

O‘zbekiston Respublikasi Vazirlar Maxkamasi

O‘zbekiston Respublikasi Oliy va O‘rta

Maxsus Ta’lim Vazirligi

Toshkent Islom Universiteti

"Informatika va axborot Texnologiyalari " kafedralari uchun

Nigmatov H., Tursunov N.X.

“Axborot xavfsizligi”

(O‘quv qo‘llanma)

Toshkent - 2018

Annotatsiya

UDK. 621.395.12

Ushbu taqdim etilayotgan qo‘llanmada kompyuter tizimi va tarmoqlarida axborotlarni himoyalash vositalari, havf xatarlar va xujum turlari, konkret tashkiliy, texnikaviy yoki uskunaviy, dasturiy, xuquqiy, jismoniy, kriptografik, kompyuter tarmoqlarining aloqa kanallarida axborotlarni himoyalash va viruslardan himoyalash vositalari keng yoritilib berilgan. Bo‘limning yakunida amaliy mashg‘ulotlar va laboratoriya ishlarini qanday o‘tkazish kerakligi to‘g‘risida yo‘riqnomalar berilgan, hamda test savollari keltirilgan.

O‘quv qo‘llanma oliy o‘quv yurtlarida ta’lim olayotgan barcha talabalar va kollej o‘quvchilari uchun ham foydali bo‘ladi degan niyatdamiz. Har qanday e’tiroz va fikrlaringizni kutib qolamiz.

Tuzuvchilar:

t.f.d., prof. X.Nigmatov

t.f.n., dots. N. Tursunov

” “Informatika va axborot texnologiyalari kafedrasi.

Mas’ul muxarrir:

Mualliflar taxriri ostida

Taqrizchilar:

p.f.d., prof. A.A.Abduqodirov

t.f.d., prof. M.A.Ismailov

Mundarija

K i r i sh.

1. **Axborot xavfsizligi fanining predmeti va vazifalari**.....
 - 1.1 Axborot xavfsizligi fani nimani o'rgatadi.....
 - 1.2. Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin.....
 - 1.3. Axborotni himoyalashning maqsaddari.....
 - 1.4. Avtomatlashtirilgan axborot tizimlarida himoyalash zaruriyati.....
2. **Axborotlarni himoyalash muammolari**.....
 - 2.1. Axborotni ximoyalash tizimi.....
 - 2.2. Tashkilotlardagi axborotlarni ximoyalash.....
 - 2.3. Himoyalash tizimining kompleksligi.....
 - 2.4. Axborotlarni tashkiliy himoyalash elementlari.....
 - 2.5. Internetda informatsion xavfsizlik.....
3. **Axborotning buzulishi**.....
 - 3.1 Kompyuter tizimlari va tarmoqlaridagi xavf-qatarlar
 - 3.2 Xujum turlari
 - 3.3 Xujumlarni aniqlash va taxlil qilish.....
 - 3.4 Xujumlarni aniqlovchi tizim
 - 3.5 Real Secure tizimi nima.....
4. **Kompyuter tizimlari va tarmoqlarida axborotni himoyalashning tashkiliy vositasi**.....
 - 4.1 Himoyalash tizimining kompleksligi.....
 - 4.2 Axborotlarni tashkiliy himoyalash elementlari.....
 - 4.3 Kompyuter tizimlari va tarmoqlarida axborotni himoyalashning uskunaviy vositasi.....
5. **Kompyuter tizimlari va tarmoklarida axborotni ximoyalashning kriptografik vositasi**.....
 - 5.1 Zamonaviy kompyuter stenografiyasi.....
 - 5.2 Kompyuter stenografiyasi istikbollari.....
 - 5.3 Kompyuter stenografiyasining asosiy vazifalari.....
 - 5.4 Konfidentsial axborotlarni ruxsatsiz kirishdan himoyalash.....
 - 5.5 Mualliflik huquqlarini ximoyalash.....
 - 5.6 Stenografik dasturlar tugrisida qisqacha ma'lumot.....
- 6 **Axborotlarni kriptografik himoyalash usullari**.....
 - 6.1 Simmetriyali kriptotizim asoslari.....
 - 6.2 Kompyuter viruslaridan ximoyalanish.....
 - 6.3 Asoslangan algoritmlar buyicha dasturli viruslarni quyidagicha tasniflash.....
7. **Antivirus dasturlari**.....
 - 7.1 Viruslarga karshi chora-tadbirlar.....
8. **Kompyuter tarmoklarida uzatilayotgan axborotni ximoyalash**.....
 - 8.1 Elektron pochtaga ruxsatsiz kirish.....
 - 8.2 Kompyuter tarmoklarida ma'lumotlarning tarqalish kanallari.....
 - 8.3 Kompyuter telefoniyasidagi himoyalash usullari.....
9. **Kompyuter tarmoqlarida ishlatiladigan kommutatsiya turlari**.....
 - 9.1 Kanallar kommutatsiyasi.....
 - 9.2 Axborotlar kommutatsiyasi.....
 - 9.3 Paketlar kommutatsiyasi.....
 - 9.4 Marshrutizatorlarning ishlash printsiplari.....
10. **Telekommunikatsiya tizimlarida axborot havfsizligi**.....
 - 10.1 Bell–Lapadula modeli. D. Denning modeli. Landver modeli.....
 - 10.2 Elektron raqamli imzo.....
 - 10.3 Telekommunikatsiya tarmoqlarida axborot havfsizligini ta'minlash texnologiyalari.....
 - 10.4 Tarmoqlarda ekranlash texnologiyalari.....

11. VPN tarmoq texnologiyasi

- 11.1 Kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalari
- 11.2 EHM himoyasini ta'minlashning texnik vositalari
- 11.3 Kompyuter tarmoqlarida ma'lumotlarni himoyalashning asosiy yo'nalishlari

12. Kriptografiya

- 12.1 Almashtirish usullari:

13. Amaliyot mashg'ulotlar va laboratoriya ishlarini bajarish uchun tavsiyalar.....

14. "Axborot xavfsizligi" fanidan test savollari.

Adabiyotlar

Axborot havfsizligi.

Kirish.

Ushbu 2 – bobda “Kompyuter tizimi va tarmoqlarida axborotlarni himoyalash” faniga tegishli bo‘lgan barcha mavzular bo‘yicha bakalavrlarga va magistrnlarga Davlat ta’lim standartlari asosida yetkazilishi shart bo‘lgan minimum bilimlar va ko‘nikmalar to‘la qamrab olingan. Zamonaviy kompyuter tizimlarini yaratilishi va global axborot tarmoqlarini paydo bo‘lishi axborotni himoya qilish muammosini keltirib chiqardi. Xar bir ma’lumot, xabar yoki axborot o‘z qiymatiga ega bo‘la boshladi. Ya’ni o‘z vaqtida yetkazib berilmagan yoki xato va soxtalashib qabul qilingan har qanday ma’lumot qabul qiluvchini yoki boshqaruv tizimini no‘to‘g‘ri qaror chiqarishiga olib keladi. Bularni to‘g‘rilash esa katta moliyaviy xarajatlarga olib kelishi mumkin. Keng kompyuterlashtirilgan va axborotlashtirilgan zamonaviy jamiyatda real qadriyatlarga ega bo‘lish, ularni boshqarish, qadriyatlarni uzatish va ularga murojaat qilish ko‘pincha nomoddiy axborotlarga, ya’ni mavjud bo‘lishi fizik tashuvchidagi birorta yozuv bilan bog‘lanishi majburiy bo‘lmagan axborotlarga asoslangandir. Shunga o‘xshash, ba’zida yuqori ahamiyatga ega bo‘lgan maxfiy axborotni ishlatishga, o‘zgartirishga, nusxalashga jismoniy va xuquqiy shaxslarning vakolatlari aniqlanadi. Shuning uchun axborotni maxfiyligi va butunligini ta’minlash bilan bog‘liq bo‘lgan barcha kerakli funktsiyalarni amalga oshirish uchun samarali vositalarni yaratish va ishlatish juda muhimdir. Axborot juda qadriyati yoki o‘ta muhim bo‘lganligi sababli bunday axborotni saqlaydigan, qayta ishlaydigan yoki uzatadigan kompyuter tizimlariga nisbatan turli – tuman yomon niyatli harakatlar mumkindir. Masalan, buzg‘unchi o‘zini boshqa foydalanuvchi kabi ko‘rsatishga intilishi, aloqa kanalini bildirmasdan eshitib olishi yoki tizim foydalanuvchilari almashayotgan axborotni ushlab olishi va o‘zgartirishi mumkin. Zamonaviy kompyuter tizimlari va tarmoqlari, Internet yomon niyatli odamlarga muhim maxfiy axborotni o‘g‘irlash, buzish yoki xalaqitlarga uchratish maqsadida korxonalar va tashkilotlarning ichki tarmoqlariga bostirib kirish uchun ko‘plab imkoniyatlar beradilar. Shu sababli

hozirda insonlarni va jamiyatni axborot xavfsizligini va axborotni himoya qilishni ta'minlash muammosini kompleks yechishni dolzarb ravishda kerakligi paydo bo'lmoqda.

Shu bilan birga ta'kidlash kerakki, o'tkazilayotgan aktiv tadqiqotlarga qaramasdan, axborot xavfsizligini yaxlit tizimini yaratishni umumlashgan nazariyasi va amaliy kontseptsiyasi (yo'nalishi) hanuzgacha yaratilmagan. Shuning uchun maxfiy axborot bilan ishlagan shaxslarga axborot xavfsizligini ta'minlash masalalarini barcha jabhalarida, ularning kompleksli va o'zaro kelishilgan xarakterini tushungan holda, yetarlicha tayyorgarlikka va mutaxassis sifatida mo'ljal ola bilishga ega bo'lishlari kerak.

Kompyuter tizimi va tarmoqlarida axborotlar almashinuvi darajasi oshib borayotganligi, ma'lumotlarni hilma hilligi, ularni telekommunikatsiya tarmoqlari orqali uzatilayotgan tezligi juda yuqori ekanligi, qabul qilayotgan foydalanuvchilarga o'z vaqtida, aniq va to'liq yetkazib berish jarayonida axborotlarni himoyalash vazifasi asosiy masalalardan biri bo'lib qolmoqda. Turli operatsion tizimlar bilan ishlaydigan kompyuterlarning axborot havfsizligini ta'minlash maqsadida ko'pgina vositalar va usullar ishlab chiqilgan. Ushbu vositalar yordamida axborot xavfsizligini ta'minlash fan asosiga kiradi.

Barcha bakalavrlarni va magistrnlarni kompyuter tizimi va tarmoqlarida axborotlarni himoyalash usullarini va vositalarini mukammal bilgan xolda amaliyotga tadbqiq etishni o'rgatishdan iboratdir.

Kompyuter tizimi va tarmoqlarida axborotlarni himoyalash uchun ishlatiladigan asosiy tashkiliy, texnikaviy, dasturiy, xuquqiy, jismoniy, kriptografik, kompyuter tizimi va tarmoqlarining aloqa kanallarida yuborilayotgan ma'lumotlarni himoyalash, hamda kompyuter viruslaridan qanday himoyalanish usul va metodlarini, hamda viruslarni payqash va ularni himoya qilish dasturlarini o'rganishdan iborat.

Fanni o'rganish uchun talabalardan kompyuter tizimi va tarmoqlarini turlari, kriptografik himoyalash vositalarini, algoritmlash va dasturlashni, xalqaro kompyuter tarmog'i bo'lmish Internetda ishlash jarayonlarini mukammal bilish talab etiladi.

Fanni o'rganish davomida talabalar kompyuter tizimi va tarmoqlarda axborotlar himoyasining buzilishi, himoya mexanizmi va asosiy himoyalash vositalari, havf va xatar turlari, kompyuter tarmoqlaridagi xujumlar, ularning turlanishi, axborotlarni himoyalash vositalarining asosiy turlaridan tashkiliy, texnikaviy, dasturiy, jismoniy, xuquqiy, kriptografik va aloqa kanallarida axborotlarni himoyalash, ekranlash texnologiyalari, shaxsiy virtual tarmoqlar texnologiyasi, himoyalash taxlil texnologiyalari, buzuvchilar ta'sirini aniqlovchi texnologiyalar, telekommunikatsiya tizimlarida himoyalash modellari, elektron raqamli imzo, elektron xukumat va hozirgi zamonoviy intellektual texnikaviy vositalarni o'rganadilar.

Kompyuter tizimlari va tarmoqlarida havfsizlik modellarini, ya'ni Bella La Padula, Denning va Landver modellari va ularning qo'llanilishini, hamda ularni buzish ehtimolining modelini, elektron raqamli imzo, kriptologiyani qo'llanilish usullarini, elektron xujjat almashinuvida axborotlarni himoyalash va VPN kompyuter tarmoqlarini yaratishni yaxshi o'rganib oladilar.

Axborot havfsizligi fani nimani o'rgatadi.

Mamlakatimiz milliy iqtisodining hech bir tarmog'i samarali va mo'tadil tashkil qilingan axborot infratuzilmasiz faoliyat ko'rsatishi mumkin emas. Hozirgi kunda milliy axborot resurslari har bir davlatning iqtisodiy va harbiy salohiyatini tashkil qiluvchi omillaridan biri bo'lib xizmat qilmoqda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot-kommunikatsiyalar texnologiyalarini qo'llash kengayadi. Turli xildagi axborotlar hududiy joylashishidan qat'i nazar bizning kundalik hayotimizga Internet xalqaro kompyuter tarmogi orqali kirib keldi. Axborotlashgan jamiyat shu kompyuter tarmog'i orqali tezlik bilan shakllanib bormoqda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo'qolib bormoqda. Jahon kompyuter tarmog'i davlat boshqaruvini tubdan o'zgartirmoqda, ya'ni davlat axborotlarning tarqalishi mexanizmini boshqara olmay qolmoqda. Shuning uchun ham mavjud axborotlarga noqonuniy kirish, ulardan

foydalanish va yo‘qotish kabi muammolar dolzarb bo‘lib qoldi. Bularning bari shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib kelmoqda. Davlatning axborot xavfsizligini ta‘minlash muammosi milliy xavfsizlikni ta‘minlashning asosiy va ajralmas qismi bo‘lib, axborot ximoyasi esa davlatning birlamchi prioritet masalalariga aylanmokda.

Axborotning muximlik darajasi qadim zamonlardan ma‘lum. Shuning uchun ham qadimda axborotni ximoyalash uchun turli hil usullar qo‘llanilgan. Ulardan biri — sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o‘qiy olmagan. Asrlar davomida bu san‘at — sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o‘n yil oldin hamma narsa tubdan o‘zgardi, ya‘ni axborot o‘z qiymatiga ega bo‘ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o‘g‘irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday kilib, axborotni ximoyalash zaruriyati tug‘iladi. Axborotni qayta ishlash sanoatining paydo bo‘lishi axborotni ximoyalash sanoatining paydo bo‘lishiga olib keladi. Avtomatlashtirilgan axborot tizimlarida axborotlar o‘zining hayotiy davriga ega bo‘ladi. Bu davr uni yaratish, undan foydalanish va kerak bo‘lmaganda yo‘qotishdan iboratdir. Axborotlar hayotiy davrining har bir boskichida ularning himoyalanganlik darajasi turlicha baholanadi. Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muhim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulkiy huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshqa moddiy hamda nomoddiy zararlar keltirishi mumkin bo‘lgan turli kirishlar va o‘g‘irlashlardan ximoyalashdir. Axborot xavfsizligi deb ma‘lumotlarni yo‘qotish va o‘zgartirishga yunaltirilgan tabiiy yoki sun‘iy xossali tasodifiy va qasddan qilingan ta’sirlardan har qanday tashuvchilarda axborotning himoyalanganligiga aytiladi. Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va hujjatlarni o‘g‘irlash yoki nusxa olishdan iborat bo‘lsa, hozirgi paytdagi xavf esa kompyuter ma‘lumotlari tuplami, elektron ma‘lumotlar, elektron massivlardan ularning egasidan ruxsat so‘ramasdan foydalanishdir. Bulardan tashqari, bu harakatlardan moddiy foyda olishga intilish ham rivojlandi. Axborotning himoyasi deb boshqarish va ishlab

chiqarish faoliyatining axborot xavfsizligini ta'minlovchi va tashkilot axborot zaxiralarining yaxlitligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta'minlovchi qat'iy reglamentlangan dinamik texnologix jarayonga aytiladi. Axborotning egasiga, foydalanuvchisiga va boshqa shaxsga zarar yetkazmoqchi bo'lgan nohuquqiy muomaladan xar qanday hujjatlashtirilgan, ya'ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo'yilgan holda moddiy jismda qayd etilgan axborot himoyalaniishi kerak.

Ammo jamiyatning avtomatlashtirishning yuqori darajasiga intilishi uni foydalaniladigan informatsion texnologiyalarning havfsizligi saviyasiga bog'liq qilib qo'yadi. Xaqiqatan, kompyuter sistemalarining keng ko'lamda ishlatilishi doimo o'sib boruvchi axborotlar xajmini, ishlash jarayonlarini avtomatlashtirishga imkon bersa-da, bu jarayonlarni agressiv ta'sirlarga nisbatan ojiz qilib qo'yadi, demak, axbort texnologiyalardan foydalanuvchilar oldida yangi muammo —axborotlarni havfsizlik muammosi ko'ndalang bo'lib qoldi.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

- **maxfiylik** — aniq bir axborotga faqat tegishli shaxslar doirasigina kirishi mumkinligi, ya'ni foydalanilishi qonuniy xujjatlarga muvofiq saklab qo'yilib, hujjatlashtirilganligi kafolati. Bu bandning buzilishi o'g'irlik yoki axborotni oshkor qilish deyiladi;
- **konfidentsiallik** - ishonchliligi, tarqatilishi mumkin emasligi, mahfiyligi kafolati;
- **yaxlitlik** — axborot boshlang'ich ko'rinishda ekanligi, ya'ni uni saklash va uzatishda ruhsat etilmagan o'zgarishlar kilinmaganligi kafolati; bu bandning buzilishi axborotni soxtalashtirish deyiladi;
- **autentifikatsiya** — axborot zahirasi egasi deb e'lon qilingan shaxs haqiqatan ham axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi;
- **apellyatsiya qilishlik** — yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo'llaniladi. Kerak bo'lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yuqoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin:

- **ishonchlilik** -- tizim me'yoriy va g'ayri tabiiy hollarda rejalashtirilganidek o'zini tutishlik kafolati;
- **aniqlilik** — hamma buyruqlarni aniq va to'liq bajarish kafolati;
- tizimga kirishni nazorat qilish - turli shaxs guruxlari axborot manbalariga xar hil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati;
- **nazorat qilinishi** — istalgan paytda dastur majmuasining hoxlagan qismini to'liq tekshirish mumkinligi kafolati;
- **identifikatsiyalashni nazorat qilish** — hozir tizimga ulangan mijoz aniq o'zini kim deb atagan bo'lsa, aniq o'sha ekanligining kafolati;
- **qasddan buzilishlarga to'sqinlik** — oldindan kelishilgan me'yorlar chegarasida qasddan xato kiritilgan ma'lumotlarga nisbatan tizimning oldindan kelishilgan holda o'zini tutishi.

Axborotni himoyalashning maqsaddari quyidagilardan iborat:

- axborotning kelishuvsiz chiqib ketishi, ugirlanishi, yo'qotilishi, o'zgartirilishi, soxtalashtirilishlarning oldini olish;
- shaxs, jamiyat, davlat xavfsizligiga bo'lgan havf-xatarning oldini olish;
- axborotni yo'q qilish, o'zgartirish, soxtalashtirish, nusxa ko'chirish, to'siqdash bo'yicha ruxsat etilmagan harakatlarning oldini olish;
- hujjatlashtirilgan axborotning miqdori sifatida huquqiy tartibini ta'minlovchi, axborot zahirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko'rinishlarining oldini olish; .
- axborot tizimida mavjud bo'lgan shahsiy ma'lumotlarning shahsiy maxfiyligini va konfidentsialligini saqlovchi fuqarolarning konstitutsion huquqlarini ximoyalash;
- davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidentsialligini saklash;
- axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chiqish va qo'llashda sub'ektlarning huquqlarini ta'minlash.

Avtomatlashtirilgan axborot tizimlarida himoyalash zaruriyati.

Axborot-kommunikatsiyalar texnologiyalarining ommaviy ravishda qoʻgʻozsiz avtomatlashtirilgan asosida boshqarilishi sababli axborot xavfsizligini taʼminlash murakkablashib va muhimlashib bormoqda. Shuning uchun ham avtomatlashtirilgan axborot tizimlarida axborotni ximoyalashning yangi zamonaviy texnologiyasi paydo boʻlmoqda. DataQuest kompaniyasining maʼlumotiga kura, 1996—2000 yillarda axborot himoyasi vositalarining sotuvdagi hajmi 13 mlrd. AQSh dollariga teng boʻlgan.

Axborotni ximoyalash tizimi.

Axborotning zaif tomonlarini kamaytiruvchi va axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yoʻqolishiga toʻsqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi — axborotni ximoyalash tizimi deyiladi.

Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning kimmatliligi, uning yoʻqotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi hamda tizimning turini, ximoyalash usullar va vositalarini aniqlashlari zarur. Axborotning qimmatliligi va talab qilinadigan ximoyaning ishonchliligi bir-biri bilan bevosita bogliq. Himoyalash tizimi uzluksiz, rejali, markazlashtirilgan, maqsadli, aniq, ishonchli, kompleksli, oson mukammallashtiriladigan va koʻrinishi tez oʻzgartiriladigan boʻlishi kerak. U odatda barcha ekstremal sharoitlarda samarali boʻlishi zarur.

Tashkilotlardagi axborotlarni ximoyalash.

Axborot hajmi kichik boʻlgan tashkilotlarda axborotlarni ximoyalashda oddiy usullarni qoʻllash maqsadga muvofiq va samaralidir. Masalan, oʻqiladigan qimmatbaho qogozlarni va elektron hujjatlarni aloxida guruxlarga ajratish va niqoblash, ushbu xujjatlar bilan ishlaydigan xodimni tayinlash va oʻrgatish, binoni qoʻriqlashni tashkil etish, xizmatchilarga qimmatli axborotlarni tarqatmaslik majburiyatini yuklash, tashqaridan keluvchilar ustidan nazorat qilish, kompyuterni himoyalashning eng oddiy usullarini qoʻllash va hokazo. Odatda, himoyalashning eng oddiy usullarini qoʻllash sezilarli samara beradi.

Murakkab tarkibli, kup sonli avtomatlashtirilgan axborot tizimi va axborot hajmi katta bo'lgan tashkilotlarda axborotni ximoyalash uchun himoyalashning majmualiy tizimi tashkil kilinadi. Lekin ushbu usul hamda ximoyalashning oddiy usullari xizmatchilarning ishiga haddan tashqari xalaqit bermasligi kerak.

Himoyalash tizimining kompleksligi.

Himoya tizimining kompleksligiga unda huquqiy, tashkiliy, muhandis-texnik va dasturiy-matematik elementlarning mavjudligi bilan erishiladi. Elementlar nisbati va ularning mazmuni tashkilotlarning axborotni himoyalash tizimining o'ziga xosligini va uning takrorlanmasligini hamda buzish qiyinligini ta'minlaydi. Aniq tizimni kup turli elementlardan iborat, deb tasavvur qilish mumkin. Tizim elementlarining mazmuni nafaqat uning o'ziga xosligini, balki axborotning qimmatligini va tizimning qiymatini hisobga olgan holda belgilangan himoya darajasini aniqlaydi. Axborotni huquqiy himoyalash elementi himoyalash choralarining haqli ekanligi ma'nosida tashkilot va davlatlarning o'zaro munosabatlarini yuridik mustahkamlash hamda personalning tashkilot kimmatli axborotini ximoyalash tartibiga rioya kilishi va ushbu tartibni buzilishida javobgarligi tasavvur kilinadi.

Axborotlarni tashkiliy himoyalash elementlari.

Himoyalash texnologiyasi personalni tashkilotning kimmatli axborotlarini ximoyalash qoidalariga rioya qilishga undovchi boshqarish va cheklash xarakteriga ega bo'lgan chora-tadbirlarni uz ichiga oladi. Tashkiliy ximoyalash elementi boshqa barcha elementlarni yagona tizimga boglovchi omil bo'lib xisoblanadi. Ko'pchilik mutaxassislarning fikricha, axborotlarni ximoyalash tizimlari tarkibida tashkiliy himoyalash 50—60 % ni tashkil qiladi. Bu hol ko'p omillarga bog'liq, jumladan, axborotlarni tashkiliy himoyalashning asosiy tomoni amalda ximoyalashning printsipi va usullarini bajaruvchi personalni tanlash, joylashtirish va o'rgatish xisoblanadi. Axborotlarni himoyalashning tashkiliy chora-tadbirlari tashkilot xavfsizligi xizmatining me'yoriy uslubiy xujjatlarida uz aksini topadi. Shu munosabat bilan ko'p hollarda yuqorida ko'rilgan tizim elementlarining yagona nomi — axborotni tashkiliy-huquqiy

ximoyalash elementini ishlatadilar. Axborotlarni muxandis-texnik ximoyalash elementi - texnik vositalar kompleksi yordamida hudud, bino va qurilmalarni qo'riqlashni tashkil qilish hamda texnik tekshirish vositalariga qarshi sust va faol kurash uchun muljallangan. Texnik ximoyalash vositalarining narxi baland bulsada, axborot tizimini ximoyalashda bu element muhim ahamiyatga ega. Axborotni himoyalashning dasturiy-matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saklanadigan kimmatli axborotlarni ximoyalash uchun muljallangan.

Shuning uchun «Kompyuter tizimlari va tarmoqlarida axborotni himoyalash» kursini o'qitishdan maqsad:

1. Axborotlarni uzatishda xavfsizlikni ta'minlashga qo'yiladigan talablarni bevosita quyidagi atamalardan aniqlash mumkin: konfidentsiallik, autentifikatsiya, yaxlitlikni saqlash, yolg'onning mumkin emasligi, foydalanuvchanlik, foydalanuvchanlikni boshqarish.
2. Ko'p xollarda yaratuvchi e'tiboridan chetda qolgan himoya sistemasining kamchiliklarini aniqlash maqsadida muammoga qarshi tomonning nuqtai nazaridan qarash lozim. Boshqacha aytganda, himoyaning u yoki bu mexanizmi yoki algoritmini yaratishda mumkin bo'lgan qarshi choralarni ham ko'rish lozim.
3. Himoya vositalaridan barcha qarshi choralar majmuasini xisobga olgan xolda foydalanish lozim.
4. Xavfsizlikni ta'minlash choralari sistemasi yaratilganidan so'ng bu choralarni qachon va qaerda qo'llash masalasini yechish lozim. Bu fizikaviy joy (ma'lum himoya vositasini qo'llash uchun tarmoq nuqtasini tanlash) yoki xavfsizlikni ta'minlovchi mantiqiy zanjirdagi joy (masalan, informatsiya uzatuvchi protokol satxi yoki satxlarini tanlash) bo'lishi mumkin.
5. Himoya vositalari, odatda, ma'lum algoritm va protokoldan farqlanadi. Ularga binoan barcha himoyadan manfaatdor informatsiyasining qandaydir qismi maxfiy bo'lib qolishi shart (masalan, shifr kaliti ko'rinishida). Bu esa, o'z navbatida, bunday maxfiy informatsiyani yaratish, taqsimlash va himoyalash metodlarini ishlab chiqish zaruriyatini tug'diradi.

Internetda informatsion xavfsizlik.

Ma'lumki internet tarmoqlararo informatsiya almashinuvini ta'minlavchi magistiraldir. Uning yordamida dunyo bilimlar manba'iga kirish, qisqa vaqt ichida ko'plab ma'lumotlar yig'ish ishlab chiqarishning va uning texnik vositalarini masofadan turib boshqarish mumkin. Shu bilan bir qatorda internetning ushbu imkoniyatlaridan foydalanib turmoqdagi begona kompyuterlarni boshqarish ularning ma'lumotlar bazasiga kirish, nusxa ko'chirish g'arazli maqsadda turli xil viruslar tarqatish kabi noqonuniy ishlarni amalga oshirish mumkin. Internetda mavjud bo'lgan ushbu xavf, informatsion xavfsizlik muammolari bevosita tarmoqlarning xususiyatlaridan kelib chiqadi.

Bizning oldingi paragraflarda qayd etib o'tganimizdek ixtiyoriy tarmoq xizmatini o'zaro kelishilgan qoida (protokol) asosida ishlovchi juftlik «Server» va «Mijoz» dastur ta'minoti bajaradi. Ushbu protokollar miqyosida ham «Server», ham «Mijoz» dasturlari ruxsat etilgan amallarini (operatsiya) bajarish vositalariga ega. Masalan, NTTR protokoldagi formatlash komandalarini Web sahifalarida joylashtirilgan tovush, video animatsiyalar va har xil aktiv ob'ektlar ko'rinishidagi mikrodasturlar. Xuddi shunday ruxsat etilgan operatsiyalar, aktiv ob'ektlardan foydalanib internetda ba'zi bir noqonuniy harakatlarni oshirish tarmoqdagi kompyuterlarga va ma'lumotlar ba'zasiga kirish hamda ularga tahdid solish mumkin bo'ladi.

Bu xavf va tahdid nimalardan iborat:

1. Tarmoqdagi kompyuterlarga ruxsatsiz kirish va uni masofadan turib boshqarish. Ularga sizning manfaatingizga zid bo'lgan dasturlarni joylashtirish mumkin.
2. Web sahifalarida joylashtirilgan «aktiv ob'ektlar» agressiv dastur kodlari bo'lib, siz uchun xavfli virus yoki josus dastur vazifasini o'tashi mumkin.
3. Internetda uzatilayotgan ma'lumotlar yo'l yo'lakay aloqa kanallari yoki tarmoq tugunlarida tutib olinishi ulardan nusxa ko'chirilishi, almashtirilishi mumkin.
4. Davlat muassasasi, korxona faoliyati, moliyaviy ahvoli va uning xodimlari haqidagi ma'lumotlarni razvedka qilinishi o'g'irlashi va shu orqali sizning shaxsiy hayotingizga, korxona rivojiga tahdid solishi mumkin.

5. Internetda e'lon qilinayotgan har qanday ma'lumot ham jamiyat uchun foydali bo'lmasligi mumkin, ya'ni internet orqali bizning ma'naviyatimizga, madaniyatimizga va e'tiqodimizga zid bo'lgan informatsiyalarni kirib kelishi ehtimoli ham mavjud.

