O’zbekiston Respublikasi Oliy va O’rta maxsus ta`lim vazirligi

Namangan muhandislik-pedagogika instituti

«Kasb ta`limi» fakulteti

Kasb ta`limi (Informatika va AT) kafedrasi

«Axborot xavfsizligi» fanidan

MA’RUZALAR MATNI

Namangan – 2016 y

Ushbu ma’ruzalar matni Kasb ta`limi (Informatika va axborot tehnologiyalar) yo’nalishi bo’yicha ta`lim olayotgan kunduzgi bo’lim talabalari uchun mo’ljallangan bo’lib, “Axborot xavfsizligi” fanidan ma’ruza mashg’ulotlarini o’tkazish bo’yicha barcha ma’lumotlarni o’z ichiga olgan.

Ma’ruzalar matnidan, “Axborot xavfsizligi” fanini mustaqil o’rganuvchi talabalar, magistrlar va o’qituvchilar foydalanishlari mumkin.

Mualliflar: S. Hoshimov Kasb ta`limi (Informatika va AT) kafedrasi dotsenti

Taqrizchilar: K. Ismanova Axborotlar texnologiyalari kafedrasi mudiri, dotsent

Ma’ruzalar matni NamMPI Kasb ta`limi (Informatika va axborot tehnologiyalar) kafedrasining umumiy majlisida ko’rib chiqilgan va ma`qullangan.
(Bayonnoma №_____ «___» _____ 2016 yil)

Ma’ruzalar matni NamMPI «Kasb ta`limi» fakulteti ilmiy-uslubiy kengashida muxokama qilingan va ko’rib chiqish uchun institut ilmiy kengashiga tavsiya etilgan.
(Bayonnoma №_____ «___» _____ 2016 yil)

Ma’ruzalar matni NamMPI ilmiy-uslubiy kengashida muxokama qilingan va chop etishga tavsiya etilgan.
(Bayonnoma №_____ «___» _____ 2016 yil)

1-MA`RUZA(2 soat). Ma`lumotlarni muhofaza kilish tushunchasi. Tizim xavfsizligining asosiy printsiplari. Himoyaning buzilishi. Ma`lumotlarning himoya kiluvchi tizimlarning modellarida interaktiv usullar tadbiqi. Kompyuter sistemalari va tarmoqlarida xavfsizlik modellari.

O'quv modullari

Kirish

1. Ma`lumotlarni muhofaza qilish tushunchasi.
2. Tizim xavfsizligining asosiy printsiplari. Himoyaning buzilishi.
3. Ma`lumotlarning himoya kiluvchi tizimlarning modellarida interaktiv usullar tadbiqi. Komp yuter sistemalari va tarmoqlarida xavfsizlik modellari.

Aniqlashtirilgan o'quv maqsadlari.Talaba bu mavzuni to'la o'zlashtirgandan so'ng:

- ❖ Ma`lumotlarni muhofaza qilish haqidagi tamoyillarni biladi;
- ❖ Sistema xavfsizligining asosiy printsiplarini bo'laklarga bo'lib, ta`rif bera oladi;
- ❖ Sistema tashkil etuvchilarining butunligi – sistema xususiyatlarinini talqin eta oladi;
- ❖ Informatsiyaning ishonchliligi printsiplarini qaysi sinfga mansubligini tasavvur eta oladi;
- ❖ Sistema tashkil etuvchisidan foydalanuvchanligi o'rtasidagi o'zaro aloqadorlikni aniqlaydi, bog'lanishlarni tahlil qila oladi.

Tayanch so'z va iboralar:

Ma`lumot xavfsizligi,informatsiya ishonchliligi,himoya modellari,sistema xavfsizligi, foydalanuvchi, kritik informatsiya, nokritik informatsiya

Kirish

"Informatika va axborot texnologiyalari" yo'nalishida tayyorlanayotgan muxandis-pedagoglar fanlardan olgan bilimlarini xalk xujaligining turli jarayonlarini ifodalovchi, axborot xavfsizligi va oddiy kriptografik shifrlash masalalarini yechish, kullay olishlari uchun kriptoanalitik usullardan foydalanish malakalariga ega bulgan malakali mutaxassislar bulishligini bugungi zamon talablari takozo etmokda.

Ildam qadamlar bilan rivojlanayotgan komp yuter axborot texnologiyalari

hayotimizda sezilarli o’zgarishlarga sabab bo’lmoqda. "Axborot" tushunchasi sotib olish, sotish, biror narsaga almashish va h. mumkin bo’lgan maxsus tovarni belgilashda tez-tez ishlatila boshlandi. Bunda axborotning narxi ko’pincha u joylashgan komp yuter tizimi narxidan yuz va ming marta yuqori bo’ladi. Demak, axborotni ruxsatsiz foydalanishdan, atayin o’zgartirishdan, yo’q qilishdan va boshqa jinoiy harakatlardan himoyalash zaruriyatining paydo bo’lishi tabiiydir.
Axborotni himoyalash muammosi komp yuter tizimlari va tarmoqlari sohasida faoliyat ko’rsatuvchi mutaxassislar hamda zamonaviy komp yuter vositalaridan foydalanuvchilar e`tiborini jalb etmoqda.

Komp yuter texnikalarining ommalashishi xamda shu soxadagi davlat strategik axamiyatidagi ishlarning olib borilishi, axborotlarni ximoyalash chora-tadbirlarini kuchaytirishni talab etadi. Bu esa, oldimizga kator vazifalarni kuyadi.

Fanning maksad va vazifalari.

Uzbekistonda iktisodiy isloxotlarni chukurlashtirish sharoitida axborot xavfsizligini ta`minlash bosh masalalardan biridir.

Axborot vositalari yordamida davlatlar, yirik korxonalar, banklar, intellektual mulk egalari, talantli menedjerlarning uzaro alokalari, kuyingki, barcha yashirin, sirli axborotlarni xavf-xatarsiz uz manziliga yetkazish muammosi tugildi.

Ushbu fanni ukitishdan maksad - talabalarda zamonaviy antivirus bazalaridan, kriptografik shifrlash uslublaridan foydalanib, axborot xavfsizligini ta`minlay olish kobiliyatini shakllantirishdan iborat.

Fanning vazifasi - viruslarni sinflarga ajratish, antivirus dasturlarini urnatish, parametrlarini sozlash xamda mustakil ravishda kriptografik uslublardan unumli foydalanish kabi bilim va kunikmalarni talabalarga urgatishdir.

Fan buyicha talabaning malakasiga kuyiladigan talablar

“Axborot xavfsizligi” fanini uzlashtirish jarayonida amalga oshiriladigan masalalar doirasida bakalavr:

- axborot xavfsizligining usul va vositalarini, shifrlash algoritmlarini, tarmok ma`lumotlarini muxofazalash uslublarini, ma`lumotlarni loyixalash boskichlarini bilishi va ulardan foydalanishni bilishi kerak;
- kriptografik usullarni uzlashtirish, kattik diskdagi ma`lumotlarni kuchirishda ximoyalash, mavjud shifrlash usullarini kullab axborotni maxfiylashtira olish kunikmalariga ega bulishi kerak.
- kompyuter tarmoklarini muxofazalash mexanizmlari, fan soxasining asosiy konsepsiyalari, ilgor firmalar tomonidan ishlab chikilgan axborot xavfsizligini ta`minlovchi zamonaviy dasturiy vositalardan foydalanish malakalariga ega bulshii kerak.

1.Ma`lumotlarni muhofaza qilish tushunchasi.

Hozirgi paytda komp yuter sistemalarida ma`lumotlarni muhofaza qilishni ta`minlash masalasi dolzarb masalalardan biri bo'lib qolmoqda. Informatsiyaning hammasi ham himoyaga muhtoj emas. Shuning uchun informatsiya o'z xarakteriga ko'ra kritik va nokritik informatsiyaga bo'linadi. **Kritik informatsiya** foydalanuvchining shaxsiy ishlab topgan ma`lumotlari bo'lib, xizmatchi informatsiya, savdo-sotiqqa oid sirlarni o'z ichiga oluvchi informatsiya yoki maxfiylikning turli ko'rinish yoki shakllariga oid informatsiya va h. bo'lishi mumkin. Bu bobda kritik ma`lumotlarni muhofaza qilish bilan bog'liq masalalarga e`tibor qaratiladi.

Ayni paytda komp yuter texnikasidan foydalanuvchilarning hammasi ham bu masalalarning muhimligini anglab yetmaydilar. Mamlakatimizning bozor iqtisodiga o'tishi ko'plab firma va banklarning tashkil etilishiga olib keldi, bu firma va banklarning samarali ishini esa komp yuterlarsiz tashkil etib bo'lmasligi hammaga ayon. Komp yuter texnikasidagi har qanday buzilish o'sha firma yoki tashkilot uchun jiddiy yo'qotishlarga olib kelishi mumkin. Shuning uchun ham ma`lumotlarni muhofaza qilish masalasiga jiddiy yondashmoq zarur.

Sistemaning xavfsizligi deganda, uning foydalanuvchi yoki egalariga, turli qasddan yoki tasodifiy qilingan ta`sirlar natijasida, katta talofotlar yetkazishga bardosh bera olish xususiyati tushuniladi. Boshqacha so'z bilan aytganda, sistema xavfsizligi deganda uning ish jarayonining bir maromda ketishiga xalaqit beruvchi to'siqlar, tasodifiy yoki ataydan puxta o'ylangan xalaqitlar, shuningdek, uning tashkil etuvchilarini o'g'irlash, o'zgartirish yoki buzishga qaratilgan urinishlarga qarshi himoya qobiliyati tushuniladi.

2.Tizim xavfsizligining asosiy printsiplari. Himoyaning buzilishi.

Sistemaning xavfsizligiga 3 ta asosiy printsiplarni ta`minlash bilan erishiladi:

1) ***Sistema tashkil etuvchilarining butunligi*** – sistema xususiyatlarining uning ish jarayonida o'zgarmasligi. Ekspluatatsiya jarayonida sistema administratori tomonidan bir qator foydali o'zgartirishlar o'tkaziladi va bu o'zgartirishlarning kam-ko'sti to'ldirilib oxirigacha yetkaziladi (masalan - WinNT sistemasiga qo'shimcha to'latuvchi paketni o'rnatish), lekin bunda talab qilingan xususiyatlar o'zgarmaydi - ilgarigidek foydalanuvchini identifikatsiya qilish va uning sistemadagi ishini ta`minlashi kerak.

2) ***Informatsiyaning ishonchliligi*** – bu informatsiyaning shunday xususiyatiki, bunda u sistemaning faqat ruxsat etilgan va tekshiruvdan o'tgan sub`ektlarigagina (foydalanuvchilar, programmalar, jarayonlar va h.) ma`lum bo'ladi.

3) ***Sistema tashkil etuvchisidan foydalanuvchanligi*** – faqat muallif sub`ektlarning sistema tashkil etuvchisidan ixtiyoriy paytda foydalana olish xususiyati. Boshqacha aytganda, sistemaning har bir foydalanuvchisi identifikatsiya qilingan va foydalanuvchining foydalanish darajasiga muvofiq holda sistema tashkil etuvchilaridan foydalanishga ruxsat etilgan bo'lishi kerak. Bunda foydalanish darajasi xizmatchining xizmat mavqei bilan emas, balki uning qat`iy funktsional majburiyatlari bilan aniqlanadi.

3.Ma`lumotlarning himoya kiluvchi tizimlarning modellarida interaktiv usullar tadbiqi. Komp yuter sistemalari va tarmoqlarida xavfsizlik modellari.

Ma`lumki, hozirda komp yuter va komp yuter sistemalari avtonom holda kam foydalaniladi. Ular odatda bir-birlari bilan lokal, korporativ va global tarmoqlar orqali bog'lanadi. Komp yuter sistemalarining ma`lumotlar bazasida katta hajmdagi informatsiya shakllangan. Uning yo'qolishi, buzilishi yoki beruxsat foydalanilishi katta iqtisodiy talofotlarni keltirib chiqarishi mumkin. Bundan chetlashish maqsadida beruxsat foydalanishlardan informatsiyani himoya qilishning har xil sistemalari qo'llaniladi.

Samaradorligi yuqori bo'lgan informatsiyani himoya qilish sistemasini ishlab chiqish avvalo, bu sistemaning kontseptsiyasini aniqlashni taqozo etadi. Tadqiqot o'tkazishda va modellashtirishda informatsiyani himoya qiluvchi vosita yuqori darajadagi himoya qobiliyatiga ega ekanligini isbotlashi lozim.

Informatsiyani himoya qiluvchi sistemalarning ko'pgina modellari ishlab chiqilgan. Biroq eng ko'p foydalaniladigan modellar quyidagilardir:

1. Bella va La-Padula; bunda **foydalanish huquqini cheklash vositalarini** qurish uchun **faol** sub`ektlar S va **passiv** sub`ektlar Q tushunchalari kiritiladi. Ushbu holda sub`ektlar foydalanishning har xil huquqlariga ega bo'ladilar. Bunday model gohida "foydalanish huquqini cheklashning matritsali modeli" deb ham yuritiladi;

2. Dening modeli – har xil darajadagi maxfiylikka ega hujjatlar bilan ishlashda informatsiyani himoya qilish vositasining ko'p sathli ierarxik modeli; bu yerda informatsiyani himoya qilishning kontsentrlashgan xalqasi tushunchasi kiritiladi. Ichki xalqalarda – maksimal maxfiylik darajasi mavjud bo'lib, tashqi qurilma (periferii)ga yaqinlashgan sari maxfiylik darajasi kamayadi;

3. Lendver modeli - shunday komp yuter tarmoqlarida foydalaniladiki, bunday tarmoqdagi ma`lumotlarni muhofaza qilish informatsiyani kiritish-chiqarish operatsiyalarining himoyasi bilan ta`minlanadi.

Ko'pgina real vaqt masshtabida ishlaydigan mavjud operatsion sistemalar uchun Bella va La-Padula himoya sistemasi kontseptsiyasidan foydalaniladi. Bu

modelda foydalanish dispetcherining qo’llanilishi talab etiladi. Informatsiyani himoya qilish sistemasining o’zi esa uchlik ko’rinishida tasvirlanadi:

Zq(S,Q,P)

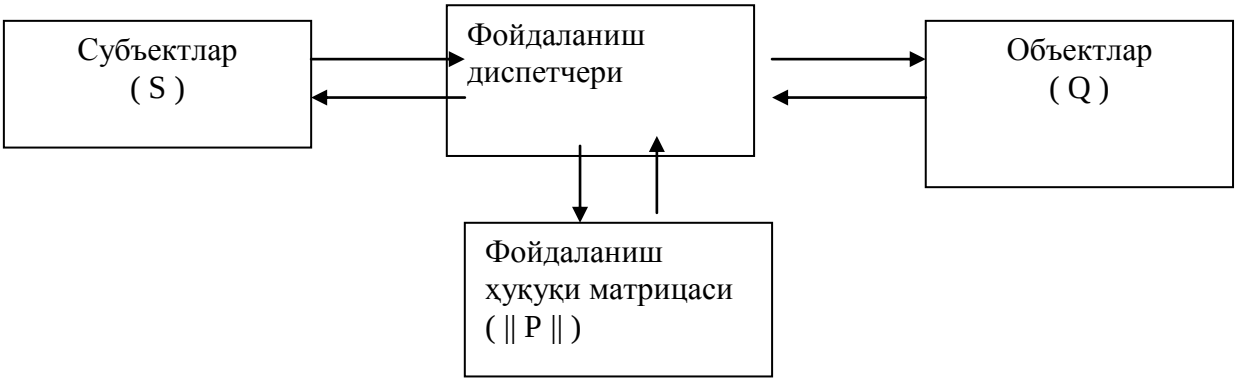
bu yerda:

S – **foydalanuvchilar** va ular programmalaridan iborat sub`ektlar hamda o’zidan-o’zi paydo qiluvchi jarayonlar, protseduralar va b.;

Q – sub`ektlar bilan so’rov olib borishi mumkin bo’lgan sistemaning **ob`ekt (resurslari) to’plami;** ob`ektlarga programmalar, protseduralar, ma`lumotlar disklari, tomlar, fayllar, alohida fayl yozuvlari va qurilmalar mansub;

P – sub`ektlarning ob`ektlardan foydalanish **huquqlari to’plami**.

Informatsiyani himoya qilish sistemasining umumiy strukturasi 1-rasmda keltirilgan.



1-rasm. Informatsiyani himoya qilish sistemasining umumiy strukturasi.

Bitta protsedura bir vaqtda ham sub`ekt, ham ob`ekt bo’lib chiqishi mumkin. Foydalanish huquqi bitli vektorlar bilan aniqlanadi. Har bir bit ta`qiqlash (zapret) yoki ruxsat berishni aniqlaydi: R, E, W, M, A, O; bu yerda R – o’qish, ye – tahrirlash, W – yozish, A – administrator, O – to’liq mulkdor (polniy sobstvennik).

Foydalanishning minimal huquqi to’rt bit bilan aniqlanadi: R, E, W, M. Foydalanish huquqini foydalanish administratori aniqlaydi va hech qaysi foydalanuvchi ||P|| matritsadan foydalanish imkoniga ega emas, lekin uni o’zgartirishi mumkin.

Ko’proq ishonchli haqiqiylikka mos model sifatida o’yin himoya modellari ifodalanadi, ya`ni bunday modellarda kamida ikkita tomon mavjud bo’ladi. Birinchi tomon informatsiyani himoya qilish sistemasini, ikkinchi tomon esa birinchi tomon vositasida qurilgan himoyani egallash sistemasini quradi.

Shunday bo’lishiga qaramasdan ko’pgina atakalar va beruxsat foydalanishga bo’lgan harakatlar passiv (ya`ni foydalanuvchi haqida informatsiya yig’ish va

nusxalash) hisoblanadi va o’zida faol atakaga tayyor potentsial buzg’unchini oshkor qilishi ham mumkin.

Himoya sistemasini ishlab chiqish himoya qilinishi lozim bo’lgan sistemaning o’zini ishlab chiqish bilan birga olib borilishi kerak.

Himoya sistemasini yaratish tajribasi quyidagi asosiy printsiplarni ajratish imkonini beradi. Ular loyihalashda e`tiborda bo’lishi kerak.

1. *Himoya mexanizmining soddaligi.* Bu printsip shunga asoslanganki, loyihalashda va ekspluatatsiyada yuzaga chiqqan ayrim xatolar foydalanishning e`tiborga olinmagan yo’llarini aniqlashga imkon beradi. Shunga asosan himoyaning apparat va programm vositalarini sinchiklab testlash kerak, biroq amaliyotda bunday tekshiruvning faqat sodda va ixcham sxemalar uchun imkoniyati mavjud.

2. *Informatsiyaning chetga chiqib ketishi mumkin bo’lgan hamma kanallarning yopiqligi.* Bu printsip har qanday ob`ektga bo’ladigan har qanday murojaat huquqini (vakolatini) tekshirishga mo’ljallangan va himoya sistemasining asosi hisoblanadi.

Bu printsipni hisobga olgan holda, foydalanishni boshqarish masalasi umumsistema sathida yechilishi lozim. Bunda ishga tushirish, buzilishlardan so’ng qayta tiklash, ajratish va profilaktik xizmat ko’rsatish kabi ish rejimlari e`tiborga olinadi. Ma`lumotlarga bo’ladigan har qanday murojaat manbaini ishonchli aniqlashni ta`minlashi zarur.

3. *Himoya mexanizmining jiddiy bo’lmagan maxfiyligi*. Keng foydalanishga mo’ljallangan himoya sistemasini amalga oshirish detallarini yashirishi shart emas. Himoya samaradorligi potentsial buzg’unchilarning mahoratiga bog’liq bo’lmasligi kerak. Chunki parollar ro’yxati himoyasini ta`minlash ancha sodda kechadi. Himoya mexanizmining maxfiy emasligi zarur hollarda, uning mutaxassislar orasidagi keng muhokama sub`ekti bo’lishi imkonini beradi.

4. *Foydalanuvchilar huquq va vakolatlarining taqsimlanishi*. Komp yuter tarmoqlari va sistemalarida bir qancha himoya kalitlarining mavjudligi qachonki foydalanishga bo’lgan huquq bir qator shartlar bajarilishi bilan aniqlangan holatdagina qulaylik tug’diradi.

5. *Minimal vakolat.* Har qanday foydalanuvchi va programma uchun topshirilgan ishni bajarish uchun zarur bo’lgan vakolatning minimal doirasi aniqlangan bo’lishi kerak. Shunga ko’ra tasodifiy buzilishlarga sabab bo’ladigan zararlar ma`lum miqdorda kamayishi mumkin.

6. *Himoya mexanizmining maksimal ixtisoslashtirilganligi*. Foydalanuvchilar orasida informatsiya almashishini istisno qilish maqsadida himoya sxemasini loyihalashda bir necha foydalanuvchilar uchun umumiy bo’lgan

parametrlar va himoya mexanizmi xarakteristikasi sonini minimumga olib kelish maqsadga muvofiq.

7. ***Psixologik jozibadorlik.*** Himoya sistemasini ekspluatatsiya qilish sodda bo'lish lozim. Foydalanuvchining himoya sistemasi haqidagi tasavvurlari uning faktlarga asoslangan imkoniyatlari bilan qanchalik mos tushsa, qo'llash jarayonida xatolar shunchalik kam bo'ladi. Ayrim sun`iy tillarning himoya sistemasiga murojaat qilishda foydalanilishi qo'shimcha xatolar manbai bo'lib xizmat qiladi. Yuqorida sanab o'tilgan printsiplarning ayrimlariga asoslangan sistemani qurishda ularni amalga oshirishda sarflanadigan katta xarajatlar bilan bog'liq jiddiy to'siqlar yuzaga keladi. Shuning uchun himoya sistemalarini loyihalashdagi muhim faktor sifatida uning iqtisodiy samaradorligini ko'rsatish mumkin.

Shuni esda tutish lozimki, faoliyatning alohida tarmoqlari (bank va moliya institutlari, informatsion tarmoqlar, davlat boshqaruv sistemalari, mudofaa va maxsus xizmat strukturalari) ma`lumotlar xavfsizligi bo'yicha maxsus chora-tadbirlar ko'rishni talab qiladi va bu tarmoqlarda yechilayotgan masalalarning xarakteri va ahamiyatiga mos holda informatsion sistemaning ishlash ishonchliligiga bo'lgan talablar juda yuqori bo'ladi.

Ma`lumotlarni muhofaza qilish masalasini ko'rib chiqishda, dastavval, ma`lumotlarni o'rinsiz (nomatlub, noma`qul) o'zgartirish yoki yo'qotishga olib keluvchi ruxsatsiz foydalanish yoki buzishning turlari bilan tanishib chiqish lozim. Bunday jiddiy tahdidlardan quyidagilarni keltirish mumkin:

- jihoz (qurilma) larning buzilishi: kabel sistemasining buzilishi, elektr manbaining o'chib-yonishi, disk sistemasining buzilishi, ma`lumotlarni arxivlash sistemasining buzilishi, serverlar, ishchi stantsiya
- lar, tarmoq kartalarining buzilishi;
- programma ta`minotining noto'g'ri ishlashi oqibatida kelib chiqadigan informatsiya yo'qolishi, programma ta`minotining nosozligi natijasida ma`lumotlarning o'zgarib ketishi yoki yo'q bo'lib ketishi, sistemaning komp yuter viruslari bilan zararlanishi natijasida ma`lumotlarning yo'qolishi va h.;
- ruxsatsiz foydalanish bilan bog'liq yo'qotishlar: informatsiyadan ruxsatsiz nusxa olish, yo'qotish yoki qalbakilashtirish, maxfiy, sir tutilishi lozim bo'lgan informatsiyani begona kishilarga tanishtirish;
- arxiv ma`lumotlarini noto'g'ri saqlash bilan bog'liq yo'qotishlar;
- xizmatchi shaxs yoki foydalanuvchining xatolari: ma`lumotlarni o'zi bilmagan holda o'zgartirish yoki yo'qotib yuborish, ma`lumotlarning yo'qolishiga yoki buzilishiga olib keluvchi programma yoki apparat ta`minotidan noto'g'ri foydalanish.

Bu tahdidlardan kelib chiqib, informatsiyani himoyalashning barcha turlarini quyidagi 3 ta sinfga bo'lish mumkin:

- ***fizik himoyalash vositalari:*** kabel sistemasini, elektr manbai sistemasini himoyalash vositalari, himoyalashning apparat vositalari, arxivlash, diskli massivlar va h.;
- ***himoyalashning programma vositalari:*** antivirus programmalari, vakolatlarni (foydalanish imkoniyatlarini) cheklash sistemasi, foydalanishni nazorat qiluvchi programma vositalari;
- ***himoyalashning ma`muriy chora-tadbirlari:*** binoga kirishni nazorat qilish, firma yoki tashkilotning xavfsizligini ta`minlash strategiyasini ishlab chiqish, favqulodda holatlarda harakat qilish rejalarini tuzib chiqish va b..

Bunday sinflash shartli ekanligini unutmaslik lozim, chunki Hozirgi zamonaviy texnologiyalar apparat-programm himoya vositalari bilan bir yo'nalishda rivojlanib bormoqda. Bunday apparat-programm vositalaridan, xususan, viruslardan himoyalanish, foydalanishni nazorat qilish va h. keng tus olmoqda.

Banklarda naqd pullar yig'ilgani kabi komp yuterda ham informatsiyaning to'planishi ham informatsiyani himoyalash maqsadida nazoratni yanada kuchaytirishni talab qiladi.

Yuridik masalalar, xususiy sir, maxfiy ma`lumotlar, milliy xavfsizlik - bularning barchasi tijorat va hukumat tashkilotlarida ichki nazoratni kuchli tashkil etishni talab qiladi. Bu yo'nalishdagi ishlar yangi «Ma`lumotlarni muhofaza qilish» fanining paydo bo'lishiga olib keldi. Ma`lumotlarni muhofaza qilish bo'yicha mutaxassis tashkilotda yig'ilgan informatsiyaning butunligi, maxfiyligi, foydalanishga yaroqliligini ta`minlashga qaratilgan ma`lumotlarni muhofaza qilish sistemasini ishlab chiqish, yo'lga qo'yish va ishlatish ishlariga mas`uldir. Uning vazifalariga informatsion resurslarni fizik (texnik vositalar, aloqa kanallari va uzoqlashtirilgan komp yuterlar) hamda mantiqiy (ma`lumotlar, amaliy programmalar va operatsion sistemalar) himoyalashni ta`minlash kiradi.

Informatsiyani himoyalash sistemasini yaratish murakkabligi shundaki, ma`lumotlar komp yuterdan o'g'irlanishi bilan bir vaqtda o'z joyida qolishi ham mumkin, ya`ni ba`zi ma`lumotlarni yo'qotish yoki o'zgartirish emas, balki butunicha nusxa ko'chirib olib ketishning o'zi kifoya qiladi.

Ma`lumotlarni muhofaza qilishni ta`minlash - qimmat hamda katta sarf-xarajatlarni talab qiladigan ish bo'lib, vositalarni sotib olish yoki o'rnatishga qancha sarf-xarajat qilinmasin, mos ta`minot sistemasining ishga layoqatli holatini va oqilona xavfsizlik chegarasini malakali aniqlash shunchalik qiyin

bo’ladi. Agar lokal tarmoq umumiy foydalaniluvchi ko’p sonli informatsiya fayllari, qimmatbaho rangli printerlar yoki litsenzion programma vositalaridan birgalikda foydalanish maqsadida ishlab chiqilgan bo’lsa, u holda informatsiyani hatto minimal shifrlash yoki deshifrlash ham talab qilinmaydi.

Informatsiyani himoyalash vositalarini loyihalash, sotib olish yoki o’rnatishni yetarlicha tahlillarni olib bormasdan turib amalga oshirish kerak emas. Tavakkalni tahlil qilish ko’plab faktorlar (ishning buzilishining paydo bo’lishi, ishning buzilishining paydo bo’lish ehtimolligi, tijorat yo’qotishlardan zarar ko’rish, sistemaning tayyorgarligi koeffitsientining kamayishi, jamoat munosabatlari, yuridik muammolar) ning ob`ektiv baholarini berishi hamda xavfsizlikning mos turlarini va darajalarini aniqlash uchun informatsiya taqdim etishi shart. Tijorat tashkilotlarining barchasi ma`lum darajada ko’p bo’lgan kritik korporativ informatsiyani katta-katta hisoblash sistemalaridan olib, ochiq sistema vositalariga uzatishda xavfsizlik sistemasidan foydalanish va uni yo’lga qo’yishda yangi, hali noma`lum bo’lgan murakkab muammolarga duch keladilar. Hozirda ko’plab tashkilotlarda tijorat ma`lumotlarini boshqarish uchun yuqori quvvatli, taqsimlangan ma`lumotlar bazasi va klientG’server texnologiyasidan foydalanilmoqda. Taqsimlanishning o’sishi bilan birga bu ma`lumotlarga ruxsatsiz kirish va ularni buzish imkoniyatlari ham ko’payib bormoqda.

Komp yuter sistemasining xavfsizligiga erishish jarayonida sistemaga ta`sir etishi mumkin bo’lgan barcha holatlarni tahlil va prognoz qilish kerak. Sistemaga ko’rsatiladigan ta`sirlar 2 turga farqlanadi - ***tasodifiy*** va ***ataydan (qasddan) qilingan ta`sirlar***.

Foydalanilgan adabiyotlar ro’yxati

1. S.Petrenko ,M.Mamaev «Texnologii zahito’ v Internete» Izdatel skiy dom «Piter» , Sankt-Peterburg, 2002 g.
2. Turskiy A. , Panov S «Zahita informatsii pri vzaimodeystvii korporativno’x setey v Internet» , FiS, Moskva, 2003 g.
3. Koshelev A.»Zahita setey i firewall» Komp yuterPress, 2000 g.
4. Faniev S. K., Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI(Axborot-kommunikatsion tizimlar xavfsizligi) G’Oliy o’quv yurt talabalari uchun mo’ljallangan.-T.:TDTU-2008.

