



O'ZBEKISTON RESPUBLIKASI ALOQA,
AXBOROTLASHTIRISH VA
TELEKOMMUNIKATSIIYA TEXNOLOGIYALARI
DAVLAT QO'MITASI

TOSHKENT AXBOROT TEXNOLOGIYALARI
UNIVERSITETI FARG'ONA FILIALI

"AXBOROT TEXNOLOGIYALARI" KAFEDRASI

Axborot xavfsizligi

fanidan
5521900- "Informatika va axborot texnologiyalari"
ta'lif yo'nalishi talabalari uchun

MA'Ruzalar matni

Kafedraning 2014 yil
29 avgust 1-sonli yig'ilishida
muxokama qilingan

Filial 2014 yil 30 avgust kungi
Uslubiy kengash
yig'ilishida tasdiqlangan

Ushbu ma’ruza matni «Axborot xavfsizligi» fanidan barcha ma’ruza mavzulari keng yoritilgan va o’zida axborot xavfsizligini ta’minlash bilan bog’liq masalalarni yechishda axborotni himoyalash texnologiyalarining o’rganish va ko’rib chiqish kabi masalalarini qamraydi. Bu fanni o’qitishdan maqsad kompyuter tizimlari va tarmoqlarida axborot xavfsizligi profiliga mos, ta’lim standartida talab qilingan bilimlar, ko’nikmalar va tajribalar darajasini ta’minlashdir.

Tuzuvchilar:

Sh.Umarov «Axborot texnologiyalari» kafedrasi katta o’qituvchi
F.M.Mulaydinov «Axborot texnologiyalari » kafedrasi assistenti

Mundarija

SO'Z BOSHI	- 4 -
Xavfsizlikning asosiy yo'nalishlari	- 6 -
Axborot-kommunikatsion tizimlar va tarmoqlarda taxdidlar va zaifliklar.....	- 9 -
2. Ma'ruza. Tarmoqdagi axborotga bo'ladijan na'munaviy hujumlar. Axborot xavfsizligi modellari.....	- 12 -
3.Ma'ruza. Axborot xavfsizligini tahminlashning asosiy yo'llari. Axborot xavfsizligining huquqiy va tashkiliy tahminoti.....	- 15 -
Axborot xavfsizligining xizmatlari va mexanizmlari. Axborot-kommunikatsion tizimlar va tarmoqlar xavfsizligiga qo'yiladigan talablar.....	- 16 -
4. Ma'ruza. Axborotni himoyalashning kriptografik usullari. Elektron raqamli imzo. - 20	-
Kriptotizimlarga qo'yilgan talablar	- 22 -
Axborotni simmetrik algoritmlar asosida kriptografik ximoyalash tamoyillari.....	- 23 -
Axborotni nosimmetrik algoritmlar asosida kriptografik ximoyalash tamoyillari. - 24 -	
Shifrlash standartlari. Kriptografik kalitlarni boshqarish. Xeshlash funksiyasi....	- 25 -
Kriptografik kalitlarni boshqarish.....	- 26 -
Xeshlash funksiyasi	- 27 -
Elektron raqamli imzo va uning zamonaviy turlari	- 27 -
5. Ma'ruza. Axborot xavfsizligida identifikatsiya va autentifikatsiya. Tarmoqlararo ekran texnologiyasi.....	- 30 -
6. Kompyuter viruslari va ularga qarshi kurashish mexanizmlari.	- 32 -
Virus nima?	- 32 -
Kompyuter viruslari qanday hosil bo'ladi?	- 33 -
Virus paydo bo'lish belgilari.	- 36 -
Virusga qarshi dasturlar	- 36 -
7. Ma'ruza. Axborot-kommunikatsion tizimlarda suqilib kirishlarni aniqlash. Mahlumotlarni uzatish tarmog'ida axborotni himoyalash.	- 38 -
Xujumlarni aniqlash.....	- 38 -
8. Ma'ruza. Virtual himoyalangan tarmoqlar. Simsiz aloqa tizimlarida axborot himoyasi.	- 40 -
Simsiz aloqa tizimlarida axborot himoyasi. Simsiz qurilmalar xavfsizligi muammolari	- 42 -
9. Ma'ruza. Xavfsizlikni boshqarish va himoya tizimini qurish.....	- 46 -
Parolli himoya va ularning zamonaviy turlari. Parollar asosida autentifikatsiyalash-	46
Elektron biznes va uning xavfsizligi muammolari.	- 48 -
Asosiy adabiyotlar.....	- 51 -

