ichida har qanday faylni yashira olish imkoniyatiga ega.

DOS muxitida 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 malumotlarni 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 USULLARI

1. ***Kriptografiya haqida asosiy tushunchalar;***
2. ***Axborotlarni kriptografiyali himoyalash tamoyillari;***
3. ***Simmetriyali kriptotizim asoslari;***
4. ***Urinlarni almashtirish usullari;***
5. ***Almashtirish usullari.***

Kriptografiya haqida asosiy tushunchalar

«Kriptografiya» atamasi dastlab «yashirish, yozuvni berkitib quymoq» ma’nosini bildirgan. Birinchi marta u yozuv paydo bulgan davrlardayok 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 mumkkn.

Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta’minlaydi. Masalan, tulov varaklarini elektron pochta orkali uzatishda uning o’zgartirilishi yoki soxta yozuvlarning qushilishi mumkin. Bunday hollarda axborotning yaxlitligini ta’minlash zaruriyati paydo bo’ladi. Umuman olganda kompyuter tarmogiga 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’l-laniladigan usullar ko’p bo’lmagan o’zgartirishlar bilan axborotlarning haqikiyligini ta’minlashi mumkin.

Nafaqat axborotning kompyuter tarmogidan ma’nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch xosil qilish juda muhim. Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiklovchi turli usullar ma’lum. Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo’lmagan protsedura. Chunki parolni quliga 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 yutuklardan 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 kullashning ba’zi birlarini ko’rib chikamiz. 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 hallarda, raqamlar to’plami bilan beriladigan ixtiyoriy tanlangan kodli suz 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 — katorli 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 muvaffakiyatli deb bulmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, kodlarning yangi kitobini yaratish va uni xamma foydalanuvchilarga tarkatish 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 kamrab oladi. Uzgartirishlarning 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 kamaytarish mumkin. Endi himoyalash ob’ekti sifatada faqat kalit xizmat qiladi. Agar kalitdan nusxa olingan bo’lsa, uni almashtirish mumkin va bu kodlashtiruvchi kitob yoki jadvalni almashtirishdan engildir. Shuning uchun ham kodlashtirish emas, balki shifrlash axborot-kommunikatsiyalar texnologiyalarida keng ko’lamda qullanilmoqda.

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 kuyidagi ikkita muammo mavjud:

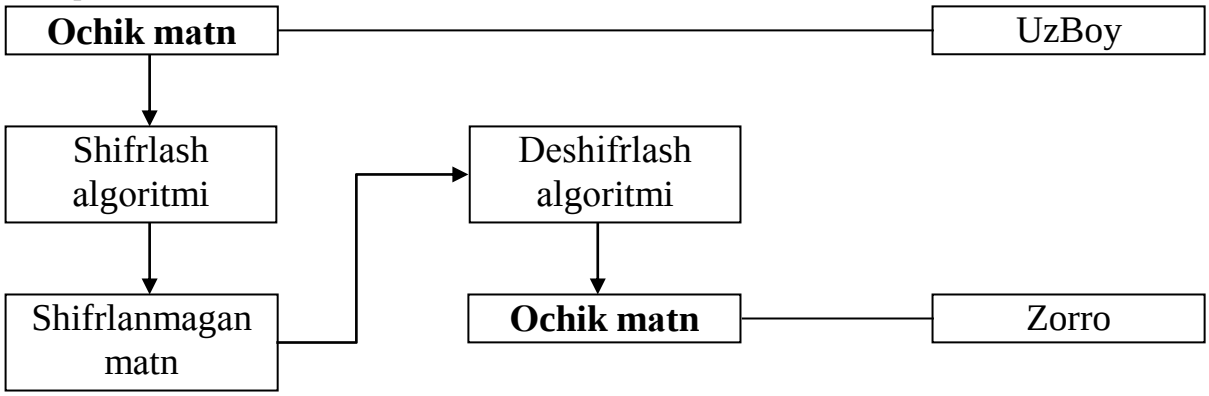
1) Axborot almashuvida ishtirok etuvchilar kanday yo’l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?

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 ko’llaniladi. Biridan ikkinchisini xisoblash usullari bilan aniqlab bo’lmaydi.

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



Ushbu usul bilan axborotning maxfiyligini ta’minlash mumkin. Agar birinchi kalit sirli bo’lsa, u holda uni elektron imzo sifatida qullash mumkin va bu usul bilan axborotni autentifikatsiyalash, ya’ni axborotning yaxlitligini ta’minlash imkoni paydo buladi.

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni echish mumkin:

• foydalanuvchini autentifikatsiyalash, ya’ni kompyuter tizimi zaxiralariga kirmoqchi bo’lgan foydalanuvchini aniklash:

• tarmok abonentlari aloqasini urnatish jarayonida ularni o’zaro autentnfikatsiyalash.

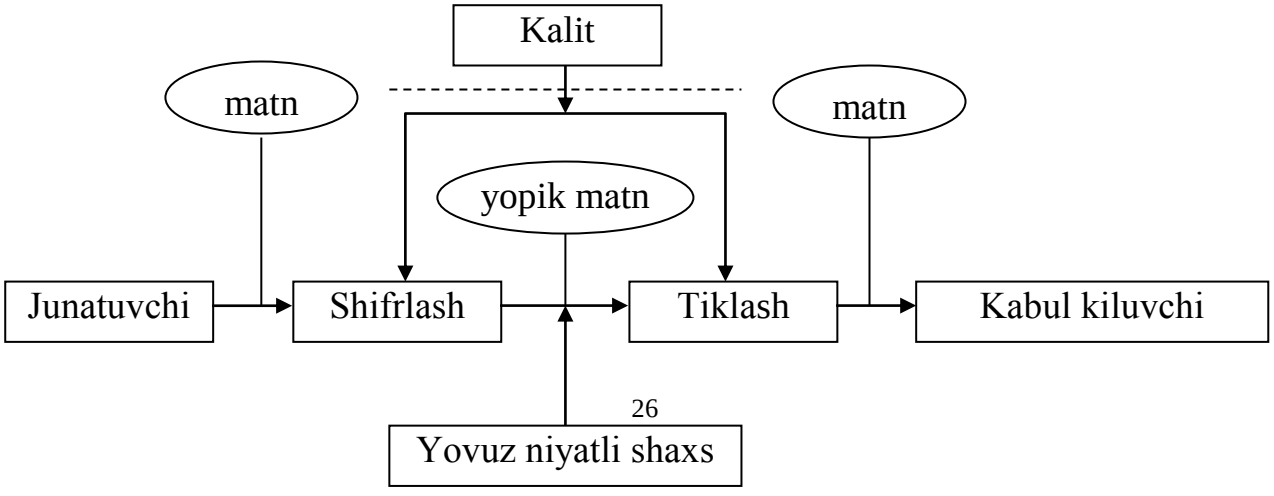
Hozirgi kunda himoyalanishi zarur bo’lgan yo’nalishlardan biri bu elektron to’lov tizimlari va Internet yordamida amalga oshiriladigan elektron savdolardir.

Axborotlarni kriptografiyali himoyalash tamoyillari

Kriptografiya — ma’lumotlarni o’zgartirish usullarining tuplami bo’lib, ma’lumotlarni himoyalash bo’yicha quyidagi ikkita asosiy muammolarni hal qilishga yunaltirilgan: **maxfiylik; yaxlitlilik.**

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

Kriptografiya tizimini sxematik ravishda kuyidagicha tasvirlash mumkin:



Bu erla kalit kandaydir ximoyalangan kanal orkali junatiladi (chizmada punktir chiziklar bilan tasvirlangan). Umuman olganda, ushbu mexanizm simmetriyali bir kalitlik tizimiga taalluklidir.

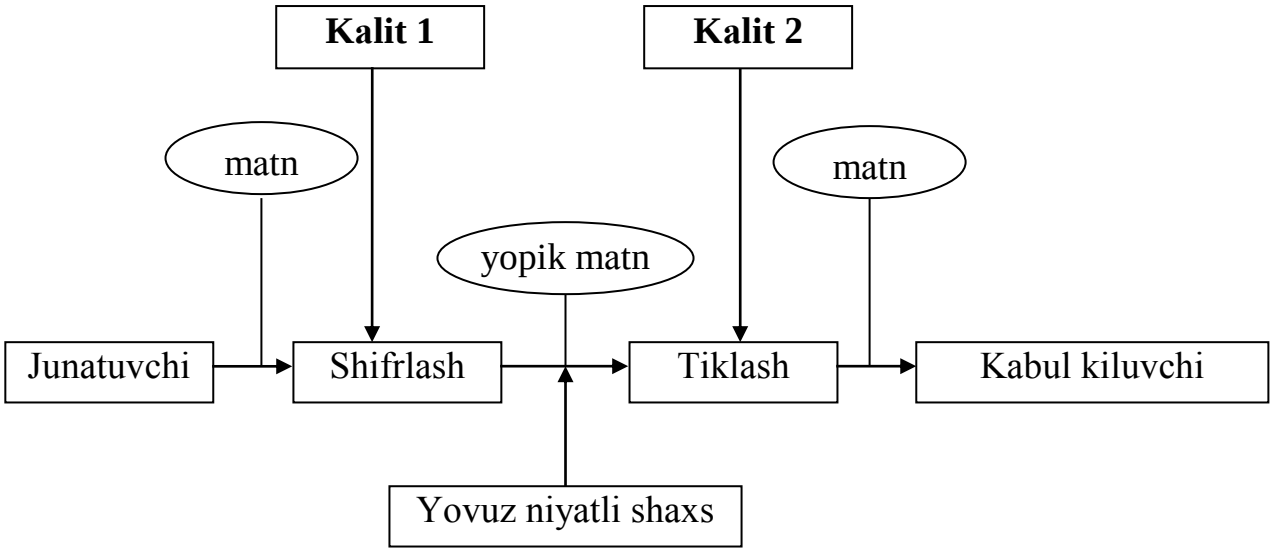
Assimmetriyali ikki kalitlik kriptografiya tizimini sxematik ravishda kuyidagicha tasvirlash mumkin:

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.

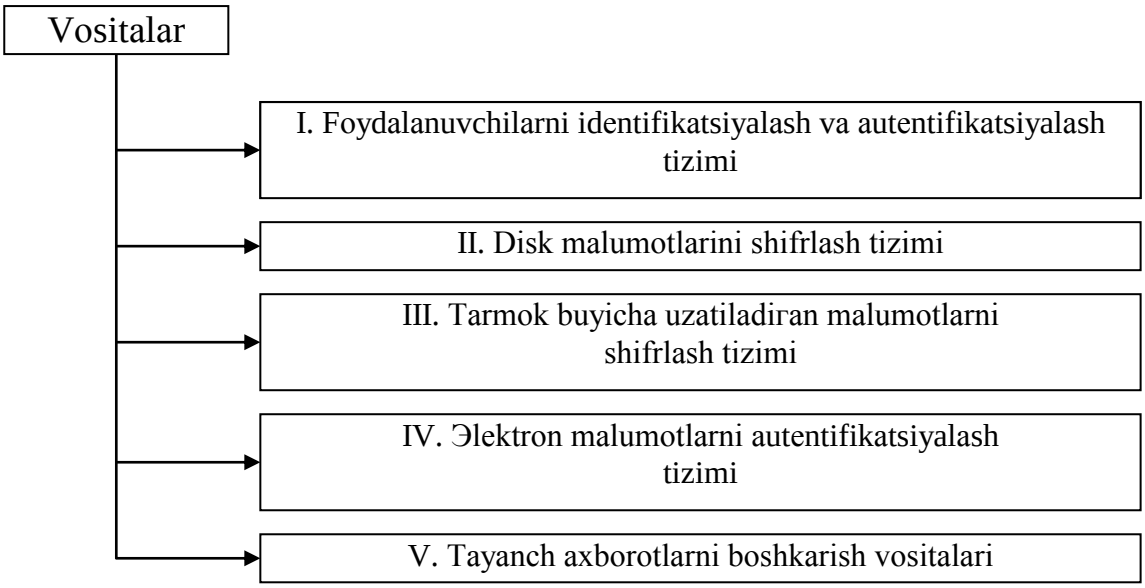
Kriptotizimning mustaxkamligi uning kaliti bilan aniklanadi va bu kriptotahlilning asosiy qoidalaridan biri bo'lib xisoblanadi.

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



Kompyuter ma'lumotlarini ximoyalashning texnik-dasturiy vositalari

Ushbu vositalarni kuyidagicha tasniflash mumkin:



1. ***Foydalanuvchchilarni identifikatsiyalash va autentifikatsiya-lash tizimi.*** Ushbu tizim foydalanuvchidan olingan ma'lumot buyicha uning shaxsini tekshirish, xakikiyligini aniklash va shundan cyng unga tizim bilan ishlashga ruxsat berish lozimligini belgilab beradi.

Bu xolda asosan foydalanuvchidan olinadigan ma'lumotni tanlash muammosi mavjud bulib, uning kuyidagi turlari mavjud:

• foydalanuvchiga ma'lum bulgan maxfiy axborot, masalan, parol, maxfiy kalit va boshkalar;

• shaxsning fiziologik parametrlari, masalan, barmok izlari, kuzning tasviri va boshkalar.

Birinchisi an'anaviy, ikkinchisi esa biometrik identifikatsiyalash tizimi, deyiladi.

II. ***Disk ma'lumotlarini shifrlash tizimi.*** Ushbu tizimning asosiy maksadi diskdagi ma'lumotlarni ximoyalashdir. Bu xolda mantikiy va jismoniy boskichlar ajratiladi. Mantikiy boskichda fayl asosiy ob'ekt sifatida bulib, fakatgina ba'zi bir fayllar ximoyalanadi. Bunga misol kilib, arxivator dasturlarini keltirish mumkin. Jismoniy boskichda disk tulaligicha ximoyalanadi. Bunga misol sifatida Norton Utilities tarkibidagi Diskreet shifrlovchi dasturni keltirish mumkin.

III. ***Tarmok buyicha uzatiladigan ma'lumotlarni shifrlash tizimi.*** Ushbu tizimda ikki yunalishni ajratish mumkin:

• kanal buyicha, ya'ni aloka kanallari buyicha junatiladigan barcha ma'lumotlarni shifrlash;

• abonentlar buyicha, ya'ni aloka kanallari buyicha junatiladigan ma'lumotlarning fakatgina mazmuniy kismi shifrlanib, kolgan xizmatchi ma'lumotlarni ochik koldirish.

IV. ***Elektron malumotlarni autentifikatsiyalash tizimi.*** Ushbu tizimda tarmok buyicha bajariladigan elektron ma’lumotlar almashuvida xujjatni va uning muallifini autentifikatsiyalash muammosi paydo buladi.

V. ***Tayanch axborotlarni boshkarish vositalari.*** Ushbu tizimda tayanch axborotlar sifatida kompyuter tizimi va tarmogida kullaniladigan barcha kriptografik kalitlar tushuniladi. Bu xolda kalitlarni generatsiyalash, saklash va taksimlash kabi boshkaruv funktsiyalarini ajratishadi.

Simmetriyali kriptotizim asoslari

Kriptografiya nuktai – nazaridan shifr — bu kalit demakdir va ochik ma’lumotlar tuplamini yopik (shifrlangan) ma’lumotlarga uzgartirish kriptografiya uzgartirishlar algoritmlari majmuasi xisoblanadi.

Kalit — kriptografiya uzgartirishlar algoritmining ba’zi-bir parametrlarining maxfiy xolati bulib, barcha algoritmlardan yagona variantini tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy kursatkich bulib **kriptomustaxkamlik** xisoblanadi.

Kriptografiya ximoyasida shifrlarga nisbatan kuyidagi talablar kuyiladi:

• etarli darajada kriptomustaxkamlik;
• shifrlash va kaytarish jarayonining oddiyligi;
• axborotlarni shifrlash okibatida ular xajmining ortib ketmasligi;
• shifrlashdagi kichik xatolarga tasirchan bulmasligi.

Ushbu talablarga kuyidagi tizimlar javob beradi:

• urinlarini almashtirish;
• almashtirish;
• gammalashtirish;
• analitik uzgartirish.