2-MA`RUZA

Tasodifiy ta`sirlar va ulardan informatsiyani

muhofaza qilish usullari. (2 soat)

O’quv modullari

1.Sistemaga talafot yetkazadigan tasodifiy ta`sirlar tushunchasi.

2.Disk va kanallarni rezervlash.

3.Informatsiyani himoya qiluvchi sistemalarning modellari.

Aniqlashtirilgan o’quv maqsadlari.Talaba bu mavzuni to’la o’zlashtirgandan so’ng:

- ❖ Ma`lumotlarni muhofaza qilish haqidagi tamoyillarni biladi;
- ❖ Sistema xavfsizligining asosiy printsiplarini bo’laklarga bo’lib, ta`rif bera oladi;
- ❖ Sistema tashkil etuvchilarining butunligi – sistema xususiyatlarinini talqin eta oladi;
- ❖ Informatsiyaning ishonchliligi printsiplarini qaysi sinfga mansubligini tasavvur eta oladi;
- ❖ Sistema tashkil etuvchisidan foydalanuvchanligi o’rtasidagi o’zaro aloqadorlikni aniqlaydi, bog’lanishlarni tahlil qila oladi.

Tayanch so’z va iboralar:

Tasodifiy ta`sirlar, Ko’zguli disklar , Disk va kanallarni rezervlash , Serverni «qaynoq» rezervlash, Uzluksiz energiya manbai.

1.Sistemaga talafot yetkazadigan tasodifiy ta`sirlar tushunchasi.

***Tasodifiy ta`sirlar*** – bu sistemaga talofot yetkazadigan yoki uni umuman ishdan chiqaradigan ta`sirlar. Masalan, elektr manbaining buzilishi, qurilmaning ishdan chiqishi, yong’in, suv bosishi va shu kabilar. Tasodifiy ta`sirlar natijasida informatsiya buzilishi yoki yo’qolishi mumkin.

2.Disk va kanallarni rezervlash.

Shuning uchun quyidagi informatsiyani himoya qilish va tiklash vositalaridan foydalanish mumkin:

Ko’zguli disklar (zerkal no’e diski) – bular disklarning fizik zararlanishi bilan bog’liq yo’qotishlarning oldini olish uchun disklarni rezervlash maqsadida foydalaniladigan disklar.

Disklarni rezervlash uchun bitta disk kontrolleriga 2 ta mutlaqo bir xil vinchester ulanadi va operatsion sistema shunga muvofiq moslashtiriladi.

So’ngra asosiy diskdagi barcha informatsiya ***ko’zguli disk*** deb nomlanuvchi ikkinchi diskda ikkilantiriladi.

Asosiy disk zararlanganda maxsus protseduralar yordamida ko’zguli diskdan barcha ma`lumotlarni qayta tiklash mumkin. qo’shimcha ravishda disk yo’lakchalarining «qaynoq» rezervlash ham ishlatiladi. Diskda «qaynoq» rezervlash sohasi ajratib olinadi. Agar ish jarayonida diskda nuqsonli yo’lakcha topilsa, bu yo’lakcha rezervlash sohasidagi yo’lakcha bilan almashtiriladi.

Disk va kanallarni rezervlash - ko’zguli disklardan foydalanishda ikkala diskning ham kanali, kontrolleri va tok manbai zararlanish ehtimoli mavjud. Ba`zi operatsion sistemalar (masalan, NetWare) kanalni butunlay rezervlay olish imkoniyatiga ega, mos ravishda ikkita diskka ulangan kontrollerdan foydalanishi mumkin. Bu kontroller va disklarni tok bilan ta`minlash uchun ikkita tok manbai kerak.

Serverni «qaynoq» rezervlash – ko’zguli diskdan ma`lumotlarni tiklash disk xotira hajmiga bog’liq ravishda bir necha soatlab vaqtni olishi mumkin. Ba`zida tarmoqda ishning bunday uzoqqa cho’zilishini kutib bo’lmaydi. Bunday hollarda serverlarni «qaynoq (goryachee)» rezervlashdan foydalanish ma`qul. Serverlarni qaynoq rezervlashning ma`nosi shuki, bunda ikkita server MSL-adapter (Microred Server Link) deb ataluvchi maxsus adapter yordamida tezlashtirilgan aloqa liniyasi orqali o’zaro bir-biriga ulanadi. Bu adapterlar o’zaro 33 m gacha uzunlikdagi koaksial kabel yoki 4 km gacha uzunlikdagi optik tolali kabel yordamida biriktiriladi. Bu usulda turli serverlarni turli binolarga joylashtirgan holda, hattoki binolarning birortasidan yong’in chiqqan sharoitda ham sistema ishining ishonchliligi va mustahkamligini ta`minlash mumkin.

Bitta serverning ishdan chiqishi tarmoq ishining to’xtab qolishiga olib kelmaydi, chunki bunda avtomatik ravishda ikkinchi rezerv-server ishga tushadi. Yuqori tezlikdagi aloqa kanalidan foydalanish evaziga rezerv-server diski ham asosiy diskdagi fayllarni o’zida saqlaydi, shuning uchun ma`lumotlarni tiklash kabi ortiqcha amallarni bajarishga hech ham xojat qolmaydi.

Uzluksiz energiya manbai – agar tarmoqning ishi yoki serverdagi ma`lumotlarning ishonchli saqlanishiga katta talab qo’yiladigan bo’lsa, u holda uzluksiz energiya manbai qurilmasidan foydalanmoq joiz. Bu qurilma shunchaki ma`lum vaqt davomida serverni tok bilan ta`minlovchi akkumulyator emas. Bu qurilma maxsus adapter orqali serverga ulanadi. Agar tok manbai bo’yicha uzilish sodir bo’lsa, qurilma serverga bu haqda signal beradi va shu signal

buyicha server sekin-asta, ma`lumotlar yo'qolishining oldini olgan holda, o'z ishini tamomlaydi.

3.Informatsiyani himoya qiluvchi sistemalarning modellari.

Mustahkamlash uchun savollar :

- Ma`lumotlar muhofazasi nimani anglatadi ?
- Disk va kanallarni rezervlash tushunchasini izohlang.
- Tasodifiy ta`sirlar tushunchasini aytib bering.
- Uzluksiz energiya manbalarini qanday turlarini bilasiz?

Foydalanilgan saytlar ro'yxati

- www.securityfocus.com-portal: materialo' po bezopasnosti
- www.sans.org-Institut SANS: stat i po bezopasnosti, proekto'
- www.xforce.iss.net-baza danno'x uyazvimostey, materialo' po bezopasnosti
- www.packetfactory.net-sayt razrabotchikov biblioteke
- blacksun.box.skG' tutorials.html-aspektam setevoy bezopasnosti raboto' s setevo'x servisov.

3-MA`RUZALAR

Қasddan qilingan ta`sirlarning turlari hamda ulardan informatsiyani himoyalash usullari **(2 soat).**

O'quv modullari

- Sistemaga qasddan qilingan ta`sirlar tushunchasi.
- Ruxsatsiz kirish (foydalanish)
- Informatsiyani himoya qiluvchi sistemalarning modellari.

Aniqlashtirilgan o'quv maqsadlari.Talaba bu mavzuni to'la o'zlashtirgandan so'ng:

❖ Ma`lumotlarni muhofaza qilish haqidagi tamoyillarni biladi;

❖ Sistema xavfsizligining asosiy printsiplarini bo'laklarga bo'lib, ta`rif bera oladi;

❖ Sistema tashkil etuvchilarining butunligi – sistema xususiyatlarinini talqin eta oladi;

❖ Informatsiyaning ishonchliligi printsiplarini qaysi sinfga mansubligini tasavvur eta oladi;
❖ Sistema tashkil etuvchisidan foydalanuvchanligi o'rtasidagi o'zaro aloqadorlikni aniqlaydi, bog'lanishlarni tahlil qila oladi.

Tayanch so'z va iboralar:

Ma`lumot xavfsizligi, informatsiya ishonchliligi, himoya modellari, sistema xavfsizligi, foydalanuvchi, kritik informatsiya, nokritik informatsiya Sistemaga qasddan qilingan ta`sirlar – bu sistema ish jarayonining bir maromda kelishiga ataydan qilingan to'sqinlik, shuningdek uning tashkil etuvchilarini o'g'irlash, o'zgartirish yoki buzishga qaratilgan urinishlardir. quyida ma`lumotlarni muhofaza qilishga qasddan qilingan tahdidlarning tasnifi va qisqacha tavsifi keltirilgan. Bu tasnif xavfsizlik administratori tez-tez duch keladigan qasddan qilingan ta`sirlarning asosiy turlarini ajrata olish va ulardan himoyalanish usullaridan foydalanish uchun kerak.

Ruxsatsiz kirish (foydalanish) (RK, RF) – bu komp yuter buzg'unchiligining eng keng tarqalgan turi. Bu tashkilotning xavfsizlik siyosatiga muvofiq kirishga ruxsati yo'q foydalanuvchining biror ob`ektdan foydalanish uchun kirish bilan bog'liq harakatdir. Bu yerda asosiy muammo "Kimda qaysi ma`lumotlar jamg'armasidan foydalanishga ruxsat bor? Kimda bu ruxsat yo'q?" savollariga javob topishdadir. Boshqacha aytganda "ruxsatsiz" atamasini aniqlash kerak.

Ta`sirining xarakteriga ko'ra RK (yoki RF) sistemaning xatolaridan foydalanuvchi faol ta`sirlar bo'ladi. RK odatda, bevosita ma`lumotlar jamg'armasiga murojaat qiladi yoki RK qonuniylashtirish maqsadida ruxsat etilgan kirish to'g'risidagi informatsiyaga ta`sir etadi. Tarmoqning har qanday ob`ekti RKga yo'liqishi mumkin. Har qanday ob`ektga RK standart yoki maxsus programma vositalari orqali amalga oshirilishi mumkin.

RK amalga oshirishi ma`lum ma`noda komp yuter tarmog'ini tashkil etish, undagi xavfsizlik siyosati, o'rnatilgan himoya vositalarining imkoniyatlari, shuningdek, administrator va operatorning vijdoniga bog'liq.

RKni amalga oshirishning 2 ta usuli mavjud:

- birinchidan, himoya sistemasini chuqur o'rganib barbod etish, ya`ni unga turli ta`sirlar ko'rsatib uning ish jarayonini to'xtatish. Bu juda murakkab va qiyin, hamma vaqt ham amalga oshavermaydigan, biroq samarali ishdir;
- ikkinchidan, nima e`tibordan chetda ekanligini kuzatish, ya`ni buzg'unchiga kerakli qaysi ma`lumotlar jamg'armasi foydalanishga ochiq yoki administrator e`tiboridan chetda ekanini aniqlash. Buni ham RK deb atash mumkin va amalga oshirish oson, lekin bu ishlar ma`lum bo'lib qoladigan bo'lsa, himoyalanish qiyin.

Bunday turdagi RKga parolni topish, parolni tuzish qoidalarini buzish, inson ismidan, takrorlanuvchi simvollardan parol sifatida foydalanish kabilarni ham kiritish mumkin. RKning ko'pchilik buzuvchi holatlariga puxta o'ylamasdan himoya vositasini tanlash, uni noto'g'ri o'rnatish yoki moslashtirish, ish jarayonini yaxshi nazorat qilmaslik, shuningdek ma`lumotlarning himoyasiga sovuqqon munosabatda bo'lish kabilar kiradi.

Imtiyozlardan noqonuniy foydalanish – atakaning bu usulini qo'llovchi buzg'unchilar odatda, shtatdan tashqari rejimda ishlovchi shtat programma ta`minoti (sistemali yoki amaliy PT) dan foydalanadilar. Amalda har qanday himoyalangan sistema favqulodda vaziyatlarda ishlatiluvchi, qurilma yoki vositalar buzilganda, mavjud xavfsizlik siyosatining buzilishi sharoitida ishlay oluvchi, bu vazifalarni bajara oluvchi vositalarga ega bo'ladi. Ba`zi hollarda foydalanuvchi sistemaning barcha naborlariga kirish imkoniyatiga ega bo'lishi kerak. Bunday vositalar kerak, lekin favqulodda xavfli bo'lishi mumkin. Bu vositalar odatda, administratorlar, operatorlar, sistema programmistlari va boshqa maxsus vazifalarni bajaruvchi foydalanuvchilar tomonidan foydalaniladi.

Bunday vositalardan foydalanishni kamaytirish maqsadida, ko'pchilik himoya sistemalari ularning vazifalarini imtiyozlar nabori yordamida amalga oshiradi – ma`lum vazifani bajarish uchun ma`lum imtiyozlar talab qilinadi. Bunday hollarda har bir foydalanuvchi o'zining imtiyozlari naboriga ega bo'ladi, oddiy foydalanuvchi – minimal, administratorlar – maksimal (imtiyozlar minimumi printsipiga muvofiq) imtiyozga ega bo'ladi. Har bir foydalanuvchi imtiyozlar nabori uning atributlari hisoblanadi va himoya sistemasi tomonidan muhofaza qilinadi. Imtiyozlarni ruxsatsiz ishg'ol qilish, shu tarzda, ma`lum vazifalarni ruxsatsiz bajarish imkoniyatlarini beradi. Bu RK (xususiy holda), ma`lum programmalarni ishga tushirish va hatto sistemani rekonfiguratsiya qilish bo'lishi mumkin.

Tabiiyki, bunday sharoitlarda imtiyozlarning kengaytirilgan nabori – bu har qanday buzg'unchining o'ylab yurgan orzusi. Bu esa unga amalda har qanday harakatlarni amalga oshirish, shu bilan birga, hatto barcha turdagi nazorat chora-tadbirlarini ko'rib aylanib chiqish imkonini beradi. Imtiyozlardan noto'g'ri foydalanish natijasida kelib chiqayotgan buzg'unchiliklar biror ob`ekt yoki butunlay sistemaga kirish maqsadida qilinayotgan aktiv ta`sirdir.

Imtiyozlarni noqonuniy ishg'ol qilish hodisasi yo himoya sistemasining o'zida biror xato paydo bo'lishi, yo sistema xususan imtiyozlarni boshqarishdagi beparvolik natijasida sodir bo'lishi mumkin. Himoya sistemasining boshqaruv qoidalariga, imtiyozlar minimumi printsiplariga qat`iy rioya qilish bilan bu xildagi buzilishlarning oldini olish mumkin.

“***Salyami***” atakasi – asosan pul hisob-kitoblari bilan shug’ullanuvchi komp yuter sistemalari uchun xarakterlidir.

“Salyami” atakasining printsipi quyidagicha: hisob-raqamlarni (schet) ishlashda butun pul birliklari (tsent, rubl , kopeek, so’m, tiyin) ishlatiladi; foizlarni hisoblash da esa hamma vaqt ham kasrli summa hosil bo’lmaydi.

Masalan, 102,87$ dan yillik 6,5% bo’lganda 31 kun uchun 0,5495726$ ni tashkilqiladi. Bank sistemasi bu summani 0,55$ gacha yaxlitlay oladi. Agar foydalanuvchi bank hisob-raqamlaridan yoki bu hisob-raqamlarni ishlovchi programmalardan foydalanish imkoniga ega bo’lsa, u bu hisob-raqam yoki programmalarni boshqa tomonga – 0,54$ gacha yaxlitlash imkoniga ega bo’ladi va hosil bo’lgan farq – 1 tsentni o’z hisobiga yozib qo’yadi. Hisob-raqamning egasi esa buni bilib qolishi gumon, agar bilib qolganda ham uni hisob-raqamni ishlash xatoligi, deb biladi va e`tibor bermaydi. Buzg’unchi esa bir kunda 10000 hisob-raqamni ishlaganda 1 tsent foyda qiladi. Shunday qilib, uning foydasi 100$ ni, bir yilda esa taxminan 300000$ ni tashkil qiladi.

Bunday atakaning nomi ham shundan kelib chiqqan, ya`ni <Salyami> kolbasasi turli navli go’shtning mayda bo’laklaridan tayyorlanadi, buzg’unchining hisob-raqami ham turli omonatchining hisobiga ko’payib boradi. Tabiiyki, bir kunda 5000-10000 bitimlarni amalga oshiruvchi tashkilotlardagina bunday atakalardan foyda olish mumkin, aks holda bunday tavakkalda hech qanday ma`no yo’q. Shunday qilib, <salyami> atakasi asosan yirik banklar uchun xavflidir. <Salyami> atakasining sabablari, birinchidan, hisoblash larda sodir bo’ladigan, yaxlitlash qoidasining u yoki bu yo’nalishda burib yuborishga imkon beradigan hisoblash xatoligi bo’sa, ikkinchidan esa, hisob-raqamlarini ishlash uchun juda katta hisoblash larni amalga oshirishdir. Bunday atakaning yutug’i nafaqat ishlanayotgan summaning miqdori, balki hisob-raqamlarning soniga ham bog’liq (ixtiyoriy hisob-raqami uchun ishlash xatoligi bir xil bo’ladi). “Salyami” atakasini sezish qiyin, agarda buzg’unchi birgina hisob-raqamning o’zidan millionlarni o’marmasa. Bunday atakani faqat amaliy programmalarning (hisob-raqamlarni ishlovchi) to’g’riligi va butunligini ta`minlash, foydalanuvchilarning hisob-raqamlariga kirishini cheklash, shuningdek, summalar oqimini doimiy nazorat qilish bilan barbod qilish, yo’qotish mumkin.

“***Yashirin kanallar***” – sistema xavfsizlik siyosatini buzuvchi, sistema jarayonlari o’rtasida informatsiyaning o’tish yo’li bo’lingan holda (s razdeleniem) informatsiyaga kirish muhitida foydalanuvchi o’zini qiziqtirgan informatsiya bilan ishlashga ruxsat ololmasligi mumkin, lekin buning uchun aylanma yo’llarni o’ylab topish mumkin. Sistemadagi har qanday harakat amalda uning boshqa elementlariga ma`lum ma`noda ta`sir ko’rsatadi. Bu bog’lanishlarni yetarlicha

kuzatish va o’rganish natijasida ma`lumotlardan bevosita yoki bilvosita foydalanish imkoniyatiga ega bo’lish mumkin.

“Yashirin kanallar” turli yo’llar bilan tashkil etilishi mumkin, masalan programma zakladkalari. Masalan, programmist avtomatlashtirilgan sistemani yaratish jarayonida o’zini qiziqtiruvchi ma`lumotlarni olish yo’llarini oldindan nazarda tutishi mumkin. Bunday holda programma yashirin tarzda programmist bilan aloqa kanalini o’rnatadi va unga talab qilingan xabarlarni uzatib turadi.

“Yashirin kanallar” dan foydalangan holda ataka qilish informatsiya maxfiyligiga putur yetkazadi, ta`sir xarakteri bo’yicha passiv hisoblanadi, ya`ni buzg’unchilik faqat ma`lumot uzatishda ro’y beradi. Yashirin kanallarni tashkil etishda shtatdagi programma ta`minotidan foydalanilsa, maxsus ishlab chiqilgan <troya> yoki virus programmalaridan shunday foydalaniladi. Ataka asosan programma yo’li bilan amalga oshiriladi.

Informatsiyani yashirin kanal bo’ylab uzatishga misol qilib, masalan, “TOTAL” so’zi o’rniga “TOTALS” so’zi ishlatilgan yakuniy hisobotni olish mumkin – bunda programmist shunday qiladiki, ma`lum sharoitlarda programma o’zi biror so’zni aniqlab, uni boshqasiga almashtirib qo’yadi. Bu kabi yashirin kanallar sifatida ikkita so’z orasidagi probellar soni, kasr sonda verguldan keyingi uchinchi yoki to’rtinchi raqam va h. (ya`ni hech kimning e`tiborini tortmaydigan ta`sir) dan foydalanish mumkin. Yashirin kanal bo’lib, shuningdek, biror ma`lumotlar naborining bor-yo’qligi, bu nabor o’lchami, yaratilgan sanasi, o’zgartirilgan sanasi va h. to’g’risidagi informatsiyani uzatish ham xizmat qilishi mumkin.

Sistemaning ikki jarayoni o’rtasidagi bog’lanishni tashkil qilishning ko’pgina usullari mavjud. Bundan tashqari, ko’pgina OS lar tarkibida (boshqaruv ostida) shunday vositalar borki, ular programmistlar va foydalanuvchilar ishini anchagina yengillashtiradi. Asosiy muammo shundaki, ruxsat etilmagan “yashirin kanallar”ni ruxsat etilganlardan, ya`ni xavfsizlik siyosati tomonidan ta`qiqlanganlaridan ajratish juda qiyin. Oxir oqibatda buni “yashirin kanallar”ning tashkilotga yetkazuvchi talofotlaridangina aniqlash mumkin. “Yashirin kanallar”ning alohida, o’ziga xos xususiyati quyidagilardan iborat:

- past darajadagi o’tkazish qobiliyati (ular orqali faqatgina kichik miqdordagi informatsiyani uzatish mumkin);
- ularni tashkil qilishdagi qiyinchiliklar;
- odatda, ular tomonidan yetkaziladigan katta bo’lmagan talofotlar.

Shuningdek, ular ko’zga ko’rinmas, sezilmaydigan bo’lishadi, shuning uchun ularga qarshi kamdan-kam hollarda maxsus himoya choralari qo’llaniladi.

Odatda, puxta ishlab chiqilgan xavfsizlik siyosatining vakolatlari yetarli bo’ladi.

«Maskarad» (inglizcha «mask» - niqob so’zidan olingan) - deganda bir foydalanuvchining boshqa foydalanuvchi nomidan harakat qilishi tushuniladi.

Bunda bu harakatlar boshqa foydalanuvchi uchun ruxsat etilgan bo’ladi. Bu yerda buzg’unchilik birovning huquq va imtiyozlarini o’zlashtirish asosida tashkil etiladi.

Bunday buzg’unchiliklar mug’ombirlik yoki modellashtirish deb ham ataladi. «Maskarad»ning asosiy maqsadi – biror harakatni boshqa foydalanuvchi nomi ostiga berkitish yoki boshqa foydalanuvchining ma`lumotlar omboriga kirish uchun yoki uning imtiyozlaridan foydalanish maqsadida, uning huquq va imtiyozlarini o’zlashtirishdan iborat.

«Maskarad» sistema himoyasini faol buzish usulidir, u bilvosita ta`sir bo’lib, boshqa foydalanuvchilarning imkoniyatlari vositasida amalga oshiriladi. Unga misol qilib, sistemaga boshqa foydalanuvchi nomi yoki paroli bilan kirishni ko’rsatish mumkin, ya`ni bunda sistema buzg’unchilik bo’lganini aniqlay olmaydi. Bunda «Maskarad»dan oldin esa sistemani buzish yoki parolni o’g’irlash jarayoni amalga oshadi. Yana bir misol, ish jarayonida boshqa foydalnuvchi nomini o’zlashtirishdir. Buni operatsion sistemalar vositalari yordamida (ba`zi operatsion sistemalarda foydalanuvchi identifikatorini ish jarayonida o’zgartirish imkoniyati mavjuddir) yoki ma`lum joydagi ma`lum informatsiyani o’zgartira oladigan programmalar (masalan, parollarni topish, sistemaga kirish parollarini o’g’irlash programmalari) yordamida amalga oshirish mumkin, va buning natijasida foydalanuvchi boshqa foydalanuvchi ismini o’zlashtiradi. Bunday amallar odatda,, sistema imtiyozlariga ega bo’lgan holda yoki sistemadagi biror xatodan foydalangan holda amalga oshiriladi. Shuningdek, komp yuter tarmog’ida boshqa foydalanuvchi tomonidan ma`lumot uzatish ham «Maskarad» deb ataladi. Identifikatorni o’zgartirish usullari turlicha bo’lishi mumkin, odatda,, ular tarmoq protokollari xususiyatlari va xatolari bilan aniqlanadi. Shunga qaramay, qabul qiluvchi uzelida ma`lumot to’g’ri ma`lumot kabi qabul qilinadi va buning natijasida tarmoq ishi jiddiy zarar ko’rishi mumkin.

Bunday axborotlarga, asosan, tarmoq konfiguratsiyasining o’zgarishiga ta`sir etuvchi-boshqaruvchi axborotlar yoki imtiyozli amallarni bajarishga olib boruvchi axborotlar kiradi.

«Maskarad» - bu korxona ishini buzish, informatsiya oqimini va tarmoq (yoki sistema) konfiguratsiyasini o’zgartirish kabi og’ir oqibatlarni keltirib chiqaruvchi, ahamiyatga molik buzg’unchilikdir. Uni bartaraf etish uchun autentifikatsiya va identifikatsiyaning ishonchli usullaridan foydalanish, sistemani buzishga urinishlardan blokirovka qilish, sistemaga kirishni nazorat qilish lozim. Shuningdek, sistema jurnalidagi «Maskarad» to’g’risida guvohlik beruvchi barcha hodisalarni e`tiborga olish va ahamiyat berish zarur.

«***Chiqindi yig'ish***» (Sborka musora). Ish tugagandan so'ng ishlanayotgan informatsiya hamma vaqt ham xotiradan to'laligicha o'chib ketmaydi, ma`lum qism ma`lumotlar operativ xotira, tashqi xotira qurilmalari yoki boshqa xotira qurilmalarida qoladi. Bu ma`lumotlar toki xotira qurilmasidan o'chirib yuborilmaguncha yoki ustidan boshqa ma`lumot yozilmaguncha xotira qurilmasida turadi, biroq o'chirib yuborilgandan so'ng ham ma`lumotlarning ma`lum qoldiqlari saqlanib qoladi. Bunday paytda bu qolgan qoldik ma`lumotlarni o'qib olish ancha qiyin bo'lsada, uni maxsus programmalar yordamida amalga oshirsa bo'ladi. Natijada yig'ilgan qoldiqlardan asosiy ma`lumotni qisman tiklash imkoniyati paydo bo'ladi. Bu jarayon «chiqindilarni yig'ish» deb nomlanadi. Bu muhim va maxfiy saqlanayotgan informatsiyaning chetga chiqib ketishiga olib kelishi mumkin.

«Chiqindi yig'ish» avtomatlashtirilgan sistema ob`ektlariga bevosita faol ta`sir etib, ulardagi informatsiya maxfiyligiga putur yetkazadi.

Bu ta`sirlardan himoyalanish uchun komp yuter apparaturasi yoki operatsion sistemasida yoki yana biror bir qushimcha apparat-programma vositalarda amalga oshirilgan maxsus mexanizmlardan foydalaniladi. Bunday mexanizmlarga misol, o'chiruvchi namuna va to'lalik belgisi ishlatiladi.

O'chiruvchi namuna – bu fayldan bo'shagan joyga yozuvchi bir qancha bitlar ketma-ketligi. Xotiraning har bir qismi bo'shatilgandan so'ng, xotiradan ma`lumot o'chirilgandan so'ng, xavfsizlik boshqaruvchisi (administratori) avtomatik ravishda bu bo'shatilgan o'ringa bitlar ketma-ketligini yozish faoliyatini olib boradi va buning natijasida o'chirilgan ma`lumotlar fizik saqlash muhitidan ham batamom yo'qotiladi.

To'lalik belgisi - bu xotiraning yozish uchun jo'natilgan, lekin hali yozib ulgurilmagan (yozilmagan yoki foydalanilmagan) uchastkalarini o'qishdan qaytaradi. Foydalanilgan xotira adresiga yuqori chegara qo'yiladi va xotira uchastkasining to'lib qolgan belgisi o'rnatiladi. Bu favqulodda foydalaniladigan (kamdan-kam uchraydigan kirishli) ketma-ket fayllarni himoyalash uchun ishlatiladi. (bu fayllar - tahrirlagichlarning yakunlovchi fayllari, kompilyatorlar, komponovshiklar va h.). Indeksli va bo'linuvchi ketma-ket fayllar uchun bu usul «joylashtirayotib o'chirish» deb nomlanadi, xotiraning uni jarayon uchun ajratayotgan paytda tozalanadi.

Sistemani buzish - bu ruxsatsiz kirish parametrlari bilan, ya`ni foydalanuvchi nomi yoki paroli bilan sistema ichiga qasddan suqilib kirish. Sistemani buzish bu faol sistemaga to'la ravishda qasddan qilingan ta`sir bo'lib, odatda, interaktiv rejimda yuz beradi. Foydalanuvchi ismi sir bo'lmasada,

"o'lja" sifatida asosan parol tanlanadi. Parolni ochish turlicha bo'lishi mumkin: ehtimolli parollarni tanlab ko'rish, boshqa foydalanuvchi parolidan foydalanilgan "Maskarad", imtiyozlarga ega bo'lish va h. Shuningdek, kirishi programmasining xatolaridan foydalangan holda ham sistemani buzish mumkin. Shunda qilib buzishda himoyalash vazifasi asosan kirish programmasining zimmasiga yuklatiladi. Parolni va nomni kiritish algoritmi, ularni shifrlash, parollarni saqlash va o'zgartirish qoidalarida xato bo'lmasligi kerak. Sistemani buzishga qarshilik ko'rsatish ham mumkin, masalan, parolni noto'g'ri kiritishga bo'lgan urinishlar sonini blokirovka yordamida yoki buzilish sodir bo'lganda operatorni xabardor qilish orqali cheklash.

Shuningdek xavfsizlik administratori sistemaning faol foydalanuvchilarini doim nazorat qilib turishi lozim: ularning ismi-sharifi, ish xarakteri, kirish-chiqish vaqti va h. dan xabardor bo'lib turish kerak. Bunday harakatlar sistemani buzilganligi to'g'risidagi faktni olish va aniqlashtirish hamda zarur chora-tadbirlarlarni qo'llashda katta yordam beradi.