Internet foydalanuvchisi ushbu xavflarni oldini olish uchun quyidagi texnik yechim va tashkiliy ishlarni amalga oshirishi zarur:

1. Shaxsiy kompyuterga va mahalliy kompyuter tarmog'iga hamda unda mavjud bo'lgan informatsion resurslarga tashqaridan internet orqali kirishni cheklovchi va ushbu jarayonni nazorat qilish imkonini beruvchi texnik va dasturviy usullardan foydalanish.
2. Tarmoqdagi informatsion muloqat ishtirokchilari va ular kuzatayotgan ma'lumotlarni asl nusxasiga mosligini tekshirish.
3. Ma'lumotlarni uzatish va qabul qilishda kriptografiya usullaridan foydalanish
4. Viruslarga qarshi nazoratchi va davolovchi dasturlardan foydalanish.
5. Shaxsiy kompyuter va mahalliy kompyuter tarmog'iga begona shaxslarni qo'ymaslik va ularda mavjud bo'lgan ma'lumotlardan nusxa olish imkoniyatlarini cheklovchi tashkiliy ishlarni amalga oshirish.

Bundan tashqari informatsion xavfsizlikni ta'minlash borasida internet foydalanuvchilari orasida o'rnatilmagan tartib qoidalar mavjud. Ulardan ba'zi birlarini keltiramiz:

- Hech qachon hech kimga internetdagi o'z nomingiz va parolingizni aytman.
- Hech qachon hech kimga o'zingiz va oila a'zolaringiz haqidagi shaxsiy hamda ishxonangizga oid ma'lumotlarni internet orqali yubormang.
- Elektron manzilingiz (*E-mail*)dan maqsadli foydalaning. Internet orqali dasturlar almashmang.
- Internetda tarqatilayotgan duch kelgan dasturlardan foydalanmang. Dasturlarni faqat ishonchli egasi ma'lum bo'lgan serverlardan ko'chiring.
- Elektron pochta orqali yuborilgan «aktiv ob'ektlar» va dasturlarni ishlatmang, yoki qo'shimchali o'z-o'zidan ochiluvchi sizga noma'lum arxiv holidagi ma'lumotlarni ochmang.
- Elektron pochta xizmatidan foydalanayotganingizda ma'lumotlarni shifrlash zarur, ya'ni kriptografiya usullaridan foydalaning.

- Egasi siz uchun noma'lum bo'lgan xatlarni ochmang.
- Egasi ma'lum bo'lgan va uning sifatiga kafolat beruvchi antivirus dasturlardan foydalaning va ularni muntazam yangilab boring.
- Internetda mavjud bo'lgan informatsion resurslar va dasturlardan ularning mualliflari ruxsatisiz foydalanmang.
- Tarmoqdagi begona kompyuter va serverlarning IP manzillarini aniqlash va shu orqali ruxsat etilmagan serverlar va informatsion resurslarga kirish nusxa ko'chirish, viruslar tarqatish kabi noqonuniy dasturlashtirish ishlari bilan shug'ullanmang, bu jinoyatdir.

Axborotni himoyalash tizimi

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

Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo'qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan xolda axborotni himoyalashning zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalarini aniqlashlari zarur. Axborotning qimmatliligi va talab qilinadigan himoyaning ishonchliligi bir-biri bilan bevosita bog'liq. Himoyalash tizimi uzluksiz, rejali, markazlashtirilgan, maqsadli, aniq, ishonchli, kompleksli, oson mukammallashtiriladigan va ko'rinishi tez o'zgartiriladigan bo'lishi kerak. U odatda barcha ekstremal sharoitlarda samarali bo'lishi zarur.

Buning uchun boshidan shart belgilaymiz. Birinchidan, faraz qilaylikki bizda xaqiqattan baxoga ega axborot bor bo'lishi kerak. Ikkinchidan, shu axborotga himoya sistemasini o'rnatish uchun biz aql bilan sarf-xarajatga tayyormiz. Bu maqsad uchun biz optimal himoyalash usullarini tanlashimiz kerak, lekin u maksimal xizmat qilishi kerak.

Zamonaviy firmaning xayoti maxalliy tarmoqsiz mumkin emas. Ya'ni bu o'tarmoq qollanuvchi qaerda bolishidan qat'iy nazar axborot almashuvini ta'minlab beradi. Xar bir

firmaning ish faoliyatining xavfsizligini ta'minlash uchun himoyalash tizimi ishlab chiqiladi.

Maxalliy tarmoqda ishlab chiqilgan axborot nixoyatda nozik bo'ladi. Tarmoqda axborotga ruxsatsiz kirish yoki turlash, yolg'on ma'lumot berishlarni keltirib chiqarishda xozirgi kunda quyidagi sabablar mavjud:

- Kompyuterda saqlanayotgan, uzatilayotgan yoki ishlab chiqiladigan axborotlar xajmining kengayishi;
- Ma'lumotlar bazasiga muximligi va maxfiligi xar hil axborotlarning kiritilishi;
- Axborotdan foydalanuvchilarning imkoniyat doirasining kengayishi;
- Masofadagi ish joylarining soni ko'payishi;
- Internet tarmog'ida ishlovchilarning ko'payishi;
- Kompyuter qo'llanuvchilari orasida axborot almashuvining avtomatizatsiyalanishi;

Xar bir himoya tizimini o'rnatganda quyidagi savollarga javob beramiz:

1. Nimani himoyalaymiz?
2. Kimdan yoki nimadan himoyalanamiz?
3. Qanaqa himoya o'rnatamiz?

Birinchi etap. Nimani himoyalash kerak.(Maxalliy tarmoq modeli)

Xar bir maxalliy tarmoqning asosiy vazifasi, kerakli axboratni qisqa vaqt ichida qo'llanuvchiga yetkazishdir. Shuning uchun axborotni himoyalashni ta'minlash muammosini xal qilishda buni ahamiyatga olish kerak. Axborot himoyalash usullarini ishlab chiqqanda, himoya tizimi xalaqit bermasligi kerak, aksincha, asosiy funktsiya - axborot almashuvini ta'minlashda yordam berishi shart. Shuning uchun himoyalash tizimining modelini ishlab chiqishda, maxalliy tarmoqning modelini yaxshi bilish kerak. Buning uchun maxalliy tarmoqning modeli - ya'ni undagi bajariladigan asosiy funtsiyalar va barcha elementlar yig'indisini aniqlab olamiz.

Asosiy xavf bu maxalliy tarmoqda ishlanayotgan axborotga qaratilgan. Axborot esa – dasturiy ta'minot yordamida ishlanadi. Shuning uchun xar bir maxalliy tarmoqning negizi bu umumiy tizimli dasturiy ta'minot bo'lib, unga operatsion tizimlar, dasturiy qobiqlar, umumiy ishlash uchun dasturlar, matnli protsessorlar, taxrirlovchilar, ma'lumotlar bazasini boshqarish tizimlari kiradi. Bulardan tashqari, axborotni ishlab chiqishda amaliy dasturiy ta'minot foydalaniladi, ya'ni mutaxassislangan masalalarni yechishda qo'llaniladi.

Axborotni ishlab chiqishda texnik moslamalar ham foydalaniladi. Axborot avtomatlashtirilgan ish joylaridan ichki va tashqi aloqa kanallari orqali tushishi mumkin. Bunda axborotni klaviatura yoki tashqi axborot tashuvchilari orqali kiritish mumkin. Bulardan tashqari boshqa tashkilotlarning axborot resurslari va global telekommunikatsion tarmoq resurslaridan foydalanish mumkin. Global telekommunikatsion tarmoqlari axborotni foydalanuvchiga yetkazishda transport xizmatini bajaradi.

«Maxalliy tarmoq foydalanuvchisi» tushunchasi – bu belgilangan tartib bo'yicha ro'yxatdan o'tgan va tarmoqni foydalanishda aniq bir xuquqqa ega shaxsga (tashkilotga) aytiladi. O'zinig xuquq doirasida qo'llanuvchi ruxsat berilgan xarakatlarga ega.

Tarmoqdagi axborot tizim administratori nazorati ostida ishlab chiqiladi, uni himoyalash xavfsizlik administratori bo'ynidagi vazifa. Tarmoqning ish xolatini saqlash uchun, amaliy dasturiy ta'minotni ishlab chiqish uchun mutaxasis – dasturchilar va texnik shaxslar jalb qilinadi. Ular ham axborotga cheklangan xuquqlari bor, lekin dasturiy ta'minotni o'zgartirishda va axborotni ishlab chiqish protsessiga cheklanmagan ta'sir ko'rsatishi mumkin.

Maxalliy tarmoqni tizim ko'rinishda olish mumkin. Bu tizim quyidagi ichki tizimlardan – boshqaruvchining ish joyi, masofadagi ish joyi, xavsizlik va tizim administratorlarining ish joylaridan tashkil topgan. Buning xar biri mustaqil ichki tizimlar. Shuning uchun axborotni himoyalashda – dekompozitsiya printsipi qo'llaniladi.

Ikkinchi etap. Kimdan yoki nimadan himoyalash kerak. (xavfsizlik xavflarining modeli)

Axborotni himoyalash savollariga qaratilgan adabiyotlarda xar hil variantli axborot xavfsizligining xavflari modelini topish mumkin. Bunda ixtiyoriy modeldan foydalanish mumkin, lekin u axborot xavfsizligiga ta'sir etish faktorlarining maksimal sonini ko'rsatish kerak.

Axborot xavfsizligining xavflari deganda nima tushuniladi? Bu – himoya ob'ektiga qarshi qaratilgan xarakat. Bunda tijorat baxoga ega yoki maxfiy axborot bo'lishi mumkin.

Axborot xavfsizligining xavflarini keltirib chiqarish omillari, ichki va tashqi bo'lishi mumkin. Bunday taqsimlanish sababi, bir hil xavfga ichki va tashqi omillarga qarab xar hil usul (parirovaniya) qo'llaniladi.

Demak, shulardan kelib chiqqan xolda axborot xavfsizligining xavflari 3-ta asosiy guruxlarga bo'linadi:

- Sub'ekt ta'siridagi xavflar (antropogen xavf);
- Texnik vositalar ta'siridagi xavflar (texnogen xavf);
- Tabiat ofatlari xavflari;

A) Birinchi gurux nixoyatta keng tarqalgan. Axborot xavfsizligining buzilishiga sababchi tashqi sub'ektlar:

- Kriminal struktura;
- Retsidivistlar va potentsial jinoyatchilar;
- Vijdonsiz hamkorlar;
- Konkurentlar;
- Siyosiy dushmanlar;

ichki sub'ektlar:

- Tashkilot xodimi;
- Filial xodimi;
- Aqli zaif shaxslar;
- Maxsus agentlar;

Bulardan kelib chiqadigan oqibatlar qoyidagilar:

I. O'g'irlik.

- a) Texnik vositalarni (vinchestr, noutbuk, sistema bloki);
- b) Axborot tashuvchilarni (qog'ozdagi, magnitli, optikali);

- v) Axborotlarni (o'qish va ruxsatsiz nusxa olish);
- g) Foydalanuvchanlikni boshqarish (kalit, parollar);

II. Almashtirish (turlash)

- a) Operatsion tizimni;
- b) Ma'lumotlar bazasini boshqarish tizimini;
- v) Amaliy dasturlarni;
- g) Axborotni;
- d) Foydalanuvchanlikni boshqarish

III. Yo'qotish (buzish)

- a) Texnik vositalarni (vinchestr, noutbuk, sistema bloki);
- b) Axborot tashuvchilarni (qog'ozdagi, magnitli, optikali);
- v) Dasturiy ta'minotni (OS, SUBD, amaliy dasturiy ta'minot);
- g) Axborotni (fayl, ma'lumot);
- d) Parollarni;

IV. Normal ishning buzilishi (uzilish)

- a) Axborotni ishlab chiqish tezligining kamayishi;
- b) Aloqa kanallarining o'tqazish imkoniyatlari;
- v) Operativ xotira xajmi;
- g) Diskdagi fazoning xajmi;
- d) Texnik vositalarning elektr bilan ta'minlanishi;

V. Xatoliklar

- a) DT, OT, SUBD larni o'rnatishda;
- b) Amaliy DT yozishda;
- v) DT ekspluatatsiyasida;
- g) Texnik vositalarning ekspluatatsiyasida;

VI. Axborotni tutib qolish (ruxsat berilmagan)

B) Ikkinchi gurux texnikaning xususiyatlariga bog'liq. Axborot xavfsizligi xavflarining texnik vositalari ham ichki va tashqi bo'lishi mumkin:

Ichki:

- Axborotni ishlab chiqishdagi sifatsiz texnik vositalar;
- Axborotni ishlab chiqishdagi sifatsiz dasturiy vositalar;
- Yordamchi vositalar (qoriqlash, signalizatsiya, telefon);
- Tashkilotda foydalanadigan boshqa texnik vositalar;

Tashqi:

- Aloqa vositalari;
- Yaqin atrofdagi xavfli ishlab chiqaruvchilar;
- Muxandislik kommunikatsiya tarmog'i (energo, suv, kanalizatsiya);
- Transport;

Bulardan kelib chiquvchi oqibatlar quyidagilar:

I. Normal ishning buzilishi

- Axborotni ishlab chiqish tizimining ishlashi buzilishi;
- Aloqa va telekommunikatsiya ishining buzilishi;
- Axborot tashuvchilarning eskirishi;
- Belgilangan foydalanuvchanlikni boshqarishning shartlarining buzilishi;
- Texnik vositalarga elektromagnit ta'sir korsatish;

Yo'qotish

- DT, OT, SUBD;
- Axborotni ishlab chiqish vositalari (broski napryajeniya, protechki);
- Bino;
- Axborot (radiatsiya, protechki);
- Ishchi xodim;

II. Turlash

- DT, OT, SUBD;
- Aloqa kanali va telekommunikatsiyada uzatilayotgan axborot;

Kompyuter tizimlari va tarmoqlaridagi xavf-qatar va xujum turlari, xujumlarni aniqlash va taxlil qilish.

Ma'lumki, kompyuter tizim (tarmog')ining asosiy komponentlari -- texnik vositalari, dasturiy-matematik ta'minot va ma'lumotlardir. Nazariy tomondan bu komponentlarga nisbatan to'rt turdagi xavflar mavjud, ya'ni uzilish, tutib qolish, o'zgartirish va soxtalashtirish:

—**uzilish** — qandaydir tashqi xarakatlar (ishlar, jarayonlar)ni bajarish uchun hozirgi ishlarni vaqtincha markaziy protsessor qurilmasi yordamida to'xtatishdir, ularni bajargandan so'ng protsessor oldingi xolatga qaytadi va to'xtatib qo'yilgan ishni davom ettiradi. Xar bir uzilish tartib raqamiga ega, unga asosan markaziy protsessor qurilmasi qayta ishlash uchun qism dasturni qidirib topadi. Protsessorlar ikki turdagi uzilishlar bilan ishlashni vujudga keltirishi mumkin: dasturiy va texnik. Biror qurilma favqulodda xizmat koo'satilishiga muxtoj bo'lsa, unda texnik uzilish paydo boladi. Odatda bunday uzilish markaziy protsessor uchun kutilmagan xodisadir. Dasturiy uzilishlar asosiy dasturlar ichida protsessorning maxsus buyruklari yordamida bajariladi. Dasturiy uzilishda dastur o'z-o'zini vaqgincha to'xtatib, uzilishga taallukli jarayonni bajaradi.

— **tutib olish** — jarayoni oqibatida g'arazli shaxslar dasturiy vositalar va axborotlarning turli magnitli tashuvchilariga kirishni qo'lga kiritadi. Dastur va ma'lumotlardan noqonuniy nusxa olish, kompyuter tarmoqlari aloka kanallaridan nomualliflik o'qishlar va xokazo xarakatlar tutib olish jarayonlariga misol bola oladi.

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

—**soxtalashtirish** — ham jarayon sanalib, uning yordamida g'arazli shaxslar tizimda xisobga olinmagan vaziyatlarni organib, undagi kamchiliklarni aniklab, keyinchalik oziga kerakli xarakatlarni bajarish maqsadida tizimga qandaydir soxta jarayonni yoki tizim va boshqa foydalanuvchilarga soxta yozuvlarni yuboradi.

Yukorida keltirilgan buzilishlar passiv va aktiv xujum atamallari bo'yicha klassifikatsiyalanganida passiv taxdidga ushlab kolish (perexvat) mansub bo'lsa, uzish (raz'edinenie), turlash (modifikatsiya) va soxtalashtirish (falsifikatsiya) aktiv taxdidga mansub ekanligini ko'rish qiyin emas.

Passiv xujumlar natijasida uzatilayotgan ma'lumotlar ushlab kolinadi yoki monitoring amalga oshiriladi. Bunda buzgunchining maksadi uzatilayotgan informatsiyani ushlab kolishdir. Passiv buzilishlarni ikkita guruxga ajratish mumkin — axborotlar mazmunini fosh etish va ma'lumotlar oqimini taxlil etish. Axborotlar mazmunini fosh etish nima ekanligi ma'lum. Telefon orkali suxbatda, elektron pochta axborotida yoki uzatilayotgan faylda muxim yoki maxfiy informatsiya bo'lishi mumkin. Tabiiyki, bunday informatsiya bilan bu informatsiya mo'ljallanmagan shaxslarning tanishishi maqbul emas. Ma'lumotlar oqimining taxlili mukammalrok xisoblanadi. Faraz kilaylik, biz axborot yoki boshka uzatiluvchi ma'lumotlar mazmunini shunday nikoblaylikki, buzguvchi axborotni uz ixtiyoriga kiritganida ham undagi informatsiyani chiqarib ololmasin. Ko'pincha axborot mazmunini nikoblashda shifrlash qo'llaniladi. Ammo axborot mazmuni shifrlash yordamida ishonchli tarzda berkitilgan bo'lsada, buzgunchida uzatiluvchi ma'lumotlarning o'ziga xos alomatlarini kuzatish imkoniyati qoladi. Masalan, uzatuvchini va axborotlarni uzatishga ishlatiluvchi uzellarni, axborotlar uzunligini va ularning almashinuv chastotasini aniklash mumkin. Bunday informatsiya ma'lumotlar almashinuvidan ko'zlangan maksadni aniklashda juda ham qo'l keladi. Himoyaning passiv buzilishlarini aniklash juda kiyin, chunki ularda ma'lumotlarga kandaydir o'zgartirishlar kiritish ko'zda tutilmaydi. Ammo bunday hil buzilishlarning oldini olishni amalga oshirsa bo'ladi. Shu sababli passiv buzilishlar xolida e'tiborni ularni aniklashga emas, balki ularning oldini olishga karatish lozim.

Aktiv xujumlar natijasida ma'lumotlar okimi uzgartiriladi yoki soxta okimlar xosil qilinadi. Bunday buzilishlarni to'rtta guruxga ajratish mumkin: imitatsiya, tiklash, axborotni turlash (modifikatsiyalash), xizmat ko'rsatishdagi xalallar.

Imitatsiya deganda, ob'ektning o'zini boshka ob'ekt qilib ko'rsatishi tushuniladi. Odatda, imitatsiya aktiv buzilishlarning boshka bir hilining urinishi bilan birgalikda bajariladi. Masalan, buzgunchi sistemalar qalmashinayotgan autentifikatsiya ma'lumotlarining

okimini ushlab qolib soʻngra autentifikatsiya axborotlarining xakikiy ketma-ketligini tiklashi mumkin. Bu esa vakolati chegaralangan obʻektning oʻzini vakolati kengroq obʻekt qilib koʻrsatishi (imitatsiya) orkali vakolatini kengaytirishga imkon beradi.

Tiklash deganda, maʼlumotlar blokini passiv ushlab qolib, keyin uni ruxsat berilmagan natijani xosil qilish maksadida retranslyatsiya qilish tushuniladi.

Maʼlumotlarni modifikatsiyalash deganda, ruxsat berilmagan natijani xosil qilish maksadida qonuniy axborot qismini oʻzgartirish yoki axborot kelishi ketma-ketligini oʻzgartirish tushuniladi.

Xizmat koʻrsatishdagi xalallar aloka yoki ularni boshkaruvchi vositalarning normal ishlashiga tuskilik kiladi. Bunday buzilishlarda muayyan maksad koʻzlanadi: masalan, obʻekt maʼlum adresatga yoʻnaltirilgan barcha axborotlarni toʻxtatib qolishi mumkin. Yana bir misol, tarmoqni atayin axborotlar oqimi bilan ortiqcha yuklash orqali yoki tarmoqni ishdan chiqarish yuli bilan barcha tarmoq ishini blokirovka qilish.

Himoyaning aktiv buzilishlarini butunlay oldini olish juda murakkab, chunki bunga fakat barcha aloka vositalarini uzluksiz fizik himoyalash orqali erishish mumkin. Shu sababli himoyaning aktiv buzilishlarida asosiy maksad ularni operativ tarzda aniklash va tezda sistemaning ishga layokatligini tiklash boʻlishi shart. Buzilishlarning oʻz vaktida aniklanishi buzgunchini toʻxtatish vazifasini ham oʻtaydi va bu vazifani buzilishlardan ogoxlantirish sistemasining kismi deb koʻrish mumkin.

Xujumlarni aniklovchi tizim nima?

Xozirgi kompyuter tarmoqlarida maʼlumotlarni himoya qilish muammolari ilgari xisoblash markazlaridan bajariladigan masalalaridan juda katta fark kiladi, yaʼni ilgari xisoblash markazlarini uzida xar hil maʼmuriy yullar bilan maʼlumotlarni himoya qilinari edi.

Bularga misollar juda kup.

1. EXMlarda fakat ruxsati bulgan kishilar ishlashi mumkin edi.
2. EXM zallariga kirish man etilgan edi. Fakat operatorlar yoki boshka ishchilar ishchilar ishlar edi.

3. Magnit lentalar, magnit disk, magnit barabanlarida joylashgan ma'lumotlar xar oyi qayta yozilib, yangilanib turilar edi

4. Xisoblash markazlari korovullar bilan muxofaza etiladi va xokazo.

Ilgari, yaqin kunlarga koorparativ tarmoqlarni himoya etish mexanizmi asosan firewall nomli tarmoqlar ekrani edi. Ya'ni tarmoqlardagi butun chiqayotgan va kirayotgan ma'lumotlarni filtrdan utkazilar edi.

Xozirgi kunda bu usullar uzini oklamay koldi. Ayniksa, ma'lumotlar ayirboshlash jarayoni juda kuchayib ketgan paytlarda tarmoqlararo filtrlari tuskin bulib tizimlarning mexnat unumdorligini tushurib yubordi. Shuning uchun ushbu filtrlarni olib tashlash va xujumlarni vaktida aniklab himoya kilish usullarini ishlab chiqish tugri deb topildi.

Bundayaktiv himoya kilish sistemalari sutkasiga 24 soat, xaftasiga 7 kun va yiliga 365 kun tuxtovsiz ishlaydigan bulishi kerak.

Real Secure tizimi nima?

Kompyuter tarmoqlarida xujum kiluvchilarni aniklab beruvchi Real Secure tizimi amerikadagi Internet Security System kompaniyasi tomonidan ishlab chiqilgan. Ushbu tizim (kurilma)-intellektual analizatordan iborat bulib kelayotgan ma'lumot paketlarini taxliletib xujumlarni aniklaydi. Bu sistema real vakt masshtabida ishlab tarmoqdagi ma'lumot paketlarini taxliletadi va tarmoqning bir segmentidagi ma'lumotlarni himoya kiladi.

Xujum bulayotganligi aniklangan xolda elektron pochta yoki konsol orkali ma'muriyat boshkaruvchiga ma'lumot beriladi. Shu bilan birgalikda ma'lumotlar ba'zasiga xujum tugrisida yozib kuyiladi va kerak bulgan paytda taxliletiladi. Agar qilinayotgan xujum sizning kompyuter tizimingizni ishdan chiqarishi mumkinligi aniklandi, avtomatik ravishda xujum etuvchi bilan aloka uziladi va marshrutizator keyingi boglanishlikni takiklaydi. Ushbu Real Secure sistemasi kompyuter tarmog'ining ichidagi hamda tashkarida kelayotgan xavfni aniklaydi va himoya kiladi.

Real Secure sistemasi tarkalgan arxitektura asosida ishlaydi va 2 ta asosiy komponentdan iboratdir, ya'ni Real Secure Detector va Real Secure Manager. Birinchi komponent kompyuter tarmogida xosil bulayotgan xujumlarni aniklaydi. U moduldan ya'ni

tarmok va sistemali agentlardan tashkil topgan. Tarmok agenti kompyuter ma'lumotlarining almashuvida bulayotgan xodisalar asosida xavf borligini aniklab beradi. Sistemali agent esa tekshirilaetgan tarmoq tuguniga ulanib, xujum bulaetganligi tugrisida xabar beradi. Ikkinchi komponent, ya'ni Real Secure Manager koipONENTI ma'lumotlarini detektordan yigish va sozlash ishlariga javob beradi.

Real Secure sistemasining kobiliyati kuyidagicha:

- a) Aniklovchi xujumlarning sonini kupligi;
- b) Nazorat etish modularini markazlashgan xolda boshkarish;
- c) Juda kup tarmok protokollarini filtrlash va taxlil kilish (TEP, UDP, IEMP);
- d) Xujumlarga xar xil variantlar asosida ta'sir etish;
- e) Xujum kilaetgan tugun bilan alokani uzish;
- f) Tarmok ekranlari va marshrutizarotlarni bomtkarish;
- g) Xar bir xujumni kayta kurib chikish va taxlil etish uchun yezib olish;
- h) Ethernet, Fast Ethernet va Token Ring tarmok interfeyslarida ishlashni ta'minlash;
- i) Maxsus uskunalar talab etmasligi;
- j) Tarmok unumdorligini pasaytirmaslik;
- k) Xisobot tarmoklarining xar xilligi;
- l) Uskunaviy va dasturiy ta'minotlarga talablarning balandmasligi va xokazo.

Xujumlarga e'tiroz etishning xar xil variantlari aniklangan xujumlarga e'tiroz etish variantlari kuyidagicha:

- a. Xujum xakida kayd etuvchi ruyxatga olish
- b. Ma'muriyatni elektron pochta yeki boshkaruv konsuli orkali ogoxlantirish
- c. Xujum kilaetgan tarmok tugunini avariya sifatida uzib kuyish
- d. Kilingan xujumlarinikurib chikish va taxlil etish uchun yezib olish
- e. Tarmoklararo ekranlarni va marshrutizatorlarni tarmok kurinishini uzgartirish va xokazolar

Uskunaviy va dasturni ta'minotlarga kuyilgan asosiy talablari

Uskunaviy ta'minot talablari:

- Protessor – Pentium Pro 200 MGts (eki Pentium II 300 MGts);
- OZU – 64 MB yeki 128 MB
- NJMT (kattik) disk – 100 MB kam bulmagan xotira (ma'lumotlar bazasi va ruyxat turlari uchun)
- Tarmok interfeysi - Ethernet, Fast Ethernet, Token Ring, FDDI

Kompyuter tizimlari va tarmoqlarida axborotni himoyalashning tashkiliy vositasi.

Axborot xajmi kichik bolgan tashkilotlarda axborotlarni himoyalashda oddiy usullarni qollash maq-sadga muvofiq va samaralidir. Masalan, oqiladigan qimmatbaxo qogozlarni va elektron xujjatlarni aloxida guruxlarga ajratish va niqoblash, ushbu xujjatlar bilan ishlaydigan xodimni tayinlash va orgatish, binoni qoriklashni tashkil etish, xizmatchilarga qim-matli axborotlarni tarqatmaslik majburiyatini yuklash, tashqaridan keluvchilar ustidan nazorat qilish, kompyuterni himoyalashning eng oddiy usullarini qollash va xokazo. Odatda, himoyalashning eng oddiy usullarini qollash sezilarli samara beradi.

Murakkab tarkibli, kup sonli avtomatlashtirilgan axborot tizimi va axborot xajmi katta bolgan tashkilotlarda axborotni himoyalash uchun himoyalashning majmuali tizimi tashkil qilinadi. Lekin ushbu usul hamda xdmoyalashning oddiy usullari xizmatchilarning ishiga xaddan tashqari xalaqit bermasligi kerak.

Himoyalash tizimining kompleksligi

Himoya tizimining kompleksligiga unda xuquqiy, tashkiliy, muxandistexnik va dasturiy-matematik elementlarning mavjudligi bilan erishiladi. Elementlar nisbati va ularning mazmuni tashkilotlarning axborotni himoyalash tizimining oziga xosligini va uning takrorlanmasligini hamda buzish qiyinligini ta'minlaydi. Aniq tizimni kup turli elementlardan iborat, deb tasavvur qilish mumkin. Tizim elementlarining mazmuni nafaqat uning oziga xosligini, balki axborotning qimmatliligini va tizimning qiymatini

xisobga olgan xolda belgilangan himoya darajasini aniqlaydi. Axborotni xuquqiy himoyalash elementi himoyalash choralarining xaqli ekanligi ma'nosida tashkilot va davlatlarning ozaro munosabatlarini yuridik mustaxkamlash hamda personalning tashkilot kimmatli axborotini himoyalash tartibiga rioya qilishi va ushbu tartibni buzilishida javobgarligi tasavvur qilinadi.

Axborotlarni tashkiliy himoyalash elementlari

Himoyalash texnologiyasi personalii tashkilotning kimmatli axborotlarini himoyalash qoidalariga rioya qilishga undovchi boshqarish va cheklash xarakteriga ega bolgan chora-tadbirlarni uz ichiga oladi. Tashkiliy himoyalash elementi boshqa barcha elementlarni yagona tizimga boglovchi omil bolib xisoblanadi. Kopchilik mutaxassislarning fikricha, axborotlarni himoyalash tizimlari tarkibida tashkiliy himoyalash 50—60 % ni tashkil qiladi. Bu xol kop omillarga bog'liq, jumladan, axborotlarni tashkiliy himoyalashning asosiy tomoni amalda himoyalashning prinsIPi va usullarini bajaruvchi personalitanlash, joylashtirish va orgatish xisoblanadi. Axborotlarni himoyalashning tashkiliy chora-tadbirlari tashkilot xavfsizligi xizmatining me'yoriy uslubiy xujjatlarida uz aksini topadi. Shu munosabat bilan kop xollarda yuqorida korilgan tizim elementlarining yagona nomi — axborotni tashkiliy-xuquqiy himoyalash elementini ishlatadilar. Axborotlarni muxandis-texnik himoyalash elementi - texnik vositalar kompleksi yordamida xudud, bino va qurilmalarni qoriklashni tashkil qilish hamda texnik tekshirish vositalariga qarshi suet va faol kurash uchun muljallangan. Texnik himoyalash vositalarining narxi baland bulsada, axborot tizimini himoyalashda bu element muxim ahamiyatga ega. Axborotni himoyalashning dasturiy-matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saklanadigan kimmatli axborotlarni himoyalash uchun muljallangan.

Kompyuter tizimlari va tarmoqlarida axborotni himoyalashning uskunaviy vositasi.