Urinlarini almashtirish shifrlash usuli buyicha boshlangich matn belgilarining matnning ma’lum bir kismi doirasida maxsus koidalar yordamida urinlari almashtiriladi.

Almashtirish shifrlash usuli buyicha boshlangich matn belgilari foydalanilayotgan yoki boshka bir alifbo belgilariga almashtirilali.

Gammalashtirish usuli buyicha boshlangich matn belgilari shifrlash gammasi belgilari, ya’ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

Taxliliy uzgartirish usuli buyicha boshlangich matn belgilari analitik formulalar yordamida uzgartiriladi, masalan, vektorni matritsaga kupaytirish yordamida. Bu erda vektor matndagi belgilar ketma-ketligi bulsa, matritsa esa kalit sifatida xizmat kiladi.

Urinlarni almashtirish usullari

Ushbu usul eng oddii va eng kadimiy usuldir. Urinlarni almashtirish usullariga misol sifatida kuyidagilarni keltirish mumkin:

— shifrlovchi jadval;
— sexrli kvadrat.

Shifrlovchi jadval usulida kalit sifatida kuyidagilar kullaniladi:

— jadval ulchovlari;
— suz yoki suzlar ketma-ketligi;
— jadval tarkibi xususiyatlari.

Misol.
Kuyidagi matn berilgan bulsin:

KADRLAR TAYYoRLASh MILLIY DASTURI
Ushbu axborot ustun buyicha ketma – ket jadvalga kiritiladi:

K	L	A	L	I	Y	T
A	A	Y	A	L	D	U
D	R	Yo	Sh	L	A	R
R	T	R	M	I	S	I

Natijada, 4x7 ulchovli jadval tashkil kilinadi.
Endi shifrlangan matn qatorlar buyicha aniklanadi, ya’ni uzimiz uchun 4 tadan belgilarni ajratib yozamiz.

KLAL IYTA AYAL DUDR YoSHLA RRTR MISI

Bu erda kalit sifatida jadval ulchovlari xizmat kiladi.

Sehrli kvadrat deb, katakchalariga 1 dan boshlab sonlar yozilgan, undagi har bir ustun, satr va diagonal buyicha sonlar yigindisi bitga songa teng bo’lgan kvadrat shaklidagi jadvalga aytilali.
Sehrli kvadratga sonlar tartibi bo’yicha belgilar kiritiladi va bu belgilar satrlar bo’yicha o’qilganda matn hosil bo’ladi.
Misol.
4x4 ulchovli sexrli kvadratni olamiz, bu erda sonlarning 880 ta xar xil kombinatsiyasi mavjud. Kuyidagicha ish yuritamiz:

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

Boshlangich matn sifatida kuyidagi matnni olamiz:
DASTURLASH TILLARI
va jadvalga joylashtiramiz:

I	S	A	L
U	T	I	A
SH	R	L	L

T	R	A	D

Shifrlangan matn jadval elementlarini satrlar buyicha ukish natijasida tashkil topadi:

ISAL UTIA SHRLL TRAD

Almashtirish usullari

Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin:

- Tsezar usuli;
- Affin tizimidagi Tsezar usuli;
- Tayanch so’zli Tsezar usuli va boshqalar.

Tsezar usulida almashtiruvchi xarflar k va siljish bilan aniqlanadi. Yuliy Tsezar bevosita k = 3 bulganda ushbu usuldan foylalangan.

k = 3 bo’lganda va alifbodagi harflar m = 26 ta bo’lganda quyidagi jalval hosil qilinadi:

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

Misol.

Matn sifatida KOMPUTER suzini oladigan bulsak, Tsezar usuli natijasida kuyidagi shifrlangan yozuv xosil buladi: NRPSBXWHU.

Tsezar usulining kamchiligi bu bir xil harflarning o’z navbatida, bir xil harflarga almashishidir.

Affin tizimidagi Tsezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo’yicha aniklanadi: at+b (mod m), bu erda a, b - butun sonlar, 0≤a, b<m, EKUB (a,m)=1.

m=26, a=3, b=5 bulganda kuyidagi jadval xosil kilinadi:

T	0	1	2	3	4	5
3t+5	5	8	11	14	17	20

6	7	8	9	10	11	12
23	0	3	6	9	12	15

13	14	15	16	17	18	19
18	21	24	1	4	7	10

20	21	22	23	24	25
13	16	19	22	25	2

Shunga mos ravishda xarflar kuyidagicha almashadi:

A	B	C	D	E	F	G	H
F	I	L	O	R	U	X	A

I	J	K	L	M	N	O	P
D	G	J	M	P	S	V	Y

Q	R	S	T	U	V	W	X
B	E	H	K	N	Q	T	W

Y	Z
Z	C

Natijada yukorida keltirilgan matn kuyidagicha shifrlanadi:

JVPYZNKRE.

Xozirgi vaktda kompyuter tarmoklarida tijorat axborotlari bilan almashishda uchta asosiy algoritmlar, ya’ni DES, CLIPPER va PGP algoritmlari kullanilmokda. DES va CLIPPER algoritmlari integral sxemalarda amalga oshiriladi. DES algoritmining kriptomustaxkamligini kuyidagi mmsol orkali xam baxolash mumkin: 10 mln. AKSh dollari xarajat kilinganda DES shifrlash ochish uchun 21 minut, 100 mln, AKSh dollari xarajat kilinganda esa 2 minut sarflanadi. CLIPPER tizimi SKIPJACK shifrlash algoritmini uz ichiga oladi va bu algoritm DES algoritmidan 16 mln, marta kuchlirokdir.

PGP algoritmi esa 1991 yilda Filipp Tsimmerman (AKSh) tomonidan yozilgan va elektron pochta orkali kuzatiladigan xabarlarni shifrlash uchun ishlatiladigan PGP dasturlar paketi yordamida amalga oshiriladi, FGP dasturiy vositalari Internet tarmogida elektron pochta orkali axborot junatuvchi foydalanuvchilar tomonidan shifrlash maksadida keng foydalanilmokda.

PGP (Pretty Good Privacy) kriptografiya dasturining algoritmi kalitli, ochik va yopik buladi.

Ochik kalit kuyidagicha kurinishni olishi mumkin:

Ushbu ochik kalit bevosita Web saxifalarda yoki elektron pochta orkali ochikchasiga yuborilishi mumkin. Ochik kalitdan foydalangan junatilgan shifrli axborotni axborot yuborilgan manzil egasidan boshka shaxs ukiy olmaydi. PGP orkali shifrlangan axborotlarni ochish uchun, superkompyuterlar ishlatilganda bir asr xam kamlik kilishi mumkin.

Bulardan tashkari, axborotlarni tasvirlarda va tovushlarda yashirish dasturlari xam mavjud. Masalan, S-toots dasturi axborotlarni BMP, GIF, WAV kengaytmali fayllarda saklash uchun kullaniladi.

Kundalik jarayonda foydalanuvchilar ofis dasturlari va arxivatorlarni kullab kelishadi. Arxivatorlar, masalan PkZip dasturida ma’lumotlarni parol yordamida shifrlash mumkin. Ushbu fayllarni ochganda ikkita, ya’ni lugatli va tugridan-tugri usuldan foydalanishadi. Lugatli usulda bevosita maxsus fayldan suzlar parol urniga kuyib tekshiriladi, tugridan-tugri usulda esa bevosita belgilar kombinatsiyasi tuzilib, parol urniga kuyib tekishriladi.

Ofis dasturlari (Word, Excel, Access) orkali ximoyalash umuman taklif etilmaydi. Bu borada mavjud dasturlap Internet da tusiksiz tarkatiladi.

6 – MAVZU: MA’LUMOTLARNING TARKALIB KETISHI VA MA’LUMOTLARGA RUXSATSIZ KIRISH

1. ***Axbopom tizimlarning ta’sirchan kismlari;***
2. ***Elektron pochtaga ruxsatsiz kirish;***
3. ***Ma’lumotlarga ruxsatsiz kirishning dasturiy va texnik vositalari.***

Axbopom tizimlarning ta’sirchan kismlari

Xozirgi vaktlarda mavjud axborot tizimlarida juda katta xajmda maxfiy axborotlar saklanadi va ularni ximoyalash eng dolzarb muammolardan xisoblanadi.

Masalan, birgina AKSh mudofza vazirligida ayni chogda 10000 kompyuter tarmoklari va 1,5 mln kompyuterlarga karashli axborotlarning aksariyat kismi maxfiy ekanligi xammaga ayon. Bu kompyuterlarga 1999 yili 22144 marta turlicha xujumlar uyushtirilgan, ularning 600 tasida Pentagon tizimlarining vaktinchalik ishdan chikishiga olib kelgan, 200 tasida esa maxfiy bulmagan ma’lumotlar bazalariga ruxsatsiz kirilgan va natijada Pentagon 25 milliard AKSh dollari mikdorida iktisodiy zarar kypgan. Bunaka xujumlar 2000 yili 25000 marta amalga oshirilgan. Ularga karshi kurashish uchun Pentagon tomonidan yangi texnologiyalar yaratishga 2002 yili Carnegie Mellon universitetiga 35,5 mln. AKSh dollari mikdorida grant ajratilgan.

Ma’lumotlarga karaganda, xar yili AKSh xukumati kompyuterlariga urtacha xisobda 250—300 ming xujum uyushtiriladi va ulardan **65 %** i muvaffakiyatli amalga oshiriladi.

Zamonaviy avtomatlashtirilgan axborot tizimlari — bu tarakkiyot dasturiy-texnik majmuasidir va ular axborot almashuvini talab etadigan masalalarni echishni ta’minlaydi. Keyingi yillarda foydalanuvchilarning ishini engillashtirish maksadida yangiliklarni tarkatish xizmati USENET-NNTP, multimedia ma’lumotlarini INTERNET-HTTP tarmogi orkati uzatish kabi protokollar keng tarkaldi.

Bu protokollar bir kancha ijobiy imkoniyatlari bilan birga anchagina kamchiliklarga xam ega va bu kamchiliklar tizimning zaxiralariga ruxsatsiz kirishga yul kuyib bermokda.

Axborot tizimlarining asosiy ta’sirchan kismlari kuyidagilar:

• INTERNET tarmogidagi serverlar. Bu serverlar: dasturlar yoki ma’lumotlar fayllarini yuk, kilish orkali, serverlarni xaddan tashkari kup tugallanmagan jarayonlar bilan yuklash orkali: tizim jurnalining keskin tuldirib yuborilishi orkali; brouzer — dasturlarini ishlamay kolishiga olib keluvchi fayllarni nusxalash orkali ishdan chikariladi;

• ma’lumotlarni uzatish kanallari — biror-bir port orkali axborot olish maksadida yashirin kanalni tashkil etuvchi dasturlar yuboriladi;

• ma’lumotlarni tezkor uzatish kanallari — bu kanallar juda kup mikdorda xech kimga kerak bulmagan fayllar bilan yuklanadi va ularning ma’lumot uzatish tezligi susayib ketadi;

• yangiliklarni uzatish kanallari — bu kanallar eskirgan axborot bilan tuldirib tashlanadi yoki bu kanallar umuman yuk kilib tashlanadi;

• axborotlarni uzatish yuli — USENET tarmogida yangiliklar paketining marshruti buziladi;

• JAVA brouzerlari — SUN firmasi yaratgan JAVA tili imkoniyatlaridan foydalanib, appletlar (applets) tashkil etish orkali ma'lumotlarga ruxsatsiz kirish mumkin buladi. JAVA — appletlari tarmokda avtomatik ravishda ishga tushib ketadi va buning natijasida foydalanuvchi biror-bir xujjatni ishlatayotgai paytda xakikatda nima sodir etilishini xech kachon kura bilmaydi, masalan, tarmok viruslarini tashkil etish na JAVA-appletlari orkali viruslarni junatish mumkin buladi yoki foydalanuvchining kredit kartalari rakamlariga egalik kilish imkoniyati vujudga keladi.

AKSh sanoat shpionajiga karshi kurash assotsiatsiyasining tekshirishlariga asosan kompyuter tarmoklari va axborot tizimlariga xujumlar kuyidagicha tasniflanadi: 20% — aralash xujumlar; 40% — ichki xujumlar va 40% — tashki xujumlar.

Juda kup xollarda bunaka xujumlar muvaffakiyatli tashkil etiladi. Masalan, Buyuk Britaniya sanoati, kompyuter jinoyatlari sababli, xar yili 1 mlrd funt sterling zarar kuradi.

Demak, yukorida olib borilgan taxlildan shu narsa kurinadiki, xozirgi paytda kompyuter tarmoklari juda kup ta'sirchan kismlarga ega bulib, ular orkali axborotlarga ruxsatsiz kirishlar amalga oshirilmokda yoki ma'lumotlar bazalari yuk kilib yuborilmokda va buning natijasida insoniyat mlrd-mlrd AKSh dollari mikdorida iktisodiy zarar kurmokda.

Elektron pochtaga ruxsatsiz kirish

Internet tizimidagi elektron pochta juda kup ishlatilayotgan axborot almashish kanallaridan biri xisoblanadi. Elektron pochta yordamida axborot almashuvi tarmokdagi axborot almashuvining 30%ini tashkil etadi. Bunda axborot almashuvi bor-yugi ikkita protokol: SMTP (Simple Mail Transfer Protocol) va ROR-3 (Post Office Rgolosol)larni ishlatish yordamida amalga oshiriladi. ROR-3 multimedia texnologiyalarining rivojini aks ettiradi, SMTP eca Appranet proekti darajasida tashkil etilgan edi. Shuning uchun xam bu protokollarning xammaga ochikligi sababli, elektron pochta resurslariga ruxsatsiz kirishga imkoniyatlar yaratilib berilmokda:

- SMTP server — dasturlarining nokorrekt urnatilishi tufayli bu serverlardan ruxsatsiz foydalanilmokda va bu texnologiya «spama» texnologiyasi nomi bilan ma'lum;

- elektron pochta xabarlariga ruxsatsiz egalik kilish uchun oddiygina va samarali usullardan foydalanilmokda, ya'ni kuyi katlamlarda vinchesterdagi ma'lumotlarni ukish, pochta resurslariga kirish parolini ukib olish va xokazolar.

Ma’lumotlarga ruxsatsiz kirishning dasturiy va texnik vositalari

Ma’lumki, xisoblash texnikasi vositalari ishi elektromagnit nurlanishi orkali bajariladi, bu esa, uz navbatida, ma’lumotlarni tarkatish uchun zarur bulgan signallarning zaxirasidir. Bunday kismlarga kompyuterlarning platalari, elektron ta’minot manbalari, printerlar, plotterlar, aloka apparatlari va x.k. kiradi. Lekin, statistik ma’lumotlardan asosiy yukori chastotali elektromagnit nurlanish manbai sifatida displeyning rol uynashi ma’lum buldi. Bu displeylarda elektron nurli trubkalar urnatilgan buladi. Displey ekranida tasvir xuddi televizordagidek tashkil etiladi. Bu esa videosignallarga egalik kilish va uz navbatida, axborotlarga egalik kilish imkoniyatini yaratadi. Displey ekranidagi kursatuv nusxasi televizorda xosil buladi.

Yukorida keltirilgan kompyuter kismlaridan boshka axborotlarga egalik kilish maksadida tarmok kabellari xamda serverlardan xam foydalanilmokda.

Kompyuter tizimlari zaxiralariga ruxsatsiz kirish sifatida mazkur tizim malumotlaridan foydalanish, ularni uzgartirish va uchirib tashlash xarakatlari tushuniladi.

Agar kompyuter tizimlari ruxsatsiz kirishdan ximoyalanish mexanizmlariga ega bulsa, u xolda ruxsatsiz kirish xarakatlari kuyidagicha tashkil etiladi:

- ximoyalash mexanizmini olib tashlash yoki kurinishini uzgartirish:
- tizimga biror-bir foydalanuvchining nomi va paroli bilan kirish.

Agar birinchi xolda dasturning uzgartirilishi yoki tizim surovlarining uztartirilishi talab etilsa, ikkinchi xolda esa mavjud foydalanuvchining parolini klaviatura orkali kiritayotgan paytda kurib olish va undan foydalanish orkali ruxsatsiz kirish amalga oshiriladi.