SO'Z BOSHI

Tez rivojlanib borayotgan kompyuter axborot texnologiyalari bizning kundalik xayotimizning barcha jabxalarida sezilarli o'zgarishlarni olib kirmokda. Xozirda "axborot tushunchasi" sotib olish, sotish, biror boshka tovarga almashtirish mumkin bulgan maxsus tovar belgisi sifatida tez-tez ishlatilmokda. Shu bilan birga axborotning baxosi kup xollarda uning uzi joylashgan kompyuter tizimining baxosida bir necha yuz va ming barobarga oshib ketmokda. SHuning uchun tamomila tabiiy xolda axborotni unga ruxsat etilmagan xolda kirishdan, kasddan o'zgartirishdan, uni ugirlashdan, yo'qotishdan va boshka jinoiy xarakterlardan ximoya qilishga kuchli zarurat tugiladi.

Kompyuter tizimlari va tarmoqlarida axborotni ximoya ostiga olish deganda, berilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchligini tizimi tarzda ta'minlash maksadida turli vosita va usullarni kullash, choralarni kurish va tadbirlarni amalga oshirishni tushunish kabul qilingan.

*Axborotni ximoya qilish deganda:*¹

- Axborotning jismoniy butunligini ta'minlash, shu bilan birga axborot elementlarining buzilishi, yoki yo'q qilinishiga yul kuymaslik;
- Axborotning butunligini saklab kolgan xolda, uni elementlarini kalbakilashtirishga (o'zgartirishga) yul kuymaslik;
- Axborotni tegishli xukukularga ega bulmagan shaxslar yoki jarayonlar orkali tarmokdan ruxsat etilmagan xolda olishga yul kuymaslik;
- Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar fakat tomonlar urtasida kelishilgan shartnomalar asosida kullanilishiga ishonish kabilar tushuniladi.

Yukorida ta'kidlab utilganlarning barchasi asosida kompyuter tarmoklari va tizimlarida axborot xavfsizligi muammosining dolzarbliji va muximligi kelib chikadi. SHuning uchun xozirgi kurs Respublikamizning oliy va urta maxsus ukuv muassasalari ukuv rejalarida munosib urin egallaydi.

Ushbu fanning vazifalari:

- Talabalarda axborot xavfsizligi tugrisidagi bilimlarni shakllantirish;
- Axborotni ximoya qilishning nazariy, amaliy va uslubiy asoslarini berish;
- Talabalarga kompyuter tarmoklari va tizimlarida axborot xavfsizligini ta'minlashning zamonaviy usullari va vositalarini kullashni amaliy jixatdan urgatish;
- Talabalarni axborotni ximoya qilish buyicha ishlab chikarilgan turli xil dasturiy maxsulotlardan erkin foydalana olish imkonini beradigan bilimlar bilan ta'minlash;

Kursni uzlashtirish natijasida talaba kuyidagilarnibilishi shart;

¹ M.G'aniyev. Axborot xavfsizligi, 2-bet

- kompyuter tarmoklari va tizimlaridagi axborot xavfsizligiga taxdid solishi kutilayotgan xavf xatarning moxiyatini va okibatlarini tushunishi;
- kompyuter tarmoklari va tizimlarida axborotni ximoya qilish buyicha kuyiladigan asosiy talablar va asoslarni uzlashtirish;
- kompyuter tarmoklari va tizimlarida axborot xavfsizlagini ta'minlashda kullaniladigan zamonaviy usullar va vositalarni bilish;
- tizimlarda axborot butunligi va ishochligini buzuvchi viruslar va boshka manbalar mavjudligini tizimli tekshirishni ta'minlash va ularni zararsizlashtirish buyicha choralarmi kurish;
- axborotni ximoya qilishda kullaniladigan zamonaviy amaliy tizimlar va dasturiy maxsulotlarni ishlata olish;

1. Ma’ruza. Kirish. Axborot xavfsizligi tushunchasi va axborotni himoyalash muammolari. Axborot-kommunikatsion tizimlar va tarmoqlarda taxdidlar va zaifliklar

Reja:

- 1. Axborot xavfsizligi tushunchasi va axborotni himoyalash muammolari**
- 2. Axborot-kommunikatsion tizimlar va tarmoqlarda taxdidlar va zaifliklar**

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

Xavfsizlikning asosiy yo’nalishlari

Axborot xavfsizligi. Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo’llanilmoqda (iqtisod, fan, ta’lim, xarbiy ish, turli texnologiyalarni boshqarish va x.k.)