Kompyuter ma'lumotlarini himoyalashning texnik-dasturiy vositalari

1. Foydalanuvchilarni identifikatsiyalashva autentifikatsiyalash tizimi
2. Disk ma'lumotlarini shifrlash tizimi
3. Tarmoq buyicha uzatiladigan ma'lumotlarnishifrlash tizimi

4. Elektron ma'lumotlarni autentifikatsiyalash tizimi

5. Tayanch axborotlarni boshqarish vositalari

Foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash tizimi. Ushbu tizim foydalanuvchidan olingan ma'lumot boyicha uning shaxsini tekshirish, xaqiqiyligini aniqlash va shundan song unga tizim bilan ishlashga ruxsat berish lozimligini belgilab beradi.

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

- foydalanuvchiga ma'lum bolgan maxfiy axborot, masalan, parol, maxfiy kalit va boshqalar;
- shaxsning fiziologik parametrlari, masalan, barmoq izlari, kuzning tasviri va boshqalar.

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

Disk ma'lumotlarini shifrlash tizimi. Ushbu tizimning asosiy maqsadi diskdagi ma'lumotlarni himoyalashdir. Bu xolda mantiqiy va jismoniy bosqichlar ajratiladi. Mantikiy boskichda fayl asosiy ob'ekt sifatida bolib, faqatgina ba'zi bir fayllar himoyalanadi. Bunga misol kilib, arxivator dasturlarini keltirish mumkin. Jismoniy boskichda disk tolaligicha himoyalanadi. Bunga misol sifatida Norton Utilities tarkibidagi Diskreet shifrllovchi dasturni keltirish mumkin.

Tarmoq buyicha uzatiladigan ma'lumotlarni shifrlash tizimi. Ushbu tizimda ikki yonalishni ajratish mumkin:

- kanal boyicha, ya'ni aloqa kanallari buyicha junatiladigan barcha ma'lumotlarni shifrlash;
- abonentlar boyicha, ya'ni aloqa kanallari buyicha jonatiladigan ma'lumotlarning faqatgina mazmuniy kismi shifrlanib, qolgan xizmatchi ma'lumotlarni ochiq qoldirish.

Elektron ma'lumotlarni autentifikatsiyalash tizimi. Ushbu tizimda tarmoq buyicha bajariladigan elektron ma'lumotlar almashuvida xujjatni va uning muallifini autentifikatsiyalash muammosi paydo buladi.

Tayanch axborotlarni boshqarish vositalari. Ushbu tizimda tayanch axborotlar sifatida kompyuter tizimi va tarmog'ida qollaniladigan barcha krIPtografik kalitlar tushuniladi.

Bu xolda kalitlarni generatsiyalash, saklash va taqsimlash kabi boshqaruv funksiyalarini ajratishadi.

Kompyuter tizimlari va tarmoklarida axborotni ximoyalashning kriptografik vositasi.

Zamonaviy kompyuter stenografiyasi.

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

Axborotni ximoyalash uchun kodlashtirish va kriptografiya usullari qo'llaniladi.

Kodlashtirish deb axborotni bir tizimdan boshqa tizimga ma'lum bir belgilar yordamida belgilangan tartib bo'yicha utkazish jarayoniga aytiladi.

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

Stenografiyaning kriptografiyadan boshqa o'zgacha farqi ham bor. Ya'ni uning maqsadi — maxfiy xabarning mavjudligini yashirishdir. Bu ikkala usul birlashtirilishi mumkin va natijada axborotni himoyalash samaradorligini oshirish uchun ishlatilishi imkoni paydo bo'ladi (masalan, kriptografik kalitlarni uzatish uchun). Kompyuter texnologiyalari stenografiyaning rivojlanishi va mukammallashuviga yangi turtki berdi. Natijada axborotni himoyalash sohasida yangi yo'nalish — kompyuter stenografiyasi paydo bo'ldi. Global kompyuter tarmoklari va multimedia sohasidagi zamonaviy progress telekommunikatsiya kanallarida ma'lumotlarni uzatish xavfsizligini ta'minlash uchun mo'ljallangan yangi usullarni yaratishga olib keldi. Bu usullar shifrlash qurilmalarining tabiiy noaniqligidan va analogli video yoki audio-signallarning serobligidan foydalanib, xabarlarni kompyuter fayllari (konteynerlar)da yashirish imkonini beradi. Shu bilan birga kriptografiyadan farqli ravishda bu usullar axborotni uzatish faktining o'zini ham yashiradi. K.Shannon sirli

yo'zuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi xisoblanadi. Zamonaviy kompyuter stenografiyasida ikkita asosiy fayl turlari mavjud: yashirish uchun mo'ljallangan xabar-fayl, va konteyner-fayl, u xabarni yashirish uchun ishlatilishi mumkin. Bunda konteynerlar ikki turda bo'ladi: konteyner-origanal (yoki «bo'sh» konteyner) - bu konteyner yashirin axborotni saqlamaydi; konteyner-natija (yoki «tuddirilgan» konteyner) - bu konteyner yashirin axborotni saqlaydi. Kalit sifatida xabarni konteynerga kiritib kuyish tartibini aniklaydigan maxfiy element tushuniladi.

Kompyuter stenografiyasi istikbollari.

Kompyuter stenografiyasi rivojlanish tendentsiyasining taxlili shuni ko'rsatadiki, keyingi yillarda kompyuter stenografiyasi usullarini rivojlantirishga qiziqish kuchayib bormoqda. Jumladan, ma'lumki, axborot xavfsizligi muammosining dolzarbligi doim kuchayib bormokda va axborotni himoyalashning yangi usullarini kidirishga rag'batlantirilayapti. Boshqa tomondan, axborot-kommunikatsiyalar texnologiyalarining jadal rivojlanishi ushbu axborotni himoyalashning yangi usullarini joriy qilish imkoniyatlari bilan ta'minlayapti, va albatta, bu jarayonning kuchli katalizatori bo'lib umumfoydalaniladigan Internet kompyuter tarmog'ining juda kuchli rivojlanishi xisoblanadi. Hozirgi vaqtda axborotni himoyalash eng kup qo'llanilayotgan soha bu — kriptografik usullardir. Lekin, bu yulda kompyuter viruslari, «mantikiy bomba»lar kabi axborotiy qurollarning kriptovositalarni buzadigan ta'siriga bog'liq ko'p yechilmagan muammolar mavjud. Boshqa tomondan, kriptografik usullarni ishlatishda kalitlarni taqsimlash muammosi ham bugungi kunda oxirigacha yechilmay turibdi. Kompyuter steganografiyasi va kriptografiyalarining birlashtirilishi paydo bo'lgan sharoitdan qutulishning yaxshi bir yo'li bo'lar edi, chunki, bu holda axborotni himoyalash usullarining zaif tomonlarini yo'qotish mumkin. Shunday kilib, kompyuter stenografiyasi hozirgi kunda axborot xavfsizligi bo'yicha asosiy texnologiyalardan biri bo'lib xisoblanadi.

Kompyuter stenografiyasining asosiy vazifalari.

Zamonaviy kompyuter stenografiyasining asosiy holatlari quyidagilardan iborat:

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

Internet kompyuter tarmog'ining axborot manbalarini taxdili quyidagi xulosaga kelishga imkon berdi, ya'ni hozirgi vaqtda stenografik tizimlar quyidagi asosiy masalalarni yechishda faol ishlatilayapti:

- > konfidentsial axborotni ruxsat etilmagan kirishdan ximoyalash;
- > monitoring va tarmoq zaxiralarini boshqarish tizimlarini yengish;
- > dasturiy ta'minotni niqoblash;
- > intellektual egalikning ba'zi bir turlarida mualliflik huquqlarini ximoyalash.

Konfidentsial axborotlarni ruxsatsiz kirishdan himoyalash.

Bu kompyuter steganografiyasini ishlatish sohasi konfidentsial axborotlarni ximoyalash muammosini yechishda eng samarali xisoblanadi. Masalan, tovushning eng kam ahamiyatli kichik razryadlari yashiriladigan xabarga almashtiriladi. Bunday o'zgarish kupchilik tomonidan tovushli xabarni eshitish paytida sezilmaydi.

Mualliflik huquqlarini ximoyalash.

Stenografiyadan foydalaniladigan yana bir sohalardan biri — bu mualliflik huquqlarini ximoyalash xisoblanadi. Kompyuterli grafik tasvirlarga maxsus belgi qo'yiladi va u ko'zga ko'rinmay qoladi. Lekin, maxsus dasturiy ta'minot bilan aniqlanadi. Bunday dastur mahsuloti allaqachon ba'zi jurnallarning kompyuter versiyalarida ishlatilayapti. Stenografiyaning ushbu yo'nalishi nafaqat tasvirlarni, balki audio va videoaxborotni ham

qayta ishlashga mo'ljallangan. Bundan tashqari uning intellektual egaligini ximoyalashni ta'minlash vazifasi ham mavjud.

Hozirgi vaktida kompyuter stenografiyasi usullari ikki asosiy yo'nalish bo'yicha rivojlanmokda:

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

Stenografik dasturlar tugrisida qisqacha ma'lumot.

Windows operatsiey muxitida ishlovchi dasturlar:

- Steganos for Win95 dasturi ishlatishda judaengil bo'lib, ayni paytda fayllarni shifrlash vaularni BMP, DIB, VOC, WAV, ASCII, HTML ken gaytmali fayllar ichiga joylashtirib yashirishda judaqudratli xisoblanadi;
- Contraband dasturi 24-bitli BMP formatdagi grafik fayllar ichida har qanday faylni yashira olish imkoniyatiga ega.

DOS muxitida ishlovchi dasturlar:

- Jsteg dasturi ma'lumotni JPG formatli fayl lar ichiga yashirish uchun muljallangan;
- FFEncode dasturi ma'lumotlarni matnli fayl lar ichida yashirish imkoniyatiga ega;
- StegoDOS dasturlar paketining axborotni tas virda yashirish imkoniyati mavjud;
- Winstorm dasturlar paketa PCX formatli fayl lar ichiga xabarni shifrlab yashiradi.

OS/2 operatsiey muxitida ishlovchi dasturlar:

- Texto dasturi ma'lumotlarni ingliz tilidagi matnga aylantiradi;
- Hide4PGP v1.1 dasturi BMP, WAV, VOC formatli fayllar ichiga ma'lumotlarni yashirish imkoniyatiga ega.

Macintosh kompyuterlari uchun mo'ljallangan dasturlar:

- Paranoid dasturi ma'lumotlarni shifrlab, tovushli formatli fayl ichiga yashiradi;
- Stego dasturining PICT kungaytmali fayl ichiga ma'lumotlarni yashirish imkoniyati mavjud.

Axborotlarni kriptografik himoyalash usullari

Kriptografiya haqida asosiy tushunchalar.

«Kriptografiya» atamasi dastlab «yashirish, yozuvni berkitib qo‘ymoq» ma’nosini bildirgan. Birinchi marta u yozuv paydo bo‘lgan davrlardayoq aytib o‘tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya’ni diskda sakdanadigan sonlar ko‘rinishida yoki hisoblash tarmoklarida uzatiladigan xabarlar ko‘rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo‘lgan har qanday axborotga nisbatan qo‘llash mumkin. Maxfiylikni ta’minlashga qaratilgan kriptografiya kengroq qo‘llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo‘llaniladigan usullarning o‘zi axborotni ximoyalash bilan bogliq bo‘lgan kup jarayonlarda ishlatilishi mumkin. Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta’minlaydi. Masalan, to‘lov varaklarini elektron pochta orqali uzatishda uning o‘zgartirilishi yoki soxta yozuvlarning qo‘shilishi mumkin. Bunday hollarda axborotning yaxlitligini ta’minlash zaruriyati paydo bo‘ladi. Umuman olganda kompyuter tarmogiga ruxsatsiz kirishning mutlako oldini olish mumkin emas, lekin ularni aniqlash mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko‘p hollarda, axborotning haqiqiylikni ta’minlash deyiladi.

Kriptografiyada qo‘llaniladigan usullar ko‘p bo‘lmagan o‘zgartirishlar bilan axborotlarning haqiqiylikni ta’minlashi mumkin. Nafakat axborotning kompyuter tarmogidan ma’nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch hosil qilish juda muxim. Axborotni uzatuvchi shaxslarning haqiqiylikni tasdiklovchi turli usullar ma’lum. Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo‘lmagan protsedura. Chunki parolni kuliga kiritgan har qanday shaxe axborotdan foydalanishi mumkin bo‘ladi. Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish va ularni kriptografik usullar bilan himoyalash mumkin, lekin kriptografiya bundan kuchliroq parolni uzluksiz o‘zgartirish imkonini beradigan protseduralarni ham ta’minlaydi. Kriptografiya sohasidagi oxirgi yutuklardan biri — rakamli signatura — maxsus xossa bilan axborotni to‘ldirish yordamida yaxlitlikni ta’minlovchi usul, bunda axborot uning muallifi bergan ochiq kalit ma’lum bo‘lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik

tekshiriladigan ma'lum usullardan ko'proq afzalliklarga ega. Kriptografiya usullarini qo'llashning ba'zi birlarini ko'rib chiqamiz. Uzatiladigan axborotning ma'nosini yashirish uchun ikki xil o'zgartirishlar qo'llaniladi: kodlashtirish va shifrlash. Kodlashtirish uchun tez-tez ishlatiladigan iboralar to'plamini uz ichiga oluvchi kitob yoki jadvallardan foydalaniladi. Bu iboralardan har biriga, ko'p hollarda, raqamlar to'plami bilan beriladigan ixtiyoriy tanlangan kodli so'z tugri keladi. Axborotni kodlash uchun xuddi shunday kitob yoki jadval talab kilinadi. Kodlashtiruvchi kitob yoki jadval ixtiyoriy kriptografik o'zgartirishga misol bo'ladi. Kodlashtirishning axborot texnologiyasiga mo'e talablar — qatorli ma'lumotlarni sonli ma'lumotlarga aylantirish va aksincha o'zgartirishlarni bajara bilish. Kodlashtirish kitobini tezkor hamda tashqi xotira qurilmalarida amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik tizimni muvaffaqiyatli deb bo'lmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, koddarning yangi kitobini yaratish va uni hamma foydalanuvchilarga tarqatish zaruriyati paydo bo'ladi. Kriptografik o'zgartirishning ikkinchi turi shifrlash uz ichiga — boshlangich matn belgilarini anglab olish mumkin bo'lmagan shaklga o'zgartirish algoritmlarini qamrab oladi. O'zgartirishlarning bu turi axborot-kommunikatsiyalar texnologiyalariga mos keladi. Bu yerda algoritmni himoyalash muhim ahamiyat kasb etadi. Kriptografik kalitni qo'llab, shifrlash algoritmining o'zida ximoyalashga bo'lgan talablarni kamaytirish mumkin. Endi himoyalash ob'ekti sifatida faqat kalit xizmat kiladi. Agar kalitdan nusxa olingan bo'lsa, uni almashtirish mumkin va bu kodlashtiruvchi kitob yoki jadvalni almashtirishdan yengildir. Shuning uchun ham kodlashtirish emas, balki shifrlash axborot-kommunikatsiyalar texnologiyalarida keng ko'lamda qo'llanilmoqda. Sirli (maxfiy) aloqalar sohasi kriptologaya deb aytiladi. Ushbu so'z yunoncha «kripto» — sirli va «logus» — xabar ma'nosini bildiruvchi suzlardan iborat. Kriptologiya ikki yunalish, ya'ni kriptografiya va kriptotahlildan iborat.

Kriptografiyaning vazifasi xabarlarining maxfiyligini va haqiqiyligini ta'minlashdan iborat.

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

Hozirgi kunda kriptotizimni ikki sinfga ajratish mumkin:

- simmetriyali bir kalitlilik (maxfiy kalitli);

- asimmetriyali ikki kalitlilik (ochiq kalitli).

Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

- 1) Axborot almashuvda ishtirok etuvchilar qanday yo'l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?
- 2) Jo'natilgan xabarning haqiqiyligini qanday aniqlasa bo'ladi?

Ushbu muammolarning yechimi ochiq kalitli tizimlarda o'z aksini topdi.

Ochiq kalitli asimmetriyali tizimda ikkita kalit qo'llaniladi. Biridan ikkinchisini xisoblash usullari bilan aniqlab bo'lmaydi. Birinchi kalit axborot jo'natuvchi tomonidan shifrlashda ishlatilsa, ikkinchisi axborotni qabul qiluvchi tomonidan axborotni tiklashda qo'llaniladi va u sir saqlanishi lozim. Ushbu usul bilan axborotning maxfiyligini ta'minlash mumkin. Agar birinchi kalit sirli bo'lsa, u holda uni elektron imzo sifatida qo'llash mumkin va bu usul bilan axborotni autentifikatsiyalash, ya'ni axborotning yaxlitligini ta'minlash imkoni paydo bo'ladi.

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

- foydalanuvchini autentifikatsiyalash, ya'ni kompyuter tizimi xazinalariga kirmoqchi bo'lgan foydalanuvchini aniqlash;
- tarmoq abonentlari aloqasini o'rnatish jarayonida ularni o'zaro autentifikatsiyalash.

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

Kriptografiya - ma'lumotlarni o'zgartirish usullarining to'plami bo'lib, ma'lumotlarni himoyalash bo'yicha quyidagi ikkita asosiy muammolarni hal qilishga yo'naltirilgan: maxfiylik; yaxlitlilik. Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o'zgartira olmaslik haqida dalolat beradi. Bu yerda kalit qandaydir himoyalangan kanal orqali junatiladi. Umuman olganda, ushbu mexanizm simmetriyali bir kalitlik tizimiga taalluklidir.

Asimmetriyali ikki kalitlik kriptografiya tizimini:

Bu holda himoyalangan kanal bo'yicha ochiq kalit junatilib, maxfiy kalit jo'natilmaydi.

Yovuz niyatli shaxslar o'z maqsadlariga erisha olmasa va kriptotaxlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u holda kriptotizim kriptomustahkam tizim deb aytiladi. Kriptotizimning mustahkamligi uning kaliti bilan aniqlanadi va bu kriptotaxlilning asosiy qoidalaridan biri bo'lib xisoblanadi. Ushbu ta'rifning asosiy ma'nosi shundan iboratki, kriptotizim barchalarga ma'lum tizim hisoblanib, uning o'zgartirilishi kup vakt va mablag talab kiladi, shu bois ham faqatgina kalitni o'zgartirib turish bilan axborotni ximoyalash talab kilinadi.

Simmetriyali kriptotizim asoslari

Kriptografiya nuqtai-nazaridan shifr — bu kalit demakdir va ochiq ma'lumotlar to'plamini yopiq (shifrlangan) ma'lumotlarga o'zgartirish kriptografiya o'zgartirishlar algoritmlari majmuasi hisoblanadi.

Kalit — kriptografiya o'zgartirishlar algoritmining ba'zi-bir parametrlarining maxfiy holati bo'lib, barcha algoritmlardan yagona variantini tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy ko'rsatkich bo'lib kriptomustahkamlik hisoblanadi.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo'yiladi:

- yetarli darajada kriptomustahkamlik;
- shifrlash va kaytarysh jarayonining oddiyligi;
- axborotlarni shifrlash oqibatida ular hajmining ortib ketmasligi;
- shifrlashdagi kichik xatolarga ta'sirchan bo'lmasligi.

Ushbu talablarga quyidagi tizimlar javob beradi:

- **o'rinlarini almashtirish;**
- **almashtirish;**
- **gammalashtirish;**
- **analitik o'zgartirish.**

O'rinlarini almashtirish shifrlash usuli bo'yicha boshlangich matn belgilarining matnning ma'lum bir qismi doirasida maxsus qoidalar yordamida o'rinlari almashtiriladi.

Almashtirish shifrlash usuli bo'yicha boshlangich matn belgalari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtiriladi.

Gammalashtirish usuli bo'iicha boshlang'ich matn belgilari shifrlash gammasi belgilari, ya'ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

Tahliliy o'zgartirish usuli bo'yicha boshlangich matn belgilari analitik formulalar yordamida o'zgartiriladi, masalan, vektorni matritsaga ko'paytirish yordamida. Bu yerda vektor matndagi belgilar ketma-ketligi bo'lsa, matritsa esa kalit sifatida xizmat qiladi.

O'rinlarni almashtirish usullari eng oddiy va eng qadimiy usuldir. O'rinlarni almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin:

— shifrovchi jadval;

— sexrli kvadrat.

Shifrovchi jadval usulida kalit sifatida quyidagilar qo'llaniladi:

- jadval o'lchovlari;

- so'z yoki so'zlar ketma-ketligi;

- jadval tarkibi xususiyatlari.

Misol.

Quyidagi matn berilgan bo'lsin:

KADRLAR TAYYoRLASh MILLIY DASTURI

Ushbu axborot ustun buyicha ketma-ket jadvalga kiritiladi:

k l a l i y t

a a y a l d u

d r y o s h l a r

r t r m i s i

Natijada, 4x7 o'lchovli jadval tashkil qilinadi.

Endi shifrlangan matn qatorlar bo'yicha aniklanadi, ya'ni o'zimiz uchun 4 tadan belgilarni ajratib yozamiz.

KLAL IYTA AYAL DUDR YoShLA RRTR MISI

Bu yerda kalit sifatida jadval o'lchovlari xizmat qiladi. Ushbu usulni murakkablashtirish maqsadida tayanch so'zni kiritsa bo'ladi. Yuqoridagi misol uchun quyidagi **MAGISTR** so'zini olamiz va oldingi jadvalga joylashtiramiz:

m a g i s t r

4 1 2 3 6 7 5

k l a l i y t

a a y a l d u

d r y o s h l a r

r t r m i s i

Ikkinchi qatordagi raqamlar harflarning alifbo tarkibidan kelib chiqadi. Shu qatordagi raqamlar bo'yicha ustunlarni tartiblaymiz:

a g i m r s t

1 2 3 4 5 6 7

l a l k t i y

a y a a u l d

r y o s h d r l a

t r m r i i s

Shifrlangan matn quyidagi ko'rinishda bo'ladi: LALK TIYA YAAU LDRYo ShDRL ATRM RIIS

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

Misol.

4x4 o'lchovli sehrli kvadratni olamiz, bu yerda son-larning 880 ta har xil kombinatsiyasi mavjud. Quyidagicha ish yuritamiz:

1 6 3 2 1 3

5 10 11 8

9 6 7 12

4 15 14 1

Boshlangich matn sifatida quyidagi matnni olamiz:

DASTURLASH TILLARI va jadvalga joylashtiramiz:

i s a l

u t i a

s h r l l

t r a d

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

ISAL UTIA ShRLL TRAD

Almashtirish usullari

Almashtirish usullari sifatida quyidagi usullar-ni keltirish mumkin:

- Sezar usuli;
- Affin tizimidagi Sezar usuli;
- Tayanch soʻzli Sezar usuli va boshqalar.

1. Sezar usulida almashtiruvchi harflar k ta siljish bilan aniklanadi. Yuliy Sezar bevosita $k=3$ bulganda ushbu usuldan foydalangan.

$k=3$ boʻlganda va alifbodagi harflar $m=26$ ta boʻlganda quyidagi jadval hosil qilinadi:

Misol.

Matn sifatida SAMARQAND soʻzini oladigan boʻlsak, Sezar usuli natijasida quyidagi shifrlangan yozuv hosil boʻladi: VDPDUTDQG.

2. Sezar usulining kamchiligi bu bir xil harflarning, oʻz navbatida, bir xil harflarga almashishidir.

3. Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula boʻyicha aniqlanadi: $at+b \pmod{m}$, bu yerda a, b — butun sonlar, $0 < a, b < m$, EKUB $(a, m) = 1$.

Hozirgi vaqtda kompyuter tarmoqlarida tijorat axborotlari bilan almashishda uchta asosiy algoritm-lar, yaʼni DES, CLIPPER va PGP algoritm-lari qoʻllanilmoqda. DES va CLIPPER algoritm-lari integral sxemalarda amalga oshiriladi. DES algoritmining kriptomustahkamligini quyidagi misol orqali ham baholash mumkin: 10 mln. AQSh dollari xarajat qilinganda DES shifrini ochish uchun 21 minut, 100 mln. AQSh dollari xarajat qilinganda esa 2 minut sarflanadi. CLIPPER tizimi SKIPJACK shifrlash algoritmini uz ichiga oladi va bu algoritm DES algoritmidan 16 mln. marta kuchliroqdir. PGP algoritmi esa 1991 yilda Filipp Simmer-man (AQSh) tomonidan yozilgan va elektron pochta orqali uzatiladigan xabarlarni shifrlash uchun ishlatiladigan PGP dasturlar paketi yordamida amalga oshiriladi. PGP dasturiy vositalari Internet tarmogʻida elektron pochta orqali axborot joʻnatuvchi foydalanuvchilar tomonidan shifrlash maqsadida keng foydalanilmoqda.

PGP (Pretty Good Privacy) kriptografiya dasturining algoritmi kalitli, ochiq va yopiq boʻladi. Ochiq kalit quyidagicha koʻrinishni olishi mumkin:

```
EDF21pI4 BEGIN PGP PUBLIC KEY BLOCK
```

```
Version: 2.6.31
```

```
mQCNazFHgwAAAEANOvroJEWEq6npGLZTqssS5EScVUPV
```

```
aRu4ePLiDjUz6U7aQr
```

Wk45dIxg0797PFNvPcMRzQZeTxY10ftyMHL/6ZF9wcx64jy
LH40tE2DOG9yqwKAn
yUDFpgRmoL3pbxXZx91OOuuzlkAz+xU6OwGx/EBKYOKPTTt
DzSLOAQxLTyGZAAUR
tClCb2IgU3dhbnNvbiA8cmpzd2FuQHNIYXRObGUtd2Vid29ya
3MuY29tPokAlQMF
h53aEsqJyQEB6JcD/RPxxg6g7tfHFiOQiaf5yaHOYGEVoxcd-
FyZXr/ITz
rgztNXRUiOqU2MDEmh2RoEcDs!fGVZHSRpkCg8iS+35sAz
9c2S+q5vQxOsZJz72B
LZl :FT7?fhC3fZZD9X91MsJH+xxX9CDx92xmllglMT25SOX
2o/uBA<rJ3K:pEI6g6xv
END PGP PUBLIC KEY BLOCK—

Ushbu ochiq kalit bevosita Web sahifalarda yoki elektron pochta orqali ochiqchasiga yuborilishi mumkin. Ochiq kalitdan foydalangan jo'natilgan shifrlan axborotni axborot yuborilgan manzil egasidan boshqa shaxs o'qiy olmaydi. PGP orqali shifrlangan axborotlarni ochish uchun, superkompyuterlar ishlatilganda bir asr ham kamlik qilishi mumkin. Bulardan tashqari, axborotlarni tasvirlarda va tovushlarda yashirish dasturlari ham mavjud. Masalan, S-tools dasturi axborotlarni BMP, GIF, WAV kengaytmali fayllarda saklash uchun qo'llaniladi. Ba'zi hollarda yashirilgan axborotning hajmi rasmning hajmidan ko'p bo'lishi ham mumkin, ya'ni olingan natija faqatgina tanlangan rasmga bog'liq bo'ladi. Kundalik jarayonda foydalanuvchilar ofis dasturlari va arxivatorlarni qo'llab kelishadi. Arxivatorlar, masalan PkZip dasturida ma'lumotlarni parol yordamida shifrlash mumkin. Ushbu fayllarni ochishda ikkita, ya'ni lug'atli va to'g'ridan-to'g'ri usuldan foydalanishadi. Lug'atli usulda bevosita maxsus fayldan so'zlar parol o'rniga qo'yib tekshiriladi, to'g'ridan-to'g'ri usulda esa bevosita belgilar kombinatsiyasi tuzilib, parol o'rniga qo'yib tekshiriladi. Ofis dasturlari (Word, Excel, Access) orqali himoyalash umuman taklif etilmaydi. Bu borada mavjud dasturlar Internet da to'siqsiz tarqatiladi.

Kompyuter viruslaridan ximoyalanish.

Hozirgi kunda kompyuter viruslari g'arazli maqsadlarda ishlatiluvchi turli xil dasturlarni- olib kelib tatbiq etishda eng samarali vositalardan biri x isoblanadi. Kompyuter viruslarini dasturli viruslar deb atash to'g'riroq bo'ladi. Dasturli virus deb avtonom ravishda ishlash, boshqa dastur tarkibiga o'z-o'zidan qo'shiluvchi, ishga qodir va kompyuter tarmoklari va aloxida kompyuterlarda o'z-o'zidan tarqalish xususiyatiga ega bo'lgan dasturga aytiladi. Viruslar bilan zararlangan dasturlar virus tashuvchi yoki zararlangan dasturlar deyiladi

Viruslarning ta'siri buyicha tasnifi:

1. Xavfsiz - fayllar tarkibini buzmaydigan;
2. Xavfli - fayllar tarkibini buzadigan;
3. Juda xavfli - kurilmalarni buzadigan;

Zararlangan disk — bu ishga tushirish sekgorida virus dastur joylashib olgan diskdir. Hozirgi paytda kompyuterlar uchun ko'pgina nokulayliklar tug'dirayotgan har xil turlardagi kompyuter viruslari keng tarqalgan. Shuning uchun ham ulardan sakdanish usullarini ishlab chiqish muhim masalalardan biri xisoblanadi. Hozirgi vaqtda 65000 dan ko'p bo'lgan virus dasturlari borligi aniklangan. Bu viruslarning katta guruxini kompyuterning ish ba-jarish tartibini buzmaydigan, ya'ni «ta'sirchan bo'lmagan» viruslar guruxi tashkil etadi.

Viruslarning boshqa rypyxlariga kompyuterning ish tartibini buzuvchi viruslar kiradi. Bu viruslarni quyidagi turlarga bo'lish mumkin: xavfsiz viruslar (fayllar tarkibini buzmaydigan), xavfli viruslar (fayllar tarkibini buzuvchi) hamda juda xavfli viruslar (kompyuter kurilmalarini buzuvchi va operator sog'lig'iga ta'sir etuvchi). Bu kabi viruslar odatda professional dasturchilar tomonidan tuziladi.

Kompyuter virusi - bu maxsus yozilgan dastur bo'lib, boshqa dasturlar tarkibiga yoziladi, ya'ni zararlaydi va kompyuterlarda o'zining g'arazli maqsadlarini amalga oshiradi.

Kompyuter virusi orqali zararlanish oqibatida kompyuterlarda quyidagi o'zgarishlar paydo bo'ladi:

- ayrim dasturlar ishlamaydi yoki xato ishlay boshlaydi;
- bajariluvchi faylning hajmi va uning yaratilgan vakti o'zgaradi;
- ekranda anglab bo'lmaydigan belgilar, turli xil tasvir va tovushlar paydo bo'ladi;
- kompyuterning ishlashi sekinlashadi va tezkor xotiradagi bo'sh joy hajmi kamayadi;

- disk yoki diskdagi bir necha fayllar zararlanadi (ba'zi hollarda disk va fayllarni tiklab bo'lmaydi);
- vinchester orqali kompyuterning ishga tushishi yo'qoladi.