Ma’lumotlarga ruxsatsiz egalik kilish uchun zarur bulgan dasturlarni tatbik etish usullari kuyidagilardir:

• kompyuter tizimlari zaxiralariga ruxsatsiz egalik kilish;

• kompyuter tarmogi aloka kanallaridagi xabar almashuvi jarayoniga ruxsatsiz aralashuv;

• virus kurinishidagi dasturiy kamchiliklar (defektlar)ni kiritish.

Kupincha kompyuter tizimida mavjud zaif kismlarni «teshik»lar, «lyuk»lar deb atashadi. Bazan dasturchilarning uzi dastur tuzish paytida bu «tushik»larni koldirishadi, masalan:

— natijaviy dasturiy maxsulotni engil yigish maksadida;

— dastur tayyor bulgandan keyin yashirincha dasturga kirish vositasiga ega bulish maksadida.

Mavjud «teshik»ka zaruriy buyruklap kuyiladi va bu buruklar kerakli paytda uz ishini bajarib boradi. Virus kurinishidagi dasturlar esa ma’lumotlarni yukotish yoki kisman uzgartirish, ish seanslarini buzish uchun ishlatiladi.

Yukorida keltirilganlardan xulosa kilib, ma’lumotlarga ruxsatsiz egalik kilish uchun dasturiy moslamalar eng kuchli va samarali instrument bulib, kompyuter axborot zaxiralariga katta xavf tugdirishi va bularga karshi kurash eng dolzarb muammolardan biri ekanligini ta’kidlash mumkin.

7 – MAVZU: KOMPYUTER TARMOKLARIDA MA'LUMOTLARNING TARKALISH KANALLARI

1. Kompyuter tormoklarining zaif kismlari. Tarmok ximoyasini tashkil kilish asoslari;

2. ***Kompyuter telefoniyasidagi ximoyalash usullari.***

Kompyuter tormoklarining zaif kismlari. Tarmok ximoyasini tashkil kilish asoslari

Xozirgi vaktda lokal xisoblash tarmokari (LAN) va global xisoblash tarmoklari (WAN) orasidagi farklar yukolib bormokda. Masalan, Netware 4x yoki Vines 4.11. operatsion tizimlari LANning faoliyatini xududiy darajasiga chikarmokda. Bu esa, ya'ni LAN imkoniyatlarining ortishi, ma'lumotlarni ximoyalash usullarini yanada takomillashtirishni talab kilmokda.

Ximoyalash vositalarini tashkil etishda kuyidagilarni e'tiborga olish lozim:

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

• foydalanuvchiga zarur bulgan ma'lumotlarning tarmokda mavjudligi:

• tarmoklarda turli firmalar ishlab chikargan shaxsiy kompyuterlarning ishlatilishi;

• tarmok tizimida turli dasturlarning ishlatish imkoniyati;

• tarmok 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;

• tarmokka bir kancha tizimlarning kushilishi;

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

• xujum nuktalarining kupligi;

• tizimga kirishni nazorat kilishning kiyinligi.

Tarmokni ximoyalash zarurligi kuyidagi xollardan kelib chikadi:

• boshka foydalanuvchilar massivlarini ukish;

• kompyuter xotirasida kolib ketgan ma'lumotlarni ukish;

• ximoya choralarini aylanib utib, ma'lumot tashuvchilarni nusxalash;

• foydalanuvchi sifatida yashirincha ishlash;

• dasturiy tutgichlarni ishlatish;

• dasturlash tillarining kamchiliklaridan foylalanish;

• ximoya vositalarini bilib turib ishdan chikarish;

• kompyuter viruslarini kiritish va ishlatish.

Tarmok, muxofazasini tashkil etishda kuyidagilarni e'tiborga olish lozim:

- muxofaza tizimining nazorati;
- fayllarga kirishning nazorati;

- tarmokda ma’lumot uzatishning nazorati;
- axborot zaxiralariga kirishning nazorati;
- tarmok bilan ulangan boshka tapmoklapga ma’lumot tarkalishining nazorati.

Maxfiy axborotni kayta ishlash uchun kerakli tekshiruvdan utgan kompyuterlarni ishlatish lozim buladi. Muxofaza vositalarining funktsional tulik bulishi muxim xisoblanadi. 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.

Tarmok, 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 xollarni tezda aniklash.

Ma’lumotlarni tarmokda uzatish paytida kriptografik ximoyalash usullaridan foydalaniladi, Kayd etish jurnaliga ruxsat etilmagan kirishlar amalga oshirilganligi xakida ma’lumotlar yozilib turilishi kerak. Bu jurnalga kirishni chegaralash xam ximoya 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 tarmokda nazoratni olib borishni kiyinlashtiradi.

Xozirgi 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 etarli darajada muxofazani ta’minlay olishi mumkin.

Kompyuter telefoniyasidagi ximoyalash 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.

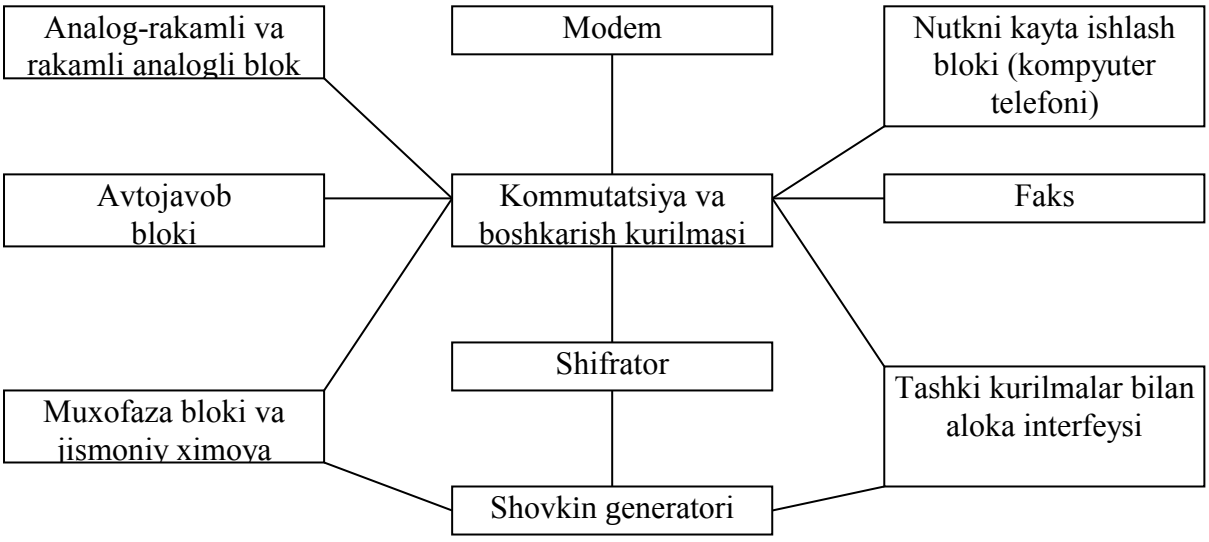
Bor-yugi un yil ilgari sotuvga CANON firmasining narxi 6000 AKSh dollari bulgan «Navigator» nomli maxsuloti chikarilgan edi va u birinchi tizimlardan xisoblanadi.

Kompyuter tslefoniyasi un yil ichida juda tez sur'atlar bilan rivojlandi. Xozirgi 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 AKSh dollari turadi. Keyingi paytlarda kompyuter telefoniyasi yunalishida 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 ximoyasini etarli darajada ta'minlash uchun Pretty Good Privacy Inc. firmasining PC Phone 1.0 dasturiy paket ishlab chikarilgan. U kompyuter telefoniyasi orkali uzatilayottan axborotlarni ximoyalash 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 $10^{-8} – 10^{-12}$).

Zamonaviy kompyuter telefoniyasi kurilmasi chizmasi kuyidagicha:



Kompyuter telefoniyasi kurilmalari kuyidagi imkoniyatlarga ega:

Kurilmalar	**Imkoniyatlar**
Kompyuter telefoni	Nutkli xabarni yozib olish va saklash, xabarlarni kayd kilish, kodni aniklab olish, kayta ulanish, xabarlarni uzatish
Shifrator	Ma'lumotlarni ximoyalash, ma'lumotlarni anikligini saklash, ma'lumotlarga kirishni chegaralash

Modem	Abonentni kayta tekshirish, xatoni tuzatish
Faks	Kriptoximoya, uzatilayotgan axborotni kisish, avtokayd etish va uzatish
Avtojavob kurilmasi	Kayd etish jurnaliga avtomatik ravishda kayd kilish, abonentni teskari aloka bilan tekshirish, tayyor kilib kuyilgan nutkli xabarlarni uzatish, kiritilayotgan xabarlarni yozib olish
Ximoya kurilmasi	Tashki datchiklardan signallar olish, xotiradagi rakamlarni avtomatik terish, ruxsatsiz alokalar xakida nutkli xabar berish, tashki kurilmalarni ulab beri shva x.k.

8 – MAVZU: KOMPYUTER TARMOKLARIDA ZAMONAVIY XIMOYALASh USULLARI VA VOSITALARI

1. Kompyuter tarmoklarida ximoyani ta'minlash usullari;

2. EXM ximoyasini ta'minlashning texnik vositalari;

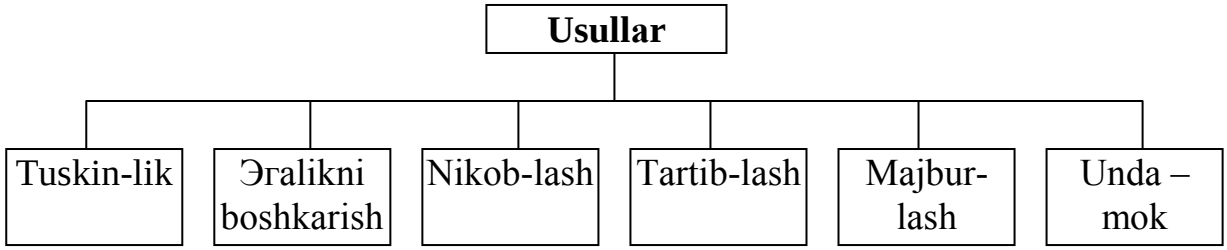
3. Kompyuter tarmoklarida ma'lumotlarni ximoyalashning asosiy yunalishlari;

4. Internet mapmogida mavjud alokaning ximoyasini (xavfsizligini) ta'minlash asoslari.

Kompyuter tarmoklarida ximoyani ta'minlash usullari

Kompyuter tarmoklarida axborotni ximoyalash deb foydalanuvchilarni ruxsatsiz tarmok, 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 funktsiyalardan 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;

• ximoyalangan zaxiralarga kilingan murojaatlarni kayd kilish;

• ruxsatsiz xarakatlarga javob berish, masalan, signal berish, uchirib kuyish surovnomani bajarishdan voz kechish va boshkalar.

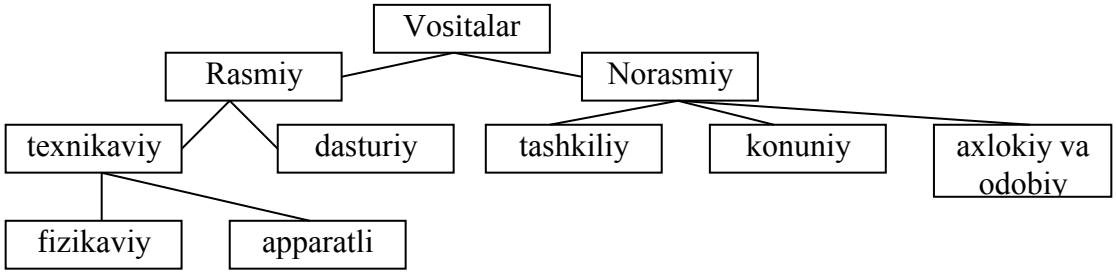
Nikoblash – ma’lumotlarni ukib olishni kiyinlashtirish maksadida ularni kriptografiya orkali kodlash.

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 ximoyalash funktsiyalarini 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 ximoyalash funktsiyalarini bajarish uchun muljallangan maxsus dasturiy ta’minotdir.

Axborotlarni ximoyalashda birinchi navbatda eng keng kullanilgan dasturiy vositalar xozirgi kunda ikkinchi darajali ximoya vositasi xisoblanadi. Bunga misol sifatida parol tizimini keltirish mumkin.

Tashkiliy ximoyalash 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 ximoyalash vositalari — bu xisoblash texnikasini rivojlanishi okibatida paydo buladigan tartib va kelishuvlardir. Ushbu tartiblar konun darajasida bulmasada, uni tan olmaslik foydalanuvchilarni obrusiga ziyon etkazishi mumkin.

Konuniy ximoyalash 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 ximoyalash 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 yunalishlar buyicha rivojlanishi; 3) ushbu boskichda kuyidagi yunalishlar buyicha rivojlanishlar kuzatilmokda:

- ximoyalash funktsiyalarini apparatli amalga oshirish;
- bir necha ximoyalash funktsiyalarini kamrab olgan vositalarni yaratish;
- algoritm va texnikaviy vositalarni umumlashtirish va standartlash.

Xozirgi kunda ma’lumotlarni ruxsatsiz chetga chikib ketish yullari kuyidagilardan iborat:

• elektron nurlarni chetdan turib ukib olish;
• aloka kabellarini elektromagnit tulkinlar bilan nurlatish;
• yashirin tinglash kurilmalarini kullash;
• masofadan rasmga tushirish;
• printerdan chikadigan akustik tulkinlarni ukib olish;
• ma’lumot tashuvchilarni va ishlab chikarish chikindilarini ugirlash;
• tizim xotirasida saklanib kolgan ma’lumotlarni ukib olish;
• ximoyani engib ma’lumotlarni nusxalash;
• kayd kilingan foydalanuvchi nikobida tizimga kirshi;
• dasturiy tuzoklarni kullash;
• dasturlash tillari va operatsion tizimlarning kamchiliklaridan foylalanish;
• dasturlarda maxsus belgilangan sharoitlarda ishga tushishi mumkin bulgan kism dasturlarning mavjud bulishi;
• aloka va apparatlarga nokonuniy ulanish;
• ximoyalash vositalarini kasddan ishdan chikarish;
• kompyuter viruslarini tizimga kiritish va undan foydalanish.

Ushbu yullardan deyarli barchasining oldini olish mumkin, lekin kompyuter viruslaridan xozirgacha konikarli ximoya vositalari ishlab chikilmagan.

Bevosita tarmok buyicha uzatiladigan ma'lumotlarni ximoyalash maksadida kuyidagi tadbirlarni bajarish lozim buladi:

- uzatiladigan ma'lumotlarni ochib ukishdan saklanish;
- uzatiladigan ma'lumotlarni taxtil kilihdan 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 ximoyasini 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 xisoblash tarmoklarida foydalanuvchi istalgan ishchi urindan tarmokda 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 xisoblash tarmoklarida kamchiliklar mavjudligini boshka xodimlardan yashirish xisoblanadi.

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 ximoyalash instrumental vositalari ishlab chikilgan. Ular dasturiy, dasturiy-texnik va texnik vositalardir.

Xozirgi kunda tarmok xavfsizligini ta’minlash maksadida ishlab chikilgan texnikaviy vositalarni kuyidagicha tasniflash mumkin:

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

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

Tarmoklararo ekranlar va shlyuzlar — tizimga keladigan xamda undan chikadigan ma’lumotlarni ma’lum xujumlar 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 tarmokning 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 ximoyaning 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.

Tarmokning zaifligini aniklash — tarmok zaxiralariga sun’iy xujumlarni 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 tarmokning zaif tomonlarini aniklaydi va ularni bartaraf etish yullarini kursatib beradi. Ushbu yunalish 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 ximoyalashda kullaniladi;

• Free Space Communication System — tarmokda 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 tarmoklarida ma'lumotlarni ximoyalashning asosiy yunalishlari

Axborotlarni ximoyalashning mavjud usul va vositalari xamda kompyuter tarmoklari 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 ximoyaning xamma asosiy usullari va vositalari intensiv rivojlanishi bilan xarakterlandi, uchinchi boskichida esa kuyidagi tendentsiyalar ravshan bulmokda:

- axborotlarni ximoyalash asosiy funktsiyalarining texnik jixatdan amalga oshirilishi;

- bir nechta xavfsizlik funktsiyalarini bajaruvchi ximoyalashning birgalikdagi vositalarini yaratish:

- algoritm va texnik vositalarni unifikatsiya kilish va standartlashtirish.