Tuynuklar - programma moduliga yashirish, xujjatsiz kirish nuqtasi. Tuynuk asosan programmaga ishni yengillashtirish maqsadida sozlash bosqichida qo'yiladi: programma moduli turli joylardan chaqiriladi, bu esa uning alohida qismlarini mustaqil sozlash imkonini beradi. Biroq keyinchalik programmist tuynukni yo'qotishni unutib qo'yadi yoki uni noto'g'ri blokirovka qilishi mumkin. Bundan tashqari, tuynuk burilgan programma modulini keyinchalik boshqa modullar bilan bog'lash maqsadida shu programma moduliga qo'yiladi, lekin keyinchalik shart-sharoitning o'zgarishi bilan bu nuqta (ya`ni tuynuk) kerak bo'lmay qoladi. Tuynukning mavjudligi programmani nostandart ko'rinishda chaqirish imkonini beradi, ya`ni bu programma himoya sistemasi nazoratida bo'lishi mumkin (bunday sharoitda programma ma`lumotlarni, sistema muhitini va hokazolarni qanday qabul qilishi noma`lum). Shuningdek, bunday paytda bu programmaning hatti-harakatini hamma vaqt ham prognoz qilib bo'lmaydi. Tuynuk bu biror loyihani ishlab chiqishda sodir bo'ladigan xatoliklar natijasida paydo bo'ladigan tahdid bo'lib, undan foydalanish o'sha loyiha yoki programma paketining o'ziga bog'liq bo'ladi. Shuning uchun bu tahdidni sinflash murakkab jarayon hisoblanadi.

Xulosa qilib aytganda tuynuklarning paydo bo'lish sabablarini quyidagicha ko'rsatish mumkin:

- tuynuklarni yo'qotishni unutish;
- tuynuklardan keyinchalik programmani sozlashda foydalanish;
- tuynukdan ishlab chiqilayotgan programma va tayyor programma (ya`ni tuynuk qo'yilgan programma) o'rtasida ko'prik sifatida foydalanish;

- berilgan programmani o’rnatgandan so’ng bu programmaga maxfiy nazoratni tashkil qilish.

Bu yerda dastlabki holat - avvaldan kutilmagan adashish bo’lib, himoya sistemasida katta bo’shliq yoki ochik tuynuk paydo bo’lishiga olib keladi. Ikkinchi va uchinchi holatlar xavfsizlik sistemasi uchun jiddiy sinov vazifasini o’taydi, bu holatda xavfsizlik sistemasi informatsion sistemani bu xavfdan ogoh qila olmaydi. To’rtinchi holat esa - bu berilgan programmadan foydalangan holda oldindan biror maqsadni ko’zlab qilingan ta`sirning birinchi qadamidir.

Shuni esda tutish lozimki, programmaning har qanday xatosi ham tuynuk hisoblanmaydi. Tuynuk bu programmani sozlash, tuzatish va ta`mirlashda keng ishlatiladigan mexanizmdir, hattoki u biror maqsadda ishlatilsada, salbiy xarakterga ega bo’lavermaydi. Yana ta`kidlash lozimki, agarda tuynuk ochiq qoldirilsa va nazorat choralari ko’rilmasa, u holda bu sistema uchun jiddiy xavfdir.

Tuynuklardagi eng katta xavf - bu operatsion sistemalardagi tuynuklardir, bunda ularni topish juda qiyin kechadi. Agar berilgan programmada tuynuk mavjudligi oldindan ma`lum bo’lmasa, uni topish uchun programma kilobayt, megabayt kodlarini ishlashga to’g’ri keladi. Bunga esa haqiqatdan olib qaraganda, deyarli erishib bo’lmaydi. Shuning uchun tuynuklarni topish bu tasodifiy jarayondir, deb hisoblanadi. Ulardan himoyalanishning yagona yo’li bu - programmada tuynuk paydo bulishiga yo’l qo’ymaslik yoki agarda programma boshqa biror uchinchi tomondan qabul qilingan bo’lsa, dastlabki programma tahlillarini o’tkazishdan iborat.

Zararli programmalar. So’nggi paytlarda maxsus yaratilgan programmalar yordamida hisoblash sistemalariga ta`sir etish hollari ko’p uchramoqda. Zararli programmalar deganda informatsiyani ishlash jarayonini to’g’ridan-to’g’ri yoki bilvosita to’xtatish, informatsiyani buzish va informatsiyani chetga oqib chiqib ketishini ta`minlovchi programmalar tushuniladi. quyida bunday programmalarning eng ko’p tarqalganlari bilan tanishib chiqamiz. Bular: "troya tulpori", virus, "qurt", "ziqna" programmalar, "parollar o’g’risi", "bomba", "qopqon".

<u>Mustahkamlash uchun savollar:</u>

- Sistemaga qasddan qilingan ta`sirlarni tushuntiring.
- sistema xavfsizlik siyosatini buzuvchi vositalarga nimalar kiradi?
- Zararli programmalar tushunchasi nimani anglatadi?
- Imtiyozlardan noqonuniy foydalanish tushunchasini izohlang.
- Ruxsatsiz kirish (foydalanish) necha turga bo’linadi ?

Foydalanilgan adabiyotlar ro'yxati:

1) Brassar. J. «Sovremennaya kriptologiya» ,Moskva, «Polimed», 1999 g.
2) Petrov A.A. «Kriptograficheskie metodo' zahito'» ,Moskva,DMK, 2000 g.
3) Romanets Yu.V., Timofeev P.A. «Zahita informatsii v sovremenno'x komp yuterno'x sistemax» , Moskva, Radio i svyaz , 1999 g.
4) Panasenko S. «Zahita elektronno'x dokumentov» ,Moskva, FiS, 2000 g.
5) Vasina ye. N., Golitsina O «Informatsionno'e resurso' i bazo' danno'x»,
6) Moskva, RGGU, 1998 g.

4-MA`RUZALAR

Komp yuter viruslari va ularni yaratishdan ko'zlangan maqsad. Virus turlari va ishlash printsiplari. AVP umumiy xarakteristikasi. (2 soat)

O'quv modullari

1. Komp yuter viruslari.
2. Komp yuter viruslari qanday paydo bo'ladi?
3. Rezident va norezident viruslar
4. Uyali telefonlar uchun viruslar.
5. Windows 98 karokchilik nusxalari bilan tarkaladigan virus.
6. Antivirus programmalar.
7. AntiViral Toolkit Pro antivirus programmasi
8. Serverlarni antivirus ximoyalash.
9. Uz-uzini ximoyalash retseptlar

Aniqlashtirilgan o'quv maqsadlari.Talaba bu mavzuni to'la o'zlashtirgandan so'ng:

- Komp yuter viruslari haqidagi tamoyillarni biladi;
- Rezident va norezident viruslarini bo'laklarga bo'lib, ta`rif bera oladi;
- Uyali telefonlar uchun viruslar xususiyatlarinini talqin eta oladi;
- Windows 98 qaroqchilik nusxalari bilan tarkaladigan

Virus qaysi sinfga mansubligini tasavvur eta oladi;
Uz-uzini ximoyalash retseptlar o'rtasidagi o'zaro aloqadorlikni aniqlaydi,
bog'lanishlarni tahlil qila oladi.

Tayanch so'z va iboralar:

Komp yuter viruslari, Rezident va norezident viruslari,himoya modellari, Uyali telefonlar uchun viruslar, foydalanuvchi, kritik informatsiya, karokchilik nusxalari, AntiViral Toolkit Pro antivirus programmasi, Serverlarni antivirus ximoyalash.

Komp yuter viruslari. Bu nima va unga karshi kanday kurashish kerak? Bu mavzuga unlab kitoblar va yuzlab makolalar yozilgan. Komp yuter viruslariga karshi minglab professional mutaxassislar ko'plab kompaniyalarda ish olib borishmokda. Bu mavzu uta qiyin va muximki ko'p e`tiborni talab kilmokda. Komp yuter virusi informatsiyani yukotish sabablaridan biri va asosiysi bo'lib kolmokda. Viruslar ko'plab tashkilot va kompaniyalarni ishlarini buzishga olib kelganligi ma`lum. Shui day ma`lumotlar mavjudki, Niderlandiya gospitallaridan birida bemorga komp yuter kuygan tashxis buyicha iste`mol kilingan dori okibatida bemor olamdan utgan. Bu komp yuter virusining ishi bulgan.

E`tiborsizlik bilan kilingan ishdan komp yuter tezda virus bilan zararlanadi. Inson kasallik virusi bilan zararlansa issikligi uzgarishi, vazni uzgarishi, xolsizlanish va ogrikning paydo bulishi kuzda tutiladi. Komp yuter virusi bilan zararlangan komp yuterlarda kuiidagilar kuzatiladi: dasturlarning ishlashining sekinlashishi, fayllartsi xajmi uzgaradi, gayritabiiy va ba`zi bir noma`lum xatoliklar, ma`lumotlar va sistema fayllari yukotilishi. Ba`zi viruslar zararsiz ko'payadi, lekin kurkinchli emas. Bu viruslar ekranga xato ma`lumot kikaradi. Ammo, bir turdagi viruslar xujum kiluvchi, ya`ni, yomon asoratlar koldiruvchi xisoblanadi. Masalan, viruslar qattiq diskdagi informatsiyalarni o'chiribtashlaydi.

Virus nima?

Mashxur «doktor» lardan biri D.N.Lozinskiy virusni kotibaga uxshatadi. Tartibli kotibani faraz kilsak, u ishga keladi va stolidagi bir kunda kilishi kerak bulgan ishlarni - qog'ozlar katlamini kuradi. U bir varogni ko'paytirib bir nusxasini uziga ikkinchisini keyingi kushni stol ga kuyadi. Keyingi stoldagi kotiba xam kamida ikki nusxada ko'paytirib, yana bir kotibaga utkazadi. Natijada kontoradagi birinchi nusxa bir necha nusxalarga aylanadi. Ba`zi nusxalar yana ko'payib boshka stollarga xam utishi mumkin.

Komp yuter viruslari taxminan shunday ishlaydi, fakat qog'ozlar urnida endi dasturlar, kotiba bu - komp yuter. Birinchi buyruq «kuchirish-nusxa olish» bulsa, komp yuter buni bajaradi va virus boshka dasturlarga utib oladi. Agar komp yuter biror zararlangan dasturni ishga tushirsa virus boshka dasturlarga tarkalib borib butun komp yuterni egallashi mumkin.

Agar bir dona virusning ko'payishiga 30 sekund vakt ketsa, bir soatdan keyin bu 1000000000 dan ortib ketishi mumkin. Aniqrogi komp yuter xotirasidagi bush joylarni band kilishi mumkin.

Xuddi shunday vokea 1988 yili Amerikada sodir bulgan. Global set orkali uzatilayotgan informatsiya orkali virus bir komp yuterdan boshkasiga utib yurgan. Bu virus Morris viru si deb atalgan.

Ma`lumotlarni virus kanday yuk kilishi mumkin degan savolga shunday javob berish mumkin:

1. Virus nusxalari boshka dasturlarga tez ko’payib utib oladi;
2. Kalendar buyicha 13-sana juma kunga tugri kelsa

hamma hujjatlarni yuk kiladi (uchiradi).

Buni hammaga ma`lum «Jerusalem» («Time» virusi xam deb ataladi) virusi juda «yaxshi» amalga oshiradi.

Ko’p xollarda bilib bulmaydi, virus kaerdan paydo buldi.

Komp yuter viruslari - ko’payuvchi, dasturlarni **{|TS||ga** kuchib olishi, yomon okibatlar keltirib chikaruvchi dasturlardir. Lekin ular kat`iy bir kurinishda bulishi belgilab kuyilmagan.

Virusni Aniqlanishi shundagi, u komp yuter sistemasida joylashib va ko’payib borishiga bog’liq. Misol uchun, nazariy jixatdan operativ sistemada virus davolab bulmaydi. Bajaruvchi kodning soxasini tuzish va uzgartirish ta`kiklangan sistema misol bulishi mumkin.

Virus xosil bulishi uchun bajariluvchi kodlar ketma-ketligi ma`lum bir sharoitda shakllanishi kerak. Komp yuter virusining xossalaridan biri uz nusxalarini komp yuter tarmoqlari orkali bajariluvchi ob`ektlarga kuchiradi. Bu nusxalar xam uz-uzidan ko’payish imkoniyatiga ega.

Komp yuter viruslari kanday xosil buladi?

Biologik viruslardan farkli ularok, komp yuter viruslarini inson tomonidan tuziladi. Viruslar komp yuter foydalanuvchilariga katta zarar yetkazadi. Ular komp yuter ishini tuxtatadi yoki qattiq diskdagi ma`lumotlarni uchiradi. Virus sistemaga bir necha yullar bilan tushishi mumkin: disketalar, dastur ta`minot yuklangan CD-ROM, tarmoq interfeysi yoki modemli boglanish, global Internet tarmogidagi elektron pochta.

Disketa viru s dan zararlanishi oson. Zararlangan komp terga disketni solib ukitilganda diskning bosh sektoriga virus tushadi.

Internet ma`lumotlar almashinishiga katta imkoniyat yaratadi. Lekin, komp yuter viruslari va zararli dasturlar tarkalishi uchun yaxshi muhit yaratadi. Albatta InternetzjaH olingan barcha ma`lumotlarda virus bor deb bulmaydi. Komp yuterda ishlovchi ko’pchilik mutaxassislar va operatorlar kabul kilinadigan ma`lumotlarni viruslardan tekshirishni doimo bajaradi. Internetla ishlayotgan har bir kishi uchun yaxshi antivirus ximoya zarur. «Kasperskiy laboratoriyasi» texnik ta`minot xizmati

statistikasiga kura, viruslardan zararlangan holatlarning 85% i elektron pochta orkali sodir bulgan. 1999 yilga nisbatan xozirgi kunda bu kursatkich 70 % tashkil etadi. «Kasperskiy laboratoriyasi» elektron pochtalarga yaxshi antivirus ximoyasi kerakligini ta`kidlaydi.

Virus tuzuvchilarga elektron pochta juda kulay. Amaliyot shuni kursatadiki, ommabop dasturlar, operatsion sistemalar, ma`lumotlarni uzatish texnologiyalari uchun viruslar ko'plab tuzilmokda. Xozirda elektron pochta biznes va boshka soxalarda mulokot uchun asosiy vosita bo'lib kolmokda. Shuning uchun virus tuzuvchilari elektron pochtaga dikkatini
karatmokda.

Virus paydo bulish belgilari.

Zararlangan komp yuterda eng muximi virusni Aniqlash. Buning uchun virusni asosiy belgilarini bilish kerak:

1. Funktsional dasturlarni ishini tuxtatish yoki noto'g'ri ishlashi;
2. Komp yuterni sekin ishlashi;
3. OS ni yuklanmasligi;
4. Fayl va kataloglarni yukolishi yoki ulardagi ma`lumotlarni buzilishi;
5. Fayllar modifikayiyasining sana va vaktining uzgarishi;
6. Fayl xajmining uzgarishi;
7. Diskdagi fayllar mikdorining keskin ko'payishi;
8. Bush operativ xotira xajmining keskin kamayishi;
9. Kutilmagan ma`lumotlar va tasvirlarning ekranga chikishi;
10. Kutilmagan tovushlarning paydo bulishi;
11. Komp yuterning tez-tez osilib kolishi.

Yukoridagi belgilar boshka sabablarga kura xam bulishi mumkinligini eslatib utamiz.

Kiskacha tarix.

80-yillarda IBM-PC bilan ishlagan kishilar bulsa 1987-89 yillardagi viruslarni tarkalishini unutishganicha yuk. Ekrandagi harflar har xil kurinishda buzilgan va foydalanuvchilar ommasi mutaxassislarga displeylarini olib kela boshlashgan. Keyinchalik komp yuter «Yankee Doodle» deb nomlangan uzga yerlik virusini chalishni boshlagan. Lekin, buni tuzatishni xech kim tashlamadi, juda tez xal buldi. Bu unlab viruslar tuplami edi.

Shunday kilib, viruslar fayllarni zararlay boshladi. «Brain» va ekranda shariklar paydo kiluvchi «Pingpong» viruslari Boot-sektor ustidan xam golib chikishdi. Bu hammasi IBM-PC dan foydalanuvchilarga unchalik yokmadi va antiviruslar paydo buldi. Birinchi antiviru yel ar dan biri ANTI-KOT: afsonaviy Oleg Kotik uzining antivirusining birinchi versiyasi dunyo yuzini kurdi. U 4 ta virusni yuk kildi. Afsuski, ANTI-KOT MSDOS kombinatsiyasidan foydalanib fayl

oxirida «Time» virusini Aniqlaidi. Boshka antiviruslar esa .som va .exe kengaytmali fayllarning har bir harfigacha zanjirlaydi.

Vakt utishi bilan viruslar ko'payib bormokda. Bularning hammasi bir-biriga uxshash, xotiraga urnashadi, sektor va fayllarga boglanadi, fayllarni, disket va vinchesterlarni yuk kiladi. Birinchilardan bo'lib, «Frodo.4096» virusi ommabop bo'lib chikdi. Bu virus INT2Ih ni egallab, DOS ga murojaat etilganda zararlangan fayl xuddi xech narsa bo'lmaganday xolda kurinish bergan. Ammo, bu MSDOS ustidan urnashib xukmini utkazgan. Bir yil xam utmasdanok «elektr suvaraklar» DOS yadrosiga urnashib olishgan. Kurinmas virus «Deast.512» deb atalgan. Kurinmaslik fikri ko'payib rivojlanib bordi: 1991 yil yozida komp yuter ulati - virus «Dir_n» paydo buldi. Birok kurinmaslarga karshi kurash sodda: RAM ni davolab xotirjam bulish mumkin.

Shunday viruslar xam kelib chikdiki, ular uzlarini shifrlab olish imkoniyatiga ega bulishdi. Bu viruslarni davolash va yuk kilish uchun maxsus kiem dasturlar yaratish kerak bulgan. Lekin bunga xech kim e`tibor bermadi, toki bu viruslarning yangi avlodlari kelib chikmaguncha.

Viruslar klassifikatsiyasi.

Xozirgi davrda 5000 dan ortik virus dasturlar ma`lum. Bularni kuyidagicha klassifikatsiga ajratish mumkin:

• Faoliyat muhitiga karab;
• Zararlantirish usuliga karab;
• Harakatlanishiga karab;
• Algoritmning axamiyatiga karab.

Faoliyat muhitidan kelib chikkan xolda viruslarni setli, faylli, yuklanuvchi kabi turlarga bulinadi. Setli viruslar har-xil setli komp yuterlarda tarkaladi. Faylli viruslar bajariluvchi fayllarga tarkaladi. Bu fayllar .som va .exe bulgan fayllar. Faylli viruslar boshka turdagi fayllarni xam zararlantirishi mumkin. Bunda fayllar boshkaruvni kabul kilmaydi, imkoniyat darajasini yukotadi. Yuklanuvchi viruslar diskning yuklovchi sektorida tarkaladi yoki
sektorning uzida joylashadi. (Boot sektor)

Viruslar zararlantirish usuliga karab rezident va rezitent bo'lmaganlarga bulinadi. Rezident viruslar zararlangan komp yuterlar operativ xotirasiga uzining yukumli bir kismini koldirib ketadi. Kachonki, operativ xotiraga murojaat kilinganda u ishga tushadi va tarkaladi. Rezident viruslar komp yuterni uchirilguncha va perezagruzka kilinguncha aktiv holatda buladi. Rezident bo'lmagan viruslar komp yuter xotirasini zararlantirmaydi, balki belgilangan vakt chegarasida aktiv holatga utadi.

Harakatlanishiga karab viruslar kuyidagi turlarga bulinadi:

• Xavfsiz, komp yuterda ishlashga xalakit bermaydi. Lekin, bush bulgan operativ xotira va diskdagi xotirani kamaytiradi. Bunday viruslar grafik va ovoz effektlarida paydo buladi.
• Xavfli viruslar komp yuter ishini buzishga olib keladi.
• Juda xavfli viruslar dasturlarni yukotilishiga, ma`lumotlarni va disk sistemasini uchib ketishiga olib keladi.

Algoritmning axamiyatiga karab viruslar kuyidagi gruppalarga bulinadi:

1. «Xamjixat-yuldoshlar» - fayllarni uzgartirmaydigan viruslar. Bu viruslar yeXE kengaytmali fayllarga kushimcha nusxa olib, bu nusxani .som yoki .bat kengaytmali fayl kilib yozib kuyadi. Bunday faylga murojaat etilganda birinchi .som yoki .bat kengaytmali fayl ishga tushadi sungra esa virus .exe kengaytmalisini ishga tushirib yuboradi.
2. "Chuvalchang-lukmalar" - bu viruslar komp yuter setlariga tarkaydi, fayl va disk sektorlarini uzgartirmaydi. Ular komp yuter seti orkali xotiraga kiradi. Boshka viruslar adreslarini topib ularga uz nusxalarini yozib kuyadi. Bunday viruslar ba`zida fayllar tuzadi, lekin umuman komp yuter resurslariga murojaat kilmaydi.
3. "Parazit" viruslar - nusxalarini disk sektori va fayllarga uzgartirib tarkatadi. Bu viruslar yukoridagilardan farklanadi.
4. "Talaba" viruslari - juda ko’p xatoliklar keltirib chikaruvchi xisoblanadi. Ular har-xil harflarni pay do kilishi kutiladi.
5. "Kurinmas Stels" virusi - uzining imkoniyatidan kelib chikib operativ sistemada fayllarni zararlantirib uz urniga boshka ma`lumotlarni kuyib "kochib koladi". Bu viruslar AVP (antivirus programmalari) ni aldab ketadi.
6. "Polimorfik-ajina-mutantlar" virusi -etarlicha tutish qiyin bulgan viruslar xisoblanadi. Ular Aniq bir joyda turmaydi (kuchib yuradi). Ko’p xollarda polimorfik viruslar uzining bir xil nusxasiga ega bulmaydi.
7. "Troyan otlari" virusi - kerakli dasturlar ichig-ya kirib olib har bir buyruq berilganda kakshatgich zarba bera oladi. U komp yuter va uning setlari orkali ko’payib sezilarli zararlarni pay po ,. kiladi. '
8. "Makro" viruslari - asosan ma`lumotlarn kayta ishlashga tuskinlik kiladi va matn muharrirlariga zarar yetkazadi. Xozirgi vaktda Microsoft Word, Exsel va Access muharrirlarida tayyorlangan hujjatlarda ko’plab uchrab turadi.

Uyali telefonlar uchun viruslar.

ILOVEYoU nomli virus uyali telefonlar uchun muljallangan. 2000 yilda Ispaniyada eng yirik Telefonika uyali aloka tarmogida bu virus tarkaldi. Virus mobil telefonlar uchun muljallangan bo’lib, matnli ma`lumotni uzatadi. U telefonii buzmaydi, ammo alokani qiyinlashtiradi. Bu virus dunyo buylab tarkalishiga yul kuyilmadi, ammo Handheld asboblar deb ataluvchi portativ komp yuterlar

tarmogini zararlantiruvchi yangi turdagi viruslarni yaratish uchun asos bulishi mumkin.

Windows 98 karokchilik nusxalari bilan tarkaladigan virus.

Karnegi-Mellon universiteta komp yuter xodisalariga javob beruvchi gurux muvofiklashtirish markazi xabariga kura 2000 yil boshida yangi virus paydo buldi. Bu Trojan.kill troyan virusi bo'lib, yana -Inst98 degan nomga xam ega. U S: diskdagi hamma ma`lumotlarni uchiradi. Dastlab u Microsoft Windows 98 operatsion tizimining krokchilik nusxalarida uchradi, birok virus elektron pochta va birgalikda foydalanilayotgan tarmoq disklari orkali xam tarkalishi mumkin. Xabar berilishicha, virus 5682 bayt ulchamdagi INSTALL.EXE faylida buladi. Ushbu fayl KEYB.COM klaviatura joylashish fayliga kuchiriladi.

REMOTE EXPLORER dasturi

1998 yil 17- dekabrda MCIG' WorldCom ichki tarmoqka Remote Explorer nomli virus xujum kildi. Buning okibatida bir kancha saytlar va bir necha ming serverlar va ishchi stantsiyalar zararlandi. Virus funktsiyasiga kura uzini System 32g'drivers ga nusxasini xosil kiladi va «Remote yexr1ogeg»xizmati kabi uzini urnatadi shundan sung uzini boshka mashinalarga nusxa kurinishini boshlaydi. (fakatgina NT tarmogida).

Virus ish bajarish jarayonida bajaruvchi fayllarni zararlashi bilan birgalikda, tanlangan matnli fayllarni xam ixtiyoriy tarzda shifrlaydi. Bu faoliyat shanba 15:00 dan yakshanba 6:00 gacha bulgan davrda kuchayadi.

Remote Explorer virusi troyaplar turidagi viruslarga kushish mumkin, chunki komp yuter kayta yuklanganda u yukoladi va virus zararlanishi uchun uni odatda tezda ishga tushirish kerak.

«Chernobo'l » virusi

1999 yil 26-aprel kuni «Chernobo'l » virusi tufayli dunyo buyicha komp yuter fojiasi sodir buldi. Zararlangan komp yuterlar xakida Angliya, Shvetsiya, Turkiya, Yaponiya, Rossiya, Janubiy Koreya, Xindiston, Mal ta, Finlendiya, Yangi Zelandiya va boshka mamlakatlardan xabar keldi. yevro Osiyo kit`asining mamlakatlari katta zarar kurdi. Umumman olganda taxminan 600000 mashina ishdan chikdi. Janubiy koreyada 300000 ta Xitoyda 100000 ta, Rossiyada 100000 ta Amerikada asosan xususiy sektor, maktablar va universitetlar (1000) zararlandi.

CIN nomli virus vinchestirdagi barcha ma`lumotlarni o'chiribtashlaydi. U Windows 95G'98 da ishlaydi. Asosiy tarkalish yuli - elektron pochta va zararlangan disketalar. Virus yeXE fayllarga yopishib oladi va iz koldirmaydi, chunki an`anaviy Aniqlash usullaridan kochish uchun «Space Filler»

xususiyatlaridan yaxshi foydalanadi. Virus kuyidagicha ishlaydi: Hard drive (qattiq disk)ning fayl tartibi yoziladigan soxaning ma`lumotning o'chiribyuboradi. Bu ma`lumotsiz sistema fayllarni kurmaydi sungra BIOS (Basic input Output System)ra ta`sir kilib, OS ni zararlaydi. Bu esa vinchestirdagi ma`lumotlarninng umuman uchirishga olib keladi

Komp yuter kachon zararlanishi noma`lum. Virusni keng tarkalishi oylab davom etgan bulishi mumkin. Virus 26-aprel kuni ishga tushdi. 1986 yil 26-aprel Chernobil fojeasi sodir bulgan kun bilan ustma-ust tushganligi uchun

Antivirus programmalar.

Komp yuter viruslaridan ximoyalanish, ularni yuk kilish va Aniqlash uchun bir necha maxsus programmalar yaratilgan. Bunday programmalar antiviruslar deb ataladi. Antivirus programmalari turlarga bulinadi:

- programma detektorlar;
- doktor-programmalar yoki fagi;
- revizor programmalar;
- filtrlovchi programmalar;
- vaktsina yoki immunitet programmalar.

Detektor-programmalar - Aniq virusning harakterli holatini kidiradi. Operativ xotira yoki fayldagi kerakli ma`lumotni Aniqlaydi. Bunday antiviruslarning kamchiligi shundaki, ular uzlariga ma`lum bulgan virusnigina Aniqlaydi.

Doktor-programmalar yoki fagi xamda vaktsina-programmalar nafakat viruslarni Aniqlaydi balki, davolaydi, fayldagi virus tanasini uchiradi, faylni asl holaticha saklab koladi. Doktor programmalar ko'p mikdordagi viruslarni Aniqlash va yuk kilish imkoniyatiga ega. Bunday programmalarga: AVP, AidsTest? Scan? Norton Antivirus, Doctor Web kiradi.

Yangi viruslar paydo bulgan sari yukoridagi antiviruslarning yangi versiyalari ishlab chikish talab etiladi.

Revizor programmalar - viruslardan ishonchli ximoya vositasi xisoblanadi. Revizorlar dasturlarni, kataloglar va diskning sistema bulimi .holatini komp yuter virusdan zararlanmasdan avval eslab koladi. Shundan keyin, foydalanuvchining xoxishiga binoan oldingi va keyingi holatlarni solishtiradi. Uzgargan holatlarni ekranga chikaradi. Fayllarni holatini solishtirishda uning uzunligi, modifikatsiya vakti va sanasi, xamda boshka parametrini solishtiradi. Revizor programmalar yetarlicha murakkab algoritmlarni xatto stels-viruslarni xam yuk kiladi, virus buzib yuborgan fayllarni uz holatiga keltiradi. Bunday antivirusga ko'p tarkalgan Rossiyaning Adinf programmasi misol buladi.

Fil tr-programmalar yoki «tozalovchi» uzida ko’p bo’lmagan rezident dasturlarni mujassamlashtiradi. Komp yuterning shubxali va virus harakterno’y beruvchi ishini Aniqlaydi. Bunday holatlarga:

1. SOM va yeXE kengaytmali fayllar tartibi buyicha;
2. Fayl atributlarini uzgarganiga karab;
3. Aniq manzil orkali diskka yozish buyicha;
4. Diskning yuklovchi sektoriga yozish buyicha;
5. Rezident programmaning yuklanishiga karab.

Biror bir programmaning ishlash davomida «tozalovchi» ishning ruxsat etilishi yoki mumkin emasligi xakida ma`lumot beradi. Fil tr-programmalar foydali xisoblanadi, u virusni ko’payib ulgurmasidan oldin Aniqlash imkoniyatini beradi. Fakat ular disk va fayllarni olmaydi. Viruslarni yuk kilish uchun boshka programmalar kerak buladi.

Vaktsina yoki immunitet programmalar zararlangan fayllarni davolaydi. Vaktsinalar doktor-programmalardan yaxshirok davolaydi. Vaktsina fakat mashxur viruslarni Aniqlaydi, bunda virus vaktsinalangan fayl yoki diskni olib zararlay olmay koladi. Xozirda vaktsinalar kam kullaniladi. Zararlangan fayl va disklardan, har bir virus tushgan komp yuterlardan uzokrok yurish virus epidemiyasidan saklanish demakdir.