Viruslar asosan disklarning yuklanuvchi sektorlarini va yexe, som, sys va bat kengaytmali fayllarni zararlaydi. Hozirgi kunda bular qatoriga ofis dasturlari yaratadigan fayllarni ham kiritish mumkin. Oddiy matnli fayllarni zararlaydigan viruslar kamdan-kam uchraydi.

Kompyuterning viruslar bilan zararlanish yo'llari quyidagilardir:

1. Disketlar orqali.
2. Kompyuter tarmoqlari orqali.
3. Boshqa yo'llar yo'q.

Xozirgi paytda hazil shaklidagi viruslardan tortib to kompyuter qurilmalarini ishdan chiqaruvchi viruslarning turlari mavjud.

Masalan. Win 95.SSh virusi doimiy saklash kurul-masi (Flash BIOS) mikrosxemasini buzadi. Afsuski, bu kabi viruslarni yo'q qilish uchun, faqat ular o'z garazli ishini bajarib bo'lgandan so'nggina, qarshi choralar ishlab chiqiladi. Win 95.SSh virusiga qarshi choralarni ko'rish imkoniyati Dr.Web dasturida mavjud. Kompyuter viruslaridan axborotlarga ruxsatsiz kirishi va ulardan foydalanishni tashkil etish. Shuni aytib o'tish lozimki, hozirgi paytda har-xil turdagi axborot va dasturlarni utirlab olish niyatida kompyuter viruslaridan foydalanish eng samarali usullardan biri hisoblanadi. Dasturli viruslar kompyuter tizimlarining xavfsizligiga taxdid solishning eng samarali vositalaridan biridir. Shuning uchun ham dasturli viruslarning imkoniyatlarini taxlil qilish masalasi hamda bu viruslarga qarshi kurashish hozirgi paytning dolzarb masalalaridan biri bo'lib qoldi. Viruslardan tashqari fayllar tarkibini buzuvchi troyan dasgurlari mavjud. Virus ko'pincha kompyuterga sezdirmasdan kiradi. Foydalanuvchining o'zi troyan dasturini foydali dastur sifatida diskka yozadi. Ma'lum bir vaqt o'tgandan keyin buzgunchi dastur uz ta'sirini ko'rsatadi. O'z-o'zidan paydo bo'ladigan viruslar mavjud emas. Virus dasturlari inson tomonidan kompyuterning dasturiy ta'minotini, uning qurilmalarini zararlash va boshqa maqsadlar uchun yoziladi. Viruslarning hajmi bir necha baytdan to o'nlab kilobaytgacha bo'lishi mumkin. Trojan dasturlari foydalanuvchiga zarar keltiruvchi bo'lib, ular buyruqdar(modullar) ketma-ketligi-dan tashkil topgan, omma orasida juda keng tarqalgandasturlar (tahrirlovchilar, o'yinlar, translyatorlar) ichiga o'rnatilgan bo'lib, bir qancha hodisalar bajari-lishi bilan ishga tushadigan «mantiqiy bomba» deb

ataladigan dasturdir. O'z navbatida, «mantiqiy bom-ba»ning turli ko'rinishlaridan biri «soat mexanizm-li bomba» hisoblanadi. Shuni ta'kidlab utish kerakki, troyan dasturlari o'z-o'zidan ko'paymasdan, kompyuter tizimi buyicha dasturlovchilar tomonidan tarqatiladi. Troyan dasturlardan viruslarning farki shundaki, viruslar kompyuter tizimlari bo'ylab tarqatilganda, ular mustakil ravimtsa hosil bo'lib, o'z ish faoliyatida dasturlarga o'z matnlarini yozgan holda ularga zarar kursatadi. Zararlangan dasturda dastur bajarilmasdan oldin virus o'zining buyruklari bajarilishiga imkoniyat yaratib beradi. Buning uchun ham virus dasturning bosh kismida joylashadi yoki dasturning birinchi buyrugi unga yozilgan virus dasturiga shartsiz o'tish bo'lib xizmat qiladi. Boshqarilgan virus boshqa dasturlarni zararlaydi va shundan so'ng virus tashuvchi dasturga ishni topshiradi. Virus hayoti odatda quyidagi davrlarni uz ichiga oladi: qo'llanilish, inkubatsiya, replikatsiya (o'z-o'zidan ko'payish) va hosil bo'lish. Inkubatsiya davrida virus passiv bulib, uni izlab topish va yo'qotish kiyin. Hosil bo'lish davrida u uz funktsiyasini bajaradi va qo'yilgan maqsadiga erishadi. Tarkibi jihatidan virus juda oddiy bo'lib, bosh kiem va ba'zi hollarda dumdan iborat. Virusning bosh qismi deb boshqarilishni birinchi bulib ta'minlovchi imkoniyatga ega bo'lgan dasturga aytiladi. Virusning dum kismi zararlangan dasturda bo'lib, u bosh qismidan alohida joyda joylashadi.

Kompyuter viruslari xarakterlariga nisbatan nerezident, rezident, butli, gibridli va paketli viruslarga ajratiladi.

1. *Faylli nerezident* viruslar tulikligicha bajarilayotgan faydda joylashadi, shuning uchun ham u faqat virus tashuvchi dastur faollashgandan sung ishga tushadi va bajarilgandan sung tezkor xotirada saklanmaydi.
2. *Rezident virus* norezident virusdan farqyairoq tez-kor xotirada saklanadi.
3. *But viruslar* bulib, bu virusning vazifasi vinchester va egiluvchan magnitli disklarning yuklovchi sektorini ishdan chiqarishdan iborat. But viruslarning boshi diskning yuklovchi but sektorida va dumi disklarning ixtiyoriy boshqa sektorlarida joylashgan buladi.
4. *Paketli virusning* bosh kismi paketli faylda joylashgan bulib, u operatsion tizim topshiriqlaridan iborat.
5. *Gibridli* viruslarning boshi paketli faylda joylashadi. Bu virus ham faylli, ham but sektorli bu-ladi.
6. *Tarmokli viruslar* kompyuter tarmoklarida tarqalishga moslashtirilgan, ya'ni tarmokli viruslar deb axborot almashishda tarqaladigan viruslarga aytiladi.

Viruslarning turlari:

- 1) *fayl viruslari*. Bu viruslar som, yexe kabi turli fayllarni zararlaydi;
- 2) *yuklovchi viruslar*. Kompyuterni yuklovchi dasturlarni zararlaydi;
- 3) *drayverlarni zararlovchi viruslar*. Operatsion tizimdagi config.sys faylni zararlaydi. Bu kompyuterning ishlamasligiga sabab buladi;
- 4) *DIR viruslari*. FAT tarkibini zararlaydi;
- 5) *stels-viruslari*. Bu viruslar uzining tarkibinio'zgartirib, tasodifiy kod o'zgarishi bo'yicha tarqaladi. Uni aniklash juda kiyin, chunki fayllarning uzlari uzgarmaydi;
- 6) *Windows viruslari*. Windows operatsiey tizimidagi dasturlarni zararlaydi.

Misol sifatida quyidagilarni keltirish mumkin:

- 1) Eng xavfli viruslardan biri Internet orqali tarqatilgan «Chernobil» virusi bo'lib, u 26 aprelda tarqatilgan va har oyning 26-kunida kompyuterlarni zararlashi mumkin.
- 2) I LOVE YOU virusi Filippindan 2000 yil 4 mayda Ye-mail orqali tarqatilgan. U butun jahon bo'yicha 45 mln. kompyuterni zararlagan va ishdan chiqargan. Moddiy zarar 10 mlrd. AKD1 dollarini tashkil kilgan.
- 3) 2003 yil mart oyida Shvetsiyadan elektron pochta orkali GANDA virusi tarqatilgan va u butun dunyoda minglab kompyuterlarni zararlagan. Bu virusni tarqatgan shaxe hozir qo'lga olingan va u 4 yil qamoq jazosiga hukm etilishi mumkin.

Asoslangan algoritmlar buyicha dasturli viruslarni quyidagicha tasniflash mumkin.

1. *Parazitli virus* — fayllarning tarkibini va diskning sektorini o'zgartiruvchi virus. Bu virus oddiy viruslar turkumidan bo'lib, osonlik bilan aniqlanadi va o'chirib tashlanadi.
2. *Replikatorli virus* — «chuvalchang» deb nomlanadi, kompyuter tarmoqlari bo'yicha tarqalib, kompyuterlarning tarmokdagi manzilini aniklaydi va u yerda o'zining nusxasini qoldiradi.
3. *Ko'rinmas virus* -- stels-virus deb nom olib, zararlangan fayllarga va sektorlarga operatsion tizim tomonidan murojaat qilinsa, avtomatik ravishda zararlangan kismlar urniga diskning toza qismini taqtsim etadi. Natijada ushbu viruslarni aniklash va tozalash juda katta kiyinchiliklarga olib keladi.
4. *Mutant virus* — shifrlash va deshifrlash algoritmlaridan iborat bo'lib, natijada virus nusxalari umuman bir-biriga o'xshamaydi. Ushbu viruslarni aniqlash juda qiyin muammo.

5. *Kvazivirus virus* -- «Trojan» dasturlari, deb nom olgan bo‘lib, ushbu viruslar ko‘payish xususiyatiga ega bulmasada, «foydali» qism-dastur xisobida bo‘lib, antivirus dasturlar tomonidan aniklanmaydi. Shu bone xam ular o‘zlarida mukammallashtirilgan algoritmlarni to‘siqsiz bajarib, qo‘yilgan maqsadlariga erishishlari mumkin.

Antivirus dasturlari.

Hozirgi vaqtda viruslarni yo‘qotish uchun ko‘pgina usullar ishlab chikilgan va bu usullar bilan ishlay-digan dasturlarni antiviruslar deb atashadi. Antiviruslarni, qo‘llanish usuliga ko‘ra, quyidagilarga ajratishimiz mumkin: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar.

1. Detektorlar — virusning signaturasi (virusga taallukli baytlar ketma-ketligi) bo‘yicha tezkor xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topadi va xabar beradi. Yangi viruslarni aniklay olmasligi detektorlarning kamchiligi xisoblanadi.
2. Faglar — yoki doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oddingi holatiga qaytaradi.
3. Vaktsinalar — yuqoridagilardan farqli ravishda himoyalalanayotgan dasturga o‘rnatiladi. Natijada dastur zararlangan deb hisoblanib, virus tomonidan o‘zgartirilmaydi. Faqatgina ma’lum viruslarga nisbatan vaktsina qilinishi uning kamchiligi hisoblanadi. Shu bois ham, ushbu antivirus dasturlari keng tarqalmagan.
4. Privivka — fayllarda xuddi virus zararlagandek iz qoldiradi. Buning natijasida viruslar «privivka kilingan» faylga yopishmaydi.
5. Filtrlar -qo‘riqllovchi dasturlar kurinishida bo‘lib, rezident holatda ishlab turadi va viruslarga xos jarayonlar bajarilganda, bu haqda foydalanuvchiga xabar beradi.
6. Revizorlar — eng ishonchli himoyalovchi vosita bo‘lib, diskning birinchi holatini xotirasida saqlab, undagi keyingi o‘zgarishlarni doimiy ravishda nazorat qilib boradi.

Detektor dasturlar kompyuter xotirasidan, fayllardan viruslarni kidiradi va aniklangan viruslar haqida xabar beradi. Doktor dasturlari nafakat virus bilan kasallangan fayllarni topali, balki ularni davolab, dastlabki holatiga qaytaradi. Bunday dasturlarga Aidstest, Doctor Web dasturlarini misol qilib keltirish mumkin. Yangi viruslarning tuxtovsiz paydo

bo‘lib turishini xisobga olib, doktor dasturlarini ham yangi versiyalari bilan almashtirib turish lozim. Filtr dasturlar kompyuter ishlash jarayonida viruslarga xos bo‘lgan shubhali harakatlarni topish uchun ishlatiladi.

Bu harakatlar quyidagicha bo‘lishi mumkin:

- fayllar atributlarining o‘zgarishi;
- disklarga doimiy manzillarda ma’lumotlarni yozish;
- diskning ishga yuklovchi sektorlariga ma’lumot larni yozib yuborish.

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

Viruslarga qarshi chora-tadbirlar.

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

- kompyuterni zamonaviy antivirus dasturlar bilan ta’minlash;
- disketalarni ishlatishdan oldin har doim virusga qarshi tekshirish;
- qimmatli axborotlarning nusxasini har doim arxiv fayl kurinishida saqlash.

Kompyuter viruslariga qarshi kurashning quyidagi turlari mavjud:

- viruslar kompyuterga kirib buzgan fayllarni uzholiga qaytaruvchi dasturlarning mavjudligi;
 - kompyuterga parol bilan kirish, disk yurituvchilarning yopiq turishi;
 - disklarni yozishdan ximoyalash;
 - litsenzion dasturiy ta’minotlardan foydalanishva o‘girlangan dasturlarni qo‘llamaslik;
 - kompyuterga kiritilayotgan dasturlarda viruslarning mavjudligini tekshirish;
 - antivirus dasturlaridan keng foydalanish;
 - davriy ravishda kompyuterlarni antivirus dasturlari yordamida viruslarga qarshi tekshirish.
- Antivirus dasturlaridan DrWeb, Adinf, AVP, BootCHK va Norton Antivirus, Kaspersky Security kabilar keng foydalaniladi.

Kompyuter tarmoklarida uzatilayotgan

axborotni ximoyalash.

Hozirgi vaqtlarda mavjud axborot tizimlarida juda katta hajmda maxfiy axborotlar saklanadi va ularni himoyalash eng dolzarb muammolardan hisoblanadi. Masalan, birgina AQSh Mudofaa vazirligida ayni chogʻda 10000 kompyuter tarmoklari va 1,5 mln kompyuterlarga qarashli axborotlarning aksariyat qismi maxfiy ekanligi hammaga ayon. Bu kompyuterlarga 1999 yili 22144 marta turlicha hujumlar uyushtirilgan, ularning 600 tasida Pentagon tizimlarining vaktinchalik ishdan chiqishiga olib kelgan, 200 tasida esa maxfiy boʻlmagan maʼlumotlar bazalariga ruxsatsiz kirilgan, va natijada Pentagon 25 milliard AQSh dollari miqdorida iqtisodiy zarar koʻrgan. Bunaqa hujumlar 2000 yili 25000 marta amalga oshirilgan. Ularga qarshi kurashish uchun Pentagon tomonidan yangi texnologiyalar yaratishga 2002 yili Carnegie Mellon universitetiga 35,5 mln. AQSh dollari miqdorida grant ajratilgan. Maʼlumotlarga qaraganda, har yili AQSh hukumati kompyuterlariga oʻrtacha hisobda 250—300 ming hujum uyushtiriladi va ulardan 65%i muvaffaqiyatli amalga oshiriladi.

Zamonaviy avtomatlashtirilgan axborot tizimlari — bu tarakqiyot dasturiy-texnik majmuasidir va ular axborot almashuvini talab etadigan masalalarni yechishni taʼminlaydi. Keyingi yillarda foydalanuvchilarning ishini yengillashtirish maqsadida yangiliklarni tarqatish xizmati USENET-NNTP, multimedia maʼlumotlarini INTERNET-HTTP tarmogʻi orqali uzatish kabi protokollar keng tarqaldi. Bu protokollar bir qancha ijobiy imkoniyatlari bilan birga anchagina kamchiliklarga ham ega va bu kamchiliklar tizimning zaxiralariga ruxsatsiz kirishga yoʻl qoʻyib bermoqta. Masalan, AQSh Axborotni ximoyalash milliy assotsiatsiyasi aʼzosi Devid Kennedi (David Keppes1u)ning maʼlumotiga kura, Buenos-Ayresda yashovchi 21 yoshli Julio Sezar Ardita (Julio Cesar Ardita) qoʻlga olingan. Buning sababi esa Ardi-taning AQSh harbiy dengiz kuchlari, NASA hamda AQSh, Braziliya, Chili, Koreya, Meksika, Tayvan universitetlari kompyuter tizimlariga hujumlar uyushtirgan-ligi va ularga ruxsatsiz kirganligidir.

Axborot tizimlarining asosiy taʼsirchan qismlari quyidagilar:

- INTERNET tarmogidagi serverlar. Bu serverlar: dasturlar yoki maʼlumotlar fayllarini yoʻq qilish or qali; serverlarni haddan tashqari koʻp tugallanmagan jarayonlar bilan yuklash

orqali; tizim jurnalining keskin to'ldirib yuborilishi orqali; brouzer — dasturlarini ishlamay qolishiga olib keluvchi fayllarni nusxalash orqali ishdan chiqariladi;

- ma'lumotlarni uzatish kanallari -biror-bir port orqali axborot olish maqsadida yashirin kanalni tashkil etuvchi dasturlar yuboriladi;
- ma'lumotlarni tezkor uzatish kanallari - - bukanallar juda ko'p miqdorda hech kimga kerak bo'lmagan fayllar bilan yuklanadi va ularning ma'lumot uzatish tezligi susayib ketadi;
- yangiliklarni uzatish kanallari - - bu kanallareskirgan axborot bilan to'ldirib tashlanadi yoki bu kanallar umuman yo'q qilib tashlanadi;
- axborotlarni uzatish yo'li -- USENET tarmogada yangiliklar paketining marshruti buziladi;
- JAVA brouzerlari — SUN firmasi yaratgan JAVA tili imkoniyatlaridan foydalanib, appletlar (applets) tashkil etish orqali ma'lumotlarga ruxsatsiz kirish mumkin bo'ladi. JAVA — appletlari tarmoqda avtomatik ravinmtsa ishga tushib ketadi va buning natijasida foydalanuvchi biror-bir hujjatni ishlatayotgan paytda haqiqatda nima sodir etilishini hech qachon kura bilmaydi, masalan, tarmoq viruslarini tashkil etish va JAVA-appletlari orqali viruslarni jo'natish mumkin bo'ladi yoki foydalanuvchining kredit kartalari raqamlariga egalik qilish imkoniyati vujudga keladi.

AQSh sanoat shpionajiga qarshi kurash assotsiatsiyasining tekshirishlariga asosan kompyuter tarmoqlari va axborot tizimlariga hujumlar quyidagicha tasniflanadi: 20% - - aralash hujumlar; 40% - - ichki hujumlar va 40% — tashqi hujumlar. Juda ko'p hollarda bunaqa hujumlar muvaffaqiyatli tashkil etiladi. Masalan, Buyuk Britaniya sanoati, kompyuter jinoyatlari sababli, har yili 1 mlrd funt sterling zarar ko'radi. Demak, yuqorida olib borilgan taxlildan shu narsa ko'rinadiki, hozirgi paytda kompyuter tarmoqlari juda ko'p ta'sirchan kismilarga ega bo'lib, ular orqali axborotlarga ruxsatsiz kirishlar amalga oshirilmoqda yoki ma'lumotlar bazalari yo'q qilib yuborilmoqda va buning natijasida insoniyat mlrd-mlrd AQSh dollari miqdorida iqtisodiy zarar ko'rmoqda.

Elektron pochtaga ruxsatsiz kirish.

Internet tizimidagi elektron pochta juda kup ishlatilayotgan axborot almashish kanallaridan biri xisoblanadi. Elektron pochta yordamida axborot almashuvi tarmoqdagi axborot almashuvining 30%ini tashkil etadi. Bunda axborot almashuvi bor-yo'g'i ikkita protokol: SMTP (Simple Mail Transfer Protocol) va ROR-3 (Post Office Rgo1oso1)larni ishlatish yordamida amalga oshiriladi. ROR-3 multimedia texnologiyalarining rivojini aks

ettiradi, SMTP esa Appranet proekti darajasida tapysil etilgan edi. Shuning uchun ham bu protokollarning hammaga ochiqpigi sababli, elektron pochta resurslariga ruxsatsiz kirishga imkoniyatlar yaratilib berilmokda:

- SMTP server — dasturlarining nokorrekt o‘rnatilishi tufayli bu serverlardan ruxsatsiz foydalanilmokda va bu texnologiya «spama» texnologiyasi nomi bilan ma’lum;
- elektron pochta xabarlariga ruxsatsiz egalik qilish uchun oddiygina va samarali usullardan foydalanilmoqta, ya’ni quyi qatlamlarda vinchesterdagi ma’lumotlarni ukish, pochta resurslariga kirish parolini ukib olish va hokazolar.

Ma’lumotlarga ruxsatsiz kirishning dasturiy va texnik vositalari.

Ma’lumki, xisoblash texnikasi vositalari ishi elektromagnit nurlanishi orqali bajariladi, bu esa, uz navbatida, ma’lumotlarni tarqatish uchun zarur bo‘lgan signallarning zaxirasidir. Bunday kismalarga kompyuterlarning platalari, elektron ta’minot manbalari, printerlar, plotterlar, aloqa apparatlari va h.k. kiradi. Lekin, statistik ma’lumotlardan asosiy yuqori chastotali elektromagnit nurlanish manbai sifatida displeyning rol uynashi ma’lum buldi. Bu displeylarda elektron nurli trubkalar o‘rnatilgan buladi. Displey ekranida tasvir xudtsi televizordagidek tashkil etiladi. Bu esa videosignallarga egalik qilish va uz navbatida, axborotlarga egalik qilish imkoniyatini yaratadi. Displey ekranidagi kursatuv nusxasi televizorda hosil bo‘ladi. Yuqorida keltirilgan kompyuter kismalaridan boshqa axborotga ruxsatsiz egalik qilish maqsadida tarmoq kabellari hamda serverlardan ham foydalanilmoqda. Kompyuter tizimlari zaxiralariga ruxsatsiz kirish sifatida mazkur tizim ma’lumotlaridan foydalanish, ularni uzgartirish va o‘chirib tashlash harakatlari tushuniladi.

Agar kompyuter tizimlari ruxsatsiz kirishdan himoyalanish mexanizmlariga ega bo‘lsa, u holda ruxsatsiz kirish harakatlari quyidagicha tashkil etiladi:

- ximoyalash mexanizmini olib tashlash yoki kuri nishini o‘zgartirish;
- tizimga biror-bir foydalanuvchining nomi va paroli bilan kirish.

Agar birinchi holda dasturning o‘zgartirilishi yoki tizim so‘rovlarining o‘zgartirilishi talab etilsa, ikkinchi holda esa mavjud foydalanuvchining parolini klaviatura orqali kiritayotgan paytda kurib olish va undan foydalanish orqali ruxsatsiz kirish amalga oshiriladi.

Ma’lumotlarga ruxsatsiz egalik qilish uchun zarur bo‘lgan dasturlarni tatbiq etish usullari quyidagilardir:

- kompyuter tizimlari zaxiralariga ruxsatsiz egalik qilish;

- kompyuter tarmog‘i aloqa kanallaridagi xabar almashuvi jarayoniga ruxsatsiz aralashuv;
- virus kurinishidagi dasturiy kamchiliklar (defektlar)ni kiritish.

Kupincha kompyuter tizimida mavjud zaif kislmlarni «teshik»lar, «lyuk»lar deb atashadi.

Ba’zan dasturchilarning o‘zi dastur tuzish paytida bu «teshik» larni qodtsirishadi, masalan:

— natijaviy dasturiy maxsulotni yengil yigish maqsadida;

—dastur tayyor bo‘lgandan keyin yashirinch dasturga kirish vositasiga ega bo‘lish maqsadida.

Mavjud «teshik»ka zaruriy buyruqlar qo‘yiladi va bu buyruqlar kerakli paytda uz ishini bajarib boradi. Virus kurinishidagi dasturlar esa ma’lumotlarni yo‘qotish yoki qisman o‘zgartirish, ish seanslarini buzish uchun ishlatiladi. Yuqorida keltirilganlardan xulosa kilib, ma’lumotlarga ruxsatsiz egalik kilish uchun dasturiy moslamalar eng kuchli va samarali instrument bo‘lib, kompyuter axborot zaxiralariga katta xavf tugdirishi va

bularga qarshi kurash eng dolzarb muammolardan biri ekanligini ta’kidlash mumkin.

Kompyuter tarmoklarida ma’lumotlarning tarqalish kanallari.

Hozirgi vaktda lokal xisoblash tarmoklari (LAN) va global hisoblash tarmoklari (WAN) orasidagi farqlar yo‘qolib bormoqda. Masalan, Netware 4x yoki Vines 4.11. operatsion tizimlari LAN ning faoliyatini hududiy darajasiga chiqarmoqda. Bu esa, ya’ni LAN imkoniyatlarining ortishi, ma’lumotlarni ximoyalash usul-larini yanada takomillashtirishni talab qilmoqda.

Himoyalash vositalarini tashkil etishda quyidagilarni e’tiborga olish lozim:

- tizim bilan aloqada bo‘lgan sub’ektlar sonining ko‘pligi, ko‘pgina hollarda esa ba’zi bir foydalanuvchilarning nazoratda bo‘lmasligi;
- foydalanuvchiga zarur bo‘lgan ma’lumotlarning tarmokda mavjudligi;
- tarmoklarda turli firmalar ishlab chiqargan shaxsiy kompyuterlarning ishlatilishi;
- tarmoq tizimida turli dasturlarning ishlatish imkoniyati;
- tarmoq elementlari turli mamlakatlarda joylashganligi sababli, bu davlatlarga tortilgan aloqa kabellarining uzunligi va ularni to‘liq nazorat qilishning qariyb mumkin emasligi;
- axborot zaxiralaridan bir vaqgning o‘zida bir qancha foydalanuvchilarning foydalanishi;
- tarmoqqa bir qancha tizimlarning qo‘shilishi;

- tarmoqning yengilgina kengayishi, ya'ni tizim chegarasining noanikligi va unda ishlovchilarning kim ekanligining noma'lumligi;
- hujum nuqqalarining ko'pligi;
- tizimga kirishni nazorat qilishning qiyinligi.

Tarmoqni himoyalash zarurligi quyidagi hollardan kelib chiqadi:

- boshqa foydalanuvchilar massivlarini o'qish;
- kompyuter xotirasida qolib ketgan ma'lumotlarni o'kish;
- ximoya choralari aylanib o'tib, ma'lumot tashuvchilarni nusxalash;
- foydalanuvchi sifatida yashirinchilik ishlash;
- dasturiy tutgichlarni ishlatish;
- dasturlash tillarining kamchiliklaridan foydalanish;
- ximoya vositalarini bilib turib ishdan chiqarish;
- kompyuter viruslarini kiritish va ishlatish.

Tarmoq muhofazasini tashkil etishda quyidagilarni e'tiborga olish lozim:

- > muhofaza tizimining nazorati;
- > fayllarga kirishning nazorati;
- > tarmoqqa ma'lumot uzatishning nazorati;
- > axborot zaxiralariga kirishning nazorati;
- > tarmoq bilan ulangan boshqa tarmoqlarga ma'lumot tarqalishining nazorati.

Maxfiy axborotni qayta ishlash uchun kerakli tekshiruvdan o'tgan kompyuterlarni ishlatish lozim bo'ladi. Muhofaza vositalarining funktsional to'liq bo'lishi muhim hisoblanadi. Bunda tizim administratorining ishi va olib borayotgan nazorat katta ahamiyatga egadir. Masalan, foydalanuvchilarning tez-tez parollarini almashtirib turishlari va parollarning juda uzunligi ularni aniklashni qiyinlashtiradi. Shuning uchun ham yangi foydalanuvchini qayd etishni cheklash (masalan, faqat ish vaqtida yoki faqat ishlayotgan korxonasida) muhimdir. Foydalanuvchining haqiqiylikini tekshirish uchun teskari aloqa qilib turish lozim (masalan, modem yordamida). Axborot zaxiralariga kirish huquqini chegaralash mexanizmini ishlatish va uning ta'sirini LAN ob'ektlariga to'laligicha o'tkazish mumkin.

Tarmoq elementlari o'rtasida o'tkazilayotgan ma'lumotlarni muhofaza etish uchun quyidagi choralarni ko'rish kerak:

- ma'lumotlarni aniklab olishga yo'l qo'ymaslik;
- axborot almashishni taxlil qdlishga yo'l qo'ymaslik;
- xabarlarini o'zgartirishga yo'l qo'ymaslik;
- yashirincha ulanishga yo'l qo'ymaslik va bu hollarni tezda aniqlash.

Ma'lumotlarni tarmoqda uzatish paytida kriptografik himoyalash usullaridan foydalaniladi. Qayd etish jurnaliga ruxsat etilmagan kirishlar amalga oshirilganligi haqida ma'lumotlar yozilib turilishi kerak. Bu jurnalga kirishni chegaralash ham himoya vositalari yordamida amalga oshirilishi lozim. Kompyuter tarmogida nazoratni olib borish murakkabligining asosiy sababi -dasturiy ta'minot ustidan nazorat olib borishning murakkabligidir. Bundan tashqari kompyuter viruslarining ko'pligi ham tarmoqda nazoratni olib borishni qiyinlashtiradi. Hozirgi vaqtgacha muhofazalash dasturiy ta'minoti xilma-xil bo'lsa ham, operatsiey tizimlar zaruriy muhofazaning kerakli darajasini ta'minlamas edi. Netware 4.1, Windows NT operatsiey tizimlari yetarli darajada muhofazani ta'minlay olishi mumkin.

Kompyuter telefoniyasidagi himoyalash usullari.

Elektron kommunikatsiyalarning zamonaviy texnologiyalari keyingi yillarda ishbilarmonlarga aloqa kanallari bo'yicha axborotning turlicha ko'rinishlari (masalan: faks, video, kompyuterli, nutkli axborotlar)ni uzatishda ko'pgina imkoniyatlar yaratib bermoqda. Zamonaviy ofis bugungi kunda aloqa vositalari va tashkiliy texnika bilan haddan tashqari to'ldirib yuborilgan va ularga telefon, faks, avtojavob apparati, modem, skaner, shaxsiy kompyuter va h.k. kiradi. Zamonaviy texnika uchun axborot-kommunikatsiyalar texnologiyasi - kompyuterlar telefoniyasi rivojlanishi bilan katta turtki berildi. Bor-yo'g'i o'n yil ilgari sotuvga CANON firmasining narxi 6000 AQSh dollari bo'lgan «Navigator» nomli mahsuloti chiqarilgan edi va u birinchi tizimlardan hisoblanadi. Kompyuter telefoniyasi o'n yil ichida juda tez sur'atlar bilan rivojlandi. Hozirgi paytda sotuvda mavjud bo'lgan «PC Phone» (Export Industries Ltd, Israel) mahsulotining narxi bor-yo'gi 1000 Germaniya markasi turadi. «Powerline-II» (Talking Technology, ShA)ning narxi esa 800 AQSh dollari turadi. Keyingi paytlarda kompyuter telefoniyasi yunalishida 70% apparat vositalarini Dialogue (USA) firmasi ishlab chikarmoqda. Kompyuter telefoniyasida axborotlarning xavfsizligini ta'minlash katta ahamiyatga ega. Masalan, telefon xakerlarining

Skotland-Yard ATSigna kirib 1,5 mln. AQSh dollari miqdorida zarar keltirishganligi xavfsizlikning zarurligini isbotlaydi. Kompyuter telefoniyasida qo'llanilayotgan nutqni aniqlovchi texnologiya telefon qiluvchining ovozidan tanib olish uchun ahamiyatga egadir. Kompyuter telefoniyasining himoyasini yetarli darajada ta'minlash uchun Pretty Good Privacy Inc. firmasining PC Phone 1.0 dasturiy paketi ishlab chiqarilgan. U kompyuter telefoniyasi orqali uzatilayotgan axborotlarni himoyalash uchun axborotlarni raqamli ko'rinishga o'tkazadi va qabul paytida esa dasturiy-texnik vositalar yordami-da qayta ishlaydi. Zamonaviy kompyuter telefoniyasi vositalarining shifrlash tezligi ham juda yuqoridir, xato qilish ehtimoli esa juda kichikdir (taxminan 10⁻⁸-10⁻¹²).