Kompyuter tarmoklarida xavfsizlikni taminlashda xujumlar 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 utkazib turish xam katta axamiyatga ega.

Internet mapmogida mavjud alokaning ximoyasini (xavfsizligini) ta'minlash asoslari

Ma'lumotlarni uzatish tizimlarining rivojlanishi va ular asosida yaratilgan telekommunikatsiya xizmat kursatish vositalarining yaratilishi bevosita foydalanuvchilarga tarmok zaxiralaridan foydalanish tartiblarini ishlab chikarish zaruriyatini paydo kildi:

• foydalanuvchining anonimligini ta'minlovchi vositalar;

• serverga kirishni ta'minlash. Server fakatgina bitta foydalanuvchiga emas, balki keng mikyosdagi foydalanuvchilarga uz zaxiralaridan foydalanishga ruxsat berishi kerak;

• ruxsatsiz kirishdan tarmokni ximoyalash vositalari.

Internet tarmogida ruxsatsiz kirishni takiklovchi tarmoklararo ekran — Fire Wall vositalari keng tarkalgan. Ushbu vosita asosan UNIX operatsion tizimlarida kuldanilib, bevosita tarmoklar orasida aloka urnatish jarayonida xavfsizlikni ta'minlaydi. Bundan tashkari, Fire Wall tizimlari tashki muxit, masalan, Internet

uchun, asosiy ma’lumotlarni va MBlarini xotirasida saklab, bevosita malumot almashuvini ta’minlashi va korxona tizimiga kirishini takiklashi mumkin.

Lekin Fire Wall tizimlarining kamchiliklari xam mavjud, masalan, E-mail orkali dasturlar junatilib, ichki tizimga tushgandan sung uzining kora niyatlarini bajarishida ushbu ximoya ojizlik kiladi.

Fire Wall sinfidagi tizimlarning asosiy kismi tashki xujumlarni kaytarish uchun muljallangan bulsa xam, xujumlar ularning 60 foizi kuchsiz ekanligini kursatdi. Bundan tashkari, Fire Wall zabt etilgan serverning ishlashiga karshilik kursata olmaydi.

Shu bois, Internet tizimida xavfsizlikni ta’minlash buiicha kuyidagi uzgarishlar kutilmokda:

• Fire Wall tizimlarining bevosita xavfsizlik tizimlariga kiritilishi;

• tarmok protokollari bsvosita foydalanuvchilarni xukuklarini aniklovchi, xabarlarning yaxlitligini ta’minlovchi va ma’lumotlarni shifrlovchi dasturiy imkoniyatlaridan iborat bulishlari. Xozirgi kunda ushbu protokollarni yaratish buyicha anchagina ishlar olib borilmokda. SKIP protokoli (Simple Key management for Internet Protocol — Internet protokollari uchun kriptokalitlarning oddiy boshkaruvi) shunga misol bula oladi.

9 – MAVZU: INTERNETDA AXBOROTLAR XAVFSIZLIGINI TA’MINLASh ASOSLARI

1. Internetda pyxcamciz kirish usullarining tasnifi;
2. ***Ruxsat etilgan manzillarning ruxsat etilmagan vaktda ulanishi;***
3. Tarmoklararo ekran va uning vazifalari;
4. Tarmoklararo ekranning asosiy komponentlari.

Internetda pyxcamciz kirish usullarining tasnifi

Global tarmoklarning rivojlanishi va axborotlarni olish, kayta ishlash va uzatishning yangi texnologiyalari paydo bulishi bilan Internet tarmogiga xar xil shaxs va tashkilotlarning e’tibori karatildi. Kuplab tashkilotlar uz lokal tarmoklarini global tarmoklarga ulashga karor kilishgan va xozirgi paytda WWW, FTP, Gophes va boshka serverlardan foydalanishmokda. Tijorat maksadida ishlatiluvchi yoki davlat siri bulgan axborotlarning global tarmoklar buyicha joylarga uzatish imkoni paydo buldi va uz navbatida, shu axborotlarni ximoyalash tizimida malakali mutaxassislarga extiyoj tugilmokda.

Global tarmoklardan foydalanish bu fakatgina «kizikarli» axborotlarni izlash emas, balki tijorat maksadida va boshka axamiyatga molik ishlarni bajarishdan iborat. Bunday faoliyat vaktida axborotlarni ximoyalash vositalarining yukligi tufayli kuplab talofotlarga duch kelish mumkin.

Xar kanday tashkilot Intenetga ulanganidan sung, xosil buladigan kuyidagi muammolarni xal etishlari shart:

• tashkilotning kompyuter tizimini xakerlar tomonidan buzilishi:

• Internet orkali junatilgan ma’lumotlarning yovuz niyatli shaxslar tomonidan ukib olinishi;

• tashkilot faoliyatiga zarar etkazilishi.

Internet loyixalash davrida bevosita ximoyalangan tarmok sifatida ishlab chikilmagan. Bu soxada xozirgi kunda mavjud bulgan kuyidagi muammolarni keltirish mumkin:

• ma’lumotlarni engillik bilan kulga kiritish;

• tarmokdagi kompyuterlar manzilini soxtalashtirish;

• TCP/IP vositalarining zaifligi;

• kupchilik saytlarning notugri konfiguratsiyalanishi;

• konfiguratsiyalashning murakkabligi.

Global tarmoklarning chegarasiz keng rivojlanishi undan foydalanuvchilar sonining oshib borishiga sabab bulmokda, bu esa uz navbatida axborotlar xavfsizligiga taxdid solish extimolining oshishiga olib kelmokda. Uzok, masofalar bilan axborot almashish zaruriyati axborotlarni olishning kat’iy chegaralanishini talab etadi. Shu maksadda tarmoklarning segmentlarini xap xil darajadagi ximoyalash usullari taklif etilgan:

• erkin kirish (masalan: WWW-server);

• chegaralangan kirishlar segmenti (uzok masofada joylashgan ish joyiga xizmatchilarning kirishi);

• ixtiyoriy kirishlarni man etish (masalan, tashkilotlarning moliyaviy lokal tarmoklari).

Internet global axborot tarmogi uzida nixoyatda katta xajmga ega bulgan axborot resurslaridan milliy iktisodning turli tarmoklarida samarali foydanishga imkoniyat tugdirishiga karamasdan axborotlarga bulgan xavfsizlik darajasini oshirmokda. Shuning uchun xam Internetga ulangan xar bir korxona uzining axborot xavfsizligini ta’minlash masalalariga katta e’tibor berishi kerak. Ushbu tarmokda axborotlar xavfsizligining yulga kuyilishi yondashuvi kuyida keltirilgan:

Lokal tarmoklarning global tarmokarga kushilishi uchun tarmoklar ximoyasi administratori kuyidagi masalalarni xal kilishi lozim:

— lokal tarmoklarga global tarmok, tomonidan mavjud xavflarga nisbatan ximoyaning yaratilishi;

— global tarmok fondalanuvchisi uchun axborotlarni yashirish imkoniyatining yaratilishi;

Bunda kuyidagi usullar mavjud:

— kirish mumkin bulmagan tarmok manzili orkali;

— Ping dasturi yordamida tarmok paketlarini tuldirish;

— ruxsat etilgan tarmok manzili bilan takiklangan tarmok manzili buyicha birlashtirish;

— ta’kiklangan tarmok protakoli buyicha birlashtirish;

— tarmok buyicha foydalanuvchiga parol tanlash;

— REDIREST turidagi ICMP paketi yordamida marshrutlar jadvalini modifikatsiyalash;

— RIR standart bulmagan paketi yordamida marshrutlar jadvalini uzgartirish;

— DNS spoofingdan foydalangan xolda ulanish.

Ruxsat etilgan manzillarning ruxsat etilmagan vaktda ulanishi

Ushbu xavf global tarmoklarning bir kancha soxalarini kamrab oladi, jumladan:

• lokal soxa;

• lokal-global tarmoklarning birlashuvi;

• muxim axborotlarni global tarmoklarda junatish;

• global tarmokning boshkarilmaydigan kismi.

Ixtiyoriy axborot tarmoklarining asosiy komponentlari bu serverlar va ishchi stantsiyalar xisoblanadi. Serverda axborotlar yoki xisoblash resurslari va ishchi stantsiyalarda xizmatchilar ishlaydi. Umuman ixtiyoriy kompyuter xam,

server xam ishchi stantsiya bulishi mumkin — bu xolda ularga nisbatan xavfli xujumlar bulishi extimoli bor.

Global tarmoq maydonlaridagi taxdid

Taxdid	Lokal maydon	LT/GT birlashuvi	GT administrator maydoni	GT boshkarilmaydigan maydoni
Tarmoklarning notugri manzili			+	+
Paketlar bilan tuldirish	+			+
Mumkin bulmagan ulanish		+		+
Mumkin bulgan ulanish	+	+		+
Parolni tanlash	+	+		+
ICMP xujumi	+	+	+	
RIP xujumi		+	+	
Ruxsatsiz uzokdan boshkarish		+	+	+
Parolni uzgartirish	+			+
DNS xujumi		+	+	
Mumkin bulmagan vaktda	+	+	+	+

Serverlarning asosiy vazifasi axorotlarni saklash va takdim kilishdan iborat.

Yovuz niyatli shaxslarni kuyidagicha tasniflash mumkin:

• axborot olishga imkoniyat olish;

• xizmatlarga ruxsat etilmagan imkoniyat olish;

• ma’lum sinfdagi xizmatlarning ish rejimini ishdan chikarishga urinish;

• axborotlarni uzgartirishga xarakat yoki boshka turdagi xujumlar.

Uz navbatida, xozirgi zamonaviy rivojlanish davomida servis xizmatini izdan chikarishga karshi kurash muammosi muxim axamiyat kasb etadi. Bu xildagi xujumlar «servisdagi buzilish» nomini olgan.

Ishchi stantsiyalarga xujumning asosiy maqsadi, asosan, qayta ishlanayotgan ma’lumotlarni yoki lokal saqlanayotgan axborotlarni olishdir. Bunday xujumlarning asosiy vositasi «Troyan» dasturlar sanaladi. Bu dastur o’z tuzilishi buyicha kompyuter viruslaridan farq qilmaydi va kompyuterga tushishi bilan o’zini bilintirmasdan turadi. Boshqacha aytganda, bu dasturning asosiy maqsadi — tarmoq, stantsiyasidagi ximoya tizimini ichki tomondan buzishdan iborat.

Bu xolatda masalani xal qilish ma’lum qiyinchilikka olib keladi, ya’ni maxsus tayyorlangan mutaxassis lozim yoki boshqa choralar qabul qilish kerak bo’ladi. Boshqa bir oddiy ximoya usullaridan biri xar qaysi ishchi stantsiyadagi tizimli fayllar va xizmat soxasidagi ma’lumotlarning uzgarishini tekshirib turuvchi revizor (ingl. ***advizer***— kiruvchi) urnatish sanaladi.

Tarmoklararo ekran va uning vazifalari

Tarmoklararo ekran — ximoyalash vositasi bulib, ishonchli tarmok, va ishonchsiz tarmok orasida ma’lumotlarga kirishni boshkarishda kullaniladi.

Tarmoklararo ekran kup komponentli bulib, u Internetdan tashkilotning axborot zaxiralarini ximoyalash strategiyasi sanaladi. Ya'ni tashkilot tarmogi va Internet orasida kuriklash vazifasini bajaradi.

Tarmoklararo ekranning asosiy funktsiyasi — ma'lumotlarga egalik kilishni markazlashtirilgan boshkaruvini ta'minlashdan iborat.

Tarmoklararo ekran kuyidagi ximoyalarni amalga oshiradi:

• urinsiz trafiklar, ya'ni tarmokda uzatiladigan xabarlar okimini takiklash;

• kabul kilingan trafikni ichki tizimlarga yunaltirish;

• ichki tizimning zaif kismlarini yashirish bilan Internet tomonidan uyushtiriladigan xujumlardan ximoyalash;

• barcha trafiklarni bayonlashtirish;

• ichki ma'lumotlarni, masalan tarmok topologiyasini, tizim nomlarini, tarmok uskunalarini va foydalanuvchilarning identifikatorlarini Internetdan yashirish;

• ishonchli autentifikatsiyani taminlash.

Kupgina adabiyotlarda **tarmoklararo ekran** tushunchasi **brandmauer** yoki **Fire Wall** deb yuritilgan. Umuman bularning xammasi yagona tushunchadir.

Tarmoklararo ekran — bu tizim, umumiy tarmokni ikki kismga ajratib, tarmoklararo ximoya vazifasini utaydi va ma'lumotlar paketining chegaradan utish shartlarini amalga oshiradigan koidalar tuplami xisoblanadi.

Odatda tarmoklararo ekran ichki tarmoklarni global tarmoklardan, ya'ni Internetdan ximoya kiladi. Shuni aytish kerakki, tarmoklararo ekran nafakat Internetdan, balki korporativ tarmoklardan xam ximoya kilish kobiliyatiga egadir. Xar kanday tarmoklararo ekran ichki tarmoklarni tulik ximoya kila oladi deb bulmaydi.

Internet xizmati va xamma protokollarning amaliy jixatdan axborotlarga nisbatan ximoyasining tulik bulmaganligi muammosi bor. Bu muammolar kelib chikishining asosiy sababi Internetning UNIX operatsion tizim bilan borlikligida.

TCR/IR (Transtnission Control Protokol/lnternet Protocol) Internetning global tarmogida kommunikatsiyani ta'minlaydi va tarmoklarda ommaviy ravishda kullaniladi, lekin ular xam ximoyani etarlicha ta'minlay olmaydi, chunki TCP/IP paketining boshida xaker xujumi uchun kulay ma'lumot kursatiladi.

Internetda elektron pochtani junatishni oddiy protokol pochta transport xizmati amalga oshiradi (SMTP - Simple Mail Transfer Protocol). Bu protokolda mavjud bulgan ximoyalashning muxim muammolaridan biri - foydalanuvchi junatuvchining maizilini kura olmasligidir. Bundan foydalanib xaker katta mikdorda pochta xabarlarini junatishi mumkin, bu esa ishchi pochta serverni xaddan tashkari band bulishiga olib keladi.

Internetda ommaviy tus olgan dastur bu Sendmail elektron pochtasidir. Sendmail tomonidan junatilgan xabarlar boskinchi xaker axborot shaklida foydalanishi mumkin.

Tarmok nomlari xizmati (Domain Name System — DNS) foydalanuvchilar nomi va xost-kompyuterini - manzilini kursatadi. DNS kompaniyaning tarmok

tuzilishi xakida ma’lumotlarni saklaydi. DNSning muammolaridan biri shundaki, bundagi ma’lumotlar bazasini mualliflashtirilmagan foylalanuvchilardan yashirish ancha kiyin. Buning natijasida, xakerlar DNS ni kupincha xost-kompyuterlarning ishonchli nomlari xakida ma’lumotlar manbasidan foydalanish uchun ishlatishi mumkin.

Uzok, terminallar emulyatsiyasi ximati uzok, tizimlarni bir-biriga ulash uchun xizmat kiladi. Bu serverdan foydalanuvchilar TELNET serveridan ruyxatdan utish va uz nomi va parolini olishi lozim. TELNET serveriga ulangan xaker dasturni shunday urnatishi mumkinki, buning natijasida u foydalanuvchining nomi va parolini yozib olish imkoniga ega buladi.

World Wide Web — WWW bu tizim Internet yoki intratarmoklardagi xar xil serverlar ichidagi ma’lumotlarni kurish uchun xizmat kiladi. WWW ning acosiy xossalaridan biri — Tarmoklararo ekran orkali anik protokol va manzillarni filtrlash zarurligini tarmokning ximoyalash siyosati karori bilan xal etilishidir.

Xar kanday tashkilotning **tarmok xavsizligi siyosati** ikki kismdan iborat buladi: tarmok servislaridan foydalanish; tarmoklararo ekranni kullash.