Iqtisodiy xavfsizlik. Milliy iqtisodda axborotlarni yaratish, tarqatish, qayta ishlash va foydalanish jarayoni hamda vositalarini qamrab olgan Yangi tarmoq vujudga keldi. «Milliy axborot resursi» tushunchasi Yangi iqtisodiy kategoriya bo’lib xizmat qilmoqda. Davlatning axborot resurslariga keltirilayotgan zarar axborot xavfsizligiga xam ta’sir ko’rsatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakllantirish va uning asosida jahon yagona axborot maydoniga kirib borish natijasida milliy iqtisodimizga turli xildagi zararlar keltirish xavfi paydo bo’lmoqda.

Mudofaa xavfsizligi. Mudofaa sohasida xavfsizlikning asosiy ob’ektlaridan bo’lib, mamlakatning mudofaa potentsialining axborot tarkibi va axborot resurslari hisoblanmoqda. Xozirgi kunda barcha zamonaviy qurollar va harbiy texnikalar juda ham kompyuterlashtirilib yuborildi. SHuning uchun xam ularga axborot quollarini qo’llash ehtimoli katta.

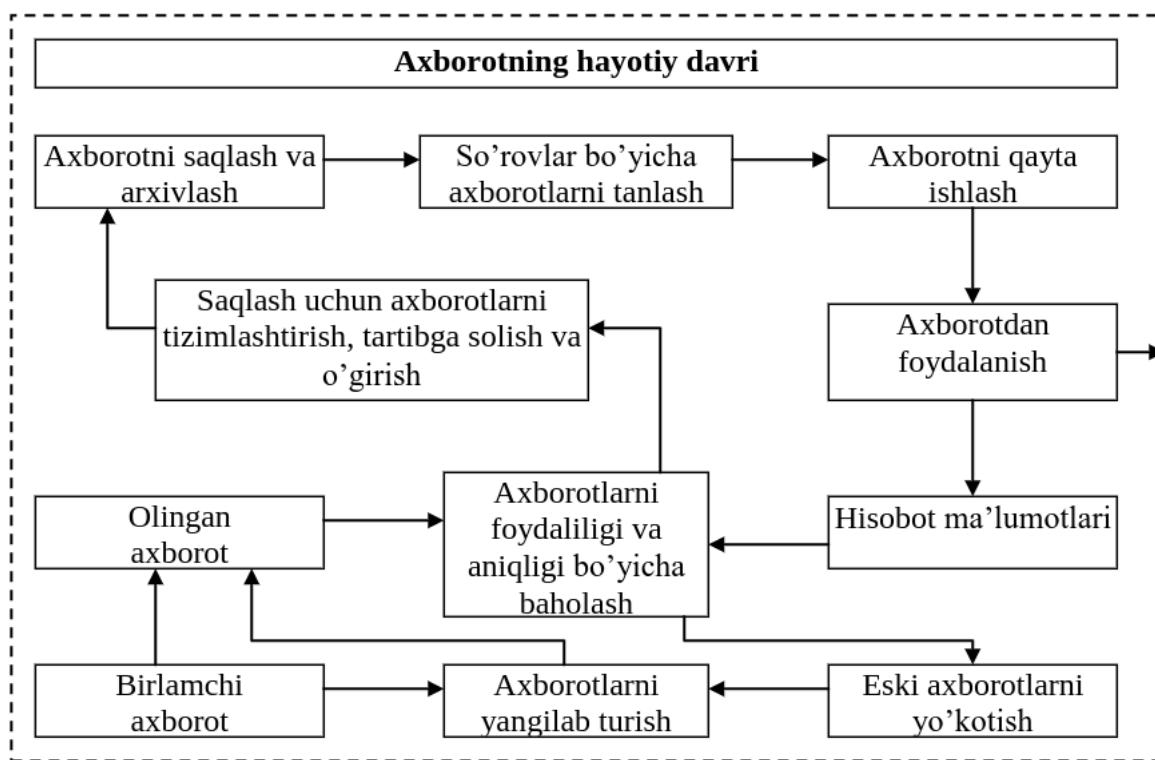
Ijtimoiy xavfsizlik. Zamonaviy axborot – kommunikatsiyalar texnologiyalarining milliy iqtisod barcha tarmoqlarida keng qo’llanishi inson psixologiyasi va jamoa ongiga «yashirin» ta’sir ko’rsatish vositalarining samaradorligini yuksaltirib yubordi.