Kompyuter tarmoqlarida ishlatiladigan kommutatsiya turlari.

I. Kanallar kommutatsiyasi.

Umuman, har qanday kommutatsiyaning asosiy vazifasi kompyuter tarmoqlarida xarakatlanayotgan ma'lumotlarni aniqlab, ularning borish manziliga qarab, yo'nalishini eng muqobil kanalini topib, yetkazib berishdan iborat. Ushbu vazifani tarmoqda o'rnatilgan marshrutizatorlar bajaradi.

Kanal kommutatsiyasining vazifasini tarmoqqa ulangan uzatuvchi bilan qabul qiluvchining orasidagi jismoniy aloqa kanalini yaratib berishdan iborat.

Asosiy avfzalliklari quyidagilardan iborat:

1. Aniq va o'zgarmas ma'lumotlarni uzatish tezligi, har qanday tezlikni o'rnatish mumkinligi.
2. Real vaqtda har qanday ma'lumotlarni (ovoz, video va boshqa) sifatli va qisqa vaqt ichida yetkazib berish.

Asosiy kamchiliklari:

1. Manzillar orasidagi tugunlarni bog'lovchi tranzit aloqa kanallari bandligi sababli tarmoqqa kirish mumkin emasligi.
2. Jismoniy aloqa kanallarini o'tkazish qobiliyatini ishlatilishi pastligi.
3. Ma'lumotlarni uzatishdan oldin ularni bog'lanishi uchun vaqtni sarflanishi.

II. Axborotlar kommutatsiyasi.

Har qanday xajmdagi (uzunlikdagi) axborotlarni uzatuvchidan qabul qiluvchiga yetkazib beruvchi printsiptga asoslangan. Axborotlar manziliga yetib borish davrida,

tugunlarda ushlanib qolishligi mumkin. Ular asosan kompyuterning disklarida saqlanadi. Shuning uchun ko‘p vaqt talab qiladi va kompyuter tarmog‘ini qimmatlashtiradi.

III. Paketlar kommutatsiyasi.

Bugungi kunda eng samarali hisoblangan kommutatsiya turi hisoblanadi. Paketlar asosan axborotlarni bo‘linishidan iborat bo‘lib, har bir paketning o‘rniga uzunligi (xajmi) 46 Baytdan 1500 Baytgacha bo‘lishligi mumkin. Har bir paket bosh sarlavxadan iborat bo‘lib, ma’lumotni yuboruvchisining va qabul qiluvchisining manzillaridan iborat bo‘ladi, hamda ular ketma – ket raqamlanadi. Paketlar har hil yo‘nalishlardan borib, oxirgi tugunda qayta yig‘iladi va qabul qiluvchiga yetkaziladi.

Asosiy avfzalliklari:

1.Kompyuter tarmog‘ining ma’lumotlarini o‘tkazish samaradorligining juda balandligi.

2.Jismoniy aloqa kanallarini o‘tkazish qobiliyatlarini dinamik ravishda o‘zgartirish mumkinligi.

Asosiy kamchiliklari:

1.Paketlar tugunlarda kutib qolishligi mumkinligi sababli ma’lumotlarni uzatish tezligi noaniqligi.

2.Kutib qolish vaqtlari paketlar tarmoqda ko‘pligida juda ham oshib ketishligi.

3.Kommutatsiya buferlarida ma’lumot paketlari ko‘paygan paytda paketlarni tushib qolishligi mumkinligi.

Paketlar kommutatsiyasi kompyuter tarmoqlari 2 sinfga bo‘linadi: 1.Virtual kanal tarmoq. 2.Deytagrammali tarmoq.

Virtual kanalli tarmoqda – bog‘lanishda yagona yo‘nalish asosida ma’lumot uzatiladi, ya’ni dinamik va statik virtual kanal bo‘ladi. Statik virtual kanalni administrator orqali yaratiladi.

Deytagrammali tarmoq elektron pochtaga o‘xshagan bo‘ladi. Ya’ni har bir paket konvertga joylashtiriladi va marshrutizator ularni har hil yo‘nalishlar bo‘yicha qabul qiluvchi oxirgi tarmoq tuguniga yetkazib beradi.

Marshrutizatorlarning ishlash printsiplari:

1. Eng qisqa yo'lni aniqlab jo'natishligi.
2. Eng minimal vaqt ichida ma'lumotlarni yetkazib berishligi.
3. Eng yuqori tezlikdagi kanallar asosida uzatishligi.
4. Eng himoyalangan aloqa kanallarini tanlab uzatishligi.
5. Eng arzon yo'nalish asosida ma'lumotlarni yetkazib berishligi va boshqalar.

Telekommunikatsiya tizimlarida axborot havfsizligi.

Xozirgi kunda kompyuter tizimi va tarmoqlariga quyidagi talablar qo'yiladi:

- Ma'lumotlarni aniq va sifatli uzatish.
- Har xil turdagi ma'lumotlarni to'g'ri taqsimlash, qayta ishlash va saqlash.
- Qabul qilingan ma'lumotlarga operativ javob berish.
- Axborot resurslarini birlashtirish va to'g'ri bo'lish va boshqalar.

Telekommunikatsiya tarmoqlarini raqamlashtirish jarayonlari bilan axborot havfsizligi muammosi oshib bormoqda. Bunga sabab ichki va tashqi havf xatarlar spektri oshib bormoqda:

- aloqa kanallaridan mo'ljallanmagan ma'lumotla chiqib ketmoqda;
- ma'lumotlar olish uchun ruhsat berilmagan aloqa kanallariga kirish ko'paymoqda;
- raqamli tarmoqlarga va tizimlarga ta'sir etish va xujum qilish rivojlanmoqda, ya'ni:
 - a) har xil kompyuter viruslarini yuborish;
 - b) dasturlarga yamoqlar qo'shish;
 - v) telekommunikatsiya tarmoqlarida ma'lumotlar almashinuvini to'sib qo'yish vositalarini qo'llash;
 - g) test dasturlarini faoliyatini buzish va xakozolar.

Shuning uchun, barcha davlatlarda telekommunikatsiya tizimlarini havfsizligini ta'minlash eng dolzarb masala hisoblanadi.

Telekommunikatsiya tizimlarida axborotlarni himoyalash maqsadlari va masalalari quyidagilardan iborat:

1. Tinchlik davrda, har hil vaziyatda yoki tasodafiy favqulot xolatlarida bo'lishidan qat'iy nazar telekommunikatsiya tizimlarining har bir qatlamida tashqi va ichki xujumlarga bardosh berib, ma'lumotlarni butunligini saqlashlik.

2. Shahs, tashkilot va davlatimizning ma'lumotlarini mahfiyligini va konfidentsialligini telekommunikatsiya tizimlarida saqlashlik.

3. Axborot havfsizligiga ta'sir etuvchi ichki va tashqi xujumlarni bashorat etib aniqlash va shunga qarshi iqtisodiy asoslangan usullarni qo'llab, xujumlarni bartaraf etish.

4. Telekommunikatsiya tizimlarida axborot xavfsizligining yagona davlat siyosatini ishlab chiqish.

5. Hozirgi kunda ishlatilayotgan usul va himoyalash vositalarini umumlashtirib standartlash.

6. Axborot havfsizligining davlatimiz tomonidan boshqarish mexanizmini ya'ni litsenziyalash faoliyatini ishlab chiqish. Barcha texnik va dasturiy vositalarni sertifikatsiyalash va hakoza.

Telekommunikatsiya tizimlari va tarmoqlarida quyidagi havf va xatarlar bo'lishligi mumkin:

- stantsiyalarda ishlayotgan xodimlarning axborot havfsizligi bo'yicha qo'yilgan talablarini buzishligi;
- ruhsat berilmagan texnik xodimlarni xonalarga kirishligi;
- ruhsatsiz ma'lumotlarni ko'chirib olishligi;
- ma'lumotlar omboridan ma'lumotlarni o'g'irlashligi;
- telekommunikatsiya tizimidagi ma'lumotlarni o'chirish yoki buzishligi va boshqalar.

Bundan tashqari:

- aloqa kanallaridan o'tayotgan ma'lumotlarni ushlab olish;
- xar hil elektron qurilmalari orqali aloqa kanallaridan uzatilayotgan ma'lumotlarni deshifrlash;
- aloqa liniyalariga radioelektron vositalari orqali ma'lumotlarni so'ndirib qo'yish, boshqarish tizimini ishdan chiqarish va boshqalar.

Ma'lumotlarni ushlab olish nafaqat akustik, yoki radiolaloqa to'lqinlaridan ushlab olinadi, balki ma'lumotlarnisimli aloqa liniyalaridan uzatilayotgan paytda ham amalga oshiriladi.

Barcha ma'lumotlarni chiqarib yuborish kanallarini shartli ravishda uch sinfga bo'lish mumkin:

1. Akustik kanallar.
2. Optik kanallar.
3. Texnik vositalardan chiqayotgan kanallar.

Himoyalalanayotgan telekommunikatsiya tizimlari va tarmoqlarining maydonlari atrofida elektromagnit to'lqinlari, elektr toki orqali o'tayotgan, hamda ko'rinadigan va

infraqizil diapazon to'liqlari orqali ma'lumotlarni bilib olish mumkinligi sababli ularni himoyalash kerak bo'ladi.–

Buzish ixtimolining modellarini yaratish uchun buzuvchini operativ–taktik, texnikaviy va analitik imkoniyatlarini aniqlab baholash zarur.

Buning uchun xujum manbaalarini bilishdan boshlanadi. Agar bunday ma'lumotlar bo'lmasa, telekommunikatsiya tarmoqlari va tizimi ob'ektlari maydoniga yaqin joylaridan akustik, optik yoki elektromagnit to'liqlarini ushlab olishidan boshlanadi. Ayniqsa ob'ektlarda ishlayotgan sotqin xodimlardan extiyot bo'lishlik lozim. Chunki ular qaerdan ma'lumotlarni so'rib olishlikni bilishadi va ularda zamonaviy texnikaviy (uskunaviy va dasturiy) razvedka vositalaridan foydalanishi mumkin.

Bell–Lapadula modeli.

Ushbu model asosan kirishni nazorat va boshqarish uchun mo'ljallangan. Ushbu modelda qo'yilgan shartlar tahlil etilib, yuqori darajali ma'lumotlarni past tabaqali sub'ektlar ko'rishi va olishligi mumkin emasligi belgilab qo'yiladi.

Bell–Lapadula klassik modeli 1975 yili MITRE Corporation kompaniyasining xodimlari Devid Bell va Leonard Lapadula tomonidan yozib chiqilgan edi. Bu modelning ishlab chiqilishiga mahfiy ma'lumotlar (xujjatlar) ni havfsizligini ta'minlash masalasi edi.

Ushbu model quyidagicha ishlaydi: xar bir sub'ektga (shahsga, xujjatlar bilan ishlaydigan xodimlarga) va ob'ektlarga (xujjatlarga) konfidentsial belgi taqdim etiladi, ya'ni eng yuqori (juda mahfiy), mahfiy (mahfiy), xizmat yuzasidan va ochiq (hamma uchun mumkin). Past darajali sub'ektlar yuqori darajali ma'lumotlarni ko'rishga yoki olishga huquqlari yo'q. Sub'ektlarga past darajali ob'ektlardan ma'lumotlarni ko'chirish ham man etiladi.

D. Denning modeli.

Ushbu model asosan auditning yozuviga asoslanib, havfsizlik buzilganligini aniqlab berishi mumkin va oltita asosiy komponentlardan tashkil topgan: 1) Sub'ektlar. 2) Ob'ektlar. 3) Audit yozuvlari. 4) Profili. 5) Anamallik yozuvlari. 6) Faollik qoidasi, ya'ni ruxsatsiz kirishni aniqlovchi tizim.

Landver modeli.

Ma'lumotlarni himoyalash o'yin modeli tizimi asosida yaratilgan. Himoya tizimini "yaratuvchi" qandaydir birlamchi variantini ishlab chiqadi. Analitik (buzuvchi) esa ma'lumotlarni olish, yoki ularni o'zgartirishga xarakat qiladi. Agar shartli "buzuvchi" maqsadga erishsa, u holda "yaratuvchi" boshqa tizim ishlab chiqadi. Shuning uchun mustaxkam tizim qachonki "buzuvchi" tamonidan o'zgartiraolmagan paytda yakunlanadi.

Elektron raqamli imzo.

Elektron imzo telekommunikatsion (ERI) tarmoqlarida uzatilayotgan matnlarni autentifikatsiya qilish uchun ishlatiladi, ya'ni qasddan mo'ljallangan holda xarakat qilayotgan shahslardan himoyalash uchun qo'llaniladi. Ushbu shahslar ma'lumotlarni ushlab olishi, soxtalashi, o'zgartirishi mumkin. Shuning uchun elektron imzoxaqiqatdan qo'l qo'ygan shahsning imzosi ekanligini va yuborilgan matn (xujjat) xaqiqiyligini tasdiqlaydi.

ERI ikki protseduradan iborat, ya'ni 1) qo'l (imzo) qo'yish va 2) tasdiqlash. Imzoni qo'yish protsedurasida mahfiy kalit ishlatiladi, tasdiqlash protsedurasida esa ochiq kalit qo'llaniladi.

ERI tashkil qilinayotgan paytda “yuboruvchi” “M” qo‘l qo‘yilayotgan matnning $h(M)$ xesh–funktsiyasini hisoblab chiqadi. Ushbu xesh – funktsiyaning $h(M)$ hisoblangan qiymatibarcha M tekstning bir qisqa (kichik) ma’lumotning blokini tashkil etadi. Shundan so‘ng hosil bo‘lgan “m” qiymat jo‘natuvchi tomonidan sirli kalit bilan shifrlanadi. Hosil bo‘lgan ikki son M matnning elektron imzosi bo‘ladi.

Yuborilgan ma’lumotni elektron raqamli imzosini tekshirish uchun “qabul” qiluvchi tomonidan $m = h(M)$ xesh – funktsiya qayta hisoblab chiqiladi va ochiq kalit orqali qabul qilingan imzo haqiqiyliги aniqlanadi.

Har bir imzo quyidagi ma’lumotlardan iborat bo‘ladi:

- imzo qo‘yilgan yil, oy, kuni; (datasi)
- qo‘yilgan imzoning farliyat davrining tugashi;
- faylni imzolagan shahsning ismi, sharifi, lavozimi, korxona yoki firmaning nomi va boshqalar;
- imzolaganning ochiq kalit nomi;
- raqamli shahsning imzosi.

Shuning uchun, yuqorida keltirilganlar asosida quyidagilar taklif etiladi:

1.Kompyuter tizimi va tarmoqlarida uzatilayotgan ma’lumotlarni butunligini ta’minlash uchun aloqa kanallarini mustaxkam himoyalash zarur.

2.Kompyuterning texnikaviy vositalarida saqlanayotgan dasturiy ma’lumotlarni va ombordagi barcha ma’lumotlarni butunligini ta’minlash kerak.

Ushbu aloqa kanallaridan borilayotgan ma’lumotlarni xatosiz yetkazib berish uchun quyidagi kodlardan foydalanishi mumkin:

- Xemming kodi, ya’ni ikkilamchi xatolarni aniqlovchi va birlamchi bog‘lanmagan xatolarni to‘g‘rilovchi;
- Bouz Choud Xori kodi, ya’ni uchlamchi xatolarni aniqlovchi va ikkilamchi xatolarni to‘g‘rilovchi;
- Fayr kodi, ya’ni paketlardagi birlamchi xatolarni ham aniqlovchi, ham to‘g‘rilovchi;
- Rid–Solomon kodi, ya’ni paket xatolarni aniqlovchi va to‘g‘rilovchi kodlar.

Telekommunikatsiya tarmoqlarida axborot havfsizligini

ta'minlash texnologiyalari.

1. Tarmoqlarda ekranlash texnologiyalari.

Tarmoq perimetri – ichki sinalgan tarmoq bilan tashqi tarmoqlardan ajratib turuvchi chegara hisoblanadi. Perimetr – tashqi xujumlardan himoyalovchi birinchi liniya. Ushbu perimetrni himoyalovchi vositalar:

- Tarmoqlararo ekranlar;
- Tarmoq qatlamidagi antivirus tizimlari;
- VNP (Virtual Private Network) – shahsiy vertual tarmoq yaratish qurilmalari;
- Perimetr himoyasi – bu ichki tarmoqni tashqi tarmoq bilan xarakatini nazorat etish. Ya'ni bular:
- Internet tarmog'iga ulanish;
- Simsiz aloqa segmentlari;
- Uzoqdan kirish Serveri;
- Filiallarga ajratilgan liniyalar.

Tarmoqlararo ekranlar (ME) – bu mahsus dasturiy yoki uskunaviy vosita bo'lib, tarmoqni ikki yoki undan ko'p bo'laklarga ajratib, tarmoq paketlarini bir yerdan ikkinchi joyga yetkazib berish uchun qabul qilingan qoida hisoblanadi. Tarmoqlararo ekranlarning (ME) asosiy mexanizmi quyidagilardan iborat:

- tarmoq trafikasini filtrlash;
- adreslarni uzatish;
- shifrlash (ya'ni VNP – shahsiy vertual tarmoq yaratish);
- autentifikatsiyalash;
- tarmoq xujumlariga qarshi chiqish;
- marshrutizatorlardagi ro'yxatni boshqarish.

Tarmoqlararo ekranlarning (ME) asosiy funktsiyalaridan hisoblanib, OSI modeli, ya'ni yetti darajali (qatlamli) modelning xoxlagan qatlamida ishtirok etish mumkin va tarmoq trafikasida filtrlash vazifasini bajaradi, ya'ni qandaydir me'zon (kriterie)ga taaluqligini tekshiradi. Masalan, TSR paketining boshiga ya'ni sarlavxasiga qarab, yoki IP datagrammani yuboruvchining adresiga qarab tekshiradi. Yoki fayl hajmiga qarab, hamda OSI modelining har xil qatlamlarida tekshirish mumkin.

Adreslarni jo‘natish (o‘tkazish) ikki hil bo‘lishi mumkin:

- statistik (ikki tomonlama);
- dinamik (adres–portlarni o‘tkazish).

Statistik translyatsiya (yuborish – jo‘natish) – bu ikki tomonlama kelishilgan holda ichki adres bilan tashqi adres to‘g‘ri kelishligi. Uzatish va qabul qilish uskunalarni ish paytida o‘zgarmasligi.

Dinamik translyatsiya esa faqat ichki tarmoqdan chiqish paytidagi bog‘lanish hisoblanadi, Masalan, ichki tarmoqdan Internetga kirish.

Bundan tashqari tarmoqlararo ekranlar (ME) ya’ni filtratsiyalashdan tashqari ular tarmoq trafiklarini shifrlashi ham mumkin. Ushbu shifrlash IP paketlarni tarmoq qatlamida bajariladi, ya’ni VPN tarmoq tuzishda shlyuz vazifasini bajaradi.

VPN tarmoq texnologiyasi

Virtual shaxsiy tarmoqlar (VPN) ikkita bir biridan ancha uzoqda joylashgan LAN mahalliy tarmoqlar umumiy keng hamma uchun ishlatiladigan (foydalaniladigan), masalan, Internet tarmog‘i orqali o‘tadigan aloqa liniyalarida axborotlarni almashinuvining havfsizligini ta’minlab beradi. Ya’ni VPN ikki LAN va LAN VPN orasidagi yoki Remote Access VPN – uzoqdagi filiallarni asosiy tarmoqqa kirishi paytida himoya ta’minlaydi.

VPN ni yaratish paytida tunnellashtirish yoki inkapsulyatsiyalash usulidan foydalaniladi. Ushbu texnologiya aloqa kanali orqali bir tarmoqdan ikkinchi tarmoqqa paketlarni uzatadi. Shu paytda birinchi tarmoq paketi (ma’lumotlar va protokollar) inkapsulyatsiyalanadi va ko‘rinadi. Inkapsulyatsiya kodlashtirish degan emas.

Tunnel – bu ochiq virtual kanal hisoblanadi, bosh nuqtasi sifatida kompyuter– VPN klient (mijoz), marshrutizator, shlyuz yoki tarmoqqa kiruvchi server (Network Access Server – NAS) bo‘lishligi mumkin. Ikkala nuqtada albatta uskunaviy va dasturiy (shifrovchi / deshifrovchi) qurilmalari bo‘lishi kerak va qabul qilingan protokol asosida ishlashi lozim. Shifrlangan va inkapsulyatsiya qilingan paketlar xar hil marshrutizator orqali oxirgi nuqtaga yetkaziladi. Tunnelning asosiy vazifasi bu konfidentsiallikni ta’minlashdan iborat.

VPN larni amalga oshirish usullari:

–Tarmoqlararo ekranlar asosida VPN yaratish. Ushbu variantda ma’lumotlarni potoklarini himoyalash uchun barcha lokal tarmoqlarida bir dona dasturiy–texnikaviy kompleks ishlatiladi.

–Tarmoq tugunining operatsion tizimiga o‘rnatilgan VPN. Ushbu variant eng ma’qul hisoblanib, standart operatsion tizim asosida bajariladi.

–Ichki tarmoq bilan umumiy tashqi tarmoq orasida mahsus kriptografik shlyuz asosida VPN tashkil etiladi.

– VPN kriptografik himoyalash marshrutizator asosida tuzilgan.Ushbu usul yuqori samarali hisoblanadi, ammo ancha qimmat bo‘ladi.

Himoyalash tahlili texnologiyalariga tarmoq skaneri asosiy birinchi qurol hisoblanadi. U juda tezlik bilan yuqori darajali havfni aniqlaydi, ya’ni tarmoq qatlamida noto‘g‘ri sozlangan tarmoqlararo ekranlarni(MSE) yoki xakerlarni buzishi mumkin bo‘lgan Web–serverlarni aniqlaydi va tahlil asosida yo‘riqnoma ishlab chiqaradi.

Ta’sir etuvchi va xujumlarni aniqlovchi komplekslar quyidagilardan iborat:

–Tarmoq ekrani (ME).

–Himoyalash vositalarning tahlili va bo‘sh joylarini qidirish.

–Xujumlarni aniqlovchi vositalar (Intrusion Detection Systems, IDS) .

Xujumlarni aniqlovchi tizim barcha buzulishlarni hisobga olishi zarur. U keng arxitekturaga ega bo‘lishi lozim.

Ushbu aniqlovchi tizim ikk turdagi komponentdan iborat bo‘ladi:

1.Nazorat qiluvchi moduldan (sensorlar, datchiklar, detektorlar) ya’ni ma’lumotlarni yig‘uvchi dasturlar.

2.Boshqaruv modulidan (konsullar, menedjerlar) ya’ni yig‘ilgan ma’lumotlarni qayta ishlash va tahlil etuvchi dasturlar.

Ikkala turdagi modullar tarmoqning bir tugunida yoki bir necha tugunlarida qo‘yilgan bo‘lishi mumkin.

Antivirus texnologiyalari asosan korxona rahbarlari vqa xodimlariga bog‘liq bo‘ladi. Tashkilot yoki korxonalaridagi kompyuterlarga faqat axborot havfsizligi bilan shug‘ullanadigan bo‘limlarning ruxsati bilan litsenziyaga ega bo‘lgan antivirus antivirus vositalaridan foydalanish ruxsat beriladi va faqat yaxshi ishonchli mutaxassis xodimlargina kompyuterlar (serverlarga) o‘rnatish taklif etiladi.

. Kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalari.

Kompyuter tarmoqlarida axborotni himoyalash deb foydalanuvchilarni ruxsatsiz tarmoq elementlari va zaxiralariga egalik qilishni man etishdagi texnik, dasturiy va kriptografik usul va vositalar, hamda tashkiliy tadbirlarga aytiladi. Bevosita telekommunikatsiya kanallarida axborot xavfsizlikni ta'minlash usul va vositalarini quyidagicha tasniflash mumkin. To'sqinlik apparatlarga, ma'lumot tashuvchilarga va boshqalarga kirishga fizikaviy usullar bilan qar-shilik ko'rsatish deb aytiladi.

Egalikni boshqarish — tizim zaxiralari bilan ishlashni tartibga solish usulidir. Ushbu usul quyidagi funktsiyalardan iborat:

- tizimning har bir ob'ektini, elementini identifikatsiyalash, masalan, foydalanuvchilarni;
- identifikatsiya buyicha ob'ektni yoki sub'ektni haqiqiy, asl ekanligini aniklash;
- vakolatlarni tekshirish, ya'ni tanlangan ish tartibi buyicha (reglament) hafta kunini, kunlik soatni, talab qilinadigan zaxiralarni qo'llash mumkin ligini tekshirish;
- qabul qilingan реглаment bo'yicha ishlash sharoitlarini yaratish va ishlashga ruxsat berish;
- himoyalangan zaxiralarga qilingan murojaatlarni qayd qilish;
- ruxsatsiz harakatlarga javob berish, masalan, signal berish, o'chirib qo'yish, so'rovnomani bajarishdan voz kechish va boshqalar.

Niqoblash — ma'lumotlarni o'qib olishni qiyinlashtirish maqsadida ularni kriptografiya orqali kodlash.

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

Majburlash — qabul qilingan qoidalarga asosan ma'lumotlarni qayta ishlash, aks holda foydalanuvchilar modtsiy, ma'muriy va jinoiy jazolanadilar.

Undamoq — axlokiy va odobiy qoidalarga binoan qabul kilingan tartiblarni bajarishga yo'naltirilgan.

Yuqorida keltirilgan usullarni amalga oshirishda quyidagicha tasniflangan vositalarni tadbiq etishadi.

Rasmiy vositalar — shaxslarni ishtirokisiz axborotlarni himoyalash funktsiyalarini bajaradigan vositalardir.

Norasmiy vositalar — bevosita shaxslarni faoliyati yoki uning faoliyatini aniklab beruvchi реглаmentlardir.

Texnikaviy vositalar sifatida elektr, elektromexanik va elektron kurilmalar tushuniladi. Texnikaviy vositalar uz navbatida, fizikaviy va apparatli bo‘lishi mumkin.

Apparat-texnik vositalari deb telekommunikatsiya qurilmalariga kiritilgan yoki u bilan interfeys orqali ulangan qurilmalarga aytiladi. Masalan, ma’lumotlarni nazorat qilishning juftlik chizmasi, ya’ni jo‘natiladigan ma’lumot yo‘lda buzib talqin etilishini aniqlashda qo‘llaniladigan nazorat bo‘lib, avtomatik ravimda ish sonining juftligini (nazorat razryadi bilan birgalikda) tekshiradi.

Fizikaviy texnik vositalar — bu avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, oddiy eshik qulflari, derazada o‘rnatilgan temir panjaralar, qo‘riqlash elektr uskunalari fizikaviy texnik vositalarga kiradi.

Dasturiy vositalar — bu axborotlarni ximoyalash funktsiyalarini bajarish uchun mo‘ljallangan maxsus dasturiy ta’minotdir. Axborotlarni ximoyalashda birinchi navbatda eng keng qo‘llanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parol tizimini keltirish mumkin.

Tashkiliy ximoyalash vositalari - bu telekommunikatsiya uskunalarining yaratilishi va qo‘llanishi jarayonida qabul kilingan tashkiliy-texnikaviy va tashkiliy-huquqiy tadbirlardir. Bunga bevosita misol sifatida quyidagi jarayonlarni keltirish mumkin: binolarning qurilishi, tizimni loyihalash, qurilmalarni o‘rnatish, tekshirish va ishga tushirish.

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

Qonuniy himoyalash vositalari — bu davlat tomonidan ishlab chiqilgan hukukiy hujjatlar sanaladi. Ular bevosita axborotlardan foydalanish, qayta ishlash va uzatishni tartiblashtiradi va ushbu qoidalarni buzuvchilarning mas’uliyatlarini aniqlab beradi. Masalan, Uzbekistan Respublikasi Markaziy banki tomonidan ishlab chiqilgan qoidalarida axborotni himoyalash guruhlarini tashkil qilish, ularning vakolatlari, majburiyatlari va javobgarliklari aniq yoritib berilgan.

Xavfsizlikni ta’minlash usullari va vositalarining rivojlanishini uch boskichga ajratish mumkin:

- 1) dasturiy vositalarni rivojlanishi;
- 2) barcha yunalishlar buyicha rivojlanishi;

3) ushbu bosqichda quyidagi yo‘nalishlar bo‘yicha rivojlanishlar kuzatilmoqda:

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

Hozirgi kunda ma’lumotlarni ruxsatsiz chetga chiqib ketish yo‘llari quyidagilardan iborat:

- elektron nurlarni chetdan turib o‘qib olish;
- aloqa kabellarini elektromagnit tulkinlar bilan nurlatish;
- yashirin tinglash qurilmalarini qo‘llash;
- masofadan rasmga tushirish;
- printerdan chiqadigan akustik to‘lqinlarni o‘qib olish;
- ma’lumot tashuvchilarni va ishlab chiqarish chikindilarini o‘g‘irlash;
- tizim xotirasida saklanib kolgan ma’lumotlarni o‘qib olish;
- ximoyani yengib ma’lumotlarni nusxalash;
- qayd qilingan foydalanuvchi niqobida tizimgakirish;
- dasturiy tuzoklarni qo‘llash;
- dasturlash tillari va operatsion tizimlarning kamchiliklarida foydalanish;
- dasturlarda maxsus belgilangan sharoitlarda ishga tushishi mumkin bo‘lgan qism dasturlarning mavjud bo‘lishi;
- aloqa va apparatlarga noqonuniy ulanish;
- ximoyalash vositalarini qasddan ishdan chiqarish;
- kompyuter viruslarini tizimga kiritish va undan foydalanish.

Ushbu yullardan deyarli barchasining oldini olish mumkin, lekin kompyuter viruslaridan hozirgacha qoniqarli himoya vositalari ishlab chiqilmagan.

Bevosita tarmoq bo‘yicha uzatiladigan ma’lumotlarni himoyalash maqsadida quyidagi tadbirlarni bajarish lozim bo‘ladi:

- uzatiladigan ma’lumotlarni ochib o‘kishdan saqlanish;
- uzatiladigan ma’lumotlarni taxlil qilishdansaqlanish;
- uzatiladigan ma’lumotlarni o‘zgartirishga yo‘l qo‘ymaslik va o‘zgartirishga urinishlarni aniklash;

ma’lumotlarni uzatish maqsadida qo‘llaniladigan dasturiy uzilishlarni aniqlashga yo‘l qo‘ymaslik;

—firibgar ulanishlarning oldini olish. Ushbu tadbirlarni amalga oshirishda asosan kriptografik usullar qo'llaniladi.