Tarmok servislaridan foydalanish siyosatiga mos ravishda Internetda servislar ruyxati aniklanadi. Bu servislapga foydalanuvchilar cheklangan kirish bilan ta’minlanadi.

Kirish usullarining cheklanilishi — foydalanuvchilar tomonidan Internet servislariga chet yullar orkali ruxsatsiz kirishni takiklash ma’nosini bildiradi.

Tarmok servislariga kirish siyosati, odatda, kuyidagi printsiplarga moyil buladi:

- Internetdan ichki tarmokka kirishni takiklash, lekin ichki tarmokdan Inlernetga kirishga ruxsat berish;
- vakolatlangan tizimlarga Internetdan ichki tarmokka cheklanilgan kirishga ruxsat berish.

Tarmoklararo ekranlarga kuyiladigan vazifaviy talablar kuyidagilardan iborat.

- tarmok darajasida filtrlashga talab;
- amaliy darajada filtrlashga talab;
- administratsiyalash va filtrlash koidalarini urnatish buyicha talab;
- tarmokli autentifikatsiyalash vositalariga talab;
- ishlarni kayd kilish va xisobni olib borish buyicha talab.

Tarmoklararo ekranning asosiy komponentlari

Tarmoklararo ekranlarning komponentlari sifatida kuyidagilarni keltirish mumkin: filtrlovchi -yullovchi; tarmok, darajasidagi shlyuzlar; amaliy darajadagi shlyuzlar.

Filtrlovchi-yullovchi — yullovchi, ya’ni kompyuter tarmogida ma’lumotlarni manzilga etkazuvchi dasturlar paketi yoki serverdagi dastur bulib, u kiradigan va chikadigan paketlarni filtrlaydi. Paketlarni filtrlash, ya’ni ularni anik tuplamga tegishliligini tekshirish, TCP/IP sarlavxasidagi ma’lumotlar buyicha amalga oshiriladi.

Filtrlashni anik xost-kompyuter, ya’ni tarmokdagi fayl va kompyuter zaxiralariga kirishni amalga oshiruvchi kompyuter yoki port, ya’ni xabarlarni junatish yoki kabul kilish maksadida mijoz va server tomonidan ishlatiladigan va odatda 16 bitli son bilan nomlanadigan dastur bilan ulanishda amalga oshirish mumkin. Masalan, foydalanuvchiga keraksiz yoki ishonchsiz xost-kompyuter va tarmoklar bilan ulanishda takiklash.

Filtrlash koidalarini ifodalash kiyin jarayon bulib, ularni testlash vositalari mavjud emas.

Birinchi koida buyicha, Internetdan keladigan TCP paketi junatuvchining porti 1023 dan katta bulsa, 123.4.5.6 manzilli kabul kiluvchiga 23-portga utkaziladi (23-port TELNET serveri bilan boglangan).

Ikkinchi koida xam xuddi shunday bulib, fakatgina 25-port SMTP bilan boglangan.

Tarmok darajasidagi shlyuzlar ishonchli mijozlardan anik xizmatlarga surovnomasini kabul kiladi va ushbu alokaning konuniyligini tekshirgandan sung ularni tashki xost-kompyuter bilan ulaydi. Shundan sung shlyuz ikkala tomonga xam paketlarni fil’trlamay junatadi.

Bundan tashkari, tarmok darajasida shlyuzlar bevosiga **server-dallol** vazifasini bajaradi. Ya’ni, ichki tarmokdan keladigan IP manzillar uzgartirilib, tashkiriga fakatgina bitta IP manzil uzatiladi. Natijada, ichki tarmokdan tashki tarmok bilan tugridan-tugri boglamaydi va shu yul bilan ichki tarmokni ximoyalash vazifasini utaydi.

Amaliy darajadagi shlyuzlar filtrlovchi-yullovchilarga mansub bulgan kamchiliklarni bartaraf etish maksadida ishlab chikilgan. Ushbu dasturiy vosita **vakolatlangan server,** deb nomlanadi va u bajarilayotgan xost-kompyuter esa amaliy darajadagi shlyuz deb ataladi.

Amaliy darajadagi shlyuzlar mijoz va tashki xost-kompyuter bilan tugridan-tugri aloka urnatishga yul kuymaydi. Shlyuz keladigan va junatiladigan paketlarni amaliy darajada filtrlaydi. Server-dallollap shlyuz orkali anik server tomonidan ishlab chikilgan ma’lumotlarni kaytadan yunaltiradi.

Amaliy darajadagi shlyuzlar nafakat paketlarni filtrlash, balki serverning barcha ishlarini kayd kilish va tarmok adminstratorini noxush ishlardan xabar kilish imkoniyatiga xam ega.

Amaliy darajadagi shlyuzlarning afzalliklari kuyidagilardan iborat:

- global tarmok tomonidan ichki tarmok tarkibi kurinmaydi;
- ishonchli autentifikatsiya va kayd kilish;
- filtrlash koidalarining engilligi;
- kup tamoyilli nazoratlarni amalga oshirish mumkinligi.

Filtrlovchi-yullovchilarga nisbatan amaliy darajadagi shlyuzlarning kamchiliklari kuyidagilardan iborat samaradorligining pastligi; narxining kimmat bulishi.

Amaliy darajadagi shlyuzlar sifatida kuyidagilarni misol kilib keltirish mumkin:

• Border Ware Fire Wall Server — junatuvchining va kabul kiluvchining manzillarini, vaktini va foydalanilgan protokollarni kayd kiladi;

• Black Hole — serverning barcha ishlarini kayd kiladi va tarmok administratoriga kutilayotgan buzilish xakida xabar junatadi.

Bulardan tashkari kuyidagi shlyuzlar xam kullaniladi:

Gauntlet Internel FirewaU, Alta Visla FireWali, ANS Interlock va boshkalar.

10 – MAVZU: ELEKTRON POChTADA AXBOROTLARGA NISBATAN MAVJUD XAVF-XATARLAR VA ULARDAN XIMOYALANISh ASOSLARI

1. Elektron pochtadan foydalanish;

2. E-mail asoslari;

3. E-taildagi mavjud muammolar;

4. Elektron pochtada mavjud xavflar;

5. Elektron pochtani ximoyalash.

Elektron pochtadan foydalanish

Elektron pochta yoki E-mail xozirgi kunda Internetdan foydalanish jarayonining eng mashxur kasmi xisoblanadi. E-mail orkali dunyo buyicha istalgan joyga bir zumning uzida xat yuborish yoki kabul kilish xamda yozilgan xatlarni fakatgina bir kishiga emas, balki manzillar ruyxati buyicha junatish imkoniyati mavjud. E-mail orkali munozaralar utkazish imkoniyati mavjud va bu yunalishda USENET serveri kul keladi.

Kupgina korxonalar uz faoliyatida bevosita E-mail tizimidan foydalanishadi. Demak, korxona va tashkilotlar raxbarlari ma’lum bir chora-tadbirlar orkali uz xodimlarini E-mail bilan ishlash, undan okilona foydalanishga urgatishi lozim. Ushbu jarayonning asosiy maksadi muxim xujjatlar bilan ishlashni tugri yulga kuyish xisoblanadi.

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

- E-mail tizimidan tashkilot faoliyati maksadlarida foydalanish;
- shaxsiy maksadda foydalanish;
- maxfiy axborotlarni saklash va ularga kirish:
- elektron xatlarni saklash va ularni boshkarish.

E-mail asoslari

Internetda asosiy pochta protokollariga kuyidagilar 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 boshka tizimlardan xatlarni kabul kiladi va ularni foydalanuvchining pochta kutisida saklaydi. Pochta serveriga interaktiv kirish xukukiga ega bulgan foydalanuvchilar uz kompyuterlaridan bevosita xatlarni ukiy oladilar. Boshka tizimdagi foydalanuvchilar esa uz xatlarini ROR-3 va IMAP protokollari orkali ukib olishlari mumkin;

POP — eng keng tarkalgan protokol bulib, serverdagi xatlarni, boshka serverlardan kabul kilingan bulsa-da, bevosita foydalanuvchi tomonidan ukib olinishiga imkoniyat yaratadi. Foydalanuvchilar barcha xatlarni yoki xozirgacha ukilmagan xatlarni kurishi mumkin. Xozirgi kunda POP ning 3-versiyasi ishlab chikilgan bulib va autentifikatsiyalash usullari bilan boyitilgan;

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

Ushbu protokol kuyidagi imkoniyatlarga ega:

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

IMAR sayoxatda bulgan foydalanuvchilar uchun RORga nisbatan kulay bulib xisoblanadi;

MIME — Internet pochtasining kup maksadli kengaytmasi suzlari kiskartmasi bulib, u xatlarning formatini aniklash imkonini beradi, ya’ni:

- matnlarni xar xil kodlashtirishda junatish;
- xar xil formatdagi nomatn axborotlarni junatish;
- xabarning bir necha kismdan iborat bulishi;
- xat sarlavxasida xar xil kodlashtirishdagi ma’lumotni joylashtirish.

Ushbu protokol rakamli elektron imzo va ma’lumotlarni shifrlash vositalaridan iborat bulib, bundan tashkari uning yordamida pochta orkali bajariluvchi fayllarni xam junatish mumkin. Natijada, fayllar bilan birga viruslarni xam tarkatish imkoniyati tugiladi.

E-taildagi mavjud muammolar

Elektron pochta bilan ishlash jarayonida kuyidagi xatolarga yul kuyish mumkin:

- xatni tasodifan junatish;
- xatning notugri manzil buyicha junatilishi;
- xatlar arxivining keskin oshib ketishi okibatida tizimning ishdan chikishi;
- yangiliklarga notugri obuna bulish;
- 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 kuyidagilar:

- foydalanuvchilarni ukitish;
- elektron pochta dasturlarini tugri konfiguratsiyalash;
- Internetdagi protokollarga tulik amal kiluvchi dasturlarni kullash.

Bundan tashkari elektron pochtaning shaxsiy maksadda ishlatilishi tashkilot raxbariyati uchun ba’zi bir muammolarni keltirib chikarishi mumkin, chunki E-mail manzilida tashkilot nomlari aks ettirilgan bulishi extimoldan xoli 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 kilish kiyin masala.

Elektron pochtada mavjud xavflar

Elektron pochta bilan ishlash jarayonida kuyidagi xavflar mavjud:

1. Junatuvchining kalbaki manzili. Kabul kilingan xatni E-mail manzili anikligiga tulik ishonch xosil kilish kiyin, chunki xat junatuvchi uz manzilini kalbakilashtirishi mumkin.

2. Xatni kulga 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 kuplab elektron xatlar junatiladi, natijada tizim ishdan chikadi. Pochta serverining ishdan chikish xolatlari kuyidagilardir:

• disk tulib koladi va keyingi xatlar kabul kilinmaydi. Agar disk tizimli bulsa, u xolda 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. «Kurkinchli» (noxush) xat. Internet orkali olinadigan elektron xatlarning umuman noma’lum shaxslar tomonidan junatilishi va bu xatda foydalanuvchilarning shaxsiyatiga teguvchi suzlar bulishi mumkin.

Elektron pochtani ximoyalash

Yukorida keltirilgan xavflarga nisbatan kuyidagi ximoyalanish usullari ishlab chikilgan:

- kalbaki manzildan ximoyalanish, bu xolda shifrlangan elektron imzolarni kullash taklif kilinadi;

- xatni kulga kiritishdan ximoyalanish, bu xolda xabarni yoki junatish kanalini shifrlash taklif kilinadi.

Ushbu ximoyalash usullari bevosita kolgan xavflarning ulushini kamaytiradi.

11 – MAVZU: ELEKTRON TULOVLAR TIZIMIDA AXBOROTLARNI XIMOYALASh

1. ***Elektron tulovlar tizimi asoslari;***
2. ***Identifikatsiyalovchn shaxsiy nomerni ximoyalash;***
3. ***POS tizimi xavfsizligini ta'minlash;***
4. ***Bankomatlar xavfsizligini ta'minlash;***
5. ***Internetda mavjud elektron tulovlar xavfsizligini ta'minlash;***
6. ***Axborotlarni ximoyalashning asosiy vosatalari.***

Elektron tulovlar tizimi asoslari

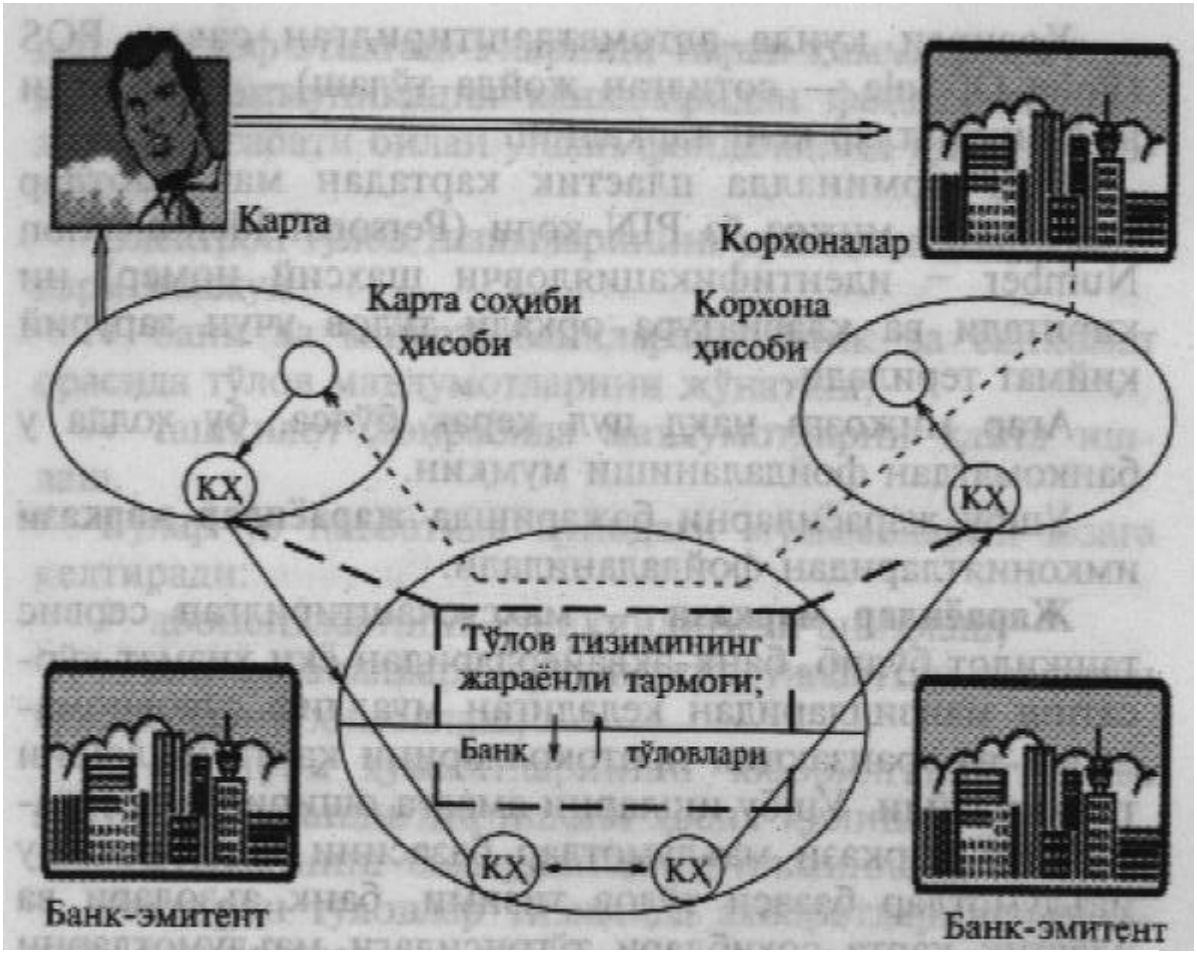
Elektron tulovlar tizimi deb bank plastik kartalarini tulov vositasi sifatada kullanilishidagi usullar va ularni amalga oshiruvchi sub'ektlar majmuasiga aytiladi.

Plastik karta — shaxsiy tulov vositasi bulib, u mazkur vositadan foydalanadigan shaxsga tovar va xizmatlarni nakdsiz pulini tulash, bundan tashkari bank muassasalari va bankomatlardan nakd pulni olishga imkon beradi.