Ekologik xavfsizlik. Ekologik xavfsizlik – global mashtabdagi muammodir. «Ekologik toza», energiya va resurs tejaydigan, chiqindisiz texnologiyalarga o'tish faqat milliy iqtisodni axborotlashtirish hisobiga qayta qurish asosidagina yo'lga qo'yish mumkin.

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

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

Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muxim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulki huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshha moddiy hamda nomoddiy zararlar keltirishi mumkin bo'lgan turli kirishlar va o'g'irlashlardan himoyalashdir.



2-rasm

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

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

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta'minlovchi va tashkilot axborot zaxiralalarining yaxlitliligi, ishonchliligi,

foydalaniш osonligi va maxfiyligini ta'minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytildi.

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

Axborot xavfsizligi nuktai nazaridan axborotni quyidagicha tarkumlash mumkin:

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

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

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

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

- **apellyatsiya qilishlik** — yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo'llaniladi. Kerak bo'lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yukoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin:

- **ishonchlilik** — tizim meyoriy va g'ayri tabiiy xollarda rejallashtirilganidek o'zini tutishlik kafolati;

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

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

- **nazorat qilinishi** — istalgan paytda dastur majmuasining xoxlagan kismini tulik tekshirish mumkinligi kafolati;

- **identifikatsiyalashni nazorat qilish** — xozir tizimga ulangan mijoz aniq o'zini kim deb atagan bulsa, aniq o'sha ekanligining kafolati;

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

Axborotni ximoyalashning maqsadlari kuyidagilardan iborat:

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

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

- axborotni yo'q qilish, o'zgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish;

- xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta'minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish;

- axborot tizimida mavjud bulgan shaxsiy ma'lumotlarning shaxsiy maxfiyligini va konfidentsialligini saklovchi fukarolarning konstitutusyon xukuklarini ximoyalash;
- davlat sirini, konunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saklash;
- axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chikish va kullashda sub'ektlarning xukuklarini ta'minlash.

Axborot-kommunikatsion tizimlar va tarmoqlarda taxdidlar va zaifliklar

Tarmoq texnologiyalari rivojining boshlang'ich bosqichida viruslar va kompyuter xujumlarining boshqa turlari ta'siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bog'liqligi katta emas edi. Hozirda, xujumlar sonining doimo o'sishi hamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bog'liqligi sharoitida mashina vaqtining yo'qolishiga olib keluvchi hatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi. Misol tariqasida keltirish mumkinki, faqat 2003 yilning birinchi choragida dunyo miqyosidagi yo'qotishlar 2002 yildagi barcha yo'qotishlar yig'indisining 50%ini tashkil etgan, yoki bo'lmasa 2006 yilning o'zida Rossiya Federeatsiyasida 14 mingdan ortiq kompyuter jinoyatchiligi holatlari qayd etilgan.

Korporativ tarmoqlarda ishlanadigan axborot, ayniqsa, zaif bo'ladi. Hozirda ruxsatsiz foydalanishga yoki axborotni modifikatsiyalashga, yolg'on axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo'ladi:

- kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot hajmining oshishi;
- ma'lumotlar bazasida muhimlik va mahfiylik darajasi turli bo'lgan axborotlarning to'planishi;
- ma'lumotlar bazasida saqlanayotgan axborotdan va hisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi;
- masofadagi ishchi joylar soninig oshishi;
- foydalanuvchilarni bog'lash uchun Internet global tarmog'ini va aloqaning turli kanallarini keng ishlatish;
- foydaluvchilar kompyuterlari o'rtaida axborot almashinuvining avtomatlashtirilishi.