AntiViral Toolkit Pro antivirus programmasi.

AVP foydalanuvchi uchun kulay interfeysga ega. Ko’plab kulayliklarni foydalanuvchi uzi belgilaydi va shu bilan birga juda ko’plab tarkalgan viruslarni yuk kila oladigan antivirus bazasiga ega.

AVP ning ish rejimi kuyidagicha: Operativ xotira nazorati. Fayllar va arxivlar nazorati.

Master Boot Record - sistema sektori, yuklovchi sektor va disk tablitsa nazorati.

AntiViral Toolkit Pro ishining axamiyatli tomoni kuyidagicha:

- Turli xil viruslarni yuk kiladi, shu bilan birga uz-uzini shifrlovchi, kurinmas va stele viruslarni, makro va Word, Excel hujjatlari viruslarini xam yuk kiladi.
- Upakovkalangan fayllarni ichini tekshiradi.
- Arxivlangan fayllarni ichini tekshiradi.
- Yumshok disk, lokal, setli va CD-ROM disklarni tekshiradi.
- Noma`lum viruslarni tekshiradi.
- Ortikcha tekshirish rejimi.
- Ob`ekt ichidagi uzgarishlarni tekshirish.

AVP programmasi markaziy boshkaruv komp yuteridan avtomatik ravishda ishlatish kulaydir. Buning uchun, avtomatik boshkaruv buyrugini tuzish talab etiladi. Ba`zi bir antiviruslarni kiskacha harakteristikasi.

Dr Solomon's Antivirus Toolkit

Viruslarni Aniqlash va ularni yukotish buyicha eng yaxshi kursatkichlarga ega , shuninig uchun xam narxi kimmat. Narxi yukoriligiga karamay (85$) bu dastur «eng yaxshi tanlov» nomiga sazovor buldi. McAfee firmasining VimsScan dasturi ko'prok «yovvoyi» virus-larni uchiradi. Dr Solomon's Antivims Toolkit dasturining interfeysida ixtiyoriy antivirus funktsiyalar, barcha ma`lum viruslarni tulik ma`lumoti va ularning zararlari xakida ma`lumotlar mavjud. Bu dastur paketiga tarkibiga kiruvchi yuklovchi disketa Bullet («Sexrli uk») ixtimyoriy sistemada viruslarni tez Aniqlaydi va yuk kiladi. Bupaketninig kamchiligi xakida yangi ma`lumotlarni tarmoq orkali yuklay olmasligi xamda yangi versiyalarni almashtirish yiliga 4 marta buladi.

F-Prot Professional

Bu dastur viruslarni yaxshi Aniqlaydi, keng sozlash imkoniyatiga ega, viruslarni Aniqlaganda elektorn aloka orkali xabar beradi. Dastur kamchiligi yangi vesriyalar bilan almashtirishda parolni zarurligi va dasturni kaytadan urnatish zarurligidir. Viruslarni Aniqlash buyicha utkazilgan testda 99 % viruslarni Aniqladi, lekin ulardan 78 % ni uchira oldi. Bu dastur paketida doimiy tekshiruvda kaysi disklar , papkalar va fayllar bulishi yoki bulmasligi imkoniyatlari mavjud. Bu esa vaktdan yutadi ya`ni avval tekshirilgan fayllarni tashlab utishi xisobiga.

IBM AntiVirus v.2.5.

Viruslarni Aniqlashda katta imkoniyatga ega bo'lib, 1 ta paketda turli operatsiey sistemalar bilan ishlash versiyalari mavjud. Dastur kamiligi virusni uchirishda konservativ (eskicha) usuldan foydalanishi. Viruslarni yangi tipini Aniqlashdazamonaviy texnologiyadan foydalaniladi.Paket narxi 49 % bo'lib, «yovvoyi» viruslarni yaxshi Aniqlaydi va yuk kiladi.

IBM AntiVirus virus dasturi agarda zararlangan fayl virus uchirishda buzilib ketsa , u xolda bu virusni uchirmaydi. Bunday holatda zararlangan fayl umuman uchiriladi va faylni rezerv nusxasidan kaytadan yuklanadi. IBM AntiVirus dasturi shunday ishlash xisobiga «yovvoyi» viruslarni 32 % ni uchira oladiAmmo boshka dasturlar kabi , IBM AntiVirus dasturi yuklovchi sektorni zaralantiruvchi viruslarni 100 % uchiradi. Afzalligi: yangi versiyalar urnatish uchun zarur fayllar IBM WEB - server orkali olish mumkin va ularni urnatish uchun dastur keng imkoniyatli menyuga ega. Bu dastur paketida Windows 95, 3.x , DOS va OS G' 2 sistemalar uchun versiyalar mavjud. ENTERPRISE EDITION itshbilarmonlari uchun dastur paketida Windows NT sistema uchun versiyasi xam mavjud.

Me Afee VirusScan for Windows 95

Viruslarni yaxshi yuk kiladi, turli operatsiey sistemalar bilan ish-lay oladi, eng arzon dastur. Kamchiligi: viruslarni yaxshi Aniqlay olmasli-gi va yangi versiyalar uchun kushimcha xak tulanishi. Me Afee VirusScan - mashxur antivirus paketlaridan biri xisoblanadi. Utkazilgan test natijalariga kura Symantec firmasining Norton Anti Virus dasturi 13 ta makroviruslarni ushladi, McAfee VirusScan 12 ta makrovirus ushladi, 1ta ya`ni Imposter nomli kam uchraydigan virusni ushlay olmadi. Virus Scan dasturi faylli viruslarni «yovvoyi» turlarini qiyin Aniqlaydi. Tekshiruv natjalariga kura dastur faylli viruslarni 93 % ni Aniqladi. Agarda ba dastur effetivligi yukori bulganda edi, u yaxshi paket xisoblanar edi. Dasturni oson va tez sistema parametrlariga moslashtirib urnatish mumkin, bunda dastur parametrlarini uz ixtyoringizga kura uzgartirishingiz mumkin.

Virus Scan narxi 45$ bo'lib, Windows 95, 3.x va NT , DOS va OS G' 2 asosiy operatsion sistemalar uchun versiyalari mavjud. Ammo dasturni imkoniyatlarin kengaytirish uchun kushimcha xak tulash kerak. Ma`lumotlar bazalarini yangilangan versiyalarni WEB da ishlatish mumkin, lekin McAfee WEB - saxifasiga kura yangi versiyalarni kompaniya texnik ta`minotini xam olish sharti bilan ishlatish mumkin. Kayd kilingan foydalanuvchilar birinchi navbatda uch oy davomida bir marta yangi versiyani bepul o lishi mumkin. Shui dan sung 49 $ ga bir yilga tuzilgan shartnoma asosida cheklanmagan mikdorda dastur yangi versiyalarni va viruslarni yangi belgilarini , xamda doimiy telefon maslaxatlarini olish mumkin.

Norton AntiVirus 2.0 for Windows 95

Afzalligi viruslarni juda yaxshi Aniqlaydi, ajoyib interfeys, avtomatik yangilanish. Kamchiligi: «yovvoyi» viruslarni 77 % ni yuk kiladi. Bu dastur tez, ishonchli va sodda mulokotli bo'lib, foydalanuvchi uchun juda kulay Mutaxassislar esa uzlariga moslashtirib olishi mumkin.

Norton AntiVirus dasturining interfeysida Live Update funktsiyasi mavjud. Bu funktsiya Web orkali dasturni va viruslar belgilar tuplamini yangilashi mumkin Shu bilan birga viruslar bilan kurash Ustasi (Virus Repair Wizard) Aniqlangan virus xakida tulik ma`lumot beradi xamda uni yuk kilish usullarni tanlash imkonini beradi. Bu usullar : viruslarni avtomatik ravishda yuk kilish ; boskichma-boskich yuk kilish, bu xolda uchirish jaraenini boshkarish mumkin.

Thunder Byte AntiVirus Utilites.

Afzalligi: faylli viruslarni yaxshi Aniqlaydi, tekshirishni juda kulayligi. Kamchiligi: viruslarni uchirishi qiyinrok, yangi foydalanuvchilar uchun uchirish jarayoni murakkab. Birinchi bor Karaganda, Thunder Byte AntiVirus Utilites dasturi (100 $) yangi virus belgilarni Web yuklash ikoniyatiga ega. Dastur chukurrok urganilganda, u paketda odatdagi a`zi bir funktsiyalar yuk , ammo bir

kator yangi mukammal funktsiyalarga ega. Bu dastur Windows 95 sistemasining «Provodnik» dasturiga uxshash interfeysiga ega bo'lib, boshka paketlarda mavjud bo'lmagan bir kator kulayliklarga ega. Tekshirishda siz aloxida disklarni , fayllarni yoki papkalarni belgilashingiz mumkin. Thunder Byte utkazilgan test natijalariga kura yuklovchi sektordagi viruslarni 100% ni Aniqlaydi, ammo ularni uchira olmaydi. Shu bilan birga dastur sikilgan fayllarni tekshirmaydi, bu esa arxivlangan fayldagi virusni Aniqlanmasligiga olib keladi. Thunder Byte dasturi komp yuterda cheklangan (korporativ) holatda foydali bulishi mumkin. Faylli viruslarni (makro - viruslardan tashkari) uchirishdan avval TBCLEAN nomli aloxida DOS utilitali disketa xosil kilish kerak. Disketadan yuklanish, tekshirish jarayonida xotiradagi virusni faollashishiga imkon kamayadi, chunki bunda zaralangan yuklovchi sektor va fayllarga murojat bulmaydi.

Evgeniy Kasperskiy Antivirusi.

AntiViral Toolkit Pro by Eugene Kaspersky (AVP) Microsoft kor-poratsiyasining test laboratoriyasida sertifikatlangan va "Desig-ned for Microsoft Windows95G'NT", " Designed for Microsoft Win-dows 98G'NT " belgilarni olgan. Bu sistemaning maxsulotlaridan biri, AVP for Windows'98? Secure Computing (AKSh va Buyuk Bri-taniya) komp yuter xavfsizligi jurnalining test laboratoriyasida IN-the-Wild viruslarni detektirlash buyicha tekshirildi va «CheckMark» belgisini oldi. Bundan tashkari , AVP boshka xalka-ro sertifikat va sovrinlarga (ICSA komp yuter xavfsizligi xal-karo amerika korporatsiyasi sovrini) ega. AVP antivrus sistemasi tarkibiga bir nechta dasturlar kiradi:

- DOS, WINDOWS 3.XX, Windows 95G'98G'NT , OSG'2 operatsion tizimlar da ishchi stantsiyalar uchun AVP versiyalaridan ;
- AVP inspektori - diskni uzgarishlardan ximoyalovchi revizor ;
- AVP for Novell Netware va AVP for Windows NT -serverlar uchun AVP versiyalari ;
- Brendmauer (Firewall - 1) lar uchun Internetda antivirus ximoya.

AVP umumiy **h***arakteristikasi.*

Umuman sistema:

- Fayllardagi, yuklash sektorlardagi va operativ xotiradagi barcha mavjud turdagi fayllarni izlaydi va uchiradi ;
- «Sikilgan» fayllarda (PKLITE, LZEXE, DIET, SOM2EXE va boshka dasturlar formatlarida) viruslarni Aniqlaydi va uchiradi ;
- ZIP, ARJ, LHA, RAR formatlardagi arxiv fayllarni tekshiradi ;
- Mashxur elektron aloka sistemalar uchun lokal aloka kutilarni virusga tekshiradi;

• Evristik mexanizm yordamida noma`lum viruslar va 32-razryadli viruslarni izlaydi ;

• Nostandart zaralaydigan va fayllarni buzuvchi viruslarni Aniqlash uchun skanerlash holati mavjud.

Ishchi stantsiyalarni ximoyalash.

Winfows 95, 98 , NT va OS G’ 2 lar uchun AVP versiyalari rezi-dent monitor yordamida fonli rejimda doimiy ximoyani ta`min-laydi.

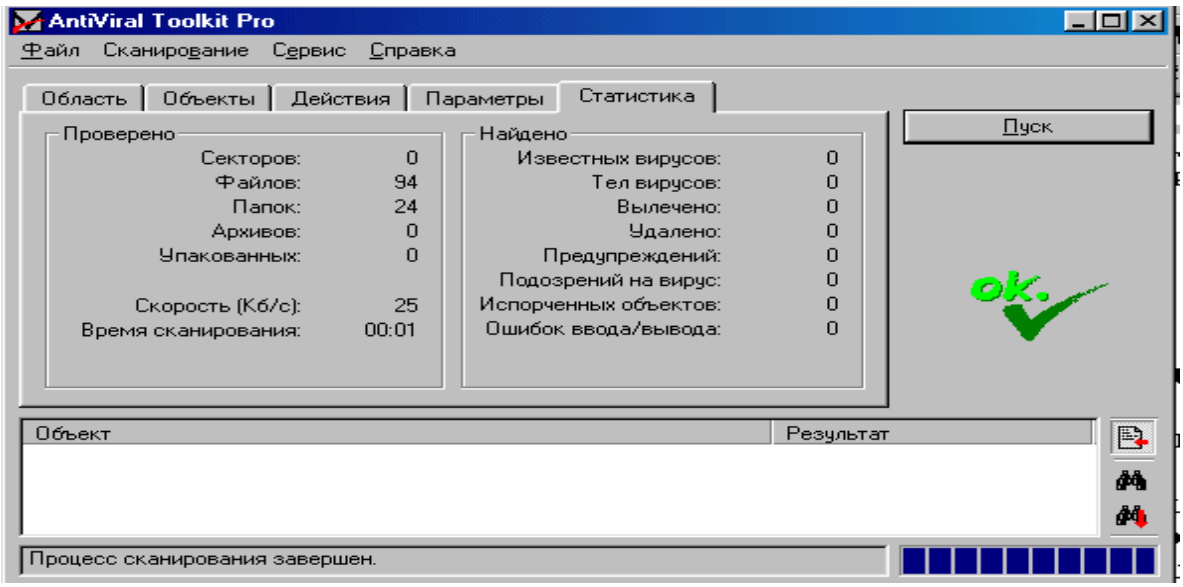
DOS uchun AVP versiyasi 2 vapriantda mavjud : interfeys bilan va buyruq satri kurinishida (AVPLITE). AVPLITE avvalgi mashinalarda (INTEL 286) xam ishlashi mumkin. AVPLITE - AVP turkumidagi boshka skanerlar imkoniyatlariga ega.

AVP INSPECTOR dasturi ishchi stantsiyalarga kushimcha ximoyani ta`minlaydi. Bu diskni uzgarishlardan ximoyalovchi revizor.Dastur Windows 95G’98G’NT boshchiligida ishlab, fayllar va direktoriyalardagi, sistemali sektorlardagi barcha uzgarishlarni Aniqlaydi.Dastur ajoyibligi, virus xisobiga va virus xisobiga bo’lmagan fayldagi uzgarishini Aniqlay olishi.Masalan, AVP Inspector yordamida sistemaning ish faoliyati (Sistemali reestr) bog’liq bulgan resurslardagi uzgarishlarni Aniqlash mumkin. AVP Inspector skanerlash (tekshirish) vaktini tejaydi, chunki AVP skaneri fakat uzgargan fayllarni tekshiradi. Bundan tashkari, dastur virus tufayli zararlangan va buzilgan fayllar yoki sektorlarni uzi tiklash imkoniyatiga ega.

AVP Inspector kulay grafik interfeys (GUI), ko’p maksadli ish yuritish, ko’p okimlilik, sof 32-razryadililik, IOS (kiritish-chikarish supervizori yoki 32-bitli drayver) drayveri orkali tugridan-tugri fizik va mantikiy disklarga murojaat kilish imkoniyatlariga ega.

Serverlarni antivirus ximoyalash.

Korporativ tarmoqlarga kirgan viruslar ko’prok salbiy ta`sir utkazadi. Shuni xisobiga, ko’plab kompaniyalar unlab, ba`zida yuzlab million dbllar yukotadi.



AVPN (yoki NorellNetware uchun Kasperkiy antivirus) - bu skaner, xam fil tr bo'lib, doimo serverdagi fayllarni nazorat kilib turadi. AVPN skaner holatida NorellNetware (3.11 versiyadan boshlab va IntranetWare fayl-serverida joylashgan) fayldagi viruslarni izlaydi, fil tr holatida fayllarni nazorat kiladi, ya`ni fayllarni ukishda, ishga tushirishda va serverga yozishda tekshiradi.

AVPN zararlangan fayllarni Aniqlagandan sung ularni boshkaruvchisiga kursatmasiga binoan, fayllar diskdan o'chiribyuborilishi, kursatilgan joyga faylni kuchirishi, fayl nomini uzgartirishi mumkin. Agar da zarurat tugilsa AVPN ishchi stantsiyani tarmoqdan uzib, tarmoq administratoriga xabar junatadi. AVPN ning skaner holatida bitta tarmoq joylashgan uzokdagi server tomlarini xam tekshiradi.

Bundan tashkari, AVPN yangi antivirus bazalarini yuklashga imkon beradi yoki antivirus baza ma`lumotlarini AVPN dan chiqmasdan turib tulik almashtirishga imkon beradi.

Tarmoq boshkaruvchisi, AVPN bilan ishlash mobaynida unga yangi sozlashlarni kiritishi va xotiraga saklashi mumkin. Shu bilan birga ishchi stantsiyadan dasturni ishag tushirishi va boshkarishi mumkin. AVPNHH skaner sifa tda foydalanilayotganda boshkaruvchi uni jadval asosida xamda ixtiyoriy vakt mobaynida ishlatishi mumkin.

AVP for Windows NT Server dasturi xam yangi kulayliklarga ega. Uning yordamida sistema boshkaruvchi tarmoqdagi antivirus xavfsizlik strategiyasining markazlashgan xolda boshkarishi mumkin.

Bu dastur ishchi stantsiyalardagi va serverlardagi AVP funktsiyasini tekshirishga imkon beradi, xamda bitta ishchi joyidan butun tarmoq bilan boshkarishga imkon beradi. Xususan, tarmoqning barcha ob`ektlarini moslashtiradi. Dastur boshkaruvchi tarmoqning joriy holati xakida tulik xisobot tuzadi va har bir ishchi stantsiya uchun avtomatik yangilash utkazadi.

Brendmauerlar uchun antivirus.

Brendmauerlar xam ximoya uchun tuziladi. Tarmoq ruxsatsiz kirishga tuskinlik kilgani bilan doimo xam viruslarni yukota olmaydi. Kasperskiy laboratoriyasi, CVP (masalan, ChekPoint Fire Wall-1) protokolini ta`minlovchi, ixtiyoriy brendmauerlar uchun AVP for Fire Wall dasturini yaratadi.

AVP for Fire Wall - bu antivirus serveri bo'lib, HTTP, FTP, SMTP va boshka protokollar buyicha kabul kilinayotgan fayllarni tekshiradi. Virus Aniqlangan holatda, u faylni davolaydi, zararlangan fayl uzatilishi tuxtatiladi, faylni aloxida katalogga joylaydi va boshkaruviga aloka orkali xabar beradi.

Uz-uzini ximoyalash retseptlar:

Eng yaxshi ximoya komp yuterga virusni yakinlashtirmaslik.

- umumiy doimo tekshirib turish ;
- disketga yozish ximoyasini urnatish ;
- yangi yuklangan fayllarni tekshirmasdan ishlatmaslik;
- shaxsiy komp yuter «berkitib» kuyish;
- doimo antivirus dasturini yangilab borish.

Antivirus dasturlarini test natijalari:

Antivirus dasturi	Platforma	Aniqlangan «yovvoyi» viruslar, %	Uchirilgan «yov-voyi» viruslar, %
DrSolomon's AntiVirus Toolkit	Windows 95	100	89
F - Prot Proffessional	Windows 95	99	78
IBM Anti Vims v.2.5	Windows 95	96	32
McAfee Virus Scan	Windows 95	93	90

Norton Anti Virus v. 2.0	Windows 95	100	77
Thunder Byte Antivirus Utilites	Windows 95	95	60
Touchstone PC - Cillin II	Windows 95	100	80
McAfee Virus Scan	WindowsNT	92	59
Norton Anti Vims v. 2.0	WindowsNT	100	76

"**Troya tulpori**" - bu shunday programmaki, u asosan xujjatlarda yozilmagan qo'shimcha harakatlarni bajaradi. qadimgi Rim Troya tulporining analogi bo'lmish "Troya tulpori" shubha o'yg'otmaydigan qobiq programmalarga ta`sir ko'rsatib, avtomatlashtirilgan sistema xavfsizligiga ta`sir ko'rsatuvchi jiddiy tahdid hisoblanadi. Xarakteriga ko'ra "Troya tulpori"paket rejimida ishlovchi programma vositalari yordamida amalga oshiriladigan faol tahdidlar turiga kiradi. U sistemaning ixtiyoriy ob`ektiga taxdid solishi mumkin. Eng xavflisi - oposredovanno'y ta`sir, ya`ni "Troya tulpori" bir foydalanuvchi vakolatlari doirasida harakat qiladi, lekin boshqa foydalanuvchi borasida esa uning shaxsini aniqlash mumkin emas.

"Troya tulpori" xavfi asosan keyinchalik sistema foydalanuvchilariga taklif etiladigan (in`om etiladigan, sotiladigan yoki almashtiriladigan) zararsiz programmaga u yoki bu usul bilan qushilgan qushimcha komandalar blokiga ta`sir etishidadir. Bu komandalar bloki biror shart (oy, yil, kun, vaqt, tashqi komanda) kiritilganda yoki bajarilganda ishga tushadi. Bunday programmani ishga tushiruvchi o'zi va o'zi bilan birga butun sistemani havf ostida qoldiradi.

Agar «troya tulpori»ni ishga tushirgan foydalanuvchi keng imtiyozlar naboriga ega bo'lsa, bu holda uning xavfi ancha yuqori bo'ladi. Bunday hollarda «troya tulpori» ni tuzgan va o'zlashtirgan hamda keng imtiyozlar naboriga ega bo'lmagan buzg'unchi boshqalarning qo'li bilan ruxsatsiz imtiyozli funktsiyalarni bajarishi mumkin. Yoki, masalan, bunday programmani ishga tushirgan foydalanuvchining ma`lumotlar nabori buzg'unchini juda qiziqtirib qolishi

mumkin, bunda buzg'unchining hatto keng imtiyozlar naboriga ega bo'lmasligi uning sistemaga ruxsatsiz ta`sirlariga to'siq bo'la olmaydi. Bunga misol qilib, 1999 yil yanvarda Internetda paydo bo'lgan tekin tarqatiluvchi Screen saver (zastavka) ni olish mumkin, u komp yuterda DES algoritmi asosidagi shifrlovchi programmani qilirishni amalga oshiradi va agar uni topsa, shifrlash kalitlarining almashinish jarayonini nazorat qilib, bu kalitlarni elektron pochta orqali Xitoydagi anonim-serverga uzatadi. Undan himoyalanishning radikal uslubi – bu programmani ijro etishda berk muhitni tashkil etishdir. Ayniqsa tashqi Internet va ichki tarmoqlarni loaqal protokollar sathida bir-biridan ajratish (agarda bu jarayon fizik satxda amalga oshirilsa yanada yaxshi bo'lardi) lozim. Shuningdek, imtiyozli va imtiyozsiz foydalnuvchilar turli ko'rinishdagi, individual ravishda saqlanishi va himoyalanishi shart bo'lgan programmalar bilan ishlagani ma`qul. Bu tadbirlardan foydalangan holdagina «troya tulpori» kabi programmalarning qabul qilinishi kamayadi.

Viruslar. Hozirda komp yuter virusiga duch kelmagan birorta ham sistema administratori yoki foydalanuvchini topib bo'lmaydi. Creative Strategy Research firmasi tomonidan o'tkazilgan tadqiqot natijalariga ko'ra so'rov o'tkazilganda 451 mutaxassisdan 64% i virusga duch kelganini ma`lum qilishadi. Hozirgi kunda ma`lum bo'lgan minglab viruslarga har oyda 100-150 shtammdan kelib qo'shilmoqda.

Virus – bu shunday programmaki, u bir programmadan ikkinchisiga tez tarqala olish xususiyatiga ega bo'lib, boshqa programmalarning tarkibiga o'zining programma tarkibini o'zgartiruvchi xususiyatlarini qo'shib qo'yadi. Virusning 2 ta asosiy xususiyati xarakterlanadi:

- o'zidan-o'zi ko'payish: uning biror ma`lumot to'plovchi yoki eltuvchi tarkibida yashash davrida kamida bitta nusxaga ko'payish xususiyati;
- hisoblash jarayoniga xalaqit berish – tirik tabiatdagi viruslarga xos parazitlik xususiyati.

Viruslar ham «troya tulpori» kabi faol ta`sir etuvchi programma bo'lib, quyidagi 4 ta qismdan iborat strukturaga ega bo'ladi:

1-qism – programma kodini aks ettiradi, virus uning yordamida EHM xotirasiga tushadi;

2-qism – virusning d isk xotirasiga, ulardagi fayllar va yuklash sektoriga ko'chirilish ishini ta`minlaydi;

3-qism – virusning o'z faoliyatini ishlash shart-sharoitlarini o'z ichiga oladi;

4-qism – virusning asosiy ishi – buzg'unchilik faoliyatini algoritmini o'z ichiga oladi.

Komp yuter viruslari ishlash sohasiga qarab:

1. Komp yuter sistemasidagi informatsiyani zararlovchi;

2. Komp yuter sistemalariga infektsiya yuqtiruvchi;
3. Komp yuter sistemalari va tarmoqlarining ishini batamom tugatuvchi turlarga bo'linadi.

Hozirgi paytda viruslarning sinflanishi, ularda qullaniladigan virusni yuqtirish usullari, ularga qarshi kurashish chora-tad irlari yaxshi o'rganilmoqda.

Viruslardan himoyalanishda ikki tomondan yondashish mumkin:

- mustaqil, alohida masala sifatida;
- avtomatlashtirilgan sistemaning umumiy xavfsizligining bir jihati sifatida.

Bu yondashuvlarning ikkisi ham o'zining alohida xususiyatlariga va mos ravishda masalani yechishning o'ziga xos usullariga ega.

Virusga qarshi kurashning bir tomoni sifatida Hozirgi paytda virusga qarshi programmalar sistemasi ishlab chiqilmoqda. Ularning ko'pchiligi mos tibbiy atamalar: «Vaktsina», «Antitoksin», «Interferon» va h. atamalar bilan atalmoqda. Umuman olgan virusga qarshi prgrammalarni 3 guruhga ajratish mumkin:

1. Fil tlovchi programmalar;
2. Virus detektorlar (virus ushlovchilar, revizor programmalar, infektsiyaga qarshi programmalar);
3. Fag programmalar.

Fil trlovchi programmalar – zaharlanishni bartaraf etish uchun ishlab chiqilgan programmalar. Ular komp yuter xotirasiga joylashib olib virusning urinishlarini va signallarini kuzatib, olib borayotgan ishlarini nazorat qiladi.

Virus detektorlar – sistema holatining foto tasvirini olib, uni doimiy ish faoliyati holati bilan taqqoslab turadi. Agarda biror o'zgarish sodir bo'lsa, xavf to'g'risidagi signalini beradi. Boshqa revizor programmalar matematik formulalar yordamida programma va ma`lumotlar butunligini aniqlab beruvchi nazorat kodlari yig'indisini hisoblash ga asoslanadi.

Fag programmalar – oddiy viruslarni topib, ildizini yo'qotishga o'rgatilgan programmalar. Ular ko'proq eski viruslarni topib yo'qotishga qulaydir.

Olib borilgan chora-tadbirlar natijasida, yuqorida keltirilgan programmalarning faoliyati natijasida oxirgi paytlarda viruslar bilan zararlanish va buzilish masshtabini kamaytirishga erishildi. Lekin bu programmalarning taraqqiyoti viruslarning taraqqiy etishiga yeta olmayapti. So'nggi yillarda komp yuter viruslaridan himoyalanishning istiqbolli yo'llaridan biri sifatida apparat va programm himoya usullarining birgalikda tashkil etilishidan foydalanilmoqda. Bunday apparat-programm vositalarga komp yuterning standart kengaytirish slotlariga o'rnatiladigan maxsus virusga qarshi platalarni misol qilish mumkin. Masalan, Intel korporatsiyasi 1994 yildayoq komp yuter tarmoqlarini virusdan himoyalashning istiqbolli texnologiyasi - Intel EtherExpress PROG'10 qurilmasini taklif qilgan edi. Intel EtherExpress PROG'10 qurilmasi komp yuterning butun

sistemasini OS yuklangunga qadar tekshirib chiquvchi virusga qarshi programmaga ham ega.

«qurt» - viruslardan farqli ravishda o'z nusxasini axborot eltuvchida qoldirmaydigan, tarmoq orqali tarqaluvchi programmalar. «qurt» tarmoqning biror zararlangan uzelini aniqlash mexanizmidan foydalangan holda, o'zining tanasi yoki biror qismini ushbu uzelga uzatadi hamda shu paytning o'zida ishga tushadi yoki biror payt poylab ishga tushadi. Bunday turdagi programmalarning eng mashhuri – «Morris qurti» bo'lib, 1988 yilda Internet xalqaro tarmog'iga katta zarar yetkazgan.

«qurt»ning tarqalishi uchun eng qulay sharoit bu – tarmoq foydalanuvchilarining bir-biriga do'stona, ishonuvchan munosabatlaridir. Undan himoyalanishning eng yaxshi usuli bu tarmoqdan ruxsatsiz foydalanishga qarshi ehtiyot choralarini qo'llashdir.

Xullas, «troya tulpori», «qurt», virus programmalar kabi zararli programmalardan himoyalanish uchun programmalarni ijro etishning berk muhitini tashkil etish, ijro etiluvchi fayllarga kirishni cheklash, ishlatilayotgan programma vositalarini testlash va h. ni amalga oshirish zarur.