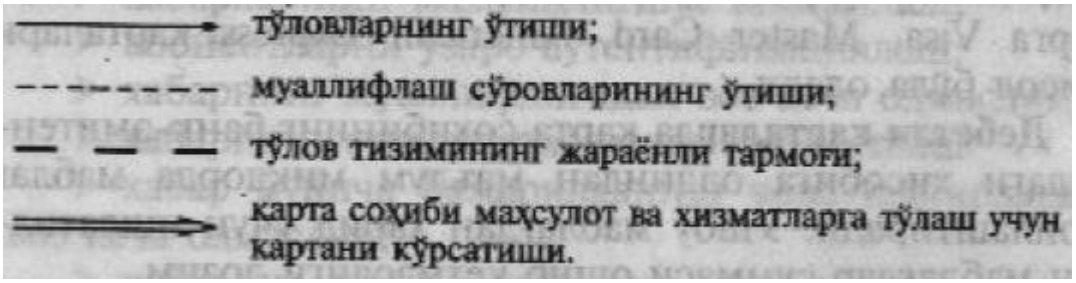
Plastik kartani tulov vositasi sifatida kabul kiluvchilar, savdo va xizmat kursatuvchi korxonalar, bank bulimlari xamda boshkalar shu plastik kartalarga xizmat kursatuvchi kabul kiluvchilar tarmogini tashkil etadi.

Elektron tulovlar tizimini yaratihda plastik kartalarga xizmat kursatish konun-koidalarini ishlab chikish va ularga rioya kilish asosiy masalalardan biri bulib xisoblanadi. Ushbu koidalar nafakat texnikaviy (ma'lumotlarni standartlash, uskunalar va boshkalar), balki moliyaviy masalalar (korxonalar bilan xisoblarni bajarish tartibi)ni xam kamrab oladi.

Elektron tulovlar tizimining faoliyatini kuyidagidek tasavvur kilish mumkin:



Bu erda:



Elektron tulovlar tizimi bilan birgalikda faoliyat kursatadigan bank ikki, ya'ni **bank-emitent va bank-ekvayer** toifasida xizmat kursatadi:

Bank-emitent plastik kartalarni ishlab chikaradi va ularning tulov vositasi sifatida kullanilishiga kafolat beradi.

Bank-ekvayer savdo va xizmat kursatuvchi tashkilotlar tomonidan kabul kilingan tulovlarni bank bulimlari yoki bankomatlar orkali amalga oshiradi.

Xozirgi kunda avtomatlashtirilgan savdo POS (Point-Of-Sale — sotilgan joyda tulash)— terminali va bankomatlar keng tarkalgan.

PQS-terminalda plastik kartadan ma'lumotlar ukiladi va mijoz uz PIN-kodi (Personal Identification Number • identifikatsiyalovchi shaxsiy nomer)ni kiritadi va klaviatura orkali tulov uchun zaruriy kiymat teriladi.

Agar mijozga nakd pul kerak bulsa, bu xolda u bankomatdan foydalanishi mumkin.

Ushbu jarayonlarni bajarishda **jarayonlar markazi** imkoniyatlaridan foydalaniladi.

Jarayonlar markazi – maxsuslashtirilgan servis tashkilot bulib, bank-ekvayerlaridan yoki xizmat kursatish manzillaridan keladigan muallif surovnomalarni va tranzaktsiya protokollarini kayta ishlashni ta'minlaydi. Ushbu ishlarni amalga oshirish uchun jarayonlar markazi ma'lumotlar bazasini kiritadi. Bu ma'lumotlar bazasi tulov tizimi, bank a'zolari va plastik karta soxiblari tugrisidagi ma'lumotlarni uz tarkibiga oladi.

Plastik kartalar tulov buyicha **kreditli yoki debetli** bulishi mumkin.

Kreditli kartalar buyicha karta soxibiga kupincha muxlati 25 kungacha bulgan vakgancha karz beriladi. Bularga Visa, Master Card, American Express kartalari misol bula oladi.

Debetli kartalarda karta soxibining bank-emitentidagi xisobiga oldindan ma'lum mikdorda mablag joylashtiradi. Ushbu mablagdan xarid uchun ishlatilgan mablaglar summasi oshib ketmasligi lozim.

Ushbu kartalar fakatgina shaxsiy emas, balki korporativ xam bulishi mumkin.

Xozirgi kunda **mikroprotsessorli kartalar** ishlab chikilmokda. Ushbu kartalarning oldingilaridan asosiy farki bu mijozning barcha ma'lumotlari unda aks ettirilgan bulib, barcha **tranzaktsiyalar,** ya'ni ma'lumotlar bazasini bir xolatdan ikkinchi xolatga utkazuvchi surovnomalar, off-line rejimda amalga oshiriladi, shu bois, ular yukori darajada ximoyalangan deb e'tirof etilgan. Ularning narxi kimmatrok bulsa-da, telekommunikatsiya kanallaridan foydalanilmaslik munosabati bilan undan foydalanish kiymati arzondir.

Elektron tulov tizimlarining kuyidagi zaif kismlari mavjud:

• bank va mijoz, banklararo, bank va bankomat orasida tulov ma'lumotlarini junatish;

• tashkilot doirasida ma'lumotlarni kayta ishlash.

Bular uz navbatida kuyidagi muammolarni yuzaga keltiradi:

• abonentlarning xakikiyligini aniklash;

• aloka kanallari orkali junatilayotgan elektron xujjatlarni ximoyalash;

• elektron xujjatlarining yuborilganligiga va kabul kilinganligiga ishonch xosil kilish;

• xujjatning bajarilishini ta'minlash.

Elektron tulovlar tizimida axborotlarni ximoyalash funktsiyalarini ta'minlash maksadida kuyidagilar amalga oshirilishi kerak:

- tizimning chetki buginlariga kirishni boshkarish;
- axborotlarning yaxlitligini nazorat kilish;
- xabarlarning maxfiyligini ta'minlash;
- abonentlarni uzaro autentifikatsiyalash;
- xabarning muallifligidan voz kecha olmaslik;
- xabarning etkazilganligini kafolatlash;
- xabar buyicha bajariladigan chora-tadbirlardan voz kecha olmaslik;
- xabarlar ketma-ketligini kayd kilish;
- ketma-ket xabarlar yaxlitligini ta'minlash.

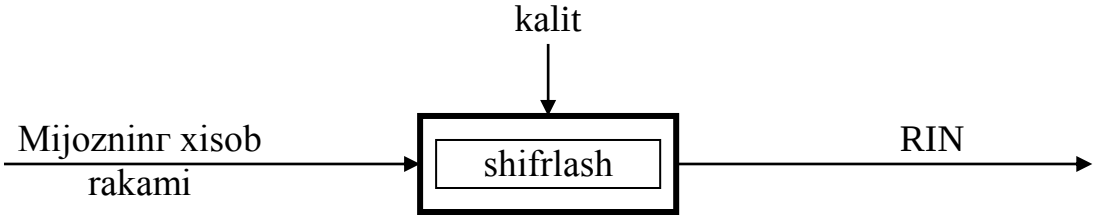
Identifikatsiyalovchn shaxsiy nomerni ximoyalash

PIN-kodlarini ximoyalash tulov tizimi xavfsizligini ta’minlashda asosiy omildir. Shu bois u fakatgina karta soxibiga ma’lum bulib, elektron tulovlar tizimida saklanmaydi va bu tizim buyicha yuborilmaydi.

Umuman olganda, PIN bank tomonidan berilishi yoki mijoz tomonidan tanlanishi mumkin. Bank tomonidan beriladigan PIN kuyidagi ikki variantdan biri buyicha amalga oshiriladi:

1) mijoz xisob rakami buyicha kriptografiya usuli bilan tashkillashtiriladi;

Ushbu jarayonni kuyidagicha tasvirlash mumkin:



Ushbu usulning afzalligi PIN kodi elektron tulovlar tizimida saklanishi shart emasligidadir, kamchiligi esa ushbu mijoz uchun boshka PIN berilishi lozim bulsa, unga boshka xisob rakami ochilishi zapypligida, chunki bank buyicha bitta kalit kullaniladi.

2) bank ixtiyoriy PIN kodni taklif kiladi va uni uzida shifrlab saklaydi. PIN kodni xotirada saklash kiyinligi ushbu usulning asosiy kamchiligi bulib xisoblanadi.

Mijoz tomonidan tanlaniladigan PIN kod kuyidagi imkoniyatlarga ega:

- barcha maksadlar uchun yagona PIN kodni kullash;
- xarflar va rakamlardan tashkil etilgan PIN kodni xotirada saklashning engilligi.

PIN kodi buyicha mijozni identifikatsiyalashtirishning ikki usuli bilan bajarish mumkin: **algoritmlashgan va algoritmlashmagan.**

Algoritmlashmagan tekshirish usulida element kiritgan PIN kod ma’lumotlar bazasidagi shifrlangan kod bilan takkoslaniladi.

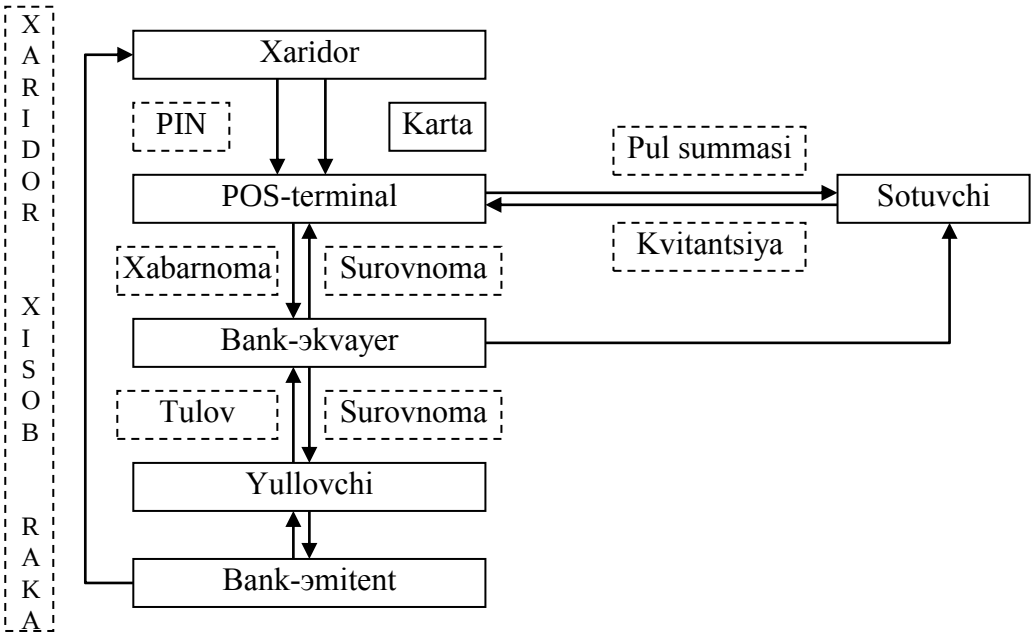
Algoritmlashgan tekshirish usulida esa mijoz kiritgan PIN kod, maxfiy kalitdan foydalangan xolda, maxsus algoritm buyicha uzgartiriladi va kartadagi yozuv bilan takkoslaniladi.

Ushbu usulning afzalliklari:

- asosiy kompyuterda PIN saklanmaydi va natijada personal tomonidan ugirlanmaydi;
- PIN kod telekommunikatsiya orkali junatilmaydi.

POS tizimi xavfsizligini ta’minlash

POS tizimini anik tasavvur kilish uchun kuyidagi chizmani keltiramiz:



Ushbu chizma buyicha xaridor uz plastik kartasini urnatib, PIN kodini kiritadi.

Sotuvchi uz navbatida pul summasini kiritadi. Shundan sung, bank-ekvayerga (sotuvchi banki) pulni kuchirish uchun surovnoma yuboriladi.

Bank-ekvayer, uz navbatida, kartaning xakikiyligini aniklash uchun surovnomani bank-emitentga junatadi. Natijada, bank-emitent pulni bank-ekvayerga sotuvchi xisobiga kuchiradi. Pul kuchirilgandan sung, bank-ekvayer tomonidai POS-terminalga xabarnoma junatiladi. Ushbu xabarda tranzaktsiya bajarilganligi xakida ma’lumot buladi.

Shundan sung, sotuvchi xaridorga maxsulot va kvitantsiyasini takdim etadi.

Uz-uzidan kurinib turibdiki, ushbu jarayonda xar xil vokealar sodir bulishi mumkin.

POS tizimining eng zaif kismi bu POS-terminaldir. Bundagi asosiy xavf bulib terminaldagi maxfiy kalitning ugirlanishi xisoblanadi.

Buning okibatlari kuyidagilar bulishi mumkin:

• oldingi tranzaktsiyalarda ishlatilgan PIN kodni tiklash;

• keyingi tranzaktsiyalarda kullaniladigan PIN kodni tiklash.

Ushbu xavflardan ximoyalanishning 3 ta usuli taklif etiladi:

- xar bir tranzaktsiyasidan sung kalitni uzgartirish;
- POS-terminal va bank-ekvayer orasidagi ma’lumotlarni maxsus kalit bilan shifrlash xamda kalitni xar bir tranzaktsiyadan sung uzgartirish;
- ochik kalitlar usuli yordamida uzatiladigan ma’lumotlarni shifrlash.

Bankomatlar xavfsizligini ta’minlash

Bankomatlar nakd pul olish, xisob rakamning xolati va pul kuchirish imkoniyatlariga ega.

Bankomat ikki rejimda ishlaydi, off-line va online.

Off-line rejimda bankomat bank kompyuterlaridan mustakil ishlaydi va bajariladigan tranzaktsiyalar xakidagi yozuvlarni uz xotirasida saklaydi xamda printerga uzatib, ularni chop kiladi.

On-line rejimda bankomat bevosita bank kompyuterlari bilan telekommunikatsiya orkali ulangan buladi. Tranzaktsiyasini amalga oshirish maksadida bankomat bankdagi kompyuter bilan kuyidagi xabaplap bilan almashadi:

- bankomat surovnomasi;
- bankning javob xabari;
- bankomatning tulovni bajarganligi xakidagi xabarni berish.

Xozirgi kunda bankomatlar tarmoklaridan bir necha banklargina foydalanadi. Bu erda mavjud bulgan asosiy muammo bu banklarning maxfiy axborotlarini (masalan, maxfiy kalit) bir-biridan ximoyalashdir.

Ushbu muammoning echimi sifatida PIN kodni, markazlashtirilgan xolda, xar bir bank tomonidan tekshirish taklif kilinadi.

Bundan tashkari bankomatlar tarmogi zonalarga taksimlanadi va xar bir zonada ZCMK (Zone Control Master Key) kalitlari, uz navbatida, kompyuter tarmogidagi kalitlarni shifrlashda kullaniladi. Malumotlarni shifrlashda esa IWK (Issuer Working Key) kalitlar ishlatiladi.

Internetda mavjud elektron tulovlar xavfsizligini ta’minlash

Xozirgi kunda Internetda kupgina axborot markazlari mavjud, masalan, kutubxonalar, kup soxali ma’lumotlar bazalari, davlat va tijorat tashkilotlari, birjalar, banklar va boshkalar.

Internetda bajariladigan elektron savdo katta axamiyat kasb etmokda. Buyurtmalar tizimining kupayishi bilan ushbu faoliyat yana keskin rivojlanadi. Natijada, xaridorlar bevosita uydan yoki ofisdan turib, buyurtmalar berish imkoniga ega bulishadi. Shu bois xam, dasturiy taminotlar va apparat vositalar ishlab chikaruvchilar, savdo va moliyaviy tashkilotlar ushbu yunalishni rivojlantirishga faol kirishishgan.

Elektron savdo — global axborot tarmoklari orkali maxsulotlarni sotish va pulli xizmatlar kursatish demakdir.

Elektron savdoning asosiy turlari kuyidagilardir:

• axborotlar sotuvi;

• elektron dukonlar;

• elektron banklar.

Axborotlar sotuvi asosan ma’lumotlar bazasidan On-line rejimda foydalanish uchun takdim etilishi mumkin.