EHM himoyasini ta'minlashning texnik vositalari

Kompyuter orqali sodir etiladigan jinoyatlar oqibatida faqatgina AQSh har yili 100 mlrd, dollar zarar ko'radi. O'rtacha har bir jinoyatda 430 ming dollar o'g'irlanadi va jinoyatchini qidirib topish ehti-moli 0,004% ni tashkil etadi. Mutaxassislarning fikricha ushbu jinoyatlarni 80%i bevosita korxonada ishlaydigan xodimlar tomonidan amalga oshiriladi.

Sodir etiladigan jinoyatlarning taxlili quyidagi xulosalarni beradi:

- ko'pgina hisoblash tarmoqlarida foydalanuvchi is talgan ishchi o'rindan tarmoqqa ulanib faoliyat kursatishi mumkin. Natijada jinoyatchi bajargan ishlarni qaysi kompyuterdan amalga oshirilganini aniklash qiyin bo'ladi.
- o'g'irlash natijasida hech nima yo'qolmaydi, shu bois ko'pincha jinoiy ish yuritilmaydi;
- ma'lumotlarga nisbatan mulkchilik xususiyati yo'kligi;
- ma'lumotlarni qayta ishlash jarayonida yo'l qo'yilgan xatolik o'z vaqtida kuzatilmaydi va tuzatilmaydi, natijada kelgusida sodir bo'ladigan xatolarning oldini olib bo'lmaydi;
- sodir etiladigan kompyuter jinoyatlari o'z vaqtida e'lon qilinmaydi, buning sababi hisoblash tarmoklarida kamchiliklar mavjudligini boshqa xodimlardan yashirish xisoblanadi.

Ushbu kamchiliklarni bartaraf qilishda va kompyuter jinoyatlarini kamaytirishda quyidagi chora-tadbirlarni o'tkazish kerak bo'ladi:

- personal mas'uliyatini oshirish;
- ishga qabul qilinadigan xodimlarni tekshiruvdan o'tkazish;
- muhim vazifani bajaruvchi xodimlarni almashtirib turish;
- parol va foydalanuvchilarni qayd qilishni yaxshi yo'lga qo'yish;
- ma'lumotlarga egalik qilishni cheklash;
- ma'lumotlarni shifrlash.

Axborot-kommunikatsiyalar texnologiyalarining rivojlanishi oqibatida ko'pgina axborotni himoyalash instrumental vositalari ishlab chikilgan. Ular dasturiy, dasturiy-texnik va texnik vositalardir.

Hozirgi kunda tarmoq xavfsizligini ta'minlash maqsadida ishlab chikilgan texnikaviy vositalarni quyidagicha tasniflash mumkin:

Fizikaviy himoyalash vositalari — maxsus elektron qurilmalar yordamida ma'lumotlarga egalik qilishni taqiqlash vositalaridir.

Mantiqiy himoyalash -- dasturiy vositalar bilan ma'lumotlarga egalik qilishni taqiqlash uchun qo'llaniladi.

Tarmoqlararo ekranlar va shlyuzlar — tizimga keladigan hamda undan chiqadigan ma'lumotlarni ma'lum hujumlar bilan tekshirib boradi va protokollashtiradi.

Xavfsizlikni auditlash tizimlari -- joriy etilgan operatsiy tizimdan o'rnatilgan parametrlarni zaifligini qidirishda qo'llaniladigan tizimdir.

Real vaqtda ishlaydigan xavfsizlik tizimi — doimiy ravishda tarmoqning xavfsizligini taxlillash va auditlashni ta'minlaydi.

Stoxastik testlarni tashkillashtirish vositalari — axborot tizimlarining sifati va ishonchliligini tek-shirishda qo'llaniladigan vositadir.

Aniq yo'naltirilgan testlar — axborot-kommunikatsiyalar texnologiyalarining sifati va ishonchliligini tekshirishda qo'llaniladi.

Xavflarni imitatsiya qilish — axborot tizimlariga nisbatan xavflar yaratiladi va himoyaning samaradorligi anikdanadi.

Statistik taxlilgichlar — dasturlarning tuzilish tarkibidagi kamchiliklarni aniklash, dasturlar kodida aniklanmagan kirish va chikish nuktalarini topish, dasturdagi o'zgaruvchilarni to'g'ri aniqlanganligini va ko'zda tutilmagan ishlarni bajaruvchi kiem dasturlarini anikdashda foydalaniladi.

Dinamik tahlilgichlar — bajariladigan dasturlarni kuzatib borish va tizimda sodir bo'ladigan o'zgarishlarni aniqlashda qo'llaniladi.

Tarmoqning zaifligishsh aniqlash — tarmoq zaxiralariga sun'iy hujumlarni tashkil qilish bilan mavjud zaifliklarni aniqlashda qo'llaniladi.

Misol sifatida quyidagi vositalarni keltirish mumkin:

- Dallas Lock for Administrator -- mavjud elektron Proximity uskunasi asosida yaratilgan dasturiy-texnik vosita bulib, bevosita ma'lumotlarga ruxsatsiz kirishni nazorat qilishda qo'llaniladi;

- Security Administrator Tool for ANALYZING Networks (SATAN) — dasturiy ta'minot bo'lib, bevosita tarmoqning zaif tomonlarini aniqlaydi va ularni bartaraf etish yo'llarini ko'rsatib beradi. Ushbu yo'nalish bo'yicha bir necha dasturlar ishlab chiqilgan, masalan: Internet Security Scanner, Net Scanner, Internet Scanner va boshqalar.
- NBS tizimi - - dasturiy-texnik vosita bo'lib, aloqa kanallarvdagi ma'lumotlarni himoyalashda qo'llaniladi;
- Free Space Communication System — tarmoqta ma'lumotlarning har xil nurlar orqali, masalan lazerli nurlar orqali almashuvini ta'minlaydi;
- SDS tizimi — ushbu dasturiy tizim ma'lumotlarini nazorat qiladi va qaydnomada aks ettiradi. Asosiy vazifasi ma'lumotlarni uzatish vositalariga ruxsatsiz kirishni nazorat qilishdir;
- Timekey — dasturiy-texnik uskunadir, bevosita EHMning parallel portiga o'rnatiladi va dasturlarni belgilangan vaqtda keng qo'llanilishini taqiqlaydi;
- IDX — dasturiy-texnik vosita, foydalanuvchining barmoq izlarini «o'qib olish» va uni taxlil qiluvchi texnikalardan iborat bo'lib, yuqori sifatli axborot xavfsizligini ta'minlaydi. Barmoq izlarini o'qib olish va xotirada saqlash uchun 1 minutgacha, uni taqqoslash uchun esa 6 sekundgacha vaqt talab qilinadi.

Kompyuter tarmoqlarida ma'lumotlarni himoyalashning asosiy yo'nalishlari

Axborotlarni ximoyalashning mavjud usul va vositalari hamda kompyuter tarmoqlari kanallaridagi aloqaning xavfsizligini ta'minlash texnologiyasi evolyutsiyasini solishtirish shuni ko'rsatmokdaki, bu texnologiya rivojlanishining birinchi bosqichida dasturiy vositalar afzal topildi va rivojlanishga ega bo'ldi, ikkinchi bosqichida ximoyaning hamma asosiy usullari va vositalari intensiv rivojlanishi bilan xarakterlandi, uchinchi bosqichida esa quyidagi tendentsiyalar ravshan bo'lmoqda:

- axborotlarni himoyalash asosiy funktsiyalarining texnik jixatdan amalga oshirilishi;
- bir nechta xavfsizlik funktsiyalarini bajaruvchi himoyalashning birgalikdagi vositalarini yaratish;
- algoritm va texnik vositalarni unifikatsiya qilish va standartlashtirish.

Kompyuter tarmoqlarida xavfsizlikni ta'minlashda hujumlar yuqori darajada malakaga ega bo'lgan mutaxassislar tomonidan amalga oshiryushshini doim esda tutish

lozim. Bunda ularning harakat modellaridan doimo ustun turuvchi modellar yaratish talab etiladi. Bundan tashqari, avtomatlashtirilgan axborot tizimlarida personal eng ta'sirchan qismlardan biridir. Shuning uchun, yovuz niyatli shaxsga axborot tizimi personalidan foydalana olmaslik chora-tadbirlarini o'tkazib turish ham katta ahamiyatga ega. Internet tarmog'ida mavjud aloqaning himoyasini (xavfsizligini) ta'minlash asoslari, ma'lumotlarni uzatish tizimlarining rivojlanishi va ular asosida yaratilgan telekommunikatsiya xizmat kursatish vositalarining yaratilishi bevosita foydalanuvchilarga tarmoq zaxiralaridan foydalanish tartiblarini ishlab chiqarish zaruriyatini paydo kildi:

- foydalanuvchining anonimligini ta'minlovchi vositalar;
- serverga kirishni ta'minlash. Server faqatgina bitta foydalanuvchiga emas, balki keng miqyosdagi foydalanuvchilarga uz zaxiralaridan foydalanishga ruxsatberishi kerak;
- ruxsatsiz kirishdan tarmoqni himoyalash vositalari. Internet tarmogida ruxsatsiz kirishni taqiqlovchi tarmoqlararo ekran -- Fire Wall vositalari keng tarqalgan. Ushbu vosita asosan UNIX operatsion tizimlarida qo'llanilib, bevosita tarmoqdar orasida aloqa o'rnatish jarayonida xavfsizlikni ta'minlaydi. Bundan tashqari, Fire Wall tizimlari tashqi muhit, masalan, Internet uchun, asosiy ma'lumotlarni va MBlarni xotirasida saqlab, bevosita ma'lumot almashuvini ta'minlashi va korxona tizimiga kirishini taqiqlashi mumkin. Lekin Fire Wall tizimlarining kamchiliklari ham mavjud, masalan, Yemail orqali dasturlar jo'natilib, ichki tizimga tushgandan so'ng o'zining qora niyatlarini bajarishda ushbu ximoya ojizlik qiladi. Fire Wall sinfidagi tizimlarning asosiy qismi tashqi hujumlarni qaytarish uchun mo'ljallangan bo'lsa ham, hujumlar ularning 60 foizi kuchsiz ekanligini ko'rsatdi. Bundan tashqari, Fire Wall zabt etilgan serverning ipshashiga qarshilik ko'rsata olmaydi.

Shu bois, Internet tizimida xavfsizlikni ta'minlash bo'yicha quyidagi o'zgarishlar kutilmoqda:

- Fire Wall tizimlarining bevosita xavfsizlik tizimlariga kiritilishi;
- tarmoq protokollari bevosita foydalanuvchilarni huquqlarini aniqlovchi, xabarlarining yaxlitligini ta'minlovchi va ma'lumotlarni shifrlovchi dasturiy imkoniyatlaridan iborat bo'lishlari. Hozirgi kunda ushbu protokollarni yaratish bo'yicha anchagina ipsharolib borilmokda. SKIP protokoli (Simple Key management for Internet Protocol - Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi) shunga misol bo'laoladi.

Kriptografiya

O‘rinlarni almashtirish usullari eng oddiy va eng kadimiy usuldir. O‘rinlarni almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin:

— shifrovchi jadval;

— sexrli kvadrat.

Shifrovchi jadval usulida kalit sifatida quyidagilar ko‘llaniladi:

- jadval o‘lchovlari;

- so‘z yoki so‘zlar ketma-ketligi;

- jadval tarkibi xususiyatlari.

Misol.

Kuyidagi matn berilgan bo‘lsin:

KADRLAR TAYYORLASH MILLIY DASTURI

Ushbu axborot ustun buyicha ketma-ket jadvalga kiritiladi:

| | | | | | | |
|---|---|----|----|---|---|---|
| k | l | a | l | i | y | t |
| a | a | y | a | l | d | u |
| d | r | yo | sh | l | a | r |
| r | t | r | m | i | s | i |

Natijada, 4x7 o‘lchovli jadval tashkil kilinadi.

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

KLAL IYTA AYAL DUDR YoShLA RRTR MISI

Bu yerda kalit sifatida jadval o‘lchovlari xizmat kiladi.

Ushbu usulni murakkablashtirish maksadida tayanch so‘zni kiritsa bo‘ladi. Yukoridagi misol uchun quyidagi

MAGISTRso‘zini olamiz va oldingi jadvalga joylashtiramiz:

| | | | | | | |
|---|---|----|----|---|---|---|
| m | a | g | i | s | t | r |
| 4 | 1 | 2 | 3 | 6 | 7 | 5 |
| k | l | a | l | i | y | t |
| a | a | y | a | l | d | u |
| d | r | yo | sh | l | a | r |
| r | t | r | m | i | s | i |

Ikkinchi katordagi rakamlar xarflarning alifbo tarkibidan kelib chikadi. Shu katordagi rakamlar bo'yicha ustunlarni tartiblaymiz:

| | | | | | | |
|---|----|----|---|---|---|---|
| a | g | i | m | r | s | t |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| l | a | l | k | t | i | y |
| a | y | a | a | u | l | d |
| r | yo | sh | d | r | l | a |
| t | r | m | r | i | i | s |

Shifrlangan matn kuyidagi ko'rinishda bo'ladi:

LALK TIYA YAAU LDRYo ShDRL ATRM RIIS,

Sexrli kvadrat deb, katakchalariga 1 dan boshlab sonlar yozilgan, undagi xar bir ustun, satr va diagonal buyicha sonlar yigindisi bitta songa teng bo'lgan kvadrat shaklidagi jadvalga aytiladi. Sexrli kvadratga sonlar tartibi bo'yicha belgilar kiritiladi va bu belgilar satrlar buyicha o'kilganda matn xosil bo'ladi.

Misol.

4x4 o'lchovli sexrli kvadratni olamiz, bu yerda son-larning 880 ta xar xil kombinatsiyasi mavjud. Kuyidagicha ish yuritamiz:

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

Boshlangich matn sifatida kuyidagi matnni olamiz:

DASTURLASH TILLARI va jadvalga joylashtiramiz:

| | | | |
|----|---|---|---|
| i | s | a | l |
| u | t | i | a |
| sh | r | l | l |
| t | r | a | d |

Shifrlangan matn jadval elementlarini satrlar bo'yicha o'kish natijasida tashkil topadi:
ISAL UTIA ShRLL TRAD

Almashtirish usullari:

Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin:

- Sezar usuli;
- Affin tizimidagi Sezar usuli;
- Tayanch so'zli Sezar usuli va boshkalar.

1. Sezar usulida almashtiruvchi xarflar k ta siljish bilan aniklanadi. Yuliy Sezar bevosita $k=3$ bulganda ushbu usuldan foydalangan.

$k=3$ bo'lganda va alifbodagi xarflar $m=26$ ta bo'lganda quyidagi jadval xosil kilinadi:

Misol.

Matn sifatida SAMARQAND so'zini oladigan bo'lsak, Sezar usuli natijasida quyidagi shifrlangan yozuv xosil bo'ladi: VDPDUTDQG.

2. Sezar usulining kamchiligi bu bir xil xarflarning, o'z navbatida, bir xil xarflarga almashishidir.

3. Affin tizimidagi Sezar usulida xar bir xarfga almashtiriluvchi xarflar maxsus formula bo'yicha aniklanadi: $at+b \pmod m$, bu yerda a, b — butun sonlar, $0 < a, b < m$, EKUB $(a, t)=1$.

Xozirgi vaktida kompyuter tarmoklarida tijorat axborotlari bilan almashishda uchta asosiy algoritm-lar, ya'ni DES, CLIPPER va PGP algoritmlari ko'llanilmokda. DES va CLIPPER algoritmlari integral sxemalarda amalga oshiriladi. DES algoritmining kriptomustaxkamligini quyidagi misol orkali xam baxolash mumkin: 10 mln. AKSh dollari xarajat kilinganda DES shifrini ochish uchun 21 minut, 100 mln. AKSh dollari xarajat kilinganda esa 2 minut sarflanadi. CLIPPER tizimi SKIPJACK shifrlash algoritmini uz ichiga oladi va bu algoritm DES algoritmidan 16 mln. marta kuchliroqtsir. PGP algoritmi esa 1991 yilda Filipp Simmer-man (AKSh) tomonidan yozilgan va elektron pochta orkali uzatiladigan xabarlarni shifrlash uchun ishlatiladigan PGP dasturlar paketi yordamida amalga oshiriladi. PGP dasturiy vositalari Internet

tarmogida elektron pochta orkali axborot jo‘natuvchi foydalanuvchilar tomonidan shifrlash maksadida keng foydalanilmokda.

PGP (Pretty Good Privacy) kriptografiya dasturining algoritmi kalitli, ochik va yopik bo‘ladi. Ochikkalit kuyidagicha ko‘rinishni olishi mumkin:

EDF21pI4 BEGIN PGP PUBLIC KEY BLOCK

Version: 2.6.31

mQCNazFHgwAAAEEOvroJEWEq6npGLZTqssS5EScVUPV

aRu4ePLiDjUz6U7aQr

Wk45dIxg0797PFNvPcMRzQZeTxY10ftyMHL/6ZF9wex64jy

LH40tE2DOG9yqwKAn

yUDFpgRmoL3pbxXZx91OOuuzlkAz+xU6OwGx/EBKYOKPTTt

DzSLOAQxLTyGZAAUR

tClCb2IgU3dhbnNvbiA8cmpzd2FuQHNIYXRObGUtd2Vid29ya

3MuY29tPokAlQMF

h53aEsqJyQEB6JcD/RPxxg6g7tfHFiOQiaf5yaHOYGEVoxcd-

FyZXr/ITz

rgztNXRUiOqU2MDEmh2RoEcDs!fGVZHSRpkCg8iS+35sAz

9c2S+q5vQxOsZJz72B

LZl :FT7?fhC3fZZD9X91MsJH+xxX9CDx92xmllglMT25SOX

2o/uBA<rJ3K:pEI6g6xv

END PGP PUBLIC KEY BLOCK—

Ushbu ochik kalit bevosita Web saxifalarda yoki elektron pochta orkali ochikchasiga yuborilishi mumkin. Ochik kalitdan foydalangan jo‘natilgan shifrlan axborotni axborot yuborilgan manzil egasidan boshqa shaxs o‘kiy olmaydi. PGP orkali shifrlangan axborotlarni ochish uchun, superkompyuterlar ishlatilganda bir asr xam kamlik kilishi mumkin. Bulardan tashkari, axborotlarni tasvirlarda va tovushlarda yashirish dasturlari xam mavjud. Masalan, S-tools dasturi axborotlarni BMP, GIF, WAV kengaytmali fayllarda saklash uchun ko‘llaniladi. Ba’zi xollarda yashirilgan axborotning xajmi rasmning xajmidan ko‘p bo‘lishi xam mumkin, ya’ni olingan natija fakatgina tanlangan rasmga boglik bo‘ladi. Kundalik jarayonda foydalanuvchilar ofis dasturlari va arxivatorlarni ko‘llab kelishadi. Arxivatorlar, masalan PkZip dasturida ma’lumotlarni parol yordamida shifrlash mumkin. Ushbu fayllarni ochishda ikkita, ya’ni lugatli va to‘gridan-to‘gri usuldan foydalanishadi. Lugatli usulda bevosita maxsus fayldan so‘zlar parol o‘rniga ko‘yib tekshiriladi, to‘gridan-to‘gri usulda esa bevosita belgilar kombinatsiyasi tuzilib, parol o‘rniga ko‘yib tekshiriladi.

Ofis dasturlari (Word, Excel, Access) orkali ximoyalash umuman taklif etilmaydi. Bu borada mavjud dasturlar Internet da to‘siksiz tarkatiladi.

Amaliyot mashg'ulotlar va laboratoriya ishlarini bajarish uchun tavsiyalar

Axborot havfsizligi qismi bo'yicha qismi bo'yicha amaliyot mashg'ulotining

Rejasi.

1. Kompyuter tizimi va tarmoqlarda havf - xatarlar qanday hosil bo'lishligini va ularning turlarini aniq bilishligi va ularni misollarda aytib berishligi.
2. Kompyuter tizimi va tarmoqlarda xujumlar qanday turlarga bo'linishligi va qanday yo'llar bilan kompyuter tizimiga kirib kelishligini misollar bilan aytib va ko'rsatib berishligi lozim. Hujumlarni qanday aniqlash va tahlil qilish mumkin?
3. Kompyuter tizimi va tarmoqlarda axborotni himolash vositalari nimalardan iborat?
4. Tashkiliy himoyalash vositalari nimalardan iborat va qanday misollar keltirish mumkin? Jismoniy himolash vositalaridan nima bilan farq qiladi?
5. Texnikaviy (uskunaviy) himoyalash vositalari qanday printsip asosida tuziladi va zamonaviy axborot texnologiyalarida qanday va qayerlarda ishlatiladi?
6. Dasturiy himoyalash vositalari qayerlarda va qanday yaratiladi? Hozirgi kunda ishlatilayotgan texnikaviy - dasturiy vositalarning ishlash printsipini aytib berish lozim.
7. Jismoniy himoyalash vositalari qanday tashkil etiladi? Ularga misollar keltiring.
8. Xuquqiy himoyalash vositalari nimalardan iborat va qanday xujjatlar bilan amalga oshiriladi? Qanday qonunlar, farmonlar, farmoyishlar, qaror va buyruqlar mavjud?
9. Fire Wall tizimi nima va u qanday ishlaydi?
10. Real Secure tizimi nima? U qanday komponentlardan iborat? Ishlash printsipi.
11. Real Secure sistemasining qobiliyati qanday?
12. Real Secure tizimi ishlashi uchun qanday uskunaviy va dasturiy ta'minotlarga talablar qo'yiladi?.
13. Internet Scanner tizimi nima? U qanday komponentlardan iborat? Ishlash printsipi.
14. Internet Scanner tizimi ishlashiga qanday talablar qo'yilgan?

15. Secret net tizimi qanday tizim? Ishlash printsipli.
16. Kriptografik himoyalash vositalarining qanday usullari bor. Ularning farqini tushuntirib berish lozim.
17. Simmetriyali kriptotizm asoslari qanday yaratiladi?.
18. Asimmetriyali ikki kalitli kriptografiya tizimi qanday tuziladi?
19. Kriptografiya himoyasida shifrlarga qanday talablar qo'yiladi? Ushbu talablarga qanday tizimlar javob beradi?
20. O'rin almashtirish usullaridan shifrovchi jadval qanday yaratiladi? Misollar bilan tushuntirib berish kerak.
21. O'rin almashtirish usullaridan sehrli kvadrat qanday yaratiladi? Misollar bilan tushuntirib berish kerak.
22. Sezar va Affin tizimdagi Sezar usuli qanday tuziladi?
23. Elektron xujjat almashish usulining ishlash printsipli qanday?
24. Elektron imzo tizimi qanday ishlaydi?
25. Kompyuter tizimi va tarmoqlarining aloqa kanallarida axborotlar qanday himoyalangani?
26. Tarmoqlararo ekranlar texnologiyasi nima?
27. VPN texnologiyasi asosida tuzilgan kompyuter tarmoqlari qanday ishlaydi?
28. Kompyuter viruslari va ularning turlari. Kimlar viruslarni yaratadi?
29. Zararli va o'ta zararli viruslar qanday ta'sir etadi?
30. Antivirus dasturlari va ularning turlari. Antivirus dasturlarini o'rnatish.

Axborot havfsizligi qismi bo'yicha

laboratoriya o'tkazish uchun quyidagi texnikaviy qurilmalar kerak:

1. Fire Wall, Real Secure, Internet Scanner, Secret net yoki boshqa texnikaviy-dasturiy vositalar.
2. VPN kompyuter tarmog'i.
3. Analogo-tsifrovoy va tsifro-analogli (ASP va SAP) almashtiruvchi qurilmalar.
4. Axborot havfsizligini aniqlovchi stendlar, o'lchov priborlari va boshqalar.

Afsuski, ushbu qurilmalar oliy o'quv yurtlarida bo'lmaganligi sababli talabalarni va magistrnlarni kelajakda yaxshi mutaxassis bo'lib chiqishligi uchun ularni yuqorida keltirilgan reja asosida amaliy mashg'ulotlar o'tkazib tushuntirishimiz kerak. Bularni esa kompyuter orqali amalga oshirish mumkin. Shuning uchun, amaliy mashg'ulot rejasi quyidagicha bo'ladi:

1. Kompyuterda uzatuvchi, qabul qiluvchi va g'arazli ob'ektning strukturasi yaratish lozim.
2. Har xil hujumlar modelini yaratib, xarakatga keltirish kerak.
3. Internet tizimidan LEX.UZ saytiga kirib O'zbekiston Respublikasida tasdiqlangan qonunlar, qarorlar, farmon va farmoyishlarni ko'chirib olish va ularni tushunish zarur.
4. Kriptografik himoyalanish vositalaridan o'rin almashtirish usullaridan shifrllovchi jadval algoritmini tuzdirish va dasturini yaratish lozim.
5. Kriptografik himoyalanish vositalaridan o'rin almashtirish usullaridan sehrli kvadrat algoritmini tuzdirish va dasturini yaratish lozim.
6. Sezar va Affin tizimdagi Sezar usuli asosida algoritm yaratish va dastur tuzish kerak.
7. Kompyuterlarga, fayllarga, papkalarga va fleshkalarga parol o'rnatishni bajarish kerak.
8. Antivirus dasturlarini kompyuterga o'rnatish usullarini amalda bajarish lozim.
9. Kompyuter xonasidagi kompyuterlar lokal tarmoqqa ulanganligi sababli sun'iy xujumlar yaratib, "Setevoe okrujenie" orqali boshqa kompyuterlarda himoyalanish usullaridan foydalanish yo'llarini modelini tuzish kerak.
10. Barcha yaratilgan va ishlab chiqilgan axborot havfsizligi algoritmlari xarakatga keltirilishi lozim.

“Axborot havfsizligi” bo‘yicha Test savollari

1. “Axborot havfsizligi” tushunchasiga quyidagi ta’riflarning qaysi biri to‘liq va to‘g‘ri berilgan?
*a) Axborot havfsizligi deb ma’lumotlarni yo‘qotish va o‘zgartirishga yo‘naltirilgan tabiiy yoki sun’iy xossali, tasodifiy yoki qasddan qilingan ta’sirlardan himoyalanganligiga aytiladi
b) Axborot havfsizligi deb ma’lumotlarni viruslardan, kompyuterning ishdan chiqishi uchun qilingan ta’sirlardan himoyalanganligiga aytiladi
c) Foydalanuvchining hulq - atvoriga bog‘liq
d) Axborot havfsizligi – bu ma’lumotlarni himoyalab saqlash.
2. Axborotni himoyalash deganda nima tushuniladi?
*a) Axborot havfsizligini ta’minlovchi xarakterliklar majmuasi
b) Kompyuterning ishdan chiqishini oldini olish
c) Ma’lumotning yo‘qotilishi va o‘zgartirilishiga yo‘l qo‘ymaslik
d) Viruslardan himoyalash.
3. Axborot havfsizligi nuqtai nazaridan axborotni qanday turkumlash mumkin?
a) ishonchlilik, maxfiylik, yaxlitlik, qasddan buzilishlarga to‘sqinlik
b) autentifikatsiya, nazorat qilinishi, tizimga kirishni nazorat qilishni nazorat qilish
*c) maxfiylik, konfidentsiallik, yaxlitlik, autentifikatsiya, appelyatsiya qilishlik
d) aniqlilik, nazorat qilishlik, ishonchlilik, maxfiylik, yaxlitlik
4. Axborot tizimiga nisbatan qanday tasnifni keltirish mumkin?
*a) ishonchlilik, aniqlilik, nazorat qilishlik, tizimga kirishni nazorat qilish, nazorat qilinishi, identifikatsiyani nazorat qilish, qasddan buzilishlarga to‘sqinlik
b) autentifikatsiya, nazorat qilinishi, konfidentsiallik, yaxlitlik, autentifikatsiya
c) konfidentsiallik, yaxlitlik, autentifikatsiya, appelyatsiya qilishlik, nazorat qilishlik
d) ishonchlilik, aniqlilik, nazorat qilishlik, maxfiylik, konfidentsiallik, yaxlitlik, autentifikatsiya, appelyatsiya qilishlik
5. Takiliy himoyalash vositalari barcha himoyalash vositalarning necha foizini tashkil etadi?
a) 35 – 40 foizini
b) 20 – 35 foizini
c) 40 - 50 foizini
*d) 50 – 60 foizini
6. “Axborot havfsizligi” va “Kompyuter havfsizligi” tushunchalarining qaysisi keng tushuncha?
*a) Axborot havfsizligi tushunchasi
b) Kompyuter havfsizligi tushunchasi
c) Ekvivalent tushunchalar
d) Ikkisi ham to‘g‘ri.

7. Axborot havfsizligini ta'minlash, kompyuterdan tashqari ya'na nimalarga bog'liq?

*a) Elektr, suv, ilig'liq tizimlari, sovutqich, kommunikatsiya manbalari va albatta xizmat ko'rsatish persanallariga bog'liq

b) Administratorning tajribaliligiga bog'liq

c) Foydalanuvchining hulq - atvoriga bog'liq

d) Insonga bog'liq.

8. Kompyuter tizimi va tarmoqlarda havf va xatarlar necha turga bo'linadi?

a) bitta

*b) ikkita

s) uchta

d) to'rtta

9. Kompyuter tizimi va tarmoqlarda axborotlarni himoyalash vositalariga qaysi birlari to'liq ko'rsatilgan?

*a) tashkiliy, texnikaviy, dasturiy, jismoniy, xuquqiy, kriptografik, aloqa kanallarda axborotlarni himoyalash, viruslardan himoyalash

b) tashkiliy, uskunaviy va dasturiy

s) kriptografik va viruslardan himoyalash

d) texnikaviy va dasturiy.

10. Xarbiy muassada va o'quv muassada axborotlar bazasining havfsizligini ta'minlash qanaqa shiyor ostida amalga oshiriladi?

*a) Xarbiy muassada - "axborot bazasini ishdan chiqarsa ham mayli, lekin axborot fosh bo'lmasin", o'quv muassada - "bizda hech qanday Mahfiylik yo'q, asosiysi ishdan chiqmasa bo'ldi"

b) Xarbiy muassada - "bizda hech qanday Mahfiylik yo'q, asosiysi ishdan chiqmasa bo'ldi", o'quv muassada - "axborot bazasini ishdan chiqarsa ham mayli, lekin axborot fosh bo'lmasin"

c) Xarbiy muassada va o'quv muassada da ham axborot mahfiligini ta'minlash birinchi o'rinda turadi

d) Maxfiy ma'lumotlarni fosh etish taqiqlanadi.