Mustahkamlash uchun savollar:

1. Komp yuter viruslari kanday xosil buladi?
2. Fil trlovchi programmalar qanday vazifani bajaradi ?
3. Fag programmalar qanday vazifani bajaradi ?
4. Virusning qanday asosiy xususiyati xarakterlanadi ?
5. Serverlarni antivirus ximoyalash tushunchasini izohlang.
6. Vaktsina», «Antitoksin», «Interferon» atamalari nimani anglatadi ?
7. Uz-uzini ximoyalash retseptlariga nimalar kiradi ?
8. Komp yuter viruslari ishlash sohasiga qarab qanday turlarga bo'linadi ?
9. "Troya tulpori" xavfini izohlang.
10. Komp yuter sistemalariga infektsiya yuqtiruvchilar tarkibini aytib bering.
11. Evgeniy Kasperskiy Antivirus dasturi imkoniyatlarini aytib bering.
12. Brendmauerlar uchun antivirus nima uchun tuziladi ?
13. «Morris qurti» tomonidan yetkazilgan zararni ifodalab bering.
14. Ishchi stantsiyalarni ximoyalash tushunchasini izohlang.

Foydalanilgan saytlar ro'yxati

- www.securityfocus.com-portal: materialo' po bezopasnosti
- www.sans.org-Institut SANS: stat i po bezopasnosti, proekto'
- www.xforce.iss.net-baza danno'x uyazvimostey, materialo' po bezopasnosti

- www.packetfactory.net-sayt razrabotchikov biblioteke
- blacksun.box.skG' tutorials.html-aspektam setevoy bezopasnosti raboto' s setevo'x servisov.
- www.phrack.com - jurnal «Phrack»
- www.cerias.purdue.edu-TSentr informatsionnoy bezopasnosti Universitet Purdu , arxiv programmnogo obespecheniya

5-Ma`ruza

Dasturlarni maxsus o'g'irlash. Raqamli imzo. Bir martalik parollar. Elektron imzolarning himoya darajasi.

O'quv modullari

1. Ziqna dasturlar tushunchasi
2. Informatsiya mahfiyligini ta`minlovchi shifrlash mexanizmi
3. Foydalanishni nazorat qiluvchi mexanizm .

Aniqlashtirilgan o'quv maqsadlari.Talaba bu mavzuni to'la o'zlashtirgandan so'ng:

- Ziqna dasturlar haqidagi tamoyillarni biladi;
- Shifrlash mexanizmi asosiy printsiplarini bo'laklarga bo'lib, ta`rif bera oladi;
- Abonentli shifrlash xususiyatlarinini talqin eta oladi;
- Raqamli imzo mexanizmlarini qaysi sinfga mansubligini tasavvur eta oladi;
- Marshrutni boshqarish va guvohlik berish mexinizmlari o'rtasidagi o'zaro aloqadorlikni aniqlaydi, bog'lanishlarni tahlil qila oladi.

Tayanch so'z va iboralar:

Ziqna dasturlar, guvohlik berish mexanizmlari,himoya modellari,sistema xavfsizligi, foydalanuvchi, kanalli shifrlash, Marshrutni boshqarish

Ziqna programmalar – bular shunday programmalarki, ular ish jarayonida sistemaning biror resursini monopollashtirib, boshqa programmalarga bu resurslardan foydalanishga yo'l qo'ymaydi. Sistema resurslariga bunday programmalarning kirishi sistemaning barcha resurslarining teng huquqli ishlash jarayoniga putur yetkazadi. Tabiiyki, bunday xujum sistemaning ishiga faol ta`sir etish hisoblanadi. Bunday bevosita hujumlarga asosan, sistemaning eng muhim ob`ektlari – protsessor, operativ xotira, kiritish-chiqarish qurilmasi, disk xotirasi duchor bo'ladi.

Ko'pchilik komp yuterlar, ayniqsa tadqiqot markazlarida fon programmalariga ega bo'ladilar, bu fon programmalarning esa ustunlik darajasi

past bo’ladi. Ammo bu ustunlik darajasining oshishi natijasida programma qolgan programmalarni blokirovka qilib qo’yadi. Aynan shunday programmalar ziqna programmalar hisoblanadi.

Agar ziqna programma cheksiz tsiklga tushib qolsa, sistema boshi berk ko’chaga kirib qoladi. Ammo ko’pchilik operatsion sistemalarda masalada foydalanilayotgan protsessor vaqtini cheklash imkoniyati mavjud. Bu boshqa programmalarga bog’liq bog’liq holda bajariladigan amallarga tegishli emas, masalan, asosiy programmaga asinxron holda bajariladigan kiritish-chiqarish amallarini keltirish mumkin; bularning ijro vaqti programma vaqti hisobidan tashqari bo’ladi. Kiritish-chiqarish amalining tugallanganligi to’g’risida asinxron axborotni olib va yana yangi kiritish-chiqarishga so’rov jo’natgandan so’ng, chin ma`nodagi cheksiz tsiklli programmaga erishish mumkin. Bunday xujumlarni asinxron xujumlar deb ham atashadi.

Ziqna programmalarga yana bir misol sifatida operativ xotiraning katta qismini band qilib oluvchi programmani keltirish mumkin. Ya`ni bunday paytda opreativ xotirada tashqi ma`lumot eltuvchidan o’tkazilgan ma`lumotlar ketma-ket joylashtiriladi. Oxir oqibatda, xotira faqat birgina programma ixtiyorida bo’lib, boshqa programmalar uchun operativ xotirada joy yetishmasligi natijasida, ularning ishi to’xtaydi. Yuqorida aytilganidek ziqna programmalar asosan sitemaning 3 asosiy resursi: protsessor vaqti, operativ xotira va kiritish-chiqarish kanallaridan birini egallashga harakat qiladi. Ammo sistemaning boshqa harqanday resursini ham egallashi mumkin: uning ishini blokirovka qilish, yoki qandaydir programma (masalan, virus) ish faoliyatining natijalaridan foydalanishi mumkin. Resurslarni egallab olishga qarshi kurashni turli ijro etiluvchi programmalarga chegaralar qo’yish (protsessor vaqti, kiritish-chiqarish amallari soni, ruxsat etilgan operativ xotira sig’imi va h.), shuningdek, ular ustidan domiy operatorlik nazoratini o’rnatish yo’li bilan amalga oshirilishi mumkin.

Parollar o’g’risi. Bu programmalarni maxsus o’g’irlashga mo’ljallangan. Sistemaga kirishga urinishda nomni va parolni kiritish so’raladi va bu parol va nom buzg’unchiga jo’natiladi, so’ngra kirishda xatolik sodir bo’lgani to’g’risida axborot chiqib, boshqaruv operatsion sistemaga qaytgandan so’ng, parolni terishda xatoga yo’l qo’ydim deb o’ylab foydalanuvchi sistemaga qaytadan kirishga harakat qiladi va bunga muvaffaq bo’ladi. Bu paytda uning nomi va parol o’g’ri-programmaning egasiga ma`lum bo’ladi. Parolni o’g’irlash boshqa usul – sistemaga kirishni boshqaruvchi programmaga ta`sir etish yo’li bilan amalga oshirilishi mumkin. Bunday tahdidni bartaraf etish uchun, avvalo, kiritilayotgan nom va parol haqikatan ham boshqa programma emas, balki sistemaning haqikiy kirish programmasida bajarilayotganligiga ishonch hosil qilish lozim. Bundan tashqari paroldan foydalanish va sistemada ishlash qoidalariga og’ishmay amal

qilish kerak. Ko’pchilik buzilishlar mug’ombirlik bilan qilingan puxta o’ylangan ta`sirlardan emas, balki oddiy beparvolik natijasida kelib chiqadi. Sistemadan chiqib ketmay turib ish o’rnini tark etmaslik tavsiya etiladi. Oxirgi marta kirgandagi vaqt va kun to’g’risidagi va xatoli kirishlar soni to’g’risidagi axborotni domiy tekshirib turish zarur. Bu yuqorida keltirilgan barcha tavsiyalar parolning o’g’irlanishidan himoya qilishga yordam beradi.

Yuqorida keltirilganlardan tashqari, parolni komprometatsiya qilishning boshqa imkoniyatlari ham mavjud. Parolni o’z ichiga olgan komandalarni komanda protseduralarida yozish tavsiya etilmaydi, tarmoqqa kirishdagi parolni ochiq e`lon qilishdan qochish kerak, chunki bu holatlarni kuzatish va natijada parolni o’g’irlash mumkin. Turli uzellarga kirishda bitta paroldan foydalanmaslik kerak. Xullas, parollardan foydalanish qoidalariga rioya qilish – bu parollarni himoyalashning eng zarur shartidir.

Yuqorida keltirilgan qasddan qilingan ta`sirlardan sistema va informatsiyani himoyalash usullarini ko’rib chiqamiz.

Shifrlash mexanizmi uzatilayotgan ma`lumot yoki ma`lumotlar haqidagi informatsiyaning maxfiyligini ta`minlaydi. Shifrlash mexanizmining algoritmida maxfiy yoki ochiq kalitdan foydalaniladi. Maxfiy kalitli usulda boshqarish va kalitni taqsimlash mexanizmlarning mavjudligi nazarda tutiladi. Shifrlashning ikki usuli farqlanadi: kanal darajasidagi protokol yordamida amalga oshirilgan ***kanalli*** va amaliy daraja (sath) yoki ba`zi hollarda predstavitel no’y sathdagi protokollar yordamida amalga oshirilgan ***abonentli (okonechnoe) shifrlash.***

Kanalli shifrlashda aloqa kanali orqali uzatilayotgan barcha informatsiya (shu bilan birga xizmatchi informatsiya) himoya qilinadi. Bu usul quyidagi xususiyatlarga ega:

- bitta kanal uchun shifrlash kalitini ochish boshqa kanallardagi informatsiyaning buzilishiga olib kelmaydi;
- xizmatchi xabarlar, xabarlarning xizmatchi maydonini o’z ichiga olgan holda, barcha uzatilayotgan informatsiya ishonchli himoyalangan;
- barcha informatsiya ma`lum oraliq uzellar, retranslyatorlar, shlyuzlar va h. uzellarda ochiqcha uzatiladi;
- bajarilayotgan operatsiyalarda foydalanuvchi ishtirok eta olmaydi;
- har bir juft uzellar uchun o’zining kaliti talab qilinadi;
- shifrlash algoritmi yetarli darajada mahkam bo’lishi kerak va shifrlash sur`atini kanalning o’tkazuvchanlik qobiliyati darajasida ta`minlashi lozim (aks holda xabarlarning tutilib qolishi ro’y beradi va natijada, sistemaning blokirovkasi yoki ishlash unumdorligining yetarlicha kamayishiga olib keladi);

- avvalgi xususiyat shifrlash algoritmini apparat usulda amalga oshirish zaruratiga olib keladi, va buning natijasida sistemaning tashkil etilishi va xizmat ko'rsatilishi xarajatlarining oshishiga olib keladi;

Abonentli (okonechnoe) shifrlash ikkita amaliy ob`ektlar o'rtasidagi uzatilayotgan ma`lumotlarning maxfiyligi va ishonchliligi ta`minlash imkoniyatini beradi. Boshqacha aytganda, uzatuvchi ma`lumotlarni shifrlaydi, qabul qiluvchi esa shifrlangan ma`lumotni deshifrlaydi. Bu usulning quyidagi xususiyatlari bor:

- faqatgina xabarning mazmunigina himoyalanadi, barcha xizmatchi informatsiyalar esa ochiqligicha qoladi;
- uzatuvchi va qabul qiluvchidan boshqa hech kim informatsiyani tiklash imkoniyatiga ega emas (agar foydalanilayotgan shifrlash algoritmi yetarlicha mustahkam bo'lsa);
- uzatish marshruti muhim emas, har qanday kanalda informatsiya himoyalangan holda qoladi;
- har bir juft foydalanuvchi uchun yagona kalit talab qilinadi;
- foydalanuvchi shifrlash va kalitlarni taqqoslash protsedurasini bilishi kerak.

U yoki bu shifrlash usulining yoki ularning kombinatsiyasining tanlanishi tavakkallar tahlilining natijalariga bog'liq. Bunda savol quyidagicha qo'yiladi: qaysi biri nozikroq: bevosita alohida aloqa kanalimi yoki turli kanallar orqali uzatilayotgan xabarning mazmunimi? Kanalli shifrlar tezroq (boshqa bundan ham tezroq algoritmlarni qo'llash mumkin), foydalanuvchi uchun ravshan, kamroq kalitlarni talab qiladi. Abonentli shifrlash nisbatan ixchamroq, saylanma tarzda foydalanilishi mumkin, biroq bunda foydalanuvchining ishtirok etishi talab qilinadi. Har qanday aniq bir sharoitda bu masala individual ravishda yechiladi.

Raqamli imzo mexanizmlari – ma`lumotlar blokini yopish va yopilgan ma`lumotlar blokini tekshirish protseduralariga ega. Dastlabki jarayon maxfiy kalitli ma`lumotlarni tiklashga yo'l qo'ymaydigan ochiq informatsiyadan foydalanadi. Maxfiy informatsiya yordamida jo'natuvchi xizmatchi ma`lumotlar blokini shakllantiradi (masalan, bir tomonlama funktsiya yordamida) qabul qiluvchi esa hammaning foydalanishi mumkin bo'lgan informatsiya asosida qabul qilingan blokni tekshiradi va jo'natuvchining haqiqiy (asl, chin) ekanligini aniqlaydi. Asl ma`lumotlar blokini faqat zarur kalitni biladigan foydalanuvchigina shakllantira olishi mumkin.

Foydalanishni nazorat* qilish *mexanizmi – tarmoq ob`ektining resurslaridan foydalanish uchun qanchalik vakolatlarga egaligini tekshiradi. Vakolatlarni tekshirish ishlab chiqilgan xavfsizlik siyosati (saylov, vakolatli yoki ixtiyoriy boshqa) va uni amalga oshirish mexanizmlarining qonun-qoidalariga muvofiq holda amalga oshiriladi.

Uzatilayotgan ma`lumotlarning butunligini ta`minlash mexanizmlari – bu mexanizmlar ma`lumotlarning alohida maydoni yoki blokining butunligini qanday ta`minlasa, to'la ma`lumotlar oqimining butunligini ham shunday ta`minlaydi. Ma`lumotlar blokining butunligi uzatuvchi va qabul qiluvchi ob`ektlar tomonidan ta`minlanadi. Uzatuvchi ob`ekt ma`lumotlar blokiga shunday qo'shimcha belgi qo'shadikik, bu belgi shu ma`lumotlarning o'zidan hosil qilingan funktsiyaning qiymatiga teng bo'ladi. qabul qiluvchi ob`ekt ham xuddi hosil qilingan funktsiyani hisoblaydi va uni qabul qilingan ma`lumot bilan taqqoslaydi. Agar bu yerda ular bir-biri bilan mos kelmasa, ma`lumotlarning butunligi buzilganligi ma`lum bo'ladi. Ma`lumotda o'zgarishni payqagandan keyin ma`lumotlarni tiklash ishlari olib boriladi.

Ma`lumotlarning butunligini qasddan buzishda mos ravishda nazorat belgisining qiymati ham o'zgartirilishi mumkin, bunday paytlarda qabul qiluvchi ma`lumotlar butunligining buzilganligini payqamaydi. Shuning uchun bunday sharoitda nazorat belgisini ma`lumotlarning va maxfiy kalitning funktsiyasi ko'rinishida shakllantirish kerak. Bunday holda nazorat belgisini maxfiy kalitni bilvosita turib to'g'ri shakllantirib bo'lmaydi va qabul qiluvchi bu o'zgartirish natijasida asl ma`lumotmi yoki yo'qligi to'g'risida aniq xulosaga keladi.

Ma`lumotlar oqimining butunligini (qayta o'zgartirishdan, qo'shimcha ma`lumot qo'shishdan, ma`lumotlarning takrorlanishidan yoki yo'qolishidan) himoya qilishni qo'shimcha tartiblash shakllari (ma`lumotlar oqimidagi xabarlarning tartibini nazorat qilish), vaqt belgilari va h.dan foydalanib amalga oshirish mumkin.

***Tarmo*q *ob`ektlarining autentifikatsiyasi mexanizmlari*** – autentifikatsiyani ta`minlashda parollar, ob`ekt xarakteristikalarini tekshirish, kriptografik metodlardan, raqamli imzo kabilardan foydalaniladi. Bu mexanizmlar odatda, bir sathli tarmoq ob`ektlarini autentifikatsiya qilishda foydalaniladi. Foydalanilayotgan usullar "uch karra qo'lni qisish" protsedurasi bilan bir vaqtda olib borilishi mumkin (jo'natuvchi va qabul qiluvchi o'rtasida autentifikatsiya va tasdiqlash parametrlari bilan axborot almashish uch karra amalga oshirilishi).

Matnni to'ldirish mexanizmlari – grafikni analiz qilishdan himoyani ta`minlash uchun ishlatiladi. Bunday mexanizm sifatida, masalan, (fiktiv) soxta axborotni generatsiya qilishdan foydalanish mumkin, bunda trafik vaqt bo'yicha doimiy intensivlikka ega.

Marshrutni bosh*qarish *mexanizmlari – marshrutlar dinamik tanlanishi mumkin yoki fizik xavfsiz qism tarmoq, retranslyatorlar, kanallardan foydalangan holda oldindan berilishi mumkin. Chirmab bog'lashga urinishda tugal (abonent) sistemalar boshqa marshrut bo'yicha bog'lanishni talab qiladi. Bundan tashqari, tanlov bo'yicha marshrutlashdan foydalanilishi mumkin (ya`ni marshrutning bir

qismi jo’natuvchi tomonidan ochiq holda xavfli uchastkalarni aylanib chiqishda beriladi).

Guvo*hlik berish mexanizmlari** – ikki yoki undan ortiq ob`ektlar o’rtasida uzatilayotgan ma`lumotlarning xarakteristikalari ***guvohlik berish mexanizmi orqali tasdiqlanishi mumkin. Tasdiqlash barcha tomonlarning ishonchiga sazovor bo’lgan uchinchi tomon - arbitr tomonidan amalga oshiriladi.

H*odisalarni topish va ishlash* (xavfli hodislarni nazorat qilish vositalari kabi) – tarmoqning xavfsizlik siyosatining buzilishiga olib keluvchi hodisalarni topishga mo’ljallangan. Bu hodisalarning ro’yxati alohida sistemalardagi ro’yxatga muvofiq keladi. Bundan tashqari, bunga yuqorida keltirilgan himoya mexanizmlarining ishidagi buzilishlar to’g’risida ma`lumot beruvchi hodisalarni ham kiritish mumkin. Bunday hollarda ko’riladigan chora-tadbirlarga turli protseduralar: tiklash, hodisalarni ro’yxatga olish, aloqani bir tomonlama uzish, hodisa haqida hisobot (jurnalga yozish) va h. protseduralarni kiritish mumkin.

Xavfsizlikni tekshirish* h*isoboti (sistema jurnali bilan tekshirish kabi) – xavfsizlikni tekshirish deganda sistema yozuvlari va faoliyatining berilgan xavfsizlik siyosatiga mosligini mustaqil tekshirish tushuniladi.

Lokal hisoblash tarmoqlarida ma`lumotlarni muhofaza qilish usuli

Tayanch so’z va iboralar:

Identifikatsiya , autentifikatsiya, Informatsiyani himoyalash, LHT, Barqaror autentifikatsiya, Statik autentifikatsiya, O’zgarmas autentifikatsiya, serverlar diski (tomi),, ishchi stantsiya, katalog **.**

Informatsiyani himoyalashning asosiy usullariga quyidagilar kiradi:

- LHT ga kirishda autentifikatsiya va identifikatsiya qilish;
- LHT ning ba`zi ob`ektlari va resurslaridan foydalanishni cheklash (alohida serverga, alohida serverlar diski (tomi) ga, ishchi stantsiya, katalog, fayllardan foydalanish, ularni o’zgartirish, o’chirish va h.k.).
- LHT da informatsiyani himoya qilishning apparat usuli.
- Ma`lumotlarni himoya qilishning programma usuli;
- Ma`lumotlarni kriptografik usulda himoya qilish, ya`ni ma`lumotlarni shifrlash (kriptlash);

1. Identifikatsiya va autentifikatsiya

Identifikatsiya va autentifikatsiya (Id va A) - foydalanuvchi va jarayonlar to’g’risidagi ma`lumotlarning haqiqiyligini (aslligini) tekshirish va aniqlash jarayonidir. Ular foydalanuvchiga sistema resurslaridan foydalanishining mumkin yoki mumkin emasligi haqida qaror qabul qilishda ishlatiladi. U yoki bu

ma`lumotdan kimlar foydalana olishi mumkinligini aniqlash ma`lumotlar sinflanishi jarayonining tarkibiy qismi bo'lishi lozim.

Autentifikatsiyaning uchta asosiy ko'rinishi mavjud bo'lib, ular - statik, barqaror va o'zgarmas. Statik autentifikatsiya parollardan va boshqa texnologiyalardan foydalanadi. Bu parol va texnologiyalarni takrorlash yo'li bilan yo'qqa chiqarish mumkin. Odatda, bu parollar takror foydalaniladigan deb nomlanadi. Barqaror autentifikatsiya bir marta ishlatiladigan parollarni yaratish uchun kriptografiyadan foydalanadi. Bu usul tarmoqqa ulanish joyiga ataka qiluvchi xabarlarni qo'yish bilan yo'qqa chiqariladi. O'zgarmas autentifikatsiya tarmoqqa ulanish joyiga ataka qiluvchi informatsiyani qo'yishdan saqlaydi.

Statik autentifikatsiya

Statik autentifikatsiya autentifikatsiyalovchi va autentifikatsiyalanuvchi tomonlar o'rtasida uzatilayotgan informatsiyani yot hujum qiluvchi tomon ko'ra olmaydigan, o'zgartira olmaydigan, qo'ya olmaydigan paytdagina himoyani ta`minlaydi. Bunday holatda buzg'unchi faqat autentifikatsiya jarayonini boshlash (buni faqat qonuniy foydalanuvchi amalga oshira oladi) va bir qator urinishlarni amalga oshirish yordamidagina ma`lumotlarni aniqlashga urinishi mumkin. Parollardan foydalanishning an`anaviy sxemalari himoyaning mana shu turidan foydalanadi. Lekin autentifikatsiya mustahkamligi asosan parollarni topishning murakkabligi hamda bu parollarning qanchalik darajada yaxshi himoyalanganligiga bog'liq bo'ladi.

Barqaror autentifikatsiya

Autentifikatsiyaning bu sinfi har bir autentifikatsiya seanslarida almashinib turadigan dinamik autentifikatsiya ma`lumotlaridan foydalanadi. Autentifikatsiyalovchi va autentifikatsiyalanuvchi orasida uzatiladigan informatsiyani tutib qolishi mumkin bo'lgan ataka qiluvchi yangi autentifikatsiya seansini autentifikatsiyalanuvchi bilan birgalikda boshlashga va qonuniy foydalanuvchi nazorati ostida niqoblash umidida ma`lumotlarni takrorlashga harakat qiladi. 1-darajali kuchaytirilgan autentifikatsiya shunday atakalardan himoya qiladiki, bu ataka natijasida oldingi seansda yozilgan autentifikatsiya ma`lumotlaridan keyingi seanslarda foydalanish mumkin bo'lmay qoladi.

Shunga qaramasdan, barqaror autentifikatsiya ma`lumotlarni faol atakalardan himoya qila olmaydi. Bunday atakalar autentifikatsiya jarayoni tugagandan so'ng foydalanuvchi tomonidan serverga jo'natiladigan komanda va ma`lumotlar ataka qiluvchi tomonidan o'zgartirilishi natijasida amalga oshiriladi. Server berilgan autentifikatsiyalanayotgan foydalanuvchi va mantiqiy ulanish

o’rtasidagi aloqani ta`minlaydi; u o’zini ushbu ulanishga taalluqli barcha komandalarning manbai deb hisoblaydi..

An`anaviy parollar barqaror autentifikatsiyani ta`minlay olmaydi. Foydalanuvchi parollari keyinchalik foydalanilishi yoki tutib qolinishi mumkin. Lekin bir martalik parollar va elektron imzolar ushbu himoya darajasini ta`minlay oladi.

O’zgarmas autentifikatsiya

Autentifikatsiyaning bu turi autentifikatsiyalanuvchi va autentifikatsiyalovchi orasida uzatiladigan ma`lumotlar oqimi orasiga informatsiya qo’shishi, o’zgartirishi va tutib qolishi mumkin bo’lgan ataka qiluvchidan hattoki, autentifikatsiya jarayoni tugagandan so’ng ham himoyani ta`minlaydi. Bunday atakalar faol ataka deb yuritilib, ataka qiluvchi, asosan, server va foydalanuvchi orasidagi bog’lanishga faol ta`sir ko’rsatadi. Himoyaning bu turini amalga oshirishning usullaridan biri foydalanuvchidan serverga jo’natilayotgan har bir ma`lumotlar bitiga ishlov berishni elektron imzolarni inertsiya qilish algoritmi yordamida amalga oshirishdan iborat. Kriptografiya asosidagi boshqa kombinatsiyalar ham mavjudki, bular yordamida autentifikatsiyani amalga oshirish mumkin. Lekin, mavjud strategiyalarda har bir ma`lumot bitini ishlash uchun shifrlashdan foydalaniladi. Aks holda ma`lumotlar oqimining himoya qilinmagan qismi shubhali holda qolishi mumkin.

Tarmoqqa kirishda va foydalanuvchi nomini kiritishda identifikatsiya, parol kiritishda autentifikatsiya amalga oshiriladi. Agarda foydalanuvchi ushbu parol va nom bilan sistemada qayd qilingan bo’lsa, unga aniq ob`ekt va resurslardan foydalanishga ruxsat etiladi. Biroq sistemaga kirishda, bu funktsiyalarning bajarilish jarayonida ba`zi farqlar mavjud. Bu farqlar ish jarayonida sistema kim ishlayotgani, uning qanday huquqlari borligi va hokazolar haqida informatsiyaga ega ekanligiga asoslanadi va shuning uchun mos holda sub`ekt savollariga javob qaytaradi. Sistemaga kirishda bularning hammasini oldindan aniqlash kerak bo’ladi. Ushbu holatda asllikni ta`minlash maqsadida foydalanuvchidan xavfsizlik yadrosi tomon borishda identifikatsiyalovchi informatsiyaning uzatilish yo’li - “ishonchli marshrut”ni tashkil etish zaruriyati tug’iladi. Amaliyot shuni ko’rsatadiki, foydalanuvchining sistemaga kirishi - himoyaning anchagina nozik joylaridan biridir: ko’pchilik hollarda parollarni sindirish, parolsiz kirish, parollarni tutib qolish va hokazo holatlar ro’y beradi. Shuning uchun foydalanuvchi ham, sistema ham o’zaro bevosita ishlayotgani, ular orasida boshqa programma yoki uzatiluvchi informatsiyalar yo’qligi haqida ishonch hosil qilishi kerak.

Foydalanuvchi identifikatorlari va ularning parollari har bir foydalanuvchi uchun yagona bo’lishi kerak.

Parollar 6 ta simvoldan kam bo'lmasligi va mashhur nomlar yoki iboralardan tuzilmasligi lozim. O'ylab topiladigan parollarning paydo bo'lishini doimiy ravishda maxsus programmalar yordamida tekshirib turish zarur. Bunday programmalarda o'ylab topiladigan parollar generatsiyasi bo'yicha qoidalar to'plami bo'lishi lozim.

Parollar maxfiy holda saqlanishi, ya`ni boshqa odamlarga aytilmasligi, programma matnida va har xil qog'ozlarda yozilmasligi hamda har 90 kunda almashtirilishi lozim. Ko'pchilik sistemalar ma`lum vaqt o'tgach parolni majburiy almashtirishi va avval foydalanilayotgan parolni yo'qqa chiqarishi mumkin.

Foydalanuvchilar byudjeti sistemaga kirishda 3 ta muvaffaqiyatsiz urinishdan so'ng "qotib qolishi" hamda noto'g'ri kiritilgan parollar nomi sistema jurnaliga kiritib qo'yilishi kerak.

Foydalanuvchi va server orasida bo'ladigan ish seansi 15 minut davomidagi faoliyatsizlikdan so'ng blokirovka qilinishi lozim. Seans ishini qayta tiklash uchun yana parol kiritish talab qilinishi kerak.

Sistemaga muvaffaqiyatli kirilganda, undan oxirgi marta foydalanilgan sana va vaqt aks ettirilishi lozim.

Foydalanuvchilar byudjeti ma`lum vaqt foydalanilmagandan so'ng blokirovka qilinishi shart.

Yuqori tavakkalli sistemalar uchun: bir qancha beruxsat kirish uchun urinib ko'rishlardan so'ng sistema ogohlantirish signalini berishi va bu urinishlarni amalga oshirayotgan foydalanuvchi uchun serverning yolg'on xabarlarini berishi lozim.

Chunki u sistemaga qo'shilgan holda turgan vaqtda xavfsizlik administratori uning joylashgan o'rnini aniqlashga harakat qiladi.

LHTni alohida resurslaridan foydalanishning chegaralanishi

Tarmoq ob`ektining tarmoq resurslaridan foydalanishda huquqlarini tekshirish amalga oshiriladi. Nazorat:

-operativ xotiradan;

-taqsimlanuvchi to'g'ridan-to'g'ri kirishli qurilmalardan;

-taqsimlanuvchi ketma-ket kirishli qurilmalardan;

-taqsimlanuvchi programma va qism programmalardan;

-taqsimlanuvchi ma`lumotlar to'plamidan foydalanishda amalga oshirilishi kerak.

Foydalanishni nazorat qilish vositalarining asosiy ob`ekti foydalaniladigan ma`lumotlar to'plami va sistema resurslaridir. Ma`lumotlar to'plamiga ma`lumot fayllari, programma fayllari va hokazolar kiradi. Sistema resurslariga esa har xil

qurilmalar, masalan, disklar, printerlar, komp yuterning operativ xotirasi va boshqalar kiradi.