Elektron dukonlar Internetda Web-site orkali tashkillashtiriladi. Bunda tovarlar ruyxati, tulov vositalari va boshkalar keltiriladi. Xarid kilingan maxsulotlar oddiy pochta orkali junatilishi yoki agar ular elektron maxsulot bulsa, bevosita Internetdan manzilga etkazilishi mumkin.

Elektron banklarni tashkil etishdan asosiy maksad bankning doimiy xarajatlarini kamaytirish va keng ommani kamrab olishdir. Shu bois, elektron banklar uz mijozlariga yukori foiz stavkalarini taklif kilishlari mumkin.

Axborotlarni ximoyalashning asosiy vosatalari

Xaridor, kredit kartasi soxibi, bevosita tarmok orkali tulovlarni bajarish uchun ishonchli va ximoyalangan vositalarga ega bulishi lozim.

Xozirgi kunda SSL (Secure Socket Layer) va SET (Secure Electronic Transactions) protokollari ishlab chikilgan:

• SSL protokoli ma’lumotlarni kanal darajasida shifrlashda kullaniladi;

• SET xavfsiz elektron tranzaktsiyalari protokoli yakinda ishlab chikilgan bulib, fakatgina moliyaviy ma’lumotlarni shifrlashda kullaniladi.

SET protokolining joriy etilishi bevosita Internetda kredit kartalar bilan tulovlar sonining keskin oshishiga olib keladi.

SET protokoli kuyidagilarni ta’minlashga kafolat beradi:

• axborotlarning tulik maxfiyligi, chunki foydalanuvchi tulov ma’lumotlarining ximoyalanganligiga tulik ishonch xosil kilishi kerak;

• ma’lumotlarning tulik saklanishi, ya’ni ma’lumotlarni uzatish jarayonida buzilmasligini kafolatlash. Buni bajarish omillaridan biri rakamli imzoni kullashdir;

• kredit karta soxibining xisob rakamini audentifikatsiyalash, ya’ni elektron (rakamli) imzo va sertifikatlar xisob rakamini audentifikatsiyalash va kredit karta soxibi ushbu xisob rakamining xakikiy egasi ekanligini tasdiklash;

• tijoratchini uz faoliyati bilan shugullanishini kafolatlash, chunki kredit karta soxibi tijoratchining xakikiyligini, ya’ni moliyaviy operatsiyalar bajarishini bilishi shart. Bunda tijoratchining rakamli imzosini va sertifikatini kullash elektron tulovlarning amalga oshirilishini kafolatlaydi.

12 – MAVZU: KOMPYUTER TIZIMLARINING XIMOYALANGANLIK DARAJASINI ANIKLASh VOSITALARI

Korxonalarda joriy etilayotgan avtomatlashtirilgan axborot tizimining xavfsizligini ta’minlash, birinchi navbatda, ushbu tizimni loyixalash boskichida kuzda tutilgan bulishi lozim. Korxona mikyosida kabul kilingan xavfsizlik siyosatining axborot tizimida kanday darajada aks ettirilishi muxim masalalardan biri xisoblanadi. Lekin, axborot-kommunikatsiyalar texnologiyalarining keskin rivojlanishi, axborot okimlari xajmining oshishi. Internet va intranet

texnologiyalarining keng mikyosda kirib kelishi bevosita avtomatlashtirilgan axborot tizimlarining axborot zaxiralarini ximoyalashga yunaltirilgan vositalarning mavjudligini ta’minlash xamda tizimda mavjud bulgan ximoya vositalarini rivojlantirishini takozo etadi.

Avtomatlashtirilgan axborot tizimlariga nisbatan mavjud bulgan xavflarni uchta yunalish buyicha ajratish mumkin:

- amaliy dasturlar;
- tarmok xizmatlari;
- operatsion tizim xizmatlari.

Amaliy dasturlarni tekshirish buyicha xozirgacha yagona vosita mavjud emas. Tarmok xizmatlari va operatsion tizim xizmatlarida kullaniladigan texnologiyalar umumiy asoslarga ega bulganligi uchun ularni tekshirish vositalari ishlab chikilgan.

Zamonaviy operatsion tizimlarda axborot zaxiralarini ximoyalash vositalarining mavjudligi ta’kidlab kelinmokda. Bularga autentifikatsiyalash, identifikatsiyalash, ruxsatsiz kirishni ta’kiklash, monitoring va audit, kriptografiya usullarining mavjudligi misol bula oladi. Albatta, ushbu vositalarning operatsion tizimlarda mavjud bulganligi korxonaning xavfsizlik siyosatiga mos keladi. Ammo, operatsion tizimning notugri konfiguratsiyalanishi va uning dasturiy ta’minotidagi mavjud xatolar okibatida axborot tizimlariga xujumlar uyushtirilishi imkoniyati paydo buladi.

Shu bois, operatsion tizimni tanlashda undagi kamchiliklarni taxlil kilish, ishlab chikaruvchi firma tomonidan yul kuyilgan xatolarning tan olinishi va ularni zudlik bilan tuzatishga kirishilishi talab etiladi.

Operatsion tizimning parametrlarining tugri urnatilganligini yoki ularning uzgarmaganligini tekshirish uchun «tizim xavfsizligini skanerlash» deb nomlanuvchi 10 ga yakin maxsus dasturlar ishlab chikarilgan. Masalan, Solaris operatsion tizimi uchun muljallangan ASET, Netware va NT uchun KSA, Unix uchun SSS dasturlari mavjud.

SSS (System Security Scanner) dasturi xakida

Ushbu dastur Unix operatsion tizimi urnatilgan kompyuterlarda xavfsizlik xolatini tekshirish va operatsion tizimning tashki xamda ichki zaif kismlarini aniklashga yunaltirilgan. Bundan tashkari u kirish xukuklarini, fayllarga egalik kilish xukuklarini, tarmok zaxiralarini konfiguratsiyalashni, autentafikatsiyalash dasturlarini va boshkalarni tekshirishi mumkin.

Dasturning kuyidagi imkoniyatlari mavjud:

- konfiguratsiyani tekshirish, ya’ni ruxsatsiz kirishlarning oldini olish maksadida konfiguratsiyani tekshirish. Bunga kuyidagilar kiradi: konfiguratsiya fayllari, operatsion tizim versiyasi, kirish xukuklari, foydalanuvchilarning zaxiralari, parollar;

- tizimdagi xavfli uzgarishlarni tekshirish. Ruxsatsiz kirishlar okibatida tizimda sodir bulgan uzgarishlarni kidirishda kullaniladi. Bunday uzgarishlarga

kuyidagilar kiradi: fayllar egallagan xotira xajmining uzgarishi, ma’lumotlarga kirish xukuki yoki fayldagi ma’lumotlarning uzgarishi, foydalanuvchilarning zaxiralarga kirish parametrlarining uzgarishi, fayllarni ruxsatsiz boshka bir tashki kompyuterlarga uzatishlar;

- **foydalanuvchi nnterfeysining kulayligi.** By interfeys yordamida nafakat dastur bilan kulay ishlash ta’minlanadi, balki bajarilgan ishlar buyicha xisobotlar xam yaratiladi;

- **masofadan skanerlash.** Tarmokdagi kampyuterlarni tekshirish va aloka jarayonida ma’lumotlarni shifrlash imkoniyati ta’minlanadi;

- **xisobotlar tuzish**. Bajarilgan ishlar buyicha tulik, xisobotlap yaratiladi. Ushbu xisobotlarda tizimning aniklangan zaif buginlarining izoxi keltiriladi va ularni tuzatish buyicha kursatmalar beriladi. Xisobot HTML yoki oddiy matn kurinishida bulishi mumkin.

SATAN dasturi xakida

Tarmok xizmatlarining ximoyalanganligini taxlil kilish buyicha birinchi bulib ishlab chikarilgan dasturlardan biri bu SATAN dasturidir. Bu dastur 20 ga yakin tarmok xizmatlaridagi zaifliklarni aniklay oladi.

Internet Scanner SAFEsuite dasturi xakida

Agar tekshiruvlar doimiy ravishda va tulik amalga oshirilishi talab kilinsa, u xakda internet Scanner SAFEsuite dasturlar paketi taklif kilinadi. Bu dasturlar paketi yordamida 140 ta ma’lum bulgan zaifliklar va tarmok vositalari, ya’ni tarmoklararo ekranlar, Web-serverlar, Unix, Windows 9.x, Windows NT tizimli serverlar va ishchi stantsiyalar, umuman TCP/IP protokoli kullaniladigan barcha vositalar tekshiriladi.

Internet Scanner SAFEsuite paketiniig umumiy imkoniyatlari kuyidagilardan iborat:

1. Avtomyatlashtirilgan va konfiguratsiyalangan skanerlash:

• avtomatlashgan identifikatsiyalash va zaif kismlar buyicha xisobot tuzish;
• doimiy reja buyicha skanerlash;
• IP manzillarni skanerlash;
• foydalanuvchi urnatgan parametrlarni skanerlash;
• zaif buginlarni avtomatik ravishda tuzatish;
• ishonchlilik va takrorlanuvchanlikni ta’minlash.

2. Xavfsizlikni ta’minlash:

• tarmok vositalarini inventarizatsiyalash va mavjud asosiy zaif buginlarni identifikatsiyalash;

• asosiy xisobotlarni takkoslash va kelgusida ulardan foydalanish uchun taxlil kilish.

3. Foydalanishning oddiyligi:

• foydalanuvchining grafik interfeysi;

• HTML turidagi tartiblangan xisobotlarni yaratish;

• skanerlashni markazlashtirilgan xolda bajarish, boshkarish va monitoring utkazish.

Internet Scanner SAFEsuite paketida kuyidagi dasturlar mavjud: Web Security Scanner, FireWall Scanner va Intranet Scanner.

Web Security Scanner bevosita Web-serverlarda mavjud zaif kismlarni aniklashga muljallangan bulib, bu dasturning imkoniyatlari kuyidagilardan iborat:

• Web-server urnatilgan operatsion tizimni auditlash;

• Web-serverda mavjud dasturlarni auditlash;

• Web-fayllarda mavjud skriptlarni auditlash;

• Web-server konfiguratsiyasini testdan utkazish;

• asosiy fayllar tizimining xavfsizlik darajasini aniklash;

• skriptlarda mavjud xatolarni aniklash;

• bajarilgan ishlar buyicha xisobotlar yaratish va xatolarni tuzatish borasida takliflar berish.

FireWall Scanner dasturi bevosita tarmoklararo ekranda mavjud bulgan zaif kismlarni aniklashga muljallangan bulib, u kuyidagi amallarni bajaradi:

• tarmoklararo ekranga xujumlar uyushtirib, uni testdan utkazish;

• tarmoklararo ekran orkali utadigan tarmok, xizmatlarini skanerlash.

Intranet Scanner dasturi kompyuter tarmogida mavjud kamchiliklarni tarmokka ruxsatsiz kirishlarini amalga oshirish orkali testdan utkazish yordamida aniklashga yunaltirilgan. Tarmokning xir xil kismlari (xost-kompyuterlar, yullovchilar, Web-serverlar, Windows 9.x/NT tizimida ishlaydigan kompyuterlar) ni tekshirishni xam amalga oshiradi.

Yukorida keltirilganlardan tashkari kompyuter tizimlariga ruxsatsiz kirishlarni doimiy ravishda nazorat kiluvchi dasturlar, masalan, Internet Security Systems kompaniyasi tomonidan ishlab chikilgan **Real Secure** dasturi xam mavjud. Bu dastur tarmokda sodir etilayotgan xodisalar, masalan, xakerlarning xujumlarini kayd kilish bilan birgalikda faol ximoya chora-tadbirlarini tashkillashtirishi mumkin. Real Secure dasturi yirik tashkilotlar uchun muljallangan bulib, xar kuni tinimsiz ishlashga muljallangan.

Real Secure dasturi ikki kismdan iborat: **filtrlash** va foylalanuvchining **grafik nnterfeysi.**

Filtrlash kismi tarmokda sodir etilayotgan xodisalarni faol kuzatish va boshkarish uchun xizmat kiladi. Dasturning ikkinchi kismi yordamida foylalanuvchi ruy bergan xodisalar xakidagi ma’lumotlarni kabul kiladi, ularni boshkaradi va tizim konfiguratsiyasini uzgartira oladi. Natijada, filtrlash va sodir etilayotgan xodisalarga nisbatan ximoya tadbirlarini avtomatik ravishda amalga oshirish mumkin buladi, masalan, kayd kilish, displeyga chikarish, xodisani man etish va boshkalar.

Bulardan tashkari barcha kayd etilgan xodisalar xakidagi malumotlarni keyinchalik real masshtabda yoki tezkor yoki sekinlashgan rejimlarda kurib chikish mumkin buladi.

Real Secure dasturi bevosita Sun OS, Solaris va Linux operatsion tizimlarida ishlash uchun muljallangan.

Axborot havfsizligi sohasida atamalar

Access - Axborotga munosabat(kirish). Axborot bilan tanishish yo u bilan biror axborot jarayonini amalga oshirish.

Access object - Munosabat (kirish) obekti. Munosabat turi va darajasi aniq qoidalar asosida cheklab qo'yilgan axborot texnologiyasi elementi va obekti.

Active attack - Tajovuz. Xavfsizlikka tah didning yuzaga chiqishi.

Active threat - Xavfsizlikka taxdid. Qasddan tizimning xolatini yomonlashtirishga qaratilgan muayyan turdagi xavf-xatarning ma'lum extimolligi.

ASCII - Armored Text - ASCII- matn. ASCII to'plamiga kiruvchi 7-bitli standart bosma simvollarda yozilib ikkili sanoq tizimida kodlangan axborot. Bu ko'rinishdagi axborot har qanday tarmoq kanali orqali uzatishga yaraydi.

Authentication information - Autentifikatsiya axboroti. Muayyan axborot manbaining yo uni egasining aslini bilib olish uchun ishlatiladigan axborot. Buknday axborot sifatida raqamli imzo, xujjat izi, manba' izi va sh.o'. bo'lishi mumkin.

Authentication- Autentifikatsiya. Muayyan axborot manbaining yo uni egasining aslini bilib olish. Bu maqsadda nosimmetrik kriptotizimdan foydalanilganda hujjatning aslini (kelib chiqishini) xujjat tuzuvchining raqamli imzosi vositasida aniqlab olinadi. Autentifikatsiya keng ma'noda qaralganda axborotning manba'idan qat'iy nazar uning faqat ichki tuzilmasi asosida butunligini aniqlashdir.

Authorized access - Ruxsatli munosabat(kirish). Axborotga va axborot texnologiyasi elementlariga nisbatan belgilab qo'yilgan cheklov qoidalariga rioya qilingan holda faol munosabatda bo'lish.

Certify - Kalitni sertifikatsiyalash. Biror kimsaning oshkora kalitini raqamli imzo bilan tasdiqlash.

Certifying Authority - Vakolatli sertifikator. Kalitni sertifikatsiyalash va buni umumiy ma'lumotlar bazasiga kiritish huquqiga ega bo'lgan ishonchga sazovor shaxs (yo shaxslar).

Confidentiality information - Axborot pinhonaligi. Axborotning u bilan bajarladigan axborot jarayonlari davomida u bilan beruhsat tanishish yo uni ko'chirib olishga yo'l qo'ymaslik xossasi.

Confidentiality information - Pinxona axborot. Xujjatlashtirilgan shunday axborotki, unga nisbatan barcha munosabatlar (ruscha, dostup) qonun bilan cheklangan.

Confidentiality mark - Maxfiylik grifi. Xujjatlashtirilgan axborotning maxfiylik darajasini ko'rsatuvchi rekvizit (masalan, o'ta maxfiy, maxfiy, pinxona, xizmatda foydalanish uchun, oshkora).

Cryptographic method - Kriptografik metod. Axborotni shifrlashga asoslangan ximoyalash usuli.

Data destruction - Axborotni yo'q qilish. Axborotni tasodifiy xato tufayli yo qasddan moddiy tashuvchidan o'chirib yuborish yokm tashuvchisi bilan birga o'g'irlab ketish.