11. Kompyuter tizimlari va tarmoqlarida mavjud havf turlari qaysi javobda to'g'ri ko'rsatilgan?

*a) Uzish (raz'edinenie), ushlab qolish (perexvat), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya)

b) Uzish (raz'edinenie), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya), aktiv

c) Ushlab qolish (perexvat), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya), passiv

d) Kompyuterdagi va uzatilayotgan ma'lumotlarni ruxsatsiz ko'chirib olish.

12. Kompyuter tizimi va tarmoqlarda xujum turlari nechta?

a) bitta

*b) ikkita

s) uchta

d) to'rtta

13. Kompyuter tizimlari va tarmoqlarida mavjud xujum turlari qaysi javobda to'g'ri ko'rsatilgan?

*a) Aktiv va passiv

b) Turlash (modifikatsiya), soxtalashtirish (falsifikatsiya), ushlab qolish (perexvat), aktiv

c) Uzish (raz'edinenie), ushlab qolish (perexvat), passiv

d) Xakerlar orqali ma'lumotlarni o'g'irlash.

14. Kompyuter tizimlari va tarmoqlarida mavjud uzish (raz'edinenie) havf turining funktsiyasiga ta'rif qaysi javobda to'g'ri ko'rsatilgan?

*a) Tizim resursi yo'q qilinadi. Natijada axborotdan foydalanuvchanlik buziladi (dostupnost)

- b) Resursdan ruxsat berilmagan foydalanuvchiga yo‘l ochiladi. Natijada axborotning mahfiligi yo‘qoladi (konfidentsialnost)
- c) Resursdan nafaqat noqonuniy foydalanishga yo‘l ochiladi, balki resurs buzg‘unchi tomonidan o‘zgartiriladi. Natijada axborotning yaxlitligi buziladi (tselostnost)
- d) Tizimga soxta ob‘ekt kiritiladi. Natijada axborotning asliga to‘g‘riligi buziladi (autentifikatsiya).

15. Kompter tizimlari va tarmoqlarida mavjud ushlab qolish (perexvat) havf turining funktsiyasiga ta‘rif qaysi javobda to‘g‘ri ko‘rsatilgan?

- *a) Resursdan ruxsat berilmagan foydalanuvchiga yo‘l ochiladi. Natijada axborotning mahfiligi yo‘qoladi (konfidentsialnost)
- b) Tizim resursi yo‘q qilinadi. Natijada axborotdan foydalanuvchanlik buziladi (dostupnost)
- c) Resursdan nafaqat noqonuniy foydalanishga yo‘l ochiladi, balki resurs buzg‘unchi tomonidan o‘zgartiriladi. Natijada axborotning yaxlitligi buziladi (tselostnost)
- d) Tizimga soxta ob‘ekt kiritiladi. Natijada axborotning asliga to‘g‘riligi buziladi (autentifikatsiya).

16. Kompter tizimlari va tarmoqlarida mavjud turlash (modifikatsiya) havf turining funktsiyasiga ta‘rif qaysi javobda to‘g‘ri ko‘rsatilgan?

- *a) Resursdan nafaqat noqonuniy foydalanishga yo‘l ochiladi, balki resurs buzg‘unchi tomonidan o‘zgartiriladi. Natijada axborotning yaxlitligi buziladi (tselostnost)
- b) Tizim resursi yo‘q qilinadi. Natijada axborotdan foydalanuvchanlik buziladi (dostupnost)
- c) Resursdan ruxsat berilmagan foydalanuvchiga yo‘l ochiladi. Natijada axborotning mahfiligi yo‘qoladi (konfidentsialnost)
- d) Tizimga soxta ob‘ekt kiritiladi. Natijada axborotning asliga to‘g‘riligi buziladi (autentifikatsiya)

17. Kompter tizimlari va tarmoqlarida mavjud soxtalashtirish (falsifikatsiya) havf turining funktsiyasiga ta‘rif qaysi javobda to‘g‘ri ko‘rsatilgan?

- *a) Tizimga soxta ob‘ekt kiritiladi. Natijada axborotning asliga to‘g‘riligi buziladi (autentifikatsiya)
- b) Tizim resursi yo‘q qilinadi. Natijada axborotdan foydalanuvchanlik buziladi (dostupnost)
- c) Resursdan ruxsat berilmagan foydalanuvchiga yo‘l ochiladi. Natijada axborotning mahfiligi yo‘qoladi (konfidentsialnost)
- d) Resursdan nafaqat noqonuniy foydalanishga yo‘l ochiladi, balki resurs buzg‘unchi tomonidan o‘zgartiriladi. Natijada axborotning yaxlitligi buziladi (tselostnost)

18. Xujumlarni passiv va aktiv deb klassifikatsiyalaganda qo‘yidagidan qaysisi to‘g‘ri ko‘rsatilgan?

- *a) Passiv-ushlab qolish (perexvat). Aktiv-uzish (raz‘edinenie), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya)
- b) Aktiv-ushlab qolish (perexvat). Passiv-uzish(raz‘edinenie), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya)
- c) Passiv-ushlab qolish (perexvat), uzish (raz‘edinenie). Aktiv- turlash (modifikatsiya), soxtalashtirish (falsifikatsiya)
- d) Passiv- ruxsatsiz kirish. Aktiv – o‘chirib tashlash.

19. Kompyuter tizimlari va tarmoqlarida qaysi xujumni aniqlash oson emas?

- *a) Passiv xujumni
- b) Aktiv xujumni barcha xarakatlarini
- c) Aktiv xujumning kompyuterga kirib olishini.
- d) Aktiv xujumning ma‘lumotlarni rxsatsiz ko‘chirib olishini.

20. Himoyaning buzilishlari deganda nimani tushunasiz?

- *a) Korxonaga tegishli informatsiyani saqlash va ishlatish havfsizligiga zarar keltiruvchi xar qanday xarakatlarga aytiladi

- b) Himoyaning buzilishlarini aniqlash va bartaraf etish xamda buzilishlar oqibatini yo'qotish mexanizmlari
- c) Ma'lumotlarni ishlash sistemalari va korxonaga tegishli axborotni tashash havfsizligi saviyasini ko'tarish mo'ljallangan servis xizmatlari
- d) Kompyuterdagi barcha ma'lumotlarni o'chib ketishi.

21. Stenografiya bilan kriptografiyaning qanday farqi bor?

- a) stenografiya xabarlarini shifrlaydi, kriptografiya esa mahfiy ma'lumotlarni yashiradi
- b) stenografiya xabarlarini kodlarga aylantirib beradi, kriptografiya esa maxfiy xabarning mavjudligini yashiradi
- *c) kriptografiya maxfiy xabar mazmunini shifrlaydi, stenografiya esa maxfiy xabarning mavjudligini yashiradi
- d) kriptografiya yovuz niyatli shaxslarga nisbatan qo'llaniladi, stenografiya esa faqat maxfiy xabarlar uchun ishlatiladi

22. Kriptologiya soxasi necha bo'limdan iborat?

- a) bitta
- *b) ikkita
- c) uchta
- d) to'rtta

23. Kritotizim necha sinfga bo'linadi?

- a) bitta
- *b) ikkita
- c) uchta
- d) to'rtta

24. Simmetriya tizim qanday tizim?

- a) bir ochiq kalitli
- b) ikki ochiq kalitli
- *c) bir yopiq kalitli
- d) bir ochiq va bir yopiq kalitli

25. Asimmetriyali tizim qanday tizim?

- a) bir yopiq kalitli
- b) ikki yopiq kalitli
- c) ikki ochiq kalitli
- *d) bir yopiq va bir ochiq kalitli

26. Kriptografiya himoyasida shifrlarga nisbatan qanday talablar qo'yiladi?

- a) shifrlarni ochish qiyin bo'lishligi, yopiq kalitlarni oson jo'natishlik, kalitlarning xajmi katta bo'lishlik
- *b) yetarli darajada kriptomustaxkamlik, shifrlash va deshifrlash jarayonining oddiyliqi, hajmlarni oshib ketmasligi, kichik jarayonlarga ta'sirjon bo'lmasligi
- c) yopiq kalitlarni oson jo'natishlik, shifrlash algoritmlarining mustaxkamligi
- d) shifr kodini ochishlik mushkul bo'lishligi, ochiq va yopiq kalitlarning xajmini kichikligi

27. O'rinlarni almashtirish, almashtirish, gammalashtirish, analitik o'zgartirish tizimlaridan qaysi birlari keng tarqalgan?

- a) o'rinlarni almashtirish
- *b) almashtirish
- c) gammalashtirish

d) analitik o'zgartirish

28. Sezar usuli qaysi tizimga kiradi?

a) o'rinlarni almashtirish

*b) almashtirish

c) gammalashtirish

d) analitik o'zgartirish

29. Himoyaning mexanizmi deganda nimani tushunasiz?

*a) Himoyaning buzilishlarini aniqlash va bartaraf etish xamda buzilishlar oqibatini yo'qotish mexanizmlari

b) Korxonaga tegishli informatsiyani saqlash va ishlatish havfsizligiga zarar keltiruvchi xar qanday xarakatlarga aytiladi

c) Ma'lumotlarni ishlash sistemalari va korxonaga tegishli axborotni tashash havfsizligi saviyasini ko'tarish mo'ljallangan servis xizmatlari

d) Himoyalash vositalarini qo'llab ma'lumotlarni tiklash.

30. Ximoya xizmati (servis) deganda nimani tushunasiz?

*a) Ma'lumotlarni ishlash sistemalari va korxonaga tegishli axborotni tashash havfsizligi saviyasini ko'tarish mo'ljallangan servis xizmatlari

b) Korxonaga tegishli informatsiyani saqlash va ishlatish havfsizligiga zarar keltiruvchi xar qanday xarakatlarga aytiladi

c) Himoyaning buzilishlarini aniqlash va bartaraf etish xamda buzilishlar oqibatini yo'qotish mexanizmlari

d) Aktiv xujumlarni bartaraf etadigan servis.

31. Kompbyuter tizimi va tarmoqlarda xujumlarni aniqlaydigan texnikaviy-dasturiy qurilmalarning qaysi birlari "olovli devor" deb ataladi?

a) Real Secure

b) Internet Scanner

c) Secret Net

*d) Fire Wall

32. Real Secure qurilmasi qanday vazifalarni bajaradi?

a) Tarmoqning zaif tomonlarini aniqlaydi

b) Tarmoqqa kirayotgan xujumlarni aniqlaydi

*c) Tarmoqqa kirayotgan xujumlarni to'sib qo'yadi

d) Havf xatar va xujum turlarini aniqlaydi

33. Real Secure qurilmasi qanday komponentlardan tashkil topgan?

a) Fire Wall Scanner, Web Security Scanner

b) Secret Net, Real Secure Manager

*c) Real Secure Detector, Real Secure Manager

d) HP Open View Plug-In Mobule

34. Real Secure qurilmasining 2.5 versiyasi bir vaqtning o'zida nechtagacha xujumlarni aniqlay oladi?

a) 486 ta

b) 994 ta

*c) 665 ta

d) 595 ta

35. Real Secure qurilmasini o'rnatish uchun shaxsiy kompyuterning operativ xotirasini hajmi qanchadan kam bo'lasligi kerak?

- a) 32 Mb
- *b) 64 Mb
- c) 128 Mb
- d) 256 Mb

36. Internet Scanner qurilmasi qanday vazifani bajaradi?

- a) Tarmoqqa kirayotgan xujumlarni aniqlaydi
- b) Tarmoqqa kirayotgan xujumlarni to'sib qo'yadi
- c) Havf xatar va xujum turlarini aniqlaydi
- d) Tarmoqning zaif tomonlarini aniqlaydi

37. Internet Scanner qurilmasi qanday komponentlardan iborat?

- a) Real Secure Detector, Real Secure Manager
- b) Fire Wall Scanner, Web Security Scanner
- c) Intranet Scanner, Fire Wall Scanner, Web – server.
- d) Fire Wall, Web Security Scanner

38. Internet Scanner qurilmasini o'rnatish uchun shaxsiy kompyuterning operativ xotirasini hajmi qanchadan kam bo'lasligi kerak?

- a) 32 Mb
- *b) 64 Mb
- c) 128 Mb
- d) 256 Mb

39. Internet Scanner qurilmasi tarmoqning nechtagacha zaif tamonlarini aniqlaydi?

- a) 694 gacha
- *b) 400 gacha
- c) 562 gacha
- d) 324 gacha

40. Qo'yidagilardan troyan dasturlarni ko'rsating?

- a) I LOVE YOU
- b) Back Orifice
- *c) Netbus
- d) Adinf.

41. Kompyuter jinoyati jaxonda:

- *a) o'sishda
- b) Pasayapti
- c) o'zgarmayapti
- d) kam o'sayapti.

42. Ko'yidagi keltirilganlardan qaysilari axborot havfsizligining asosiy aspektlari bo'ladi.

- *a) Mahfiylik (konfidentsialnost)
- b) Yaxlitlik (tselostnost)
- c) Foydalanuvchanlikni boshqarish (dostupnost)
- d) Soxtalashtirish (avtentifikatsiya)

43. Melissa – bu:

- *a) virus

- b) bomba
- c) cherv
- d) mutant.

44. Melissa – bu:

- *a) MS-Word fayllari uchun makrovirus
- b) PDF fayllari uchun makrovirus
- c) EXE fayllari uchun makrovirus
- d) COM fayllari uchun makrovirus.

45. Jaxon bo‘ylab kompyuter jinoyatlaridan o‘rtacha zarar qancha?

- *a) Yuz minglab dollar
- b) Yuzlab dollar
- c) o‘nlab dollar
- d) millionlab dollar.

46. Eng xatarli havfni ko‘rsating?

- *a) Personalning noqasddan qilingan xatolari
- b) Virusli infektsiya
- c) Xakerlarning xujumlari
- d) Kompyuterning buzilishi.

47. Ma’lumotlarni ushlab qolish (perexvat) nimaga havf soladi?

- *a) Mahfiylikka (konfidentsialnost)
- b) Yaxlitlikka (tselostnost)
- c) Foydalanuvchanlikni boshqarishga (dostupnost)
- d) Soxtalashlikka.

48. Ma’lumotlarni uzish (raz’edinenie) nimaga havf soladi?

- *a) Foydalanuvchanlikni boshqarishga (dostupnost)
- b) Yaxlitlikka (tselostnost)
- c) Mahfiylikka (konfidentsialnost)
- d) Soxtalashlikka.

49. Ma’lumotlarni turlash (modifikatsiya) nimaga havf soladi?

- *a) Yaxlitlikka (tselostnost)
- b) Foydalanuvchanlikni boshqarishga (dostupnost)
- c) Mahfiylikka (konfidentsialnost)
- d) Soxtalashlikka.

50. Ma’lumotlarni soxtalashtirish (falsifikatsiya) nimaga havf soladi?

- *a) Asliga to‘g‘riligiga (autentifikatsiya)
- b) Foydalanuvchanlikni boshqarishga (dostupnost)
- c) Mahfiylikka (konfidentsialnost)
- d) Soxtalashlikka.

51. Asosiy himoya xizmatini (servis) ko‘rsating?

- *a) Mahfiylik (konfidentsialnost), asliga to‘g‘riligi (autentifikatsiya), yaxlitligi(tselostnost), yolg‘onning mumkin emasligi(nevozmojnost otkaza), resurslardan foydalanuvchanlik (kontrol dostupa), foydalanuvchanlikni boshqarish(dostupnost)
- b) Simmetrik shifrlash algoritmi, assimetrik shifrlash algoritmi, xesh – funktsiya
- c) Uzish (raz’edinenie), ushlab qolish(perexvat), turlash(modifikatsiya), soxtalashtirish(falsifikatsiya)

d) Texnikaviy vositalardan foydalanish

52. Asosiy himoya mexanizmini ko'rsating?

- *a) Simmetrik shifrlash algoritmi, assimetrik shifrlash algoritmi, xesh – funktsiya
- b) Mahfiylik (konfidentsialnost), asliga to'g'riligi (autentifikatsiya), yaxlitligi (tselostnost), yolg'onning mumkin emasligi (nevozmojnost otkaza), resurslardan foydalanuvchanlik (kontrol dostupa), foydalanuvchanlikni boshqarish (dostupnost)
- c) . Uzish (raz'edinenie), ushlab qolish (perexvat), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya)
- d) Niqoblash, tartiblash

53. Kompyuter tizimlari va tarmoqlarida zamonaviy himoyalashning asosiy usullari va vositalariga nimalar kiradi?

- *a) Tashkiliy, dasturiy, huquqiy, kriptografik, fizikaviy
- b) Niqoblash, tartiblash, majburlamoq, undamoq
- c) Rasmiy, norasmiy
- d) Texnikaviy vositalardan foydalanish

54. Kompyuter tizimlari va tarmoqlarida zamonaviy himoyalashning fizikaviy texnik vositasiga ta'rif bering?

- *a) Avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, eshik qulflari, derazadagi temir panjaralar va x.z
- b) Axborotlarni himoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus ta'minotdir. Masalan, parol tizimi
- c) Telekommunikatsiya uskunalarining yaratilishi va qo'llanishi jarayonida qabul qilingan tashkiliy-texnikaviy va tashkiliy-huquqiy tadbirlardir. Masalan, binolarning qurilishi, tizimni loyixalash va x.z
- d) Kriptografik usullardan foydalanish

55. Kompyuter tizimlari va tarmoqlarida zamonaviy himoyalashning dasturiy vositasiga ta'rif bering?

- *a) Axborotlarni himoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus ta'minotdir. Masalan, parol tizimi
- b) Avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, eshik qulflari, derazadagi temir panjaralar va x.z
- c) Telekommunikatsiya uskunalarining yaratilishi va qo'llanishi jarayonida qabul qilingan tashkiliy-texnikaviy va tashkiliy-huquqiy tadbirlardir. Masalan, binolarning qurilishi, tizimni loyixalash va x.z
- d) Simmetrik va asimmetrik shifrlash usuli.

56. Kompyuter tizimlari va tarmoqlarida zamonaviy himoyalashning tashkiliy vositasiga ta'rif bering?

- *a) Telekommunikatsiya uskunalarining yaratilishi va qo'llanishi jarayonida qabul qilingan tashkiliy-texnikaviy va tashkiliy-huquqiy tadbirlardir. Masalan, binolarning qurilishi, tizimni loyixalash va x.z
- b) Axborotlarni himoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus ta'minotdir. Masalan, parol tizimi
- c) Avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, eshik qulflari, derazadagi temir panjaralar va x.z
- d) Aloqa kanallarida axborotlarni saqlash

57. Kompyuter tizimlari va tarmoqlarida zamonaviy himoyalashning xuquqiy himoyalash vositasiga ta'rif bering?

- a) Korxona raxbari tomonidan ishlab chiqilgan huquqiy xujjatlar
- b) Axborotlarni himoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus ta'minotdir. Masalan, parol tizimi

c) Avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, eshik qulflari, derazadagi temir panjaralar va x.z.

*d) Davlat qonunlari, farmonlar, farmoyishlar, buyruqlar va x.z.

58. Kompyuter virusi bu:

*a) maxsus yozilgan dastur

b) xakerning maxsuloti

c) zararlaydigan dastur

d) xavf-xatar va xujum turi

59. Kompyuter virusini kimlar yaratadi?

*a) yosh dasturchilar, profesional dasturchilar, ilmiy tadqiqotchilar

b) xakerchilar

c) profesional dasturchilar

d) antivirus dastur yaratuvchilar

69. "Virus" so'zi lotincha nimani anglatadi?

a) kasallik

b) buzuvchi

*c) tarqalish

d) zarar keltiruvchi

70. Kompyuterning viruslar bilan zararlanish yo'llarini ko'rsating?

*a) disketlar orqali, kompyuter tarmoqlari orqali, fleshkalar va x.z.

b) faqat kompyuter tarmoqlari orqali

c) klaviatura, sichqoncha orqali

d) insonlar o'zi kiritadi

71. I LOVE YOU virusi qaysi mamlakatdan va qachon tarqatilgan?

*a) Filippindan, 2000 yil 4 mayda Ye-mail orqali

b) AQShdan, 2000 yil 4 mayda Ye-mail orqali

c) Finlyandiyadan, 2000 yil 4 mayda Ye-mail orqali

d) Rossiyadan kelgan

72. Kompyuter viruslari turlarini ko'rsating?

*a) fayl, yuklovchi, drayverlarni zararlovchi, DIR, stels, Windows viruslari

b) parazitli, replikatorli, ko'rinmas, mutant, kvazivirus viruslari

c) nerezident, rezident, but, paketli, gibridli, tarmoqli viruslari

d) but, paketli replikatorli, ko'rinmas, mutant

73. Kompyuter dasturli viruslarini asoslangan algoritmlariga nisbatan ajratilgan qatorni ko'rsating?

*a) parazitli, replikatorli, troyanli, ko'rinmas, mutant, kvazivirus viruslari

b) fayl, yuklovchi, drayverlarni zararlovchi, DIR, stels, Windows viruslari

c) nerezident, rezident, but, paketli, gibridli, tarmoqli viruslari

d) rezident, but, paketli, yuklovchi, drayverlarni zararlovchi

74. Kompyuter viruslari xarakterlariga nisbatan ajratilgan qatorni kursating?

*a) nerezident, rezident, but, paketli, gibridli, tarmoqli viruslari

b) parazitli, replikatorli, ko'rinmas, mutant, kvazivirus viruslari

c) fayl, yuklovchi, drayverlarni zararlovchi,

d) DIR, stels, Windows viruslari

75. Yashash muxiti bo'yicha viruslarning tasniflashi qanday?

- a) rezidentli, xavfli, juda xavfli, troyanli
- b) rezident bo'lmagan, xavfli, juda xavfli, parazitli
- c) ko'rinmaydigan, replikatorli, rezidentli, tarmoqli
- *d) tarmoqli, faylli, yuklanadigan, faylli yuklanadigan

76. Zararlantirish usuli bo'yicha viruslar qanday tasniflanadi?

- a) faylli, xavfli, rezident bo'lmagan
- b) juda xavfli, mutant, troyan, parazitli
- c) rezidentli, rezident bo'lmagan
- d) xavfsiz, replikatorli, ko'rinmaydigan

77. Ta'sir etish darajasi bo'yicha viruslar qanday tasniflanadi?

- a) xavfli, ko'rinmaydigan, replikatorli
- b) xavfsiz, parazitli, tarmoqli
- c) yuklanadigan, juda xavfli
- *d) xavfli, xavfsiz, juda xavfli

78. Algoritmning xususiyatlari bo'yicha viruslar qanday tasniflanadi?

- *a) parazitli, replikatorli, troyanli, ko'rinmaydigan, mutantlar
- b) rezidentli, yuklanadigan, tarmoqli, faylli
- c) rezident bo'lmagan, xavfli, juda xavfli, troyanli
- d) tarmoqli, yuklanadigan, xavfli, troyanli

79. Virusga qarshi qanday dastur turlari mavjud?

- a) antivirus dasturlari
- b) filtrlar
- c) texnik vositalar
- d) detektorlar, doktorlar, vaktsinalar, taftishchilar, filtrlar

80. Antiviruslarning qo'llanish usuliga ko'ra taqsimlanishini ko'rsating?

- *a) detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar
- b) fayl, yuklovchi, drayverlarni zararlovchi, DIR, stels, Windows
- c) nerezident, rezident, but, paketli, gibridli, tarmoqli
- d) doktorlar, vaktsinalar, filtrlar

81. Zamonaviy antiviruslarni ko'rsating?

- *a) DrWeb, Adinf, AVP, BootCHK, Norton Antivirus, Kaspersky Security
- b) Internet Security System, AVP, BootCHK, Norton Antivirus
- c) JAVA, Adinf, AVP, Norton Antivirus, USENET, BootCHK
- d) DrWeb, BootCHK, Kaspersky Security, Norton Antivirus

82. Asosiy himoya xizmatini (servis) ko'rsating?

- *a) Mahfiylik (konfidentsialnost), asliga to'g'riligi (avtentifikatsiya), yaxlitligi(tselostnost), yolg'onning mumkin emasligi(nevozmojnost otkaza), resurslardan foydalanuvchanlik(kontrol dostupa), foydalanuvchanlikni boshqarish(dostupnost)
- b) Simmetrik shifrlash algoritmi, assimmetrik shifrlash algoritmi, xesh – funktsiya
- c) Uzish (raz'edinenie), ushlab qolish(perexvat), turlash(modifikatsiya), soxtalashtirish(falsifikatsiya)
- d) Kriptografik himoyalash vositasini qo'llash

83. Asosiy himoya mexanizmini ko'rsating?

- *a) Simmetrik shifrlash algoritmi, assimmetrik shifrlash algoritmi, xesh – funktsiya

- b) Mahfiylik (konfidentsialnost), asliga to'g'riligi (avtentifikatsiya), yaxlitligi (tselostnost), yolg'onning mumkin emasligi (nevozmojnost otkaza), resurslardan foydalanuvchanlik (kontrol dostupa), foydalanuvchanlikni boshqarish (dostupnost)
- c) . Uzish (raz'edinenie), ushlab qolish (perexvat), turlash (modifikatsiya), soxtalashtirish (falsifikatsiya)
- d) Texnikaviy vositalardan foydalanish

84. Kriptografik himoyalash usulining qaysi shifrlash algoritmda ikki kalit ishlatiladi?

- a) Simmetrik shifrlash algoritmi
- *b) Asimmetrik shifrlash algoritmi
- c) Simmetrik va asimmetrik shifrlash algoritmi
- d) Kriptotaxlil algoritmda

85. Quyida keltirilgan kriptografik himoyalash usulining qaysi biri mustaxkam va ko'p qo'llaniladi?

- a) Simmetrik shifrlash algoritmi
- *b) Asimmetrik shifrlash algoritmi
- c) O'rin almashtirish usuli
- d) Xesh-funktsiya

86. Real Secury tizimi nechanchi yilda ishlab chiqilgan?

- a) 1996 y
- b) 1999 y.
- *s) 1998 y.
- d) 1991 y.

87. Real Secure sistemasi nechta blokdan iborat?

- a) 3 ta
- *b) 2 ta
- s) 1 ta
- d) 4 ta.

88. Real Secure sistemasi qanday vazifani bajaradi?

- a) Tarmoqda uzatilaetgan paketlarni tugunlarda taqsimlaydi
- *b) Tarmoqdan kelaetgan xujumlarni aniqlaydi va ularni tusib qo'yadi
- s) Kompyuter tarmog'ining xolatini aniqlaydi
- d) Tarmoqning zaif tomonini aniqlaydi.

89. Fire Wall qanday vazifani bajaradi?

- a) Kompyuter tarmog'ining aloqa kanallaridan kelayotgan havf-xatarlarni aniqlaydi
- b) Tarmoqda uzatilaetgan paketlarni tugunlarda taqsimlaydi
- *s) Kelayotgan havf-xatarlarni aniqlaydi va aloqa yo'lini to'sib qo'yadi
- d) Tarmoqda uzatilaetgan paketlarni tugunlarda taqsimlaydi

90. Fire Wall qanday ma'noni anglatadi?

- a) Tarmoqning havfsizligi bildiradi
- *b) Olovli yoki toshli devor ma'nosini bildiradi
- s) Havf xatarlarni aniqlaydi
- d) xujumlar yo'lini to'sib qo'yish ma'nosini

91. Internet Scanner sistemasi qachon ishlab chiqilgan?

- a) 1994 y
- b) 1996 y

*s) 1998 y

d) 1995 y.