3. Ma`lumotlarni kriptografik usulda himoya qilish

Ob`ektlar orasida uzatiladigan maxfiy ma`lumotlarni kriptografik o'zgartirishlar yordamida (ma`lumotlarni shifrlar orqali o'zgartirish) himoya qilish - ma`lumotlarning mazmunini yashirish maqsadida shifrlash muammosini yechishning imkoniyatlaridan biridir. Foydalanuvchi kalitni bilmasa uning uchun ma`lumotdan foydalanishning imkoniyati bo'lmaydi. Shifrlangan ma`lumotlardan faqatgina kalitni bilganlargina foydalanishi mumkin va shuning uchun shifrlangan ma`lumotlarni ushlab qolish beruxsat foydalanuvchilar uchun hech qanday ma`noga ega emas.

4. LHT himoyasining apparat usullari

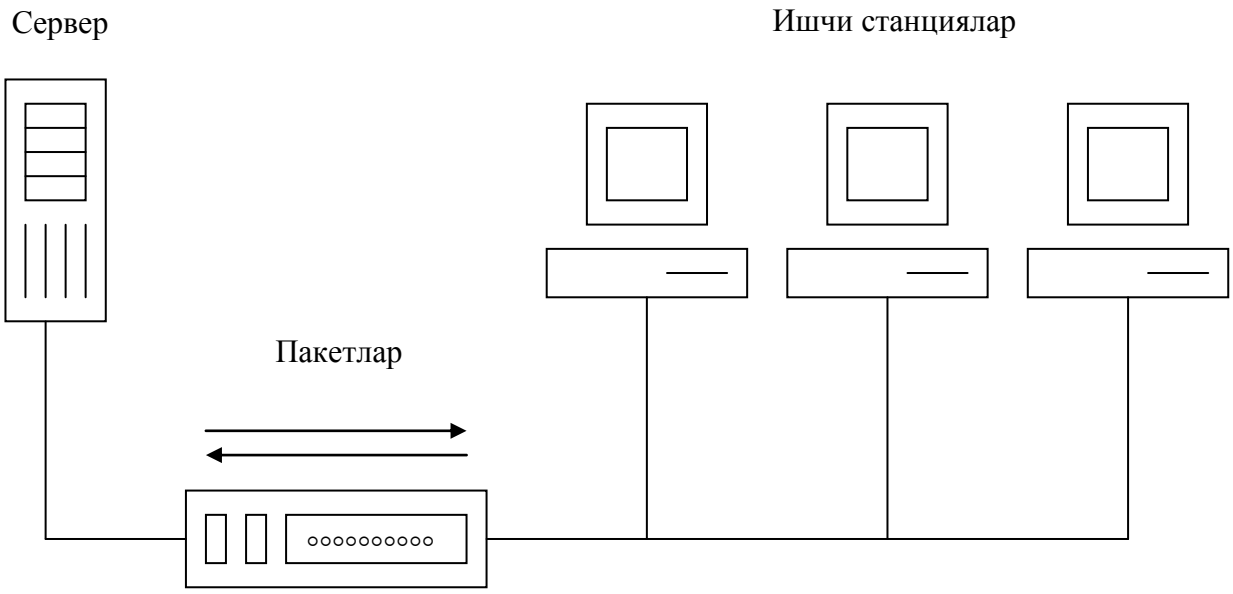
Apparat vositalar tarmoqqa yashirin ulanish, uzatishning fizik muhitiga (kabellar, optik tolali liniyalarga) ulanish, ishchi stantsiya va serverlar orasida uzatiladigan protokollarning ushlab qolinishi, xabarlarning tutib qolinishi va hokazolardan himoya qilish imkonini beradi.

LHTning texnik vositalari tarkibiga kiruvchi har xil elektron va elektron-mexanik qurilmalar himoyaning apparat vositalari deb yuritiladi hamda mustaqil holda yoki boshqa vositalar bilan birgalikda ba`zi himoya funktsiyalarini bajaradi. Hozirgi vaqtda LHTning hamma qurilmalariga ulanishi mumkin bo'lgan ko'p sonli apparat vositalar qo'llanilmoqda.

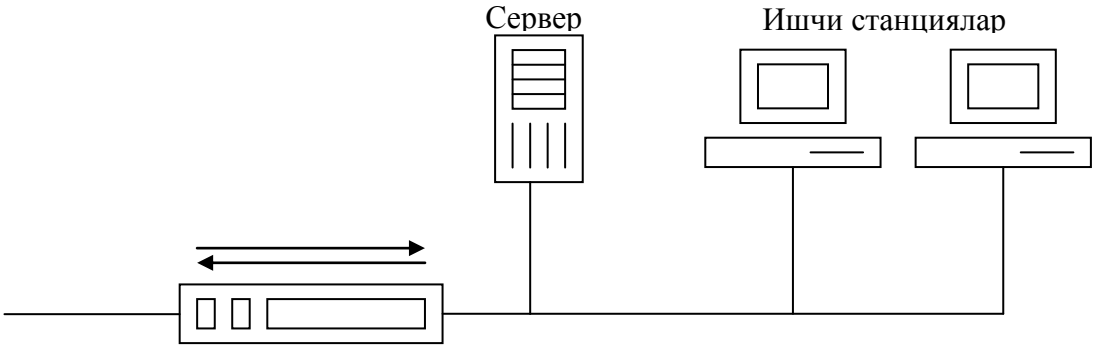
Informatsiyani himoya qilishning apparat vositalariga quyidagilar kiradi:

1. Tarmoq ekranlari.
2. Tarmoqlararo ekran fil trlari.
3. Protokollarni kriptlash (shifrlash) qurilmalari va h.

1. Tarmo*q *ekrani asosan korporativ tarmoqlar (lokal tarmoqlar)da qo'llaniladi. Bu qurilmaning himoyasi asosida protokollarni, serverlarni va ishchi stantsiyalarning yagona tarmoq adreslarini fil trlash printsipi yotadi. Fil trlash printsipi o'zida nimani ifodalashini qisqacha quyidagi misolda ko'rib o'tamiz. Faraz qilaylik, bitta fayl-server va bitta ishchi stantsiyadan iborat lokal tarmoq mavjud. Tarmoq ekrani server va ishchi stantsiya orasiga ulanadi. Deylik, fayl-serverning yagona adresi 00000111, ishchi stantsiyanikini esa 00000222. Tarmoq ekranining xotirasiga yagona adreslar albatta, shifrlangan ko'rinishda kiritiladi. Bu parametrdan tashqari u yerga stantsiyalar orasidagi almashinadigan protokol tipini, bu mashinalarning ish vaqti oralig'ini va boshqa ko'pgina parametrlarni shifrlangan ko'rinishda kiritish mumkin. Server va ishchi stantsiyaning informatsiya almashinuvi vaqtida tarmoq ekrani uzatilayotgan protokol paketidan yuqorida sanab o'tilgan



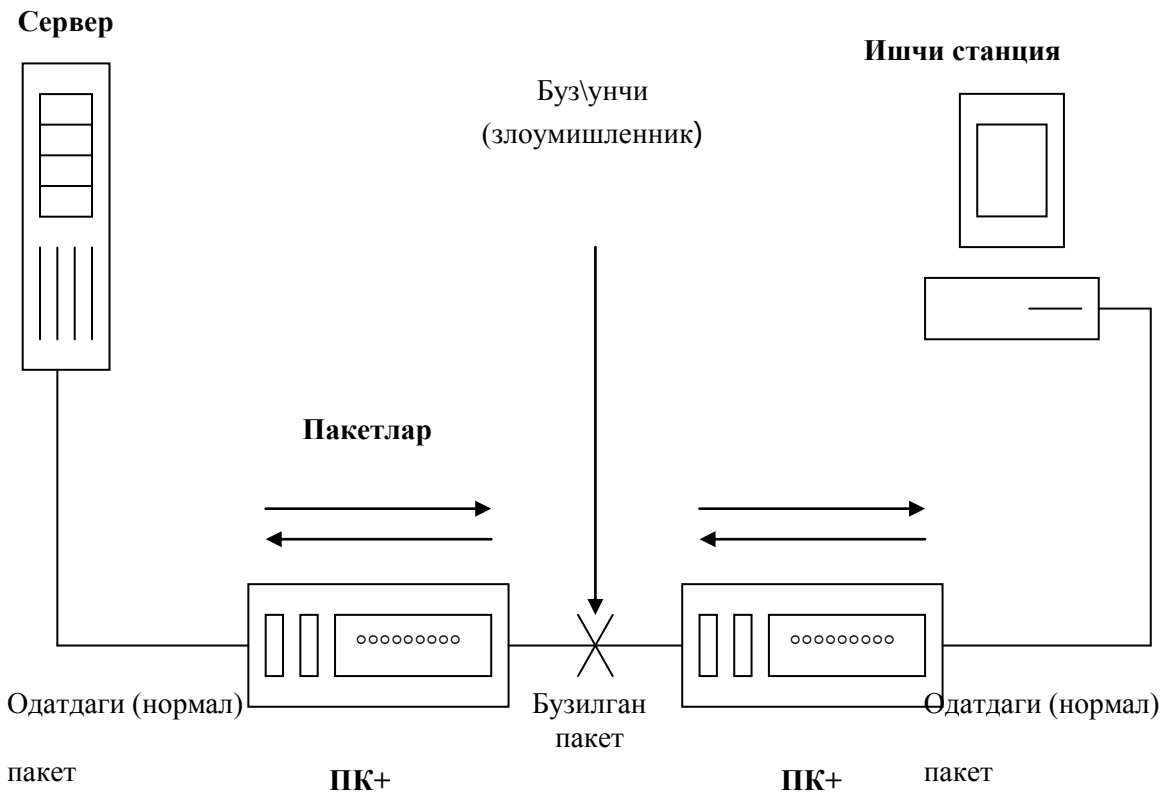
parametrlarni olib, o’z xotirasida saqlanayotgan parametrlar bilan taqqoslaydi. Parametrlar mos kelgan holda tarmoq ekrani bu paketni mo’ljallangan punktga uzatadi (2-rasm).



2-rasm. Tarmoq ekranining ulanish sxemasi.

Deylik, bunday himoya sistemasiga 00000333 yagona tarmoq adresidagi ishchi stantsiya bilan buzg’unchi ulandi. Tarmoq ekrani bu adresni o’z xotirasida saqlanayotgan adres bilan taqqoslaydi va farqni aniqlaydi. Keyin bu paket mo’ljallangan punktga uzatilmaydi.

Tarmoqlararo ekran fil trlari. Bular ham tarmoq ekranlariga o’xshash, ammo ulardan farqli ravishda tarmoqlararo ekran fil trlari global tarmoqlarda qo’llaniladi. Masalan, Internet xalqaro tarmog’iga chiqish imkoniga ega bo’lgan hisoblash tarmog’ini Internetdan bo’ladigan hujumlardan himoya qilish uchun tarmoqlararo ekran fil trlari ikki tarmoq tutashgan joyga ulanadi (3-rasm).



3-rasm. Tarmoqlararo ekranning ulanish sxemasi.

3. Protokollarni kriptlash (shifrlash) qurilmasi (PKq). Bunday qurilmalardagi himoya printsipi stantsiyalar orasida uzatilayotgan paketlarni shifrlash yo'li bilan o'zgartirishga asoslangan. Bu qurilmalar server va stantsiyalar orasiga ketma-ket ulanadi. Ularda shifrlash va deshifrlash kalitlarini kiritish uchun maxsus pul t mavjud.

PKq to'g'ridan-to'g'ri fayl-serverning chiqish yo'liga ulanadi. Deylik, fayl-server eshiklari qulflangan alohida binoda joylashgan. Fayl-serverdan chiqadigan kabel bo'yicha "tanib bo'lmas darajada buzilgan" paketlar uzatiladi. Buzg'unchi bu buzilgan tekstni ilg'ay oladigan tarmoq adapteri (Network adapter)ni topa olmaydi. Matnni o'qish uchun birgina imkoniyat – paketlarni kriptlash qurilmasiga ega bo'lish va davriy ravishda o'zgarib turadigan deshifrlash kalitini bilish lozim.

Katta tezkorlikka ega magistral liniyalarini shifrlashda informatsiya oqimi bo'yicha (potoklab) shifrlash sistemasidan foydalaniladi. SEC-17 qurilmasi 256 KbitG's dan 2304 KbitG's gacha bo'lgan shifrlash tezligini ta`minlaydi, uning kaliti 72 ta o'n oltilik raqamlardan tashkil topgan; SEC-15 qurilmasi 1034 tadan ortiq statik aloqador bo'lmagan kalitlarga ega bo'lish imkoniyatini beradi. Potoklab shifrlash printsiplari MSDS MARCRYP shifrlash apparatura qurilmalarida foydalaniladi. CSD 807 potoklab shifrlash qurilmasining kalit

ketma-ketligi generatorida 31-razryadli siljituvchi registr, SDE 100 qurilmasi generatorida esa ikkita siljituvchi registr qo'llaniladi.

Standart shifrlash apparaturalariga DES algoritmiga asoslangan Cidex-HX qurilmasini kiritish mumkin. Shifrlash tezligi 56 KbitG's dan 7 MbitG'c gacha. DES 1000 avtonom shifrlash bloki ham ko'p sonda ishlab chiqarilmoqda, unda ham DES shifrlash protsedurasidan foydalaniladi, shifrlash tezligi - 38,4 Kbit-s dan 710 Kbit-s gacha. Savdo-sotiq bilan faoliyat ko'rsatuvchi har xil sektorlarda shifrlash-deshifrlash protsessori FACOM 2151A ishlatiladi. U ham DES algoritmiga asoslangan bo'lib, tezligi 2,4 Kbit-c dan 19,2 Kbit-s gacha.

Mustahkamlash uchun savollar:

1. Protokollarni kriptlash (shifrlash) qurilmasini izohlang.
2. Tarmoqlararo ekran fil trlari qanday tarmoqda qo'llaniladi ?
3. LHT himoyasining apparat usullarini tushuntirib bering.
4. Ma`lumotlarni kriptografik usulda himoya qilish printsiplarini tushuntiring.
5. tarmoq resurslaridan foydalanish huquqlariga nimalar kiradi ?

Mustahkamlash uchun savollar:

1. Guvohlik berish mexanizmlari nimani anglatadi ?
2. xavfsizlikni tekshirish deganda nima tushuniladi ?
3. Marshrutni boshqarish mexanizmlari
4. Virusning qanday asosiy xususiyati xarakterlanadi ?
5. Serverlarni antivirus ximoyalash tushunchasini izohlang.
6. Uzatilayotgan ma`lumotlarning butunligini ta`minlash mexanizmlari deganda nima tushuniladi?
7. Uz-uzini ximoyalash retseptlariga nimalar kiradi ?
8. Komp yuter viruslari ishlash sohasiga qarab qanday turlarga bo'linadi ?

Mustahkamlash uchun savollar:

1. O'zgarmas autentifikatsiya nimani anglatadi ?
2. Autentifikatsiyaning uchta asosiy ko'rinishi deganda nima tushuniladi ?
3. Marshrutni boshqarish mexanizmlari tushunchasini izohlang.
4. Informatsiyani himoyalashning asosiy usullariga nimalar kiradi ?
5. Serverlarni antivirus ximoyalash tushunchasini izohlang.
6. Uzatilayotgan ma`lumotlarning butunligini ta`minlash mexanizmlari
7. An`anaviy parollar barqaror autentifikatsiyani ta`minlay oladimi ?

Foydalanilgan adabiyotlar:

- Panasenko S. «Zahita elektronno'x dokumentov» , Moskva, FiS, 2000 g.

➢ Vasina ye. N., Golitsina O «Informatsionno'e resurso' i bazo' danno'x», Moskva, RGGU, 1998 g.
➢ Popov I.I. «Avtomatizirovanno'e informatsionno'e sistemo'» , Moskva, RGGU, 1998 g.
➢ Mitchell Sh. «Tol kovo'y slovar komp yuterno'x texnologii», Moskva,2000g

Foydalanilgan saytlar ro'yxati

- www.securityfocus.com-portal: materialo' po bezopasnosti
- www.sans.org-Institut SANS: stat i po bezopasnosti, proekto'
- www.xforce.iss.net-baza danno'x uyazvimostey, materialo' po bezopasnosti
- www.packetfactory.net-sayt razrabotchikov biblioteke

6-Ma`ruza

Axborot xavfsizligining dastur vositalari. Ma`lumotni Himoya kiluvchi dastur vositalari guruhi.

O'quv modullari

1. Informatsiyani himoya qiluvchi programma vositalari.
2. Tarmoq bo'ylab uzatiladigan xavfsizlik modeli
3. Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati

Aniqlashtirilgan o'quv maqsadlari.Talaba bu mavzuni to'la o'zlashtirgandan so'ng:

❖ Programma vositalari haqidagi tamoyillarni biladi;
❖ Informatsiyani himoya qiluvchi programma vositalari asosiy printsiplarini bo'laklarga bo'lib, ta`rif bera oladi;
❖ Tarmoq bo'ylab uzatiladigan xavfsizlik modelidan foydalanish xususiyatlarinini talqin eta oladi;
❖ Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati qaysi sinfga mansubligini tasavvur eta oladi;
❖ Ma`lumotlar to'plami va sistema resurslari ko'rinishi o'rtasidagi o'zaro aloqadorlikni aniqlaydi, bog'lanishlarni tahlil qila oladi.

Tayanch so'z va iboralar:

xavfsizlik xizmati**,** Informatsiyani himoyalash, LHT, Tarmoq**,** Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati**,** Informatsiyani himoya qiluvchi programma vositalari**,** serverlar diski (tomi),, ishchi stantsiya, qism programmalar **.**

Informatsiyani himoya qiluvchi hamma programma vositalarini ikkita asosiy guruhga bo’lish mumkin:
-informatsiyani himoya qilishning namunaviy (tipovoy) vositalari;
-informatsiyani himoya qilishning maxsus vositalari.
Namunali vositalarga “o’rnatilgan himoya vositalari” taalluqli. Ular tarmoq operatsion sistemalarida ifodalangan.
Maxsus vositalarga quyidagilar kiradi:
-tarmoq monitoringi vositalari;
-kriptografik sistemalar.

1.Informatsiyani himoya qiluvchi programma vositalari.

Programma vositalari yordamida parollar bilan himoya qilish usuli foydalanuvchi va ShEHM orasida shunday muloqot asosida tuzilganki, bunday ShEHM operatsion sistemasidan toki to’g’ri parol kiritilmaguncha foydalanish ta`qiqlanadi. Parol foydalanuvchi tomonidan maxfiy holda saqlanadi va beruxsat foydalanishning oldini olish uchun davriy ravishda almashtirib turiladi.

Parollardan foydalanish usuli eng oddiy va arzon, biroq ishonchli himoyani ta`minlay olmaydi. Xuddi shu EHM yordamida sinab ko’rish va xatoliklar usulidan foydalanib, qisqa vaqtda amaldagi parolni ochish hamda ma`lumotlardan foydalanish imkoniga ega bo’lish mumkin. Parollardan foydalanish usulining nozik tomoni shundaki, foydalanuvchilar odatda juda sodda va eslab qolishga (shu bilan birga o’ylab topishga) qulay parollarni tanlashadi. Ular juda uzoq vaqt davomida almashtirilmaydi, gohida esa foydalanuvchilar almashgan vaqtda ham oldingi kabi qoladi. Ushbu kamchiliklarga qaramasdan, sistema boshqa apparat va programm himoya usullari yordamida himoyalangan bo’lsa-da, ko’pchilik hollarda parollardan foydalanish maqsadga muvofiq hisoblanadi.

Odatda, programma parollaridan foydalanish usuli foydalanish ob`ekti va turi bo’yicha cheklashlarni amalga oshiruvchi boshqa programma usullari bilan birga olib boriladi. Mantiqan o’xshash sistemalarni foydalanishni boshqaruvchi matritsalar ko’rinishida ifodalash mumkin. Ular har xil foydalanuvchilar va ma`lumotlar uchun mo’ljallangan foydalanish turlarini aniqlaydi. Bu matritsa kam sonli real elementlardan tashkil topgan bo’lib, himoyaning umumiy tamoyili har xil himoya qilingan alohida ma`lumotlar yoki ma`lumotlar bloki bilan bog’langan foydalanishni boshqarish ro’yxatlari ko’rinishida amalga oshiriladi.

Har bir shunday ro’yxat hamma ma`lumot ob`ektlari va ushbu ob`ektlardan foydalanish huquqini olgan foydalanuvchilar guruhining nomini o’z ichiga oladi. Bu jarayonning to’g’ri tashkil etilishini kuzatish operatsion sistema tomonidan bajariladi. Shu bilan birga, boshqarish maqsadida bunday ro’yxat foydalanishga

ruxsat berilgan barcha operatsiyalar: programmani o’qish, yozish va bajarishlarni o’z ichiga oladi.

Har bir ro’yxatga olingan foydalanuvchi uchun operatsion sistema u haqidagi qisqacha ma`lumotlar: foydalanuvchi parolini (albatta shifrlangan), foydalanuvchilar guruhining identifikatori va foydalanuvchining ma`lumotlarga nisbatan huquqini o’zida saqlaydi. Masalan, Unix operatsion sistemasi fayl egasiga o’zining har bir faylidan boshqa foydalanuvchilarning faqat o’qish va yozish (o’zgartirish) huquqini beradigan imkoniyat tug’diradi. Agar fayl bajarilishi lozim bo’lgan programma bo’lsa, Unix operatsion sistemasi fayl egasiga ushbu programmani bajarishga ruxsat etiladigan foydalanuvchini aniqlash imkoniyatini yaratadi.

2.Tarmoq bo’ylab uzatiladigan xavfsizlik modeli

Operatsion muhit sathida ma`lumotlarni programmali himoya qilish Hozirgi vaqtda mikroprotsessorlarda ham o’z apparat ta`minotiga ega bo’ldi. Kristallarda tashkil etilgan bunday apparat vositalarga misol tariqasida Intel firmasining 16-razryadli 80286 va undan keyin chiqarilgan mikroprotsessorlarini keltirish mumkin. Unda ko’zda tutilgan har xil imkoniyatlar, masalan, ob`ektlarni aniqlash va manipulyatsiya imkoniyatlari, shu bilan birga, xotirani boshqarishning apparat vositalar tomonidan to’g’ridan-to’g’ri ta`minlanishi ma`lumotlarni himoya qilishning ishonchli yadrosini shakllantirish imkonini beradi. 80286 mikroprotsessori ma`lumotlar himoyasini har xil sathlarda amalga oshiradi. Har bir masalaga ajratilgan alohida virtual adreslar makoni muloqotning ko’zda tutilgan sohasida joylashgan segmentlardan foydalanish imkonini beradi. Hatto qo’yilgan masala o’zining adreslari oralig’ida ham, markaziy protsessor tomonidan belgilangan kirish (o’qish va yozish uchun) turlari bo’yicha qat`iy segmentlarga bo’lishdan chetga chiqmasligi kerak.

Xotira segmentiga har bir murojaatda ruxsat etilganligini aniq tekshirish ham ko’zda tutiladi. Intel firmasining oldin ishlab chiqargan boshqa mikroprotsessor modellaridan farqli o’laroq, 80286 himoyaning 4 sathiga ega: bu aniq talablarga bog’liq holda har xil detalizatsiya darajasiga ega amaliy va sistema programmalarining himoyasini ta`minlash imkonini beradi.

Shunga qaramay, informatsiyani LHTda samaraliroq himoya qilish uchun tarmoq operatsion sistemasi tomonidan taqdim etiladigan vositalar, ya`ni foydalanishni cheklash vositalari yetishmaydi. Shuning uchun informatsiyani himoya qilishning qo’shimcha apparat va programm vositalariga ehtiyoj seziladi. Himoyaning programma vositalariga ma`lumotlarni shifrlash programmalarini kiritish mumkin. Hozirgi paytda ushbu maqsad uchun yo’naltirilgan talaygina

tayyor programmalar mavjud. Bularga bizning mamlakatda va chet ellarda keng tarqalgan “SagOsf”, “Vesta”, “ORTIS” va boshqa programma mahsulotlarini kiritish mumkin. Lekin bu vositalarning foydali tomonlarini sharhlash shart emas. Birinchidan, shifrlash va deshifrlash algoritmi bu programmalarni ishlab chiqqanlar uchun ma`lum, demak bitta chetga chiqish kanali mavjud. Ikkinchidan, har qanday ma`lumotni shifrlash va deshifrlash operatsiyasi uchun ma`lum vaqt talab qilinadi. Bu katta hajmli ma`lumotlar va ko’p sonli foydalanuvchilarga ega tarmoqlar bilan ishlayotganda ancha sezilarli bo’ladi.

Bu dalillarga asosan quyidagi xulosaga kelish mumkin: yuqori darajada ma`lumotlarni kriptografik himoya qilishning programma usulida amalga oshirilishi hisoblash tarmoqlarining foydalanuvchilari oldiga jiddiy muammoni qo’yadi. Agarda faqatgina programmali kriptografik vositalar ko’zda tutilsa, u holda yoki protsessor unumdorligini oshirish kerak, yoki ko’p sonli protsessorlarni birlashtirgan holda parallel hisoblash larni qo’llash kerak.

Bundan tashqari, bu usuldagi himoyada yana bir e`tiborga molik xavf mavjud bo’lib, ma`lumotlar tarmog’i bo’ylab uzatiladigan xavfsizlik modeli (end-to end security model) uchun kriptografik ta`minotning (kalitlar va b.) uzluksiz himoyada bo’lishi talab qilinadi. Bu talab har qanday muddat: informatsiyaning sekundlardagi yoki o’nlab yillar davomidagi himoyasi uchun taalluqlidir. Masalan, kredit kartochka nomeri yoki abonent-sotib oluvchining PIN-KODi sotuvchiga hech qachon oshkor etilmasligi kerak. Programmali kriptografik himoya usulidan foydalanganda bu informatsiya odatdagi universal komp yuter yordamida hisoblanadi va qayta ishlanadi. Natijada amaliy jihatdan himoyalanmagan holda beriladi. Bunday holdan apparat vositalarni qo’llash bilan chiqish mumkin.

LHTda informatsiyani himoya qilish uchun faqatgina programma vositalarini emas, balki apparat vositalarni ham qo’llash kerak ekan. qo’shimcha ravishda informatsiyani himoya qiladigan hamma apparat vositalari real vaqt masshtabida ishlashini hisobga olish lozim.

Ko’pgina tashkilotlar ma`lumotlarni ishlash va uzatish uchun LHT va uning vositalaridan foydalanadilar. Ma`lumki, signallarni uzatishda sim yoki antenna sifatida har qanday o’tkazish liniyasi (simli liniya)dan foydalanish mumkin. Shuning uchun uzatuvchi qurilmaga ulanish uchun va shu bilan birga, informatsiyaning chetga chiqib ketishi uchun qulay imkoniyatlar bor. Shuni qo’rqmasdan ta`kidlash mumkinki, kimga aloqa kanalidan foydalanish mumkin bo’lsa, u sistemani boshqaradi. LHT foydalanuvchilari o’zlarining ma`lumotlari tarmoqda munosib himoyalanganligiga ishonch hosil qilishlari lozim.

Komp yuter informatsiyalarini ruxsatsiz foydalanishdan himoya qilish dolzarb masalalardan biri bo’lib qolmoqda. LHTning himoyasi butun lokal

tarmoqni o’z ichiga olishi kerak. Bu uning foydalanuvchilari uchun juda muhimdir. Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati, shu bilan birga ularni ishlash va uzatish vositalari butun LHT bo’ylab tarqatilgan bo’lishi lozim. Masalan, LHTdagi bitta komp yuterda ma`lumotlardan foydalanishni boshqarish sistemasi mavjud, boshqa birida esa mavjud emas. Ushbu holda birinchi komp yuterda kuchli himoya qilingan faylni ikkinchi komp yuterga uzatish hech qanday ma`noga ega bo’lmaydi. LHT xavfsizligi muammosini yechishda apparat vositalar yordamida shifrlash alohida ahamiyatga ega.

3.Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati

Operatsion sistemani himoya qilish sistemalari

Komp yuter sistemalari himoyasini ta`minlashning asosiy usuli operatsion sistemaning vosita va usullaridan foydalanishdir, qo’shimcha vositalardan farqli ravishda operatsion sistema sathida himoya sistemasini tashkil etish yetarli darajadagi ishonchlilikni kafolatlaydi va bunday himoya “o’rnatilgan” deb yuritiladi.

NetWare LHTda ma`lumotlarni himoya qilish sistemasi quyidagi tadbirlarni o’z ichiga oladi:

-foydalanuvchining paroli va nomini o’zlashtirish yo’li bilan LHTga beruxsat ulanishdan himoya hamda kunning aniq vaqtida aniq nom bilan foydalanuvchining LHTdan foydalanishining cheklanishi;

-ishonchli huquqlar sistema (sistema doveryaemo’x prav) (trustee rights). U foydalanuvchi qaysi fayl yoki kataloglardan foydalanishi hamda ular bilan qanday amallar o’tkazishni tekshirish (nazorat qilish) imkonini beradi;

-fayl va kataloglar uchun atributlar sistemasi. U fayl va kataloglarning LHTda taqsimlanishi, yozilishi, ko’rilishi va nusxa olinishi imkoniyatini aniqlaydi.

Har qanday ko’p foydalanuvchili sistema birgalikda foydalaniladigan resurslardan foydalanishni cheklash vositalari bilan ta`minlanishi kerak. Novell NetWare tarmoqlarida bunday resurslar fayl-serverdagi ma`lumotlar va tarmoq printerlari hisoblanadilar.

NetWare 386da amalga oshirilgan foydalanishni cheklash sistemasi yetarli darajada kuchli va qulaydir. Hamma foydalanuvchilar sistema administratori tomonidan guruhlarga bo’linadi. Har bir guruh o’z huquqiga ega bo’lishi mumkin, shu bilan birga birgina foydalanuvchi bir vaqtda har xil guruhlarda joylashishi mumkin.