Data falsification - Axborotni soxtalashtirish. Axborot jarayonlari davomida axborot mazmunini qastdan buzib o'zgartirish.

Data protection - Axborot ximoyasi. Axborotning pinxonaligi, butunligi va qobilligini ta'minlashga qaratilgan huquqiy, siyosiy, tashkiliy, texnikaviy va dasturiy tadbirlar majmui.

Data transmission blocking - Axborot uzatishni to'sish. Axborot uzatishni qastdan yo tasodifiy xato tufayli to'xtatib, yo'lini o'zgartirib yo kechiktirib qo'yishdan iborat bo'lgan axborot xavfsizligining buzish turi.

Decryption - Shifrni ochish. Shifrlangan axborotni tushunarli shaklga aylantirish. Buning uchun maxfiy kalitdan foydalaniladi.

Digest - raqamli iz(daydjest). Axborotning ixcham bir tomonlama xisoblanadigan funktsiyasi yoki faylning nazorat jamlamasi. Axborot o'zgarsa daydjest ham o'zgaradi.

Digital Signature - Raqamli imzo. Axborotning raqamli izi(daydjesti)ning shu axborotning xaqiqiyligini tasdiqlovchi sub'ektning maxfiy kaliti bilan shifrlangan shakli. Raqamli imzo shu sub'ektga tegishli ekaniga ishonch xosil qilish uchun axborotning raqamli izini hammaga ma'lum bo'lgan funktsiya asosida hisoblab topib, natijani raqamli imzo egasining oshkora kaliti bilan ochilgan imzosi bilan taqqoslash (verifikatsiyalash) yetarli.

Documented information - Xujjatlashtirilgan axborot. Moddiy tashuvchida aks etgan va uni belgilovchi rekvizitlarga ega bo'lgan muayyan axborot.

Encryption - Shifrlash. Axborotni undan xabardor bo'lishi lozim bo'lmagan shaxslar uchun mutlaqo tushunarsiz shaklga keltirish amali, ximoya usuli .

Enforcement - Majburlash. Foydalanuvchi yoki ijrochiga nisbatan moddiy yoki jinoiy javobgarlik taxdidi ostida axborot jarayonlari koidalarining bajarilishiga erishishga asoslangan ximoya usuli.

Identification - Identifikatsiya. Ko'rsatilgan identifikatorni uning egasiga takdim etilgan identifikator bilan takkoslash.

Identifier - Identifikator. Axborot jarayoni subekti , vositasi va obekti(axborot)ga takdim etiladigan, fakat unga biriktirilgan noyob belgi, simvollar qatori.

Information procedure - Axborot jarayoni. Axborotni yaratish, olib- yig'ish, saqlash, himoyalash, izlash, uzatish, taqsimlash, undan foydalanish yoki unga ishlov berish jarayonlaridan biri.

Information (data) integrity - Axborotning butunligi. Axborotning axborot jarayonlari davomida uni beruxsat o'zgartirish yoki yo'qotishga yo'l qo'ymaslik xossasi.

Information availability - Axborot qobilligi. Axborotning unga nisbatan ruxsat berilgan axborot jarayonlarini bajarilishiga yaroqlik va tayyorlik xossasi.

Information distortion - Axborot buzilishi. Axborotning axborot jarayonlari davomida xalal beruvchi tashqi ta'sirlar yo jarayon vositalari va ishtirokchilarining tasodifiy xatolari yo qasddan qilingan ishlar tufayli o'zgarib qolishi.

Information modification - Axborot modifikatsiyasi. Axborot mazmuni yo xmiqdorining axborot jarayonlari davomida o'zgarishi.

Information security - Axborot xavfsizligi. Axborotninig va axborot jarayonlarini amalga oshirish vositalarining ma'lum turdagi tasodifiy va qasddan qilinadigan tahdidlardan himoyalanganlik holati

Information security service - Axborot xavfsizligini ta'minlash tizimi. Axborot xavfsizligini ta'minlovchi siyosiy, huquqiy, tashkiliy, texnikaviy va dasturiy tadbirlar, vositalar va meyorlar tizimi.

Information user - Axborot foydalanuvchisi. Axborot bilan biror axborot jarayonini amalga oshiruvchi sub'ekt (shaxs, tashkilot).

Information's security - Axborotning xavfsizligi. Axborotning tasodifiy yo qasddan qilinadigan tahdidlarga qarshi pinxonalikni, butunlikni va qobillikni saqlab qolish xossasi.

Introducer - Vositachi. Ochiq kalitlarning o'z egasiga taalluqligiga kafillik berishga vakolatli shaxs yo tashkilot. PGP dasturida vositachilar ularning ochiq kalitiga ma'lum ishonch darajasi taqdim etish orqali tayinlanadilar.

Intruders (hacker) - Axborot jinoyatchisi. Axborot xavfsizligini buzgan sub'ekt (shaxs, tashkilot).

Key - Kalit. Shifrlash, shifrni ochish, raqamli imzo qo'yish va verifikatsiya(ishonib olish)da ishlatiladigan raqamli kod. Kalitlar nosimmetrik kriptotizimlarda juft(oshkora va mahfiy) xolda hosil qilinadi va bog'lamlarda

saqlanadi. Simmetrik kriptotizimlarda faqat bitta(mahfiy) kalit ishlatiladi. Aralash kriptotizimlarda kalitlar juftiga qo'shimcha tarzda mahfiy seans aliti ishlatiladi.

Key Escrow - Kalitni deponirlash. Uchinchi tomonga o'z maxfiy kalitining nusxasini berish amaliyoti. Bunda uchinchi tomon shifrlangan axborotni bilib olish imkoniga ega.

Key Fingerprint - Bosma iz. Oshkora kalitni noyob tarzda ifodalovchi(belgilovchi) raqam va harflar qatori. Kalit egasidan telefon orqali Bosma izini so'rab olib o'zingizdagi uning oshkora kaliti Bosma izi nushasi bilan taqqoslab, kalit nusxasining haqiqiy yo qalbaki ekanini bilish mumkin.

Key ID - Kalit identifikatori. Kishi o'qisa bo'ladigan kalitlar juftini noyob usulda belgilovchi qator. Kalitlarning ikki jufti bir xil foydalanuvchi identifikatoriga ega bo'lishi mumkin. Lekin kalit identifikatorlari har xil bo'ladi.

Key Pair - Kalitlar jufti. Oshkora va unga mos maxfiy kalit. Oshkor kalitli tizimda har bir foydalanuvchi kamida bitta kalitlar juftiga ega.

Keyring - Bog'lam. Kalitlar to'plami. Har bir foydalanuvchi oshkora kalitlar boylamiga va maxfiy kalitlar boylamiga ega.

Masking - Niqoblash. Axborotni axborot jarayenlari davomida kriptografik usul bilan berkitish.

Obstacle - To'siq. Ximoyalanadigan axborotga axborot jinoyatchisining yo'lini fizikaviy to'sib qo'yish asosida axborotni ximoyalash usuli.

Passiv attack - Nofaol tajovuz. Xavfsizlikka nofaol taxdidning yuzaga chiqishi.

Passiv threat - Xavfsizlikka nofaol taxdid. Tizim xolatini buzmasdan turib undan axborotning begonalarga beruxsat chiqib ketish xavfi.

Password - Parol. Amaliy munosabat boshlash uchun ishlatiladigan, subektning siri xisoblanadigan identifikator. Tizimga kirish uchun klaviatura tugmalarini bosish ketma-ketligi.

Physical threat - Fizikaviy xavf. Oqibati tizimga fizikaviy xavf keltiradigan taxdid.

Plaintext - Ochiq matn. SHifrlanmagan va imzolanmagan odatdagicha o'qib-tushuniladigan matn.

Potection strategy - Himoya strategiyasi. Malum tahdidlardan ximoyalanishni taminlashga qaratilgan mezonlarning formal tarifi.

Private Key - Maxfiy kalit. Bilishi shart bo'lgan sub'ektlardan boshqa xechkimga oshkora qilinmaydigan kalit. Simmetrik kriptotizimlarda shifrlash va

shifrni ochish uchun, nosimmetrik kriptotizimlarda raqamli imzo qo'yish va axborot shifrini ochish uchun ishlatiladi.

Private Keyring - Maxfiy kalitlar boylami. Boylam egasiga tegishli bir yo undan ortiq maxfiy kalitlar to'plami.

Protection model - Ximoya modeli. Axborot ximoyasi tizimini aks ettirib, uni xavfsizlik darajasini tadqiq etishga imkon beruvchi tizim.

Public Key - Oshkora kalit. Axborotni shifrlash va raqamli imzoning to'g'riligini tekshirish uchun ishlatiladigan kalit. Oshkora kalit boshqalarga erkin tarqatiladi va birov uni bilgan bilan unga mos maxfiy kalitni hisoblab topaolmaydi.

Public Keyring - Oshkora kalitlar bog'lami. Oshkora kalitlar to'plami. Uning tarkibida boylam egasining ham o'z oshkora kaliti bor.

Public-Key Cryptography - Oshkora kalitli(nosimmetrik) kriptografiya. Oshkora va maxfiy kalitlar juftidan foydalanishga asoslangan va ishlatiladigan aloqa kanalining himoyalangan bo'lishini talab qilmaydigan kriptotizimlar texnologiyasi.

Regulation - Tartibga solish. Axborotga beruxsat munosabatda bulishni minimumga keltirishga qaratilgan texnologiyaga asoslangan ximoya usuli.

Screening - Ekranlash. Tarmoklararo ekran(branmauer)ning ruxsat etilmagan tashki axborot okimlarini utkazmay ichki tarmok xavfsizligini saklash vazifasi.

Security audit - Xavfsizlikni tekshirish. Axborot tizimi va tarmog'ining hamda axborotlarning xavfsizlik xolatini tekshirib baholash.

Security model - Xavfsizlik modeli. Axborot xavfsizligi siyosatining formal ifodasi.

Security policy - Xavfsizlik siyosati. Axborot xavfsizligini taminlashga va tajovuz oqibatlarini tugatishga qaratilgan meyorlar majmui.

Signature - Imzo. Maxfiy kalit vositasida hosil qilinadigan raqamli kod. Imzo uni verifikatsiyalash jarayonida axborot aslini(manba'ini,egasini,tasdiqlovchisini) aniqlash imkonini beradi. Raqamli imzo maxfiy kalit va imzolanayotgan xujjat mazmunining funktsiyasidir.

Subject privilege - Mualliflashtirilgan kirish sub'ekti. Axborot tizimi obektlariga va axborotga amaliy munosabatda bo'lish uchun belgilab qo'yilgan xuquqlarga ega bulgan subekt.

Trojan horse - Troyan oti. Sub'ektning qonuniy vakolatlaridan foydalanib axborotga beruxsat munosabatda bo'lishga imkon beruvchi qo'shimcha pinxona vazifalarni amalga oshiruvchi dastur.

Trusted - Ishonchli. Ochiq kalit ishonchli, agar uni siz yo biror siz vakil etgan kimsa sertifikatsiyalagan bo'lsa.

Trusted computer system - Ximoyalangan kompyuter tizimi. Ximoya vositalari majmui o'rnatilgan kompyuter tizimi.

Unauthorized access - Beruxsat munosabat. Sub'ekt tomonidan axborotga va axborot vositalariga nisbatan cheklab kuyilgan qoidalarning buzilishi.

Unauthorized action - Beruhsat faoliyat. Sub'ektning axborot jarayonlarini amalga oshirish qoidalariga zid faoliyati.

User ID - Kalit foydalanuvchisi identifikatori. Kalitlar juftini belgilovchi jumla. Bunday jumla sifatida odatda kalit egasining to'la nomi va uning elektron pochtasi manzili ishlatiladi.

Verification - Ishonib olish(Verifikatsiya). Axborotga mahfiy kalit bilan qo'yilib, oshkora kalit bilan ochilgan raqamli imzoni shu axborotning raqamli izi (daydjesti) bilan taqqoslash. Verifikatsiya axborot chindan ham unda ko'rsatilgan sub'ektga tegishliligini va o'zgartirib qo'yilmaganligini isbotlashga imkon beradi.

Vulnerability - Axborot zaifligi. Axborotning uni pinxonaligi, butunligi yo qobilligiga putur yetkazuvchi ta'sirlarga dosh berolmaslik xossasi.

Adabiyotlar:

1. R.X. Alimov, B.Y. Xodiev, K.A. Alimov, S.U. Usmonov, B.A. Begalov, N.R. Zaynalov, A.A. Musaliev, F. Fayzieva, «Milliy iqtisodda axborot tizimlari va texnologiyalari», O'quv qo'llanma, T. Sharq, 2004 yil.
2. M.T. Gafurova, D.Ch. Dursunov, V.I. Rapoport, B.Y. Xodiev. Proektirovanie sovremenno'x informatsionno'x texnologiy. Uchebnoe posobie.- Toshkent, TDIU, 1994.-96 s.
3. Informatsionno'e sistemo' v ekonomike: Uchebnik/Pod red. prof. V.V. Dika.- M.:Finanso' i statistika,1996.-272 s.
4. Informatika: Uchebnik/Pod red. N.V. Makarovoy. -M.: Finanso' i statistika, 1997.-768s.
5. /ulomov S.S. va boshq. Iqtisodiy informatika: Oliy o'quv yurtlarining iqtisodiy mutaxassisliklari uchun darslik.
6. /ulomov S.S., Shermuhammedov A.T., Begalov B.A.; S.S. /ulomovning umumiy tahriri ostida. —T.: «O'zbekiston», 1999. —528 b.
7. Kozo'rev A.A. Informatsionno'e texnologii v ekonomike i upravlenii: Uchebnik, 2-e izd. .—SPb.: Izd-vo Mixaylova V.A., 2001. —360 s.
8. Xodiev B.Y., Musaliev A.A., Begalov B.A. Vvedenie v informatsionno'e sistemo' i texnologii. Uchebnoe posobie /Pod red. akad. S.S. Gulyamova. — T.:TGEU, 2002. —156 s.
9. Shafrin Y.A. Informatsionno'e texnologii. —M.: Laboratoriya Bazovo'x Znaniy, 1998. —704 s.
10. Petrov B.N. Informatsionno'e sistemo'. – SPb.: Piter, 2003. – 688s.:il.

+o'shimcha adabiyotlar:

1. Dening V., Essig G., Maas S. Dialogovo'e sistemo' "Chelovek-EVM". Adaptatsiya k trebovaniyam polzovatelya: Per. s angl.- M.: Mir,1984.-112 s.,il.
2. Dovgyallo A.M. Dialog polzovatelya s EVM: Osnovo' proektirovaniya i realizatsii.-Kiev:Naukova dumka,1981
3. Kouts R., Vleymink I. Interfeys "chelovek-kompyuter": Per. s angl.-M.: Mir, 1990.-501 s.
4. Gafurova M.T., Dadabaeva R.A. Personal kompyuterlarning programm sistemalari.- Toshkent, TDIU, 1992.-100 bet.
5. R.Person Windows 95 v podlinnike: Per. s angl.-SPb: VNV- Sankt-Peterburg, 1996.-736 s.
6. A.I. Marchenko, V.P. Pasko Word 7.0 dlya Windows 95: K.: Torgovo-izdatelskoe byuro VNX, 1996.-464 s.
7. Kompyuterlashtirishni yanada rivojlantirish va axborot kommunikatsion texnologiyalarini joriy etish to'\risida \\Xabarnoma. –2002, №2.
8. Gafurova M.T., Dursunov D.Ch. Standartizatsiya oformleniya diplomno'x, kursovo'x proektov i laboratorno'x rabot: Metodicheskie ukazaniya.—T.: TDIU,1988.—80 b.
9. Ostreykovskiy V.A. Informatika. M.: Vo'sshaya shkola, 1999.
10. IBM PC dlya polzovatelya. Figurnov V.E. M.: Infra, 2001.

11. Raxmonqulova S.I. Shaxsiy kompyuterda ishlash. Toshkent - “Shark”, 1998.
12. Djoy Kreynak. Internet. Sankt-Peterburg, Piter, 1999.
13. www.piter.com
14. www.intuit.ru
15. www.it-study.ru
16. www.informatika.ru
17. www.edu.uz
18. www.ref.uz