92. Internet Scanner sistemasi qanday funktsiyani bajaradi?

a) Olovli yoki toshli devor ma'nosini bildiradi

b) Kompyuter tarmog'ining xolatini aniqlaydi

*s) Havf-xatarlar va xujumlarni kirish yo'lini aniqlab beradi

d) Tarmoq xujumlarini aniqlaydi

93. O'rinlarni almashtirish usullaridan "shifrllovchi jadval" usulida qanday kalit ko'p ishlatiladi?

*a) Jadval o'lchovlari

b) So'z yoki so'z ketma-ketligi

s) Jadval tarkibi xususiyatlari

d) Raqamli belgilar

94. Sehrli kvadrat o'rin almashtirish usulida kalit sifatida nima ishlatiladi?

a) So'z yoki so'z ketma-ketligi

b) Jadval o'lchovlari

*s) Ustun, satr va diagonal sonlar yig'indisi

d) Jadval tarkibi xususiyatlari

95. Kriptologiya degani yunoncha nimani anglatadi?

a) ma'lumotlar havfsizligi

*b) kriptο – sirli va logus – xabar

s) Yozuvni sirli qilish

d) shifrlash

96. Kriptologiya nechta yo'nalishdan iborat?

a) 3 ta

*b) 2 ta

s) 1 ta

d) 4 ta

97. Kompyuter tarmoqlaridagi aloqa kanallarining qaysi biri yuqori axborot havfsizligini ta'minlaydi?

a) UTP kabellari

b) Koaksial kabellari

*s) Shisha tolali kabellar

d) Simsiz aloqa kanallari

98. Kompyuter tarmoqlarini tashkil etayotgan simsiz aloqa kanallarining qaysi biri yuqori havfsizlikka ega?

a) WiFi

b) WiMax

*c) Bluetooth

d) Sun'iy yo'ldoshlar

99. Secret Net sistemasi qaysi davlatda ishlab chiqilgan?

a) AQSh

b) Germaniya

*s) Rossiya

d) Frantsiya

100. Kompyuter tarmoqlarida eng ko‘p tarqalgan ximoyalash vositalari?

- a) Real Secure sistemasi
- b) Internet Scanner sistemasi
- *s) Fire Wall lar
- d) Kriptografik himoyalash

101. Korxona, tashkilot va firmalarda asosiy himoyalash vositalaridan qaysi biri ko‘p ishlatiladi?

- a) Texnikaviy va dasturiy vositalar
- b) Xuquqiy vositalar
- *s) Tashkiliy vositalar.
- d) Jismoniy vositalar

102. Ishonchlilik – bu:

- a) hamma buyruqlarni aniq va to‘liq bajarish kafolati
- *b) tizim me‘riy va g‘ayri tabiiy xollarda rejalashtirilganidek o‘zini tutishlik kafolati
- s) istalgan paytda dastur majmuasining xoxlagan qismini to‘liq tekshirish mumkinligi kafolati
- d) hozir tizimga ulangan mijoz aniq o‘zini kim deb atagan bo‘lsa, aniq o‘sha ekanligi

103. Maxfiylik – bu:

- a) ishonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati
- *b) aniq bir axborotga faqat tegishli shaxslar tegishli shaxslar doirasigina kirishi mumkinligi
- s) xozir tizimga ulangan mijoz aniq o‘zini tekshirish mumkinligi kafolati
- d) istalgan paytda dastur majmuasining xoxlagan qismini to‘liq tekshirish mumkinligi kafolati

104. Autentifikatsiya – bu:

- a) istalgan paytda dastur majmuasining xoxlagan qismini to‘liq tekshirish mumkinligi kafolati
- *b) ishonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati
- s) axborot zaxirasi egasi deb e‘lon qilingan shaxs xaqiqatan ham axborotning egasi ekanligiga beriladigan kafolat
- d) aniq bir axborotga faqat tegishli shaxslar tegishli shaxslar doirasigina kirishi mumkinligi

105. Konfidentsiallik – bu:

- a) yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo‘llaniladi. Kerak bo‘lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati
- b) oldindan kelishilgan me‘yorlar chegarisida qasddan xato kiritilgan ma‘lumotlarga nisbatan tizimning oldindan kelishilgan xolda o‘zini tutishi
- *s) ishonchliligi, tarqatilishi mumkin emasligi, mahfiyligi kafolati
- d) aniq bir axborotga faqat tegishli shaxslar tegishli shaxslar doirasigina kirishi mumkinligi

106. Yaxlitlik – bu:

- a) xozir tizimga ulangan mijoz aniq o‘zini tekshirish mumkinligi kafolati
- b) istalgan paytda dastur majmuasining xoxlagan qismini to‘liq tekshirish mumkinligi kafolati
- *s) axborot boshlang‘ich ko‘rinishda ekanligi, ya‘ni uni saqlash va uzatishda ruxsat etilmagan o‘zgarishlar qilinmaganligi kafolati, bu bandning buzilishi axborotni soxtalashtirish deyiladi.
- d) kerak bo‘lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati

107. FireWall atamasi qanday tarjima qilinadi?

- *A) olovli devor
- B) tikanli sim
- C) tikanli devor
- D) olovli sim

108. FireWall atamasi nimani anglatadi?

- *A) tarmoqdagi himoya tizimini
- B) internet hududining chegarasini
- C) hech kim tomonidan nazorat qilinmaydigan hududni
- D) moderator tomonidan nazorat qilinadigan resurslar yig'indisini

109. SLIP qisqartmasi qaysi iboradan olingan?

- *A) Serial Number Internet Protocol
- B) Serial Number Information Protocol
- C) Serial Network Information Protocol
- D) Super Network Information Protocol

110. PPP qisqartmasi qaysi iboradan olingan?

- A) Point to Point Protocol
- B) Peer to Peer Protocol
- C) Parent to Parent Protocol
- D) Personal Point Protocol

111. SLIP va PPP protokollarining farmoyishlari to'plami qanday nomlanadi?

- *A) AT
- B) FTT
- C) ABS
- D) SARA

112. SLIP va PPP protokollarining farmoyishlari to'plami qanday nomlanadi?

- A) Falles
- *B) Hayes
- C) Hano
- D) Tetris

113. DSL standartining eng qulay tomonini ko'rsating.

- A) mavjud telefon liniyalaridan foydalanadi
- B) DSL modemi juda arzon
- C) DSL 10 Mb/s tezlikda ishlaydi
- D) bu standartda trafik eng arzon

114. DSL standartida signal polosasining quyi qismi nimaga mo'ljallangan?

- *A) telefon aloqasi uchun
- B) axborotni uzatish uchun
- C) axborotni qabul qilish uchun
- D) bo'sh qoldirilgan

115. DSL standartida signal polosasining o'rta qismi nimaga mo'ljallangan?

- A) telefon aloqasi uchun
- *B) axborotni uzatish uchun
- C) axborotni qabul qilish uchun
- D) bo'sh qoldirilgan

116. DSL standartida signal polosasining yuqori qismi nimaga mo'ljallangan?

- A) telefon aloqasi uchun
- B) axborotni uzatish uchun

- *C) axborotni qabul qilish uchun
- D) bo'sh qoldirilgan

117. Quality of Service atamasi qanday ma'noni anglatadi?

- A) sifat miqdori
- B) xizmat miqdori
- *C) xizmat sifati
- D) miqdor sifati

118. Wi Fi 802.11b standartida tarmoqda ma'lumotlarni uzatish ko'pi bilan tezligi nechaga teng?

- A) 5.4 Mb/s
- *B) 11 Mb/s
- C) 54 Mb/s
- D) 110 Mb/s

119. Wi Fi texnologiyasining asosiy kamchiligini ko'rsating.

- *A) xakerlarning bu tarmoqqa oson kira olishi
- B) bog'lanish tezligining pastligi
- C) trafikning juda qimmatligi
- D) barchasi to'g'ri

120. Sun'iy yo'ldosh orqali internetga ulanishda keng tarqalgan usul nima deb ataladi?

- A) ikki tomonlama usul
- *B) gibrid (aralash) usuli
- C) Hi Fi usuli
- D) asinxron usul

121. Sun'iy yo'ldosh orqali internetga chiqishda NOC qisqartmasi nimani bildiradi?

- *A) Network Operation Center
- B) Name Operation Center
- C) Network Organization Center
- D) Name Organization Center

122. Sun'iy yo'ldosh orqali internetga chiqishda NOC deb nima nomlangan?

- *A) Sun'iy yo'ldoshning yerdagi stantsiyasi
- B) Sun'iy yo'ldoshning kompyuter tizimi
- C) Sun'iy yo'ldoshning aloqa kanali
- D) kompyuterga ulanadigan likopcha va signalni kuchaytirish qurilmasi

123. Bluetoothli qurilmalarning aloqa chastotasi joylashgan polosa qanday nomlanadi?

- A) sanoat, aloqa, tibbiyot
- B) sanoat, ilmiy, qurilish
- *C) sanoat, ilmiy, tibbiy
- D) aloqa, ilmiy, tibbiy

124. Brauzerdan foydalanishda dilni xira qiladigan narsa nima?

- *A) serverlarga murojaat qilinganda paydo bo'ladigan muammolar
- B) ularning narxlari juda balandligi

- C) yuqori tezlikda ulanishni talab qilishi
- D) parol tizimidagi kamchiliklar

125. Service is unaviable degan yozuv qanday xatoni bildiradi?

- *A) chaqirishga behuda urinish
- B) kirish taqiqlangan
- C) vakolat berilmagan
- D) bunday nomli resurs yo‘q

126. Access forbidden degan yozuv qanday xatoni bildiradi?

- A) chaqirishga bexuda urinish
- *B) kirish taqiqlangan
- C) vakolat berilmagan
- D) bunday nomli resurs yo‘q

127. Internet global tarmogi deb nimaga aytiladi (komp. tarmok.)?

- A) biror inshootning turli kavatlarida joylashgan kompyuterlar boglanishi
- B) bir nechta lokal tarmoklarning boglanishi
- *C) turli shaxar va mamlakatlardagi kompyuterlar boglanishi
- D) bir nechta kompyuterlar va printerning boglanishi

128. Kaysi protokol Internetda asosiy xisoblanadi (komp. tarmok.)?

- A) HTTP
- B) HTML
- C) TCP
- *D) TCP/IP

129. Kompyuterlar orasida axborot almashuvi uchun tashqi axborot tashuvchilar kerak bo‘lmasligiga sabab?

- a) Protessorning ishlash tezligining yukoriligi
- *b) Tarmok o‘rnatilishi
- c) Lazerli sichkoncha
- d) Kattik diskning xajmining kengayishi

130. Kompyuter tarmoklari orkali bajariladigan asosiy ishlarni kursating?

- *a) Ma’lumotlarni tez, ixtiyoriy hajmda va xohlagan vaqtda uzatish mumkin
- b) Ma’lumotlarni taxrirlashning kengligi
- c) Ovoz berishi
- d) Xavfning oldini olishi

131. Tarmoqqa kompyuterlar ulashning turlarini ko‘rsating?

- a) Server, klient, baza
- *b) Tuxumsimon, yulduzcha, doirasimon, umumiy shinali, aralash
- c) yulduzcha, doirasimon, kabel
- d) Internet, umumiy shinali, aralash

132. Serverga ta’rif bering?

- a) tarmoqdagi boshqa kompyuterlardan xizmat oluvchi kompyuter
- *b) tarmoqdagi boshqa kompyuterlarga xizmat ko‘rsatuvchi kompyuter
- c) bir rangli va ajratilgan serverli
- d) tarmoqdagi hamma kompyuterlar teng huquqqa ega

133. Quyidagi elektron manzilning kaysisi to'g'ri yozilmagan?

- *a) yoshlarmarkazi@rambler.ru
- b) yoshmarkazrambler@.ru
- c) yoshlar@markazirambler.ru
- d) yoshmarkazrambler.ru

134. Quyidagi elektron manzildan tashkilot (provayder) nomini aniklang?

Info@youthcenter.uz

- a) Info
- *b) youthcenter
- c) uz
- d) @.uz

135. Elektron pochta nima?

- *a) Elektron pochta maxsus programma bo'lib, uning yordamida Siz dunyoning ixtiyoriy joyidagi elektron adresga xat, xujjat va umuman ixtiyoriy faylni jo'natishingiz xamda qabul qilib olishingiz mumkin
- b) Elektron pochta virusdan tozalash programma bo'lib, uning yordamida Siz dunyoning ixtiyoriy joyidagi elektron adresga xat, xujjat va umuman ixtiyoriy faylni virusdan tozalab olishingiz mumkin
- c) Elektron pochta rasm chizish dasturi
- d) Xabarlarni himoyalash uchun xizmat qiladi

136. Abonent tizimining xududiy joylashuviga ko'ra xisoblash tarmog'ini uchta asosiy sinflarini kursating?

- *a) global (WAN - Wide Area Network), mintakaviy (MAN - Memrorolitan Area Network), lokal (WAN - Local Area Network)
- b) global (Local - Wide Area Network), mintakaviy (MAN - Memrorolitan Area Network), lokal (WAN - Local Area Network)
- c) global (WAN - Local Area Network), mintakaviy (MAN - Local Area Network), lokal (WAN - Local Area Network)

137. Quyidagi tasdiqlardan qaysi biri to'g'ri?

- A) internet jamiyati internetni boshqaradi
- *B) internet markaziy boshqaruvga ega emas
- C) internet davlat tomonidan boshqariladi
- D) internet xalqaro tashkilot tomonidan boshqariladi

138. Provayderlar nima bilan shug'ullanadilar?

- A) internet protokollarini ishlab chiqadilar
- B) yangi standartlar ishlab chiqadilar
- *C) foydalanuvchilarga internet xizmatlarini ko'rsatadilar
- D) internetdagi domen nomlari ro'yxatini tuzadilar

139. Quyidagilardan qaysilari provayder?

- A) Intel
- B) Microsoft
- C) IBM
- *D) East Telecom

140. Registratorlar nima ish qiladilar?

- A) tarmoqqa ulangan texnikani qayd qiladilar

- *B) domen (soha) nomlarini qayd qiladilar
- C) tarmoqdagi axborot oqimini qayd qiladilar
- D) tarmoqdagi axborot resurslarini qayd qiladilar

141. InterNIC qisqartma qaysi iboradan olingan?

- A) Internet Name Identification Center
- B) Internet New Information Center
- *C) Internet Network Information Center
- D) International Net Information and Communication

142. Quyidagi tasdiqlardan qaysisi to'g'ri?

- A) internet markazlashtirilgan tarzda davlat tomonidan moliyalashtiriladi
- *B) internetni moliyalash markazlashtirilmagan
- C) internet markazlashtirilgan tarzda xalqaro tashkilot tomonidan moliyalashtiriladi
- D) internet faqat tijorat tashkilotlari tomonidan moliyalashtiriladi

143. Mintaqaviy tarmoq haqidagi to'g'ri tasdiqni ko'rsating.

- *A) mintaqaviy tarmoq biron hudud ichida internet faoliyatini ta'minlaydi va qo'llab quvvatlaydi
- B) mintaqaviy tarmoq biron hudud ichida joylashgan barcha kompyuterlarni birlashtiradi
- C) mintaqaviy tarmoq biron davlat hududida joylashgan barcha kompyuterlarni birlashtiradi
- D) barcha javoblar to'g'ri

144. ISP qisqartmasi qaysi jumladan olingan?

- A) Information Services Promotor
- *B) Internet Services Provider
- C) International Services Promotor
- D) Internet Services Promotor

145. TCP qisqartma qaysi iboradan olingan?

- *A) Transmission Control Protocol
- B) Transmission and Communication Protocol
- C) Telecommunication Packet
- D) Telecommunication Protocol

146. Internet otaxonlari deb nom olgan olimlar nimani yaratganlar?

- A) Elektron pochtoni
- B) Birinchi veb brauzerni
- C) Elektron pochtoning birinchi dasturini
- *D) TCP ni

147. Internet qaysi tarmoq asosida vujudga kelgan?

- A) GalaxyNet
- *B) ARPAnet
- C) IPnet
- D) TCPnet

148. IP qisqartma qaysi iboradan olingan?

- A) Information Protocol
- *B) Internet Protocol
- C) Information Pocket
- D) Internet Pocket

149. TCP protokoli tarmoq bo‘ylab uzatiladigan xabarni nimalarga bo‘lib chiqadi?

- A) klasterlarga
- B) sektorlarga
- *C) paketlarga
- D) bo‘laklarga bo‘lmaydi

150. Qaysi qurilma kompyuter tarmog‘iga tegishli emas?

- A) hub
- B) gateway
- C) bridge
- *D) flash driver

151. Mahalliy tarmoq yaratish uchun qaysi qurilma kerak bo‘ladi?

- *A) hub (tugun)
- B) gateway (shlyuz)
- C) bridge (ko‘prik)
- D) repeater (takrorlagich)

152. Mahalliy tarmoqlarni bir-biri bilan ulash uchun qaysi qurilmadan foydalaniladi?

- A) hub (tugun)
- B) gateway (shlyuz)
- *C) bridge (ko‘prik)
- D) repeater (takrorlagich)

153. Turli turdagi tarmoqlarni bir-biri bilan bog‘lash uchun qaysi qurilmadan foydalaniladi?

- A) hub (tugun)
- *B) gateway (shlyuz)
- C) bridge (ko‘prik)
- D) repeater (takrorlagich)

154. Susaygan signalni kuchaytirish uchun qaysi qurilmadan foydalaniladi?

- A) hub (tugun)
- B) gateway (shlyuz)
- C) bridge (ko‘prik)
- *D) repeater (takrorlagich)

155. Tarmoqning kirish nuqtasiga nima ulanadi?

- A) Internetga kirgan foydalanuvchi kompyuteri
- *B) yuqori tezlikdagi axborot magistrali
- C) Serverlar
- D) Umumiy foydalanish uchun mo‘ljallangan printerlar

156. Multimedia koridori nima?

- *A) yuqori tezlikdagi axborot magistrallari
- B) tarmoqdagi DVDlarga ega shaxsiy kompyuterlar
- C) multimedia mahsulotlari saqlanadigan server
- D) shaxsiy kinoteatr deb nom olgan jihozlarga ega kompyuter

157. WAN qisqartma qaysi iboradan olingan?

- A) world area net

- B) wide addressed net
- C) world access net
- *D) wide area net

158. DSL usulida internetga ulanishda hozirgi kunda qanday eng katta tezlik taklif qilinayapti?

- A) 128 kb/s
- B) 256 kb/s
- C) 512 kb/s
- *D) 1024 kb/s

159. Uyali aloqa telefonlari oddiy modem sifatida ishlatilganda internetga ulanish tezligi qanday bo'ladi?

- A) 40-50 kb/s
- B) 60-80 kb/s
- *C) 120-160 kb/s
- D) 180-240 kb/s

160. Uyali aloqa telefonlarining 3G standartida internetga ulanish tezligi qanday bo'ladi?

- A) 0,5 Mb/s
- B) 1,2 Mb/s
- C) 2,4 Mb/s
- *D) 3,6 Mb/s

161. DSL qisqartmasi qaysi iboradan olingan?

- *A) digital subscriber lines
- B) discret subscriber lines
- C) digital super lines
- D) discret super lines

162. DSL ning qanday usuli ADSL deb ataladi?

- *A) asinxron DSL
- B) adresli (manzilli) DSL
- C) aktiv (faol) DSL
- D) amerika DSLi

163. FireWall atamasi nimani anglatadi?

- *A) tarmoqdagi himoya tizimini
- B) internet hududining chegarasini
- C) hech kim tomonidan nazorat qilinmaydigan hududni
- D) moderator tomonidan nazorat qilinadigan resurslar yig'indisini

164. SLIP qisqartmasi qaysi iboradan olingan?

- *A) Serial Number Internet Protocol
- B) Serial Number Information Protocol
- C) Serial Network Information Protocol
- D) Super Network Information Protocol

165. PPP qisqartmasi qaysi iboradan olingan?

- *A) Point to Point Protocol
- B) Peer to Peer Protocol
- C) Parent to Parent Protocol
- D) Personal Point Protocol

166. SLIP va PPP protokollarining farmoyishlari to'plami qanday nomlanadi?

- *A) AT
- B) FTT
- C) ABS
- D) SARA

167. SLIP va PPP protokollarining farmoyishlari to'plami qanday nomlanadi?

- A) Falles
- *B) Hayes
- C) Hano
- D) Tetris

168. DSL modamlari orasidagi masofa 3 km bo'lsa, ular orasidagi aloqa tezligi eng ko'pi bilan qancha bo'lishi mumkin?

- A) 1 Mb/s
- B) 2 Mb/s
- C) 4 Mb/s
- *D) 8 Mb/s

169. DSL modamlari orasidagi masofa 6 km bo'lsa, ular orasidagi aloqa tezligi eng ko'pi bilan qancha bo'lishi mumkin?

- A) 1 Mb/s
- *B) 2 Mb/s
- C) 4 Mb/s
- D) 8 Mb/s

170. Quality of Service atamasi qanday ma'noni anglatadi?

- A) sifat miqdori
- B) xizmat miqdori
- *C) xizmat sifati
- D) miqdor sifati

171. Wi Fi marshrutizatorlari yana qanday nomlanadi?

- *A) simsiz ulanish nuqtasi
- B) simsiz tarmoq abonentlari
- C) Wi Fi korrektorlari
- D) Wi Fi analizatorlari

172. Wi Fi texnologiyasining asosiy kamchiligini ko'rsating.

- *A) xakerlarning bu tarmoqqa oson kira olishi
- B) bog'lanish tezligining pastligi
- C) trafikning juda qimmatligi
- D) barchasi to'g'ri

173. Sun'iy yo'ldosh orqali internetga ulanishda keng tarqalgan usul nima deb ataladi?

- A) ikki tomonlama usul
- *B) gibrid (aralash) usuli
- C) Hi Fi usuli
- D) asinxron usul

174. Sun'iy yo'ldosh orqali internetga chiqishda NOC qisqartmasi nimani bildiradi?

- *A) Network Operation Center
- B) Name Operation Center
- C) Network Organization Center
- D) Name Organization Center

175. Sun'iy yo'ldosh orqali internetga chiqishda NOC deb nima nomlangan?

- *A) Sun'iy yo'ldoshning yerdagi stantsiyasi
- B) Sun'iy yo'ldoshning kompyuter tizimi
- C) Sun'iy yo'ldoshning aloqa kanali
- D) kompyuterga ulanadigan likopcha va signalni kuchaytirish qurilmasi

176. Bluetoothli qurilmalar aloqa uchun qaysi chastotadan foydalanadilar?

- A) 1,8 GGts
- B) 2,0 GGts
- *C) 2,2 GGts
- D) 2,4 GGts

177. Bluetoothli qurilmalarning aloqa chastotasi joylashgan polosa qanday nomlanadi?

- A) sanoat, aloqa, tibbiyot
- B) sanoat, ilmiy, qurilish
- *C) sanoat, ilmiy, tibbiy
- D) aloqa, ilmiy, tibbiy

178. Butun olam to'rining asosini nima tashkil etadi?

- *A) veb sahifalar
- B) brauzerlar
- C) serverlar
- D) mijoz kompyuterlari

179. Veb sahifa deb qanday sahifalarga aytiladi?

- *A) to'rdagi sahifalarga
- B) chop etilgan xujjat sahifalariga
- C) Word da yaratilgan xujjat sahifalariga
- D) Server ishining natijalari aks etgan sahifalarga

180. Gipermurojaatlar nimaga murojaat qiladilar?

- *A) kompyuterlarga
- B) Serverlarga
- C) to'rda e'lon qilingan sahifalarga
- D) shlyuzlarga

181. Gipermurojaatlar nimadan foydalanadilar?

- *A) URL
- B) Hub
- C) WWW
- D) SLIP

182. Veb sahifada nimalarni aks ettirish mumkin?

- A) matn va grafika
- B) audio va video
- C) gipermurojaatlar
- *D) barchasi to'g'ri

183. To'ring mijoz kompyuterida ishlaydigan dasturiy ta'minoti nima deb ataladi?

- A) gipermatn
- B) server
- *C) brauzer
- D) veb sahifa

184. Gipermurojaatlar nima yordamida yaratiladi?

- *A) HTML
- B) HTTP
- C) XML
- D) TelNet

185. Server dasturiy ta'minoti qaerda ishlaydi?

- A) mijoz kompyuterlarida
- B) mehmon kompyuterlarda
- *C) mezbbon kompyuterlarda
- D) aloqa magistrallarida

186. URL nimaga xizmat qiladi?

- *A) to'rdagi resurslarning joylashgan yerini topishga
- B) server kompyuterlarining nomini topishga World Wide Web – butun olam to'ri 24
- C) mijoz kompyuterlarining IP manzilini topishga
- D) server kompyuterlarining IP manzilini topishga

187. Veb saytning kontenti deb nimaga aytiladi

- A) uning tuzilishining grafik tasviri
- *B) uning mazmunini tashkil etuvchi materiallar
- C) veb saytdagi materiallarni tasvirlash uchun ishlatiladigan texnologiyalar yig'indisi
- D) veb saytdagi ichki bog'lanishlarning to'liq grafik tasviri

188. Ovoz va video materiallarni veb sahifaga joylash uchun nima qilish kerak? World Wide Web – butun olam to'ri 25

- A) mayda bo'laklarga ajratib chiqish
- *B) raqamli ko'rinishga o'tkazish
- C) analogli ko'rinishga o'tkazish
- D) hammasini bitta faylga joylash

189. Ovoz va video materiallarni veb sahifaga joylashdan oldin nima tavsiya qilinadi?

- A) paketlarga ajratish
- *B) hajmini kamaytirish
- C) hammasini bitta faylga joylash
- D) hammasi to'g'ri

190. Brauzerdan foydalanishda dilni xira qiladigan narsa nima?

- *A) serverlarga murojaat qilinganda paydo bo'ladigan muammolar
- B) ularning narxlari juda balandligi
- C) yuqori tezlikda ulanishni talab qilishi
- D) parol tizimidagi kamchiliklar

191. Service is unaviable degan yozuv qanday xatoni bildiradi?

- *A) chaqirishga behuda urinish
- B) kirish taqiqlangan
- C) vakolat berilmagan
- D) bunday nomli resurs yo‘q

192. Access forbidden degan yozuv qanday xatoni bildiradi?

- A) chaqirishga bexuda urinish
- *B) kirish taqiqlangan
- C) vakolat berilmagan
- D) bunday nomli resurs yo‘q

193. Unauthorized degan yozuv qanday xatoni bildiradi?

- A) chaqirishga bexuda urinish
- B) kirish taqiqlangan
- *C) vakolat berilmagan
- D) bunday nomli resurs yo‘q

194. Server does not have a DNS Entry degan yozuv qanday xatoni bildiradi?

- A) chaqirishga bexuda urinish
- B) kirish taqiqlangan
- C) vakolat berilmagan
- *D) bunday nomli resurs yo‘q

195. Bella-Lapadulla modeli nimaga asoslangan?

- *a) sirli xujjatlar bilan ishlashga
- b) ochiq va xizmat yuzasidan foydalanishga
- c) sirli ma'lumotlarni shifrlashga
- d) sirli ma'lumotlarni ko‘chirib olishga

196. Bella-Lapadulla modeli nechanchi yilda ishlab chiqilgan?

- a) 1965 yilda
- b) 1970 yilda
- *c) 1975 yilda
- d) 1979 yilda

197. D.Denning modeli nimaga asoslangan?

- a) ma'lumotlarning maxfiyligini aniqlashga
- *b) axborot xavfsizligi buzilishini audit yozuvlari asosida aniqlashga
- c) axborot havfsizligining buzilishini terminallar yordamida aniqlashga
- d) xabarlar aniq yetib kelganligini aniqlashga

198. D.Denning modeli nechta asosiy komponentlardan iborat?

- a) 5 ta
- *b) 6 ta
- c) 7 ta
- d) 8 ta

199. Landver modeli nimaga asoslangan?

- a) xujum turlarini aniqlashga
- b) sirli ma'lumotlarni aniqlashga
- *c) himoyalash vositasini mustaxkamligini aniqlashga
- d) himoya turlarini belgilashga

200. Kompyuter tizimi va tarmoqlarining aloqa kanallarida axborotlarni himoyalash qanday asosiy vositalarga asoslangan?

a) texnikaviy – dasturiy, xuquqiy

b) kriptografik, jismoniy, tashkiliy

*c) texnikaviy- dasturiy, tashkiliy, xuquqiy

d) texnikaviy, kriptografik, jismoniy

Asosiy adabiyotlar:

1. Nigmatov X. Informatsionnaya bezopasnost. Zashita informatsii v setyax telekommunikatsii. Shymkent. 2013. 188 str.
2. Nigmatov X. Kompyuternye seti i sistemy v IP telefonii. Shymkent.2013. 240 str.
3. Nigmatov X. Sistemy i ustroystva sputnikovoy i mobilnoy radiosvyazi. Shymkent. 2013. 304 str.
4. Abduganiev A.A. Internet asoslari.Toshkent. 2011.20 bet.
5. Abduganiev A.A. Internet muloqat vositasi. Toshkent. 2011. 21.bet.
6. Abduganiev A.A. Internetning texnik va texnologik ta'minoti. Toshkent. 2011. 23 bet.
7. Gerasimenko V.A. □ Zashita informatsii v avtomatizirovannykh sistemax obrabotki dannyx Moskva: 1998.
8. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musaeva M.A. Kompyuter tizimlarida axborotni himoyalash. Ma'ruza matnlari. TDIU Toshkent, 2003.
9. Devid Kozhev. □Elektronnaya kommertsiya□ (Ingliz tilidan tarjima kilingan) Moskva: 199 □Russkaya redaktsiya□nashriyoti.
10. Anin B.Yu. Zashita kompyuternoy informatsii SPb. BHV – Sankt – Peterburg,2001.
11. Makarov N.V. □Informatika□Moskva: 2001. □Finansy i statistika□nashriyoti. 3 – nashr.
12. Zavgorodno'y V.I. Kompleksnaya zashita informatsii v kompyuternyx sistemax – M.: Logos, 2001
13. Stepanov Ye.A. Korneev I.K. Informatsionnaya bezopastnost i zashita informatsii. M.: Infra, 2002.
14. Yarochkin V.I. Informatsionnaya bezopasnost. M.: Letopisets 2001.
15. Romantsev Yu.V., Timofeev P.A., Shangin V.F. □Zashita informatsii v kompyuternyx sistemax i setyax□ Moskva: 2001. Radio i svyaz nashriyoti.
16. Ermatov Sh.T. Kompyuter tizimlarida axborotni himoya qilish. Elektron darslik. Toshkent, 2003
17. Baichev S.G. Основы современной криптографии. – M.: Goryachaya liniya – Telekom. 2001. – 1200s.
18. Galatenko V.A. Основы информационной безопасности – M.:INTUIT RU □Internet□ – Университет Информационных Технологий□2003 – 280s.

19. Domashev A.V., Gruntovich M.M. i dr. Programmirovaniye algoritmov zashity informatsii. Ucheb. Posob. F2 – e izd., isp. I dop. – M.: Izdatel Molgacheva S.V. Izdatelstvo "Nolidj" 2002. – 416s.

Qo'shimcha adabiyotlar:

1. Belkin. P.Yu. "Programmno – apparatnye sredstva obespecheniya informatsionnoy bezopasnosti" Moskva: 1999. "Radio i svyaz" nashriyoti.
2. Timofeev P.A. "Printsiipy zashity informatsii v kompyuternykh sistemax" Moskva: 1999 "Konfident" nashriyoti.
3. Shangin V.F. "Zashita informatsii i informatsionnaya bezopastnost" 2 qismi Moskva: "MIET" 2000.
4. Kamilov Sh.M., Zakirova T.A., Musaeva M.A. Microsoft Office xujjat va dasturini ruxsatsiz murojaat etishdan saqlash. Toshkent, TDIU. 2003.
5. Shinder.Debra, Littldjon. Osnovy kompyuternykh setey. – M.: Izdatelskiy dom. "Vtlyams" 2003. – 656 s.
6. Ermatov Sh.T. Axborotni ximoya qilishning kriptografik usullari. Uslubiy qo'llanma, Toshkent, TDIU, 2003
7. Heglov A.Yu. Zashita kompyuternoy informatsii ot nesanksinirovannogo dostupa. – SPb.: Nauka i texnika, 2004. – 384 s.
8. Internet saytlari :
 - 1) Alta Vista [http:// www altavista. com /](http://www.altavista.com/)
 - 2) Fast Search [http: // www alltheweb. com/](http://www.alltheweb.com/)
 - 3) Go To [http: //goto. com](http://goto.com)
 - 4) Cooglt [http: // www / google. com/](http://www/google.com/)
 - 5) Hot Bot [http: // hotbot. lycos. com/](http://hotbot.lycos.com/)
 - 6) Inktomi [http: www. Inrtomi. com/](http://www.Inrtomi.com/)
 - 7) Look Smart [http: // www. Looksmart. com/](http://www.Looksmart.com/)
 - 8) Lycos [http: www/ lycos. com /](http://www/lycos.com/)
 - 9) MSN Search [http: // search. msn. com/](http://search.msn.com/)
 - 10) Nothern Iight [http: www. nothernlight. com/](http://www.nothernlight.com/)
 - 11) Snap [http: // www. yahoo/ com/](http://www.yahoo.com/)
 - 12) Yahoo! [Http: www. yahoo. com/](http://www.yahoo.com/)
 - 13) TGEU: [www. tsue. uz](http://www.tsue.uz)
 - 14) KGEI: [adm @kspei. kcn.ru](mailto:adm@kspei.kcn.ru)
 - 15) UAGU: [svitlana @napa-dil. org.ru](mailto:svitlana@napa-dil.org.ru)
 - 16) GUIKT: [bshunev @ lycos. com](mailto:bshunev@lycos.com)
 - 17) UZTEST. [com](http://www.uztest.com)
 - 18) [http: // www.cov. uz](http://www.cov.uz)
 - 19) Anopt [http://www. library. yale. uz](http://www.library.yale.uz)
 - 20) Yndex [http: // www. aport. ru](http://www.aport.ru)
 - 21) Tela [http: // www yandex. ru](http://www.yandex.ru)

- 22) All Stars [http:// www. stars. ru](http://www.stars.ru)
- 23) IREX: [www. lrex. Org](http://www.lrex.Org)
- 24) Rambler: [www. Rambler. Ru.](http://www.Rambler.Ru)