Novell NetWare da guruhlarni boshqarish uchun guruhlar administratori tushunchasi kiritiladi. Guruhlar administratori tarmoqda sistema administratori tomonidan qo’yiladigan hamma huquqlarga ega bo’lmasligi ham mumkin.

NetWare 386 operatsion sistemasida kataloglar va fayllardan bir xilda foydalanish mumkin. Shu bilan birga, bu foydalanish to'la yoki qisman bo'lishi mumkin. Masalan, ma`murfayllarga yozish emas, balki undan o'qishga ruxsat berishi mumkin. Foydalanuvchi agarda unda mos katalog tarkibini ko'rish huquqiga ega bo'lmasa, diskdagi katalog va fayllarni ko'ra olmaydi.

Har bir katalogdan foydalanuvchida maksimal huquqlar niqobi mavjud bo'lib, u maksimal imtiyozlarni o'z ichiga oladi. Foydalanuvchining esa bu imtiyozlarga ega bo'lish imkoni mavjud. quyida bu niqobdagi sakkizta huquq keltirilgan:

-ochiq fayllarni o'qish huquqi;
-ochiq fayllarga yozish huquqi;
-fayllarni ochish huquqi;
-yangi fayllarni yaratish huquqi;
-fayllarni yo'qotish huquqi;
-ichki kataloglarni yaratish, qayta nomlash va o'chirish huquqi hamda kataloglar ichidagi qism kataloglarga va uning ichki kataloglariga ishonchli huquq o'rnatish;
-fayl va kataloglar qidiruvini amalga oshirish huquqi;
-fayl xususiyat (atribut) larini o'zgartirish qilish huquqi.

LAN Manager, Windows NT va LAN Server tarmoq OSlari NetWare OSiga nisbatan kam foydalaniladi, ular klientG'server programm texnologiyasining boshlang'ich keng rivojlanishi uchun ko'proq mos keladi. Ko'pchilik mutaxassislar hisoblashadiki, kelajakda NetWare OSsi o'z peshqadamlik holatini yo'qotishi, uning o'rnini esa yuqoridagi OSlar egallashi mumkin. Lekin hozircha NetWare OS si eng ko'p tarqalgan va mashhur sistema bo'lib qolmoqda.

Fayl-server va ishchi stantsiyalar oblastlarda tashkil etilgan. Oblast – bu serverlar va ishchi stantsiyalar guruhi bo'lib, unda ma`lumotlarni himoya qilishga bo'ladigan o'xshash talablar mavjud. LAN Manager va LAN Server boshqaruvidagi katta tarmoqlarda bir necha oblastlarni o'rnatish imkoniyati bor. Oblastlar foydalanuvchilar tarmoq va tarmoq resurslaridan foydalanishni nazorat qilish oddiy usullarni beradi. Foydalanuvchi bir necha oblastlarda ro'yxatdan o'tishi mumkin, lekin tarmoqqa faqat bu oblastlardan biri orqali ulanishi mumkin.

LAN Manager va LAN Server boshqaruvidagi tarmoqlarda foydalanuvchi sathidagi ma`lumotlar himoyasi ruxsat berish sistemasi va tarmoqqa ulanilishdagi nazoratdan iborat.

Har bir ro'yxatdan o'tgan foydalanuvchi o'z paroliga ega. Aniq oblastdagi tarmoqdan foydalanish uchun foydalanuvchi o'z ismini va parolini ko'rsatadi. Tarmoq administratori bir necha foydalanuvchi uchun aniq vaqtda, aniq kunda yoki aniq ishchi stantsiyasidan foydalanishni cheklashi mumkin. Bu cheklashlar

foydalanuvchilar taqsimlangan resurslardan foydalanish huquqlariga chegara o’rnatishi mumkin.
Foydalanuvchi fayl va kataloglarga quyidagi atributlarni berishi (o’rnatishi) mumkin:

-Atributlarni almashtirish	- fayllarni faqat o’qish uchun yoki faqat yozish uchun belgilaydi;
-Yaratish	- fayl va kataloglar yaratadi;
-O’chirish	- fayl va kataloglarni o’chiradi;
-Bajarish	- EXE, BAT yoki COM kengaytmali fayllar bajarilishini ishga tushiradi, bu fayllardan nusxa olish yoki o’qishni amalga oshirmaydi;
-O’qish	- fayllardan nusxa olish va o’qish, programmani ishga tushirish, kataloglarni almashtirish va fayllar uchun OSG’2 sistemasining kengaytirilgan atributlarning qo’llanishi imkonini beradi;
-Yozish	- faylni yozish imkonini beradi.

Ko’rilayotgan LAN Manager va LAN Server tarmoq operatsion sistemalari fayl-serverning klaviaturasi va ekranidan foydalanishni nazorat qilish imkonini beradi. Fayl-server o’zining maxsus ajratilmagan ish rejimida foydalanuvchiga bosmalash navbatini boshqarish va ko’zdan kechirish imkonini beradi. Lekin ro’yxatdan o’tgan foydalanuvchilar taxalluslarini va boshqa ma`muriy ma`lumotlarni o’zgartirishga yo’l qo’ymaydi. Ma`muriy ma`lumotlar bilan ekrandan foydalanish uchun foydalanuvchi maxsus parolni kiritishi zarur.

LAN Manager sistemasining farqli xususiyati tarmoq aloqalarini xotirlab qolishidir. Foydalanuvchilar LHTga navbat bilan ulanishlarida avtomatik tarzda so’nggi seanslardagi aloqaga ega bo’lishadi. Bu xususiyatni G’PERSISTANTq komandalar Ķ NET USE optsiyasi yordamida bekor qilishi yoki ruxsat berishi mumkin.

LAN Manager sistemasida NetWare Connectivity deb nomlanadigan maxsus vosita bo’lib, bir vaqtda LAN Manager boshqaruvi ostidagi fayl-server va NetWare boshqaruvi ostidagi fayl-serverdan bir xilda foydalanish imkonini beradi.

LAN Manager sistemasi masofadan ma`muriy boshqarish vositasiga ega. Agar siz ma`mur imtiyozlariga ega bo’lsangiz, siz foydalanuvchilarni qabul qilishingiz yoki foydalanuvchilar safdan chiqarishingiz mumkin va OSG’2 yoki LAN Manager boshqaruvidagi har qanday ishchi stantsiya bilan boshqa ma`muriy masalalarni bajarishingiz mumkin. Shunday qilib, ma`muriy vazifalarni bajarish uchun albatta fayl - serverda bo’lishga ehtiyoj yo’q.

LAN Manager taqsimlangan resurslar yoki qurilmalardan foydalanishni cheklash uchun parol o’rnatish vositasiga ega. Bu xususiyat LAN Server operatsion sistemasida mavjud emas.

Ikkala sistema ham tarmoqdan foydalanish uchun parollar va oblastlar vositasida ma`lumotlarni himoya qilish kontseptsiyasidan ayrim farqli usullar bilan foydalandilar.

Tarmoq monitoringi vositalari. Tarmoq monitoringi vositalari tarmoq unumdorligini doimiy tahlil qilish uchun mo’ljallangan. Bunday vositalarda asosiy e`tibor tarmoq statistikasini yig’ishga qaratilgan. Aniq xatolarni yoki nosozliklarni aniqlash uchun xizmat qiladigan tashxislash (diagnostik) asboblaridan farqli ravishda tarmoq monitoringi vositalari tarmoq ishi haqida doimiy ma`lumot yig’ish uchun foydalaniladi. Bu tashxislash asboblar yordamida tarmoq statistikasini yig’ib bo’lmaydi, degani emas. Monitoring vositalari esa xato qaerda paydo bo’lganini aniqlash imkonini bermaydi. Bunday qurilmalarning har birida tarmoqning samarali ishini qo’llab-quvvatlash uchun qurilma strukturasida o’z o’rni bor.

Tarmoq monitoringi quyidagi funktsiyalarni ta`minlashi kerak:

-kadrlarning izidan borish - kuzatish chastotasi (tarmoq bo’yicha bir sekundda uzatiladigan kadrlar soni va yuklanish koeffitsientining haqidagi joriy qiymatni chiqarish);

-bu qiymatlarning vaqtga bog’liqlik grafigini chiqarish;

-elektron jadvallar formatida tarmoq ishining statistikasini chiqarish;

-har bir ishchi stantsiya bo’yicha tarmoq statistikasini chiqarish;

-MAS - adreslar va stantsiya nomlarining bog’lanish imkoniyatini amalga oshirish;

-ko’plikdagi va yagona nizolar haqida ma`lumot chiqarish;

-tarmoqda foydalanilayotgan protokolni aniqlash;

-paketlarning ushlab qolinishi va uning natijalari saqlanishini bajarish;

-aniq paketlar tipini tahlil qilish uchun paketlar ushlab qolinishida fil trlashni amalga oshirish;

Shunday qilib, tarmoq monitoringi vositalari tarmoqda bo’ladigan har qanday o’zgarishni rejalashtirish uchun zarur hamma informatsiyani chiqarishi kerak.

Mustahkamlash uchun savollar:

1. Kriptosistema nima?
2. Shifrlash usullari xususitlarini sanang.
3. Kriptografiya fani haqida so’zlab bering.
4. Fayl-server va ishchi stantsiyalarni tushuntiring.

Mustahkamlash uchun savollar:

1. Ma`lumotlar tarmog'i bo'ylab uzatiladigan xavfsizlik modelini izohlang.
2. Informatsiyani himoya qiluvchi programma vositalari qanday guruhlarga bo'linadi
3. o'rnatilgan himoya vositalari **nimani anglatadi ?**
4. Ma`lumotlarni kriptografik usulda himoya qilish printsiplarini tushuntiring.
5. tarmoq resurslaridan foydalanish huquqlariga nimalar kiradi ?

Foydalanilgan adabiyotlar ro'yxati

- S.Petrenko ,M.Mamaev «Texnologii zahito' v Internete» Izdatel skiy dom «Piter» , Sankt-Peterburg, 2002 g.
- Turskiy A. , Panov S «Zahita informatsii pri vzaimodeystvii korporativno'x setey v Internet» , FiS, Moskva, 2003 g.
- Koshelev A.»Zahita setey i firewall» Komp yuterPress, 2000 g.
- Oliver .V.G. «Novo'e texnologii i oborudovanie» ,SPb:BHV-Sankt – Peterburg,2000 g.
- Brassar. J. «Sovremennaya kriptologiya», Moskva, «Polimed», 1999 g.
- Petrov A. «Kriptograficheskie metodo' zahito'» , Moskva,DMK, 2000 g.
- Romanets Yu.V., Timofeev P.A. «Zahita informatsii v sovremenno'x komp yuterno'x sistemax», Moskva, Radio i svyaz , 1999 g.

7-Ma`ruza

Ma`lumotlarni muhofaza qilishning kriptografik usullari
(2-soat)

O’quv modullari

1. Kriptografiya” termini
2. Sifatli shifrlash kriteriyasi (mezoni)
3. Ma`lumot uzatishdagi shifrlash va deshifrlash
4. Shennon modeli bo’yicha ma`lumotlarni shifrlash
5. Informatsiyani autentifikatsiyalash kontseptsiyasi

Aniqlashtirilgan o’quv maqsadlari.Talaba bu mavzuni to’la o’zlashtirgandan so’ng:

- ❖ Kriptografiya haqidagi tamoyillarni biladi;
- ❖ Sifatli shifrlash kriteriyasi asosiy printsiplarini bo’laklarga bo’lib, ta`rif bera oladi;
- ❖ Ma`lumot uzatishdagi shifrlash va deshifrlashda foydalanish xususiyatlarinini talqin eta oladi;
- ❖ Shennon modeli bo’yicha ma`lumotlarni shifrlash qaysi sinfga mansubligini tasavvur eta oladi;
- ❖ Informatsiyani autentifikatsiyalash kontseptsiyasi ko’rinishi o’rtasidagi o’zaro aloqadorlikni aniqlaydi, bog’lanishlarni tahlil qila oladi.

Tayanch so’z va iboralar:
Kriptografiya**,** Ma`lumot uzatishdagi shifrlash, Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati**,** Informatsiyani himoya qiluvchi programma vositalari**,** Informatsiyani autentifikatsiyalash kontseptsiyasi**.**

Kriptografiya haqida

“Kriptografiya” termini dastavval “yozilgan narsani yashirish” ma`nosini anglatgan. Dastlab u yozuv paydo bo’lgan vaqtda tilga olingan (Kanh, 1967). Hozirgi vaqtda kriptografiya deganda har qanday shaklda: diskda saqlanayotgan ma`lumot yoki informatsion tarmoq bo’ylab uzatilayotgan xabarlar shaklidagi informatsiyaning mazmunini yashirish tushuniladi. Shu bilan birga uni programma ta`minotida, grafika yoki nutqda, raqamlar bilan kodlanishi mumkin bo’lgan hamma joyda qo’llash mumkin. Kriptografiya faqatgina maxfiylikni ta`minlashdan boshqa keng qo’llanilish sohasiga ega. Aniqroq qilib aytganda kriptografiyada

foydalaniladigan usullar informatsiya himoyasi bilan aloqador boshqa ko’pgina ilovalarda ham foydalanilishi mumkin.

Kriptografiya beruxsat foydalanishlardan himoya qilish bilan informatsiyaning maxfiyligini ta`minlaydi. To’lov hisoblarini elektron pochta tarmog’i orqali jo’natishda hisob o’zgartirilishi yoki unga qalbaki yozuvlar qo’shilishi mumkin. Bu holda xabarning butunligini (to’laligini) ta`minlash zarur. Amaliyotda hisoblash tarmog’iga yomon maqsadda kirishni mutlaq ishonch bilan oldini olish mumkin emas, lekin bu kirish dalilining (faktining) o’zi to’g’ri aniqlab olinishi (ilg’ab olinishi) mumkin. Xabarning butunligini tekshirishning bu jarayoni xabar haqiqiyligini o’rnatish deb yuritiladi. Kriptograf vo’a iyada foydalaniladigan usullar kam o’zgartirishlar bilan xabar haqiqiyligini o’rnatishga qo’llanilishi mumkin. Shunga o’xshash ma`lumotlar hamda xotirada saqlanuvchi programmalar butunligi ta`minlanishi mumkin.

Xabarning hisoblash tarmog’i orqali buzilishsiz o’tganini bilish bilan birga uning avtor orqali jo’natilganiga ham ishonch hosil qilish lozim. Jiddiy aldash holatlarining ko’pchiligi bir foydalanuvchining o’zini boshqa bir kishi qilib ko’rsatishi bilan aloqador. Xabarni uzatishni amalga oshiruvchi shaxsning haqiqiyligini tasdiqlovchi har xil usullar mavjud. Parollar bilan informatsiya almashishi anchagina universal, lekin bu juda sodda protsedura bo’lib, parolga ruxsati bo’lgan shaxs undan foydalana oladi. Agarda ehtiyotkorlik choralariga rioya qilinsa parollar samaradorligini oshirish mumkin; ularni kriptografik usullar bilan himoya qilish mumkin, lekin kriptografiya parollarni uzluksiz o’zgartirishni talab etadi.

Kriptografiya sohasidagi yutuqlardan biri - raqamli signatura (imzo) - butunlikni maxsus xususiyatlar bilan xabar to’ldirish yordamida ta`minlash usuli. Bu qachonki xabar avtoriga tegishli ochiq kalit ma`lum bo’lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalitlar yordamida butunlikni tekshirish usullariga nisbatan e`tiborli yutuqlarga ega.

Kriptografiyaning qo’llanilish usullaridan bir nechtasini ko’rib o’tamiz. Aloqa tarmog’idan foydalanib o’yin tashkil etishda mumkin bo’lgan aldashdan qutulish uchun informatsiya himoyasini ta`minlash qiziqish tug’diradi. Boshqa misol: bir-biriga ishonmaydigan ikkita sherik o’rtasida shartnoma bo’yicha to’lov. Programma vositalariga kelganda, bu yerda, kriptografik usullar maxfiylikni ta`minlash, butunlikni tekshirish va ma`lumotlar haqiqiyligini o’rnatish uchun foydalaniladi. Uzatiladigan xabar mazmunini yashirish uchun o’zgartirishning ikki tipi: kodlash va shifrlash qo’llaniladi. Kodlash uchun tez-tez foydalaniladigan iboralardan tashkil topgan kodli kitob yoki jadvallar foydalaniladi. Dekodlash uchun ham xuddi shunday kitob yoki jadval talab qilinadi. Kodli kitob yoki jadval ixtiyoriy kriptografik o’zgartirish misolini beradi.

Kodlash informatsion texnologiyasiga mos keluvchi talablar qatorli ma`lumotlarni raqamga va aksincha o’zgartirishdan tashkil topgan. Kodlovchi kitobni tashqi xotira qurilmalarida yuqori foydalanishda amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik sistemasi tashkil etish usulini omadli hisoblab bo’lmaydi. Yana bir kamchiligi shundan iboratki, agar kitobdan qachondir beruxsat foydalanish amalga oshirilsa, u holda yangi kodlar kitobini tashkil etish va uni hamma foydalanuvchilarga tarqatish lozim bo’ladi.

Kriptografik o’zgartirishning ikkinchi tipi shifrlash bo’lib, u o’z ichiga dastlabki matnni foydalanib bo’lmaydigan shaklga (shifrlangan matnga) simvollar orqali o’zgartirish protsedura (algoritmi)ni qamrab olgan. O’zgartirishning bu tipi informatsion texnologiyaga mos keladi. Bu yerda protsedurasi (algoritmi) ni himoya qilish ahamiyatli hisoblanadi. Kriptografik kalitni qo’llagan holda shifrlash protsedurasining himoyasiga bo’lgan talabni kamaytirish mumkin. Ushbu holda himoya faqat kalitgagina tegishli bo’lib qoladi. Agarda kalitdan nusxa olingani sezilsa, uni almashtirish mumkin. Bu esa kodlovchi kitob yoki jadvalni almashtirishdan ko’ra osonroq kechadi. Shuning uchun informatsion texnologiyada kodlashga nisbatan shifrlashdan keng foydalaniladi.

Informatsiyani kriptografik himoya qilish vositalari

Kriptografiya - informatsiyani begonalar tomonidan o’qilishini himoya qilish haqidagi fandir. Himoyaga shifrlash orqali erishiladi, ya`ni bu shunday o’zgartirishki, unda himoya qilingan kirish ma`lumotlarini maxsus informatsiya - kalitni bilmasdan turib ochish mushkul. Kalit deganda kriptosistemaning sir saqlanayotgan oson o’zgartiriluvchi qismi tushuniladi. Kriptosistema - teskari o’zgartirishlar kaliti yordamida tanlanadigan oila bo’lib, u himoya qilinayotgan ochiq matnni shifrogrammaga va yana aksiga o’zgartiradi. Shifrlash usullari kamida quyidagi ikkita xususiyatga ega bo’lgani ma`qul:

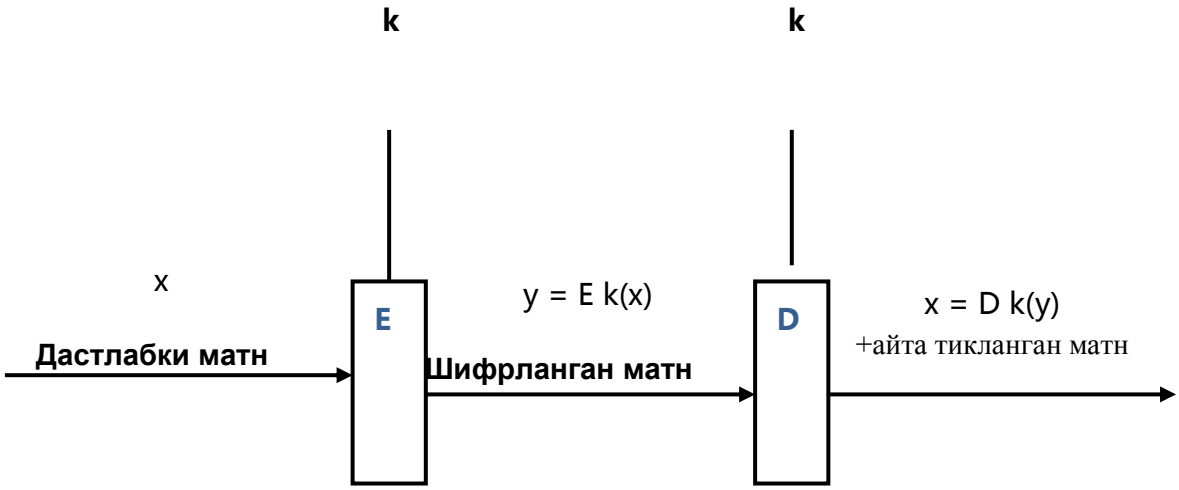
-qonuniy qabul qiluvchi teskari o’zgartirishni bajarishi va xabarni rasshifrovka qila olishi mumkin;

-xabarni ushlab qolishi mumkin bo’lgan raqib - kriptoanalitikka. U dastlabki xabarni ma`lum vositalar va vaqt sarfisiz qayta tiklay olmaydi.

Sifatli shifrlash kriteriyasi (mezoni)

Uzatilayotgan ma`lumotlarning mazmunini yashirishga qaratilgan shifrlash protsedurasi 5-rasmda ko’rsatilgan. Uzatish jarayoni har biri ikkita kirish va bitta chiqishga ega bo’lgan ikkita algoritm - ye (Encipherment) va D (Decipherment)dan foydalanadi. ye shifrlash algoritmida dastlabki matn k kalitdan

foydalanish bilan y shifrlangan matnga o’zgartiriladi. So’ngra D deshifrlash algoritmida y matn k kalit yordamida qayta tiklanadi.



5-rasm. Ma`lumot uzatishdagi shifrlash va deshifrlash sxemasi.

Matnni o’zgartirish uchun ikkita o’zaro teskari funktsiya yagona kalit bilan ishlatiladi: shifrlash uchun – yqEk(x) va deshifrlash uchun – xqDk(y); bu yerda k - E va D funktsiyalarning parametri.

Algoritmni mutlaq yashirishni ta`minlash asosiy maqsad hisoblanmaydi, chunki u ochilgan holatda yangi algoritm ishlab chiqishga to’g’ri keladi. Shunday qilib, shifrning ishonchliligi “algoritm ma`lum” degan ehtimollik bilan baholanadi. Agar kalit ochilgan bo’lsa, algoritm ham ochiq hisoblanadi, chunki protsedura deshifrlangan, D funktsiya ma`lum. Agar k kalit ochilmagan bo’lsa, dastlabki matnni shifrlangan holatdan qayta tiklab bo’lmaydi. Amalda deshifrlovchi (kriptoanalitik) shifrlangan matn tarkibidagiga nisbatan anchagina ko’p informatsiyadan foydalanadi. U shifrlangan matnlarni uzoq vaqt davomida yig’ishi va ularning xususiyatlarini o’rganishi mumkin. Gohida dastlabki matnning alohida qismini tiklashga va ortiqchalik xususiyatlari, formatlar hamda simvolli kodlash usullari haqida informatsiya olishga muvaffaq bo’linadi. Amaliy kriptografiyada, dastlabki matnda ortiqchalik mavjud, degan ehtimollik ishlatiladi. Kriptografiya va kriptoanaliz asosida “kodlangan matn matndan tabiiy tilda olingan” degan ehtimollik yotadi. Komp yuter matnlari ko’proq ortiqchalikka ega, chunki harf va sonlar 8-bitli baytlar bilan ifodalangan ASCII kodi simvollaridan tashkil topgan. Har bir baytda odatda, bitta, uzun matnlarda esa ikki yoki uchta ortiqcha bit paydo bo’lishi mumkin.

Ko’pchilik analiz usullarida dastlabki matnni ma`lum va kriptoanalitik dastlabki unga mos shifrlangan matnning uzun ketma-ketliklaridan foydalanishi mumkin, deb taxmin qilinadi. Agar faqat matnlar qismidan foydalanilsa, vaziyat og’irlashadi, lekin amalda bunday yondashuvning muvaffaqiyatli qo’llanishiga misollar ham uchraydi.

Shennon modeli bo’yicha ma`lumotlarni shifrlash

1949 yilda K.Shennon o’zining "Maxfiy aloqa sistemalari nazariyasi" nomli ma`ruzasida kriptografik sistemaning modelini taklif etdi

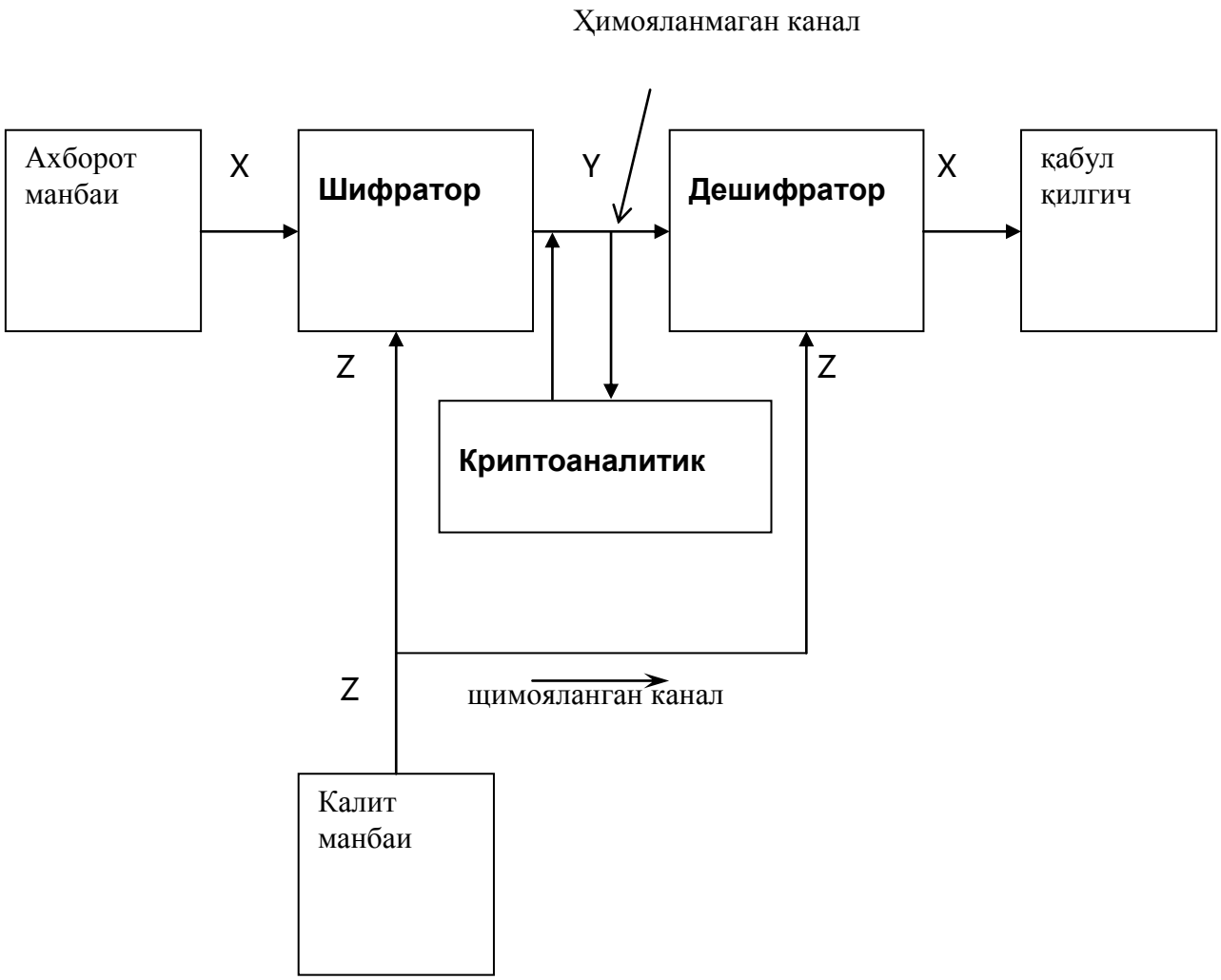
Axborot manbaida ochiq matn $Xq\{x_1, x_2, ..., x_m\}$ shakllantiriladi. Kalitlar manbaida esa kalitning K ta belgisi - ma`lum sondagi chekli alfavitdagi belgilar hosil qilinadi. Shifrator ochiq matn X ni shifrmatn $Yq\{y_1, y_2, ..., y_n\}$ ga o’zgartiradi. Eng so’nggi o’zgartirishni quyidagicha yozish mumkin: $YqE_z(x)$

(1)

Deshifrator esa shifrmatnni qabul qilib, asl holiga tiklaydi:

$$XqD_z(y) \qquad (2)$$

Bu kriptografik sistemada maxfiy kalit $Zq\{z_1, z_2, ..., z_k\}$ uzatilayotgan himoyalangan kanal eng muhim qism bo’lib xizmat qiladi.



6- rasm. Shennon modelining sxemasi.

Kalit shifratorda ham, deshifratorda ham bir qiymatli o’zgartirishlar (1), (2) ni bajarish uchun foydalaniladi. Shuni qayd etish lozimki, X, Y, Z - bir-biriga bog’liq bo’lmagan tasodifiy miqdorlardir. X miqdorning statistik xususiyatlari axborot manbaida aniqlanadi, Y va Z esa kriptografik sistemani ishlab chiquvchining nazorati ostida bo’ladi. Raqib-kriptoanalitikning vazifasi esa, shifrmatnni tahlil qilish natijasida ochiq matn va kalitga ega bo’lishdan iboratdir. Shennon kriptografik sistemaning mustahkamligini, chidamliligini nazari va amaliy nuqtai nazardan ko’rib chiqib, quyidagi ikkita savolni qo’ydi:

1 - nazariy tomondan. Agar raqib-kriptoanalitik kriptogrammani tahlil qilish uchun zarur barcha vositalarga ega bo’lsa va uning vaqt imkoniyatlari cheklanmagan bo’lsa, sistemaning ishonchliligi qay darajada bo’ladi?

2 - amaliy tomondan. Agar raqib-kriptoanalitik kriptogrammani tahlil qilish uchun yetarli vositalarga ega bo’lmasa va uning vaqt imkoniyatlari cheklangan bo’lsa, u holda sistemaning ishonchliligi qay darajada bo’ladi?

1-savolga Shennon nazariy nuqtai nazardan quyidagicha javob beradi: nazariy chidamli shifrni tuzish uchun maxfiy kalitning hajmi ko’pchilik amaliy qo’llashlar (tadbiqotlar) uchun yo’l qo’yib bo’lmas darajada katta. Ya`ni u bu yerda ikkita fikrga tayanadi:

1. Maxfiy kalit faqat bir marta ishlatiladi;
2. Kriptoanalitik faqat shifrmatnga ega bo’lishi mumkin (ya`ni ochiq matnni olish imkonyaitiga ega emas).

Bu fikrlarga asoslanib, mutlaq maxfiylik deganda, har qanday ochiq matn X va shifrmatn Y uchun X va Y larning statistik aloqador emasligini tushunish mumkin, ya`ni:

P(XqxG’Yqy)qP(Xqx) (3)

Boshqacha aytganda, raqib-kriptoanalitik kriptogrammani tahlil qilish uchun ixtiyoriy vaqt va hisoblash imkoniyatlaridan foydalanmasin, ochiq matnning aposterior ehtimollik taqsimotini yaxshilay olmaydi. Yuqoridagilarga asoslangan holda Shennon nazariy tomondan mutlaq maxfiy sistemalar mavjud, degan xulosaga keladi.

Informatsiya nazariyasi apparatini qo’llab, (1) va (2) larni quyidagicha yozish mumkin:

H(YG’X, Z) q0 (4)

H(XG’Y, Z) q0 (5)

va mutlaqo maxfiy sistemani quyidagicha tasvirlash mumkin:

H(XG’Y) qH(X) (6)

Yuqoridagi ifodalardan maxfiy kalitli kriptografik sistema uchun quyidagi ifodani keltirib chiqarish mumkin:

H(XG’Y) ≤ H(X, ZG’Y) q H(ZG’Y) q H(XG’Y,Z) q H(ZG’Y) ≤ H(Z)

(6) dan foydalanib, quyidagini olamiz:

H(X) ≤H(Z) (7)

Ya`ni maxfiy kalitning noaniqlik darajasi ochiq matnning noaniqlik darajasidan katta bo’lishi kerak. Boshqacha aytganda, kalit ochiq matndan qisqa bo’lmasligi kerak, ya`ni K ≥ X.

Shunday qilib, bu yerda maxfiy kalit muammosi paydo bo’ladi. Buni shunday tushuntirish mumkinki, amalda mutlaq maxfiylikka erishib bo’lmas ekan, chunki ochiq matnning bitta belgisi uchun maxfiy kalitning bitta belgisi to’g’ri keladi va katta hajmdagi informatsiyaga buni qo’llash uchun hisoblash texnikasi vositalarining qudrati yetmaydi. Mukammal bo’lmagan shifrlarni tahlil qilishda Shennon kalitning ishonchsizlik funktsiyasini kiritdi:

f(n)qH(ZG’ y_1, y_2, ..., y_n) (8)

va f(n)≈0 uchun eng kichik n sonining tanholik masofasini aniqladi. Kalitning ishonchsizlik funktsiyasi, shifrmatnning dastlabki n belgisini tahlil qilayotgan

kriptoanalitik uchun kalitning naoaniqlik o'lchovi bo'lib xizmat qiladi. Shunday qilib, agar shifrmatnning u ta belgisi ma`lum bo'lsa, u holda y_1, y_2, ..., y_n ga asoslanib maxfiy kalitning loaqal bitta qiymatini topish mumkin. To'liq aniqlangan "tasodifiy shifrlar" uchun Shennon quyidagi formulalarni taklif etdi:

$$u \approx \frac{H(Z)}{r \log Ly}, \qquad (9)$$

$$r = 1 - \frac{H(X)}{N \log Ly} \qquad (10)$$

bu yerda:

r - shifrmatnning ortiqchaligi;

N - shifrmatn uzunligi, belgilar soni;

Ly - belgilarni o'z ichiga olgan alfavitning umumiy hajmi;

ya`ni r - Ly hajmli alfavitdan N belgi uzunligiga ega bo'lgan shifrmatnning ortiqchaligi.

Agar LxqLy bo'lsa va kalit tasodifiy tarzda tanlansa, u holda

$$u \approx \frac{k}{r} \qquad (11)$$

bo'ladi.

Agar kriptografik sistemada LxqLyqLz bo'lsa va u ingliz tilidagi matnni shifrlashda ishlatilsa, u holda Nq3G'4 qiymatni olgandan so'ng, ingliz tilidagi matnning k ta belgisi ochiladi. Masalan, ko'pi bilan 77 bitga yaqin shifrmatnni tahlil qilish asosida 56 bit uzunlikka ega bo'lgan maxfiy kalitni nazariy jihatdan tiklash mumkin.

(11) ifodada $r \to \infty$ bo'lganda, Shennon tomonidan olingan yana bir muhim natija $u \to \infty$ ni esda tutish lozim bo'ladi. Shunday qilib, ortiqchalikning yo'qligi, ya`ni ma`lumotlarni siqish ochiq matn va maxfiy kalitni tiklashda kriptoanalitikning ishini yanada qiyinlashtiradi. Afsuski, bir vaqtning o'zida ham mukammal, ham real axborot manbalari uchun amalda qo'llash mumkin bo'lgan siqish metodlari ishlab chiqilmagan.

Axborotlarning aslligi. Ma`lumotlarni shifrlashning nazariy asoslari 40-yillarning oxirida ishlab chiqilgan bo'lsa, ma`lumotlarning aslligi masalalari bilan jiddiy shug'ullanishga esa yaqindagina kirishildi. Shifrlashdan asosiy maqsad informatsiyani beruxsat tanishishdan himoyalash bo'lsa, autentifikatsiyadan asosiy maqsad esa informatsiya almashinish jarayoni ishtirokchilarini yasamalashtirish (imitatsiya) asosida amalga oshirilayotgan aldovdan himoyalashni ta`minlash, ya`ni, masalan, haqiqiy shifrmatn kelgunga qadar shifrmatnni qalbakilashtirish; haqiqiy shifrmatn yetib kelgandan so'ng yolg'on informatsiyani uning o'rniga qabul qildirish.

Mustahkamlash uchun savollar:

1. Kriptografiya termirnini ta`riflang.
2. Sifatli shifrlash kriteriyasi (mezoni) haqida gapirib bering.
3. Ma`lumot uzatishdagi shifrlashga nimalar kiradi ?
4. Ma`lumot uzatishdagi deshifrlashga nimalar kiradi ?
5. Shennon modeli bo'yicha ma`lumotlarni shifrlash mezonini qisqacha ifodalab bering.

Foydalanilgan adabiyotlar ro'yxati

- Turskiy A. , Panov S «Zahita informatsii pri vzaimodeystvii korporativno'x setey v Internet», FiS, Moskva, 2003 g.
- Koshelev A.»Zahita setey i firewall» Komp yuterPress, 2000 g.
- Oliver .V.G. «Novo'e texnologii i oborudovanie» ,SPb:BHV-Sankt – Peterburg,2000 g.
- Brassar. J. «Sovremennaya kriptologiya» ,Moskva, «Polimed», 1999 g.
- Petrov A. «Kriptograficheskie metodo' zahito'» ,Moskva,DMK, 2000 g.
- Romanets Yu.V., Timofeev P.A. «Zahita informatsii v sovremenno'x komp yuterno'x sistemax» , Moskva, Radio i svyaz , 1999 g.

8-Ma`ruza
Bir kalitli kriptografik sistemalar. (2 soat)

O'quv modullari

1. Kriptosistema klassifikatsiyasi
2. Bir kalitli kriptografik sistemalar
3. Blokli shifrlar
4. Oddiy o'rin almashtirish shifrlari

Aniqlashtirilgan o'quv maqsadlari.Talaba bu mavzuni to'la o'zlashtirgandan so'ng:

- Kriptografiya haqidagi tamoyillarni biladi;
- Kriptosistema klassifikatsiyasi asosiy printsiplarini bo'laklarga bo'lib, ta`rif bera oladi;
- Bir kalitli kriptografik sistemalar foydalanish xususiyatlarinini talqin eta oladi;
- Blokli shifrlar qaysi sinfga mansubligini tasavvur eta oladi;

❖ Oddiy o’rin almashtirish shifrlari ko’rinishi o’rtasidagi o’zaro aloqadorlikni aniqlaydi, bog’lanishlarni tahlil qila oladi.

Tayanch so’z va iboralar:
Kriptografiya, Kriptosistema klassifikatsiyasi, Ma`lumotlarni himoya qiluvchi xavfsizlik xizmati, Blokli shifrlar , Oddiy o’rin almashtirish shifrlari.

Kriptosistema klassifikatsiyasi

Kalitlardan foydalanish xarakteri bo’yicha ma`lum kriptosistemalarni ikkita turga bo’lish mumkin: simmetrik (bir kalitli, maxfiy kalitli) va asimmetrik (ochiq kalitli).

Birinchi holda jo’natuvchi shifratori va qabul qiluvchi deshifratorida yagona kalitdan foydalaniladi. Shifrator ochiq matnning funktsiyasi hisoblangan shifrmatnni tuzadi. Funktsiyaning aniq ko’rinishi maxfiy kalit orqali aniqlanadi. Xabarni qabul qiluvchi deshifratori teskari o’zgartirishni amalga oshiradi. Maxfiy kalit sir saqlanadi va xabar jo’natuvchi tomonidan qabul qiluvchiga kanal bo’ylab uzatiladi. Bu kanal dushman kriptoanalitiki tomonidan kalitning ushlab qolinishidan xoli hisoblanadi. Odatda, Kirxgof qonuni bo’yicha: shifr mustahkamligi faqatgina kalit maxfiyligi bilan aniqlanadi, ya`ni kriptoanalitikka maxfiy kalitdan boshqa shifrlash va deshifrlash jarayonining hamma tafsilotlari (detali) ma`lum.

Ochiq kalitli kriptografik sistemalar foydalanuvchiga himoyalanmagan kanal orqali xavfsiz ma`lumot uzatish imkonini beradi. Bunday kriptosistemalar asimmetrik, ya`ni undagi jo’natuvchi va qabul qiluvchi har xil kalitga ega bo’lishi lozim.

Shifrlash va deshifrlash algoritmida ishlatilayotgan har xil kalitlarning biri orqali ikkinchisini hosil qilish imkoni yo’q. Bitta kalit shifrlash uchun, ikkinchisi deshifrlash uchun ishlatiladi. Ochiq kalitli sistemalardagi asosiy printsip bir tomonlama yoki takrorlanmaydigan funktsiyalar hamda maxfiy yo’lli bir tomonlama funktsiyalarga asoslanadi.

Kalitlarni hisoblash xabarni qabul qilish oluvchi tomonidan amalga oshiriladi. U keyinchalik faqatgina o’zi foydalanadigan maxfiy kalitlarni o’zida olib qolib, boshqa - ochiq kalitni oshkor bo’lishidan ikkilanmay xabar jo’natuvchiga yuboradi. Bu ochiq kalitdan foydalangan holda har qanday abonent matnni shifrlashi va qabul qiluvchiga jo’natishi mumkin. Hamma ishlatiladigan algoritmlar umumiy foydalaniladigan hisoblanadi. Shifrlash va deshifrlash funktsiyalari o’zaro aloqadagi kalitlar jufti (ochiq va maxfiy) bilan ta`minlangan bo’lsa qaytuvchi, ochiq kalit esa o’zida maxfiy kalitdan qaytmaydigan kalitni

ifodalashi lozim. Shunga ko’ra shifrmatn o’zida ochiq matnning qaytmas funktsiyasini ifodalashi lozim.

Қaytmas funktsiyalarni tadqiq etish asosan quyidagi yo’nalishlar bo’yicha olib boriladi: darajaga diskret ko’tarish - DH (Diffi Xellman) algoritmi, oddiy sonlarni ko’paytirish - RSA (Rayvest, Shamir, Eydlman) algoritmi, xatolarni to’g’rilovchi Goppa kodlaridan foydalanish, NP-to’lalik masalalari, xususan, Shamir tomonidan ochilgan “ryukzakni taxlash masalasi” asosidagi Merkl va Xellman kriptoalgoritmlari va boshqalar.

Birinchi sistema (DH) kalitlarni ochiqdan-ochiq tarqatishni ta`minlaydi, ya`ni maxfiy kalitlarni uzatishdan bosh tortish imkonini beradi. Hozirgi kunda mustahkam va qulay ochiq kalitlar sistemasidan biri hisoblanadi. Ikkinchi (RSA) usulining ishonchliligi katta sonni ko’paytuvchilarga ajratish murakkabliligi bilan o’lchanadi. Agar ko’paytuvchilar 100 ta o’n xonali raqamlar tartibidagi uzunlikka ega bo’lsa, u holda eng mashhur ko’paytuvchilarga ajratish usuli uchun ham 100 mln. yil mashina vaqti zarur, shifrlash va deshifrlash har bir blok uchun 1-2 s tartibni talab etadi. NP-to’lalik masalalari kombinatorikada yaxshi ma`lum va umumiy holda o’ta murakkab hisoblanadi, biroq mos shifrni tuzish oddiy emas.

Ochiq kalitli sistemada blokli shifrlardagi kabi shifrlanuvchi blokning hajmi katta bo’lishi kerak. Hozirgi kunda yuqori samaradorlikdagi ochiq kalitli sistema topilganicha yo’q. Deyarli hamma joyda ochiq kalitli kriptosistemalardan foydalanish chegaralangan.

Bir kalitli kriptografik sistemalar

Blokli shifrlar

Odatda, xabarning ochiq matni ixtiyoriy uzunlikka ega bo’ladi. Gohida uning yetarli darajada katta hajmga ega bo’lishini e`tiborga olib, u fiksirlangan (o’zgarmas) uzunlikdagi mayda bloklarga bo’linadi. Bu bloklar matnlari bir-biriga bog’liq bo’lmagan holda alohida-alohida shifrlanadi.

Yagona kalitga ega blokli shifrlar 3 guruhga bo’linadi:

-o’rnini almashtirish shifrlari;

-o’rniga qo’yish shifrlari;

-qo’shma shifrlar.

Simvollar ketma-ketligi tartibini o’zgartirish yo’li bilan xabar mazmunini yo’qotishga mo’ljallangan o’rnini almashtirish shifrlaridan foydalanishda ochiq matn belgilari berilgan blok chegarasida bir nechta qoida (kalit) bo’yicha almashtiriladi. Buning natijasida ularning joylashish tartibi va informatsiyaning mazmuni buziladi. Bunda oddiy va murakkab o’rin almashtirish shifrlari farqlanadi.

Oddiy o’rin almashtirish shifrlari

Oddiy o’rin almashtirish shifrlari tanlangan o’rin almashtirish kaliti (qoidasi) ga mos holda matndagi harflar guruhini qayta tartiblaydi. Buning uchun oddiy shifrlash protsedura (kalit)larini beruvchi maxsus jadvallardan foydalanilodi. Unga ko’ra xabardagi harflar o’rnini almashtirish amalga oshirilgan. Bunday jadvaldagi kalit sifatida jadval o’lchamlari hamda almashtirish yoki jadvalning boshqa maxsus xususiyatlarini beruvchi ibora (fraza)lar xizmat qiladi.

Oddiy o’rin almashtirish shifriga misol 8-rasmda keltirilgan.

Устунлар

Қаторлар

B	I	A	T	U	A
A	R	K	E	Ch	M
H	N	U	T	R	I
O	I	L	D	A	Z
D	F		A	T	`

BIATUA ARKEChM HNUTRI OILDAZ DF AT`

8-rasm. Oddiy o’rin almashtirish shifri

8-rasmdan ko’rinib turibdiki, “BAHODIRNI FAKUL TETDA UCHRATAMIZ” xabarini shifrlash uchun uni 5 qator va 6 ustundan iborat jadval ko’rinishida yozib olamiz. Xabar matni bo’sh joy qoldirmasdan ustunlar bo’yicha yoziladi. Agarda oxirgi ustun to’lmay qolsa, uni ixtiyoriy harf bilan to’ldirish mumkin. Shifrlangan xabarni olish uchun berilgan matn qator bo’yicha chapdan o’ngga qarab o’qiladi va guruhlab yoziladi (ushbu holatda 5 ta raqamli guruh). Oxirgi protsedura shifrlash jarayoniga taalluqli bo’lmay, balki ma`nosi yo’qolgan matnni qulay yozish uchun bajariladi. Bunday matnni asliga tiklash uchun jadvalning o’lchami - qator va ustunlar sonidan iborat kalitni bilish lozim.

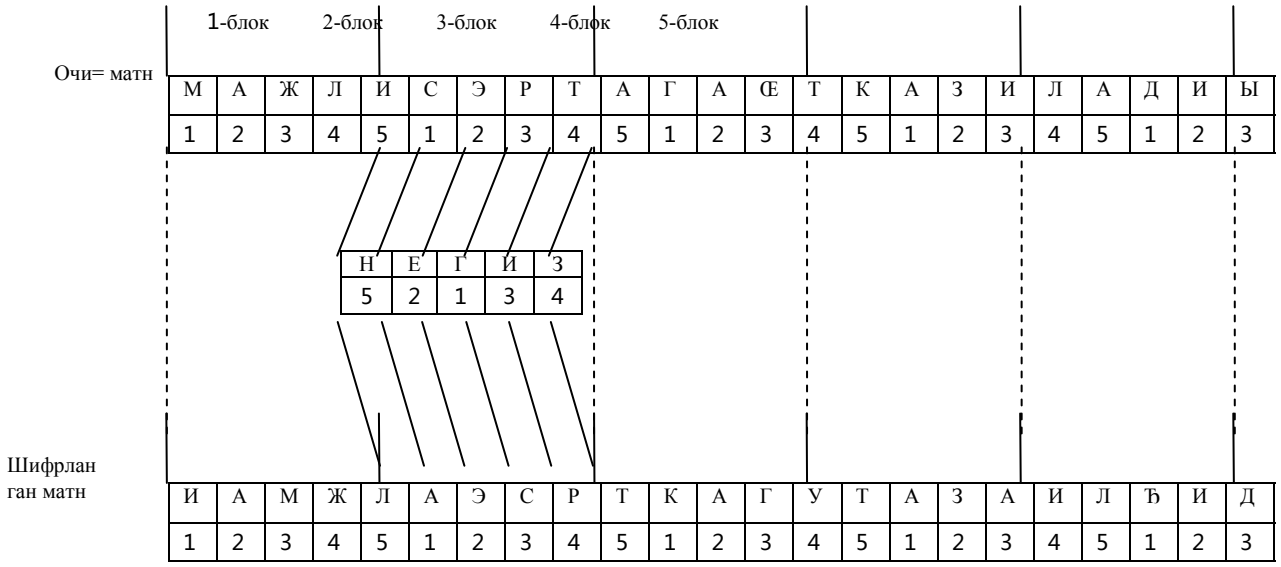
Amalda ko’proq ishlatiladigan, yuqoridagi usulga o’xshash shifrlashning yana bir usulini ko’rib o’tamiz. U shu bilan farqlanadiki, jadval ustun va satrlarining o’rni kalit so’z bo’yicha almashtiriladi. Ushbu holda ibora yoki jadval qatoridagi sonlar naboridan kalit sifatida foydalaniladi.

Shifrlashda shifrlanadigan matn ketma-ket qatorlar bo’yicha yoziladi va simvollar qaytarilmaydi. Kalitni eslab qolishni osonlashtirish uchun kalit so’zdan foydalaniladi. Uning harflari alfavitdagi o’rniga qarab nomerlanadi va u o’rin almashtirish qoidasini beradi.

9-rasmda oddiy o’rin almashtiridan foydalanilgan shifrlash jarayoni keltirilgan.

“MAJLIS ERTAGA O’TKAZILADI” xabarini shifrlash talab qilinsin.

Bu xabarni shifrlash uchun so’zlar orasiga bo’sh joy qoldirmasdan yozib olamiz va 52134 nomerli kalit tanlaymiz. Ushbu 5 ta raqamdan tashkil topgan kalitga ko’ra hamma informatsion xabarni 5 ta harfdan tashkil topadigan bloklarga bo’lamiz. Bo’lishdan so’ng bizda 4 ta 5 harfdan iborat to’liq blok va 1 ta 2 harfdan iborat blok hosil bo’ladi.



rasm. Oddiy o’rin almashtirish shifri.

Bunday holatda oxirgi harflar guruhi blok to’lguncha ixtiyoriy simvollar bilan to’ldiriladi. Bizning misolda 3 ta harf yetishmaydi. Shuning uchun ixtiyoriy o’, q, g’ harflari bilan blokni to’ldiramiz.

Keyin 52134 kalitidan foydalanib, berilgan ochiq matndagi harflarning o’rni almashtiriladi. Masalan, kalitning birinchi raqami -5. Bu shuni ko’rsatadiki, yangi hosil bo’layotgan shifrlangan blokning birinchi xonasiga ochiq matn birinchi blokidan 5 raqamiga mos harf yoziladi. Kalitning ikkinchi raqami - 2, demak, shifrlangan matning ikkinchi harfi ochiq matn blokidagi ikkinchi harf - A bo’ladi. Shifrlash shu tarzda ketma-ket davom etadi.

Nihoyat, hamma bloklarda o’rin almashtirish o’tkazilgandan so’ng, shifrlangan matnni olamiz. Uni o’qib, dastlabki matndan hech qanday ma`no qolmaganligiga ishonch hosil qilamiz.

Kalitni eslab qolishni osonlashtirish maqsadida kalit so’z ishlatiladi. Berilgan holda bu so’z - “NEGIZ”. Unda kalitdagi 1 raqami G harfiga mos, ya`ni bu so’zda kelayotgan harflar ichida alfavitda birinchi harf hisoblanadi. 2 raqamiga esa ye harfi mos keladi va hokazo.

Xuddi shu xabarni 5 ta qator va 5 ta ustundan iborat (kalit so’z uzunligicha) jadval yordamida ham shifrlash mumkin. Berilgan matn ustunlar bo’yicha yoziladi va jadval holatiga keladi (10-rasm).

Калит

N	E	G	I	Z
5	2	1	3	4
M	S	G	A	D
A	E	A	Z	I
J	R	O’	I	O’
L	T	T	L	q
I	A	K	A	g’

G	E	I	Z	N
1	2	3	4	5
G	S	A	D	M
A	E	Z	I	A
O’	R	I	O’	J
T	T	L	q	L
K	A	A	g’	I

ЬІрин алмаштиришдан сынг

Берилган матн

10-rasm. Jadval yordamida shifrlash

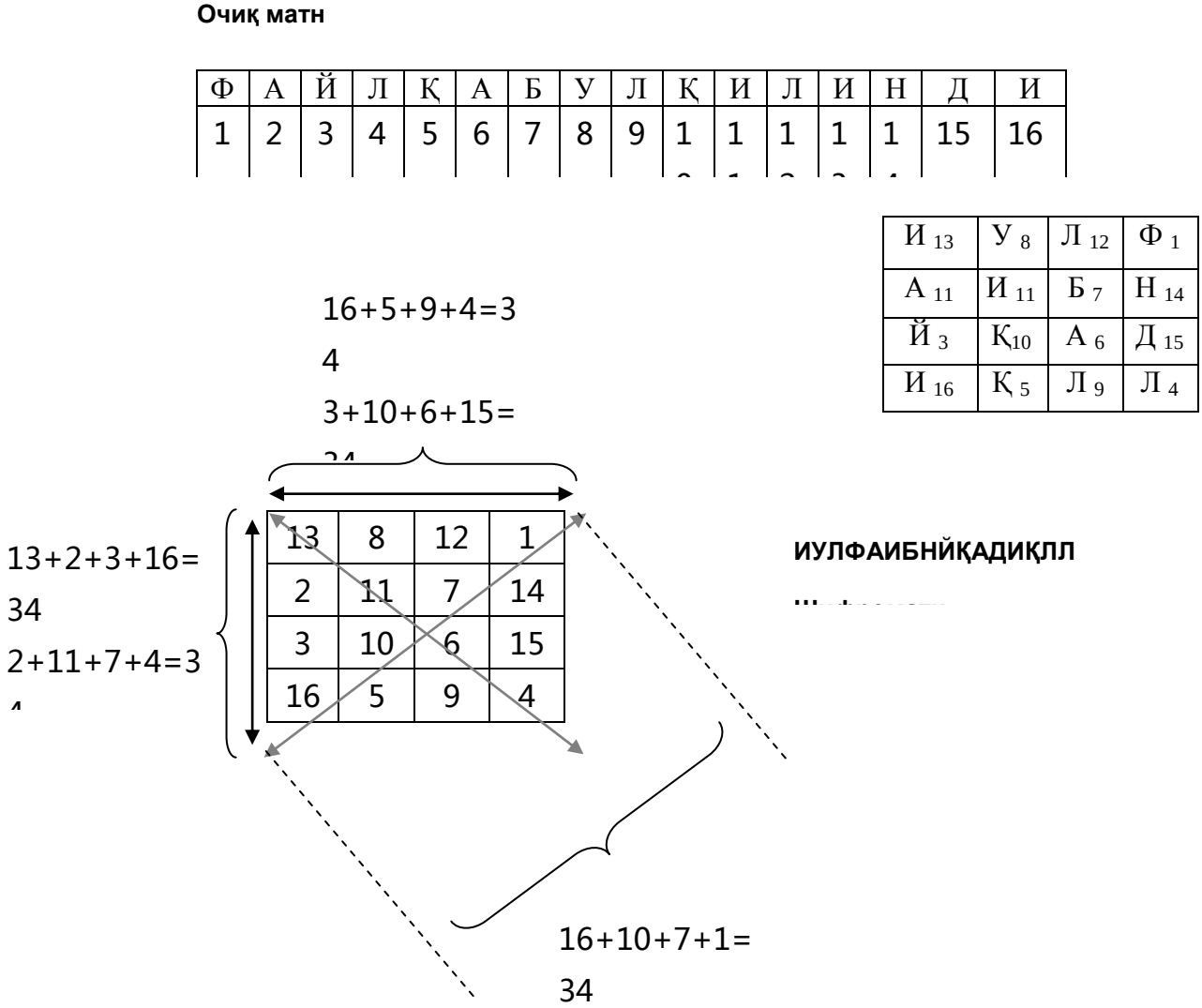
Kalit so’z ustunlar o’rnini almashtirish qoidasini beradi. Hosil bo’lgan ikkinchi jadval birinchisidan butunlay farq qiladi.

Ushbu shifrning asosiy kamchiligi undagi past kriptomustahkam lik hisoblanadi. Shifrlangan matnni ko’paytuvchilarga ajratib (variantlar ko’pchilikni tashkil etmaydi), shifrlashda foydalanilgan kodli so’zning ehtimolli uzunligini oson aniqlab olish mumkin.

Yuqorida hosil qilingan shifrlangan matnning kriptomustahkam ligini oshirish uchun uni yana bir bor shifrlash mumkin. Shifrlashning bu usuli “ikki marta o’rnini almashtirish” nomi bilan mashhur. Bu usulning ma`nosi quyidagicha. Birinchi shifrlashdan olingan matn ikkinchi marta boshqa o’lchamdagi jadval (qator va ustunlar soni boshqacha tanlanadi) yordamida shifrlanadi. Bundan tashqari, bitta jadvalda qatorlar, boshqasida esa ustunlar o’rnini almashtirish mumkin. Berilgan matn bilan jadvalni “zigzag”, "ilonsimon”, “spiralsimon” usullar bo’yicha to’ldirish mumkin.

“Sirli kvadratlar” nomli oddiy o’rin almashtirish shifridan o’rta asrlardayoq foydalanishgan (11-rasm).

Sirli kvadratlar deb, hamma tomonlari teng, 1 dan boshlab natural sonlar bilan to’ldirilgan jadvalga aytiladi. To’ldirilgan sonlar qo’shilganda ustun bo’yicha ham, qator bo’yicha ham bir xil son hosil bo’lishi kerak (bizning misolda bu son - 34). Berilgan matn “FAYL qABUL qILINDI”.



Sirli kvadratni to’ldirishda berilgan matndagi nomerlangan harflar jadvalga ko’chiriladi. Masalan, 1 raqami matndagi F bilan, 10 raqami q bilan va hokazo almashtiriladi. Ochiq matn jadvalga ko’chirilgandan so’ng jadval qator bo’yicha o’qiladi va natijada harf o’rinlari almashgan shifrmatn hosil bo’ladi.

Mustahkamlash uchun savollar:

1. Jadval yordamida shifrlashni ta`riflang.
2. Sifatli shifrlash kriteriyasi (mezoni) haqida gapirib bering.
3. Oddiy o’rin almashtirish shifrlariga nimalar kiradi ?
4. Ma`lumot uzatishdagi deshifrlashga nimalar kiradi ?

5. Shennon modeli bo’yicha ma`lumotlarni shifrlash mezonini qisqacha ifodalab bering.
6. Sirli kvadratning maqsadi nimalardan iborat?

Foydalanilgan adabiyotlar ro’yxati

- Turskiy A., Panov S «Zahita informatsii pri vzaimodeystvii korporativno’x setey v Internet», FiS, Moskva, 2003 g.
- Koshelev A.»Zahita setey i firewall» Komp yuterPress, 2000 g.
- Oliver .V.G. «Novo’e texnologii i oborudovanie» ,SPb:BHV-Sankt – Peterburg,2000 g.
- Brassar. J. «Sovremennaya kriptologiya» ,Moskva, «Polimed», 1999 g.
- Petrov A. «Kriptograficheskie metodo’ zahito’» ,Moskva,DMK, 2000 g.
- Romanets Yu.V., Timofeev P.A. «Zahita informatsii v sovremenno’x komp yuterno’x sistemax» , Moskva, Radio i svyaz , 1999 g.