Axborot xavfsizligiga tahdid deganda axborotning buzilishi yoki yo'qotilishi xavfiga olib keluvchi himoyalanuvchi ob'ektga qarshi qilingan harakatlar tushuniladi. Oldindan shuni aytish mumkinki, so'z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommertsiya qiymatiga ega bo'lgan qismi xususida ketyapti.

Zamonaviy korporativ tarmoqlar va tizimlar duchor bo'ladigan keng tarqalgan tahdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlikka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi manba) bo'lishi mumkin. Bunday ajratish to'g'ri, chunki bitta tahdid uchun (masalan, o'g'irlash) tashqi va ichki manbalarga qarshi harakat usullari turlicha bo'ladi. Bo'lishi

mumkin bo'lgan tahdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta'minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi.

Tez-tez bo'ladigan va xavfli (zarar o'lchami nuqtai nazaridan) tahdidlarga foydalanuvchilarning, operatorlarning, ma'murlarning va korporativ axborot tizimlariga xizmat ko'rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba'zida bunday xatoliklar (noto'g'ri kiritilgan ma'lumotlar, dasturdagi xatoliklar sabab bo'lgan tizimning to'xtashi yoki bo'zilishi) to'g'ridan to'g'ri zararga olib keladi. Ba'zida ular niyati buzuq odamlar foydalanishi mumkin bo'lgan nozik joylarni paydo bo'lishiga sabab bo'ladi. Global axborot tarmog'ida ishslash ushbu omilning yetarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo'lishi mumkin, oxirgisi ayniqsa xavfli.

Zarar o'lchami bo'yicha ikkinchi o'rinni o'g'irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishslash rejimlari va himoyalash choralari bilan a'lo darajada tanish bo'lgan tashkilot shtatidagi xodimlar aybdor bo'lib chiqdilar. Global tarmoqlar bilan bog'langan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan yetarlicha nazorat yo'qligi bunday faoliyatga qo'shimcha imkon yaratadi.

Xafa bo'lgan xodimlar (hatto sobiqlari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon yetkazishlari mumkin. Xodim ishdan bo'shanida uning axborot resurslaridan foydalanish xuquqi bekor qilinishi nazoratga olinishi shart.

Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo'lishi mumkin bo'lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo'lib tuyulmasa ham, Internetda ishslash tajribasi ko'rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga duchor bo'lar ekan. Xavf-xatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog'i kompyuterlarining xujumlarga qarshi turishi yoki bo'lmanida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha himoyalananmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko'rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan sasofadan foydalanish xollari alohida ko'rilishi lozim.

Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti duchor bo'ladigan xavf-xatar baholanishi va zarur choralar ko'rilishi zarur. Ravshanki, himoyaga tahdidni nazoratlash va zarur choralar ko'rish uchun tashkilotning sarf-harajati tashkilotda aktivlar va resurslarni himoyalash bo'yicha hech qanday choralar ko'rilmaganida kutiladigan yo'qotishlardan oshib ketmasligi shart.

Umuman olganda, tashkilotning kompyuter muhiti ikki xil xavf-xatarga duchor bo'ladi:

1. Ma'lumotlarni yo'qotilishi yoki o'zgartirilishi.
2. Servisning to'xtatilishi.

Tahdidlarning manbalarini aniqlash oson emas. Ular niyati buzuq odamlarning bostirib kirishidan to kompyuter viruslarigacha turlanishi mumkin.

Bunda inson xatoliklari xavfsizlikka jiddiy tahdid hisoblanadi. 1.1-rasmda korporativ axborot tizimida xavfsizlikning buzilish manbalari bo'yicha statistik ma'lumotlarni tasvirlovchi aylanma diagramma keltirilgan.



1.1-расм. Хавфсизликнинг бузилиши манбалари.

1.1.-rasmda keltirilgan statistik ma'lumotlar tashkilot ma'muriyatiga va xodimlariga korporativ tarmoq va tizimi xavfsizligiga tahdidlarni samarali kamaytirish uchun xarakatlarni qaerga yo'naltirishlari zarurligini aytib berishi mumkin. Albatta, fizik xavfsizlik muammolari bilan shug'ullanish va inson xatoliklarining xavfsizlikka salbiy ta'sirini kamaytirish bo'yicha choralar ko'rilishi zarur. Shu bilan bir qatorda korporativ tarmoq va tizimga ham tashqaridan, ham ichkaridan bo'ladigan xujumlarni oldini olish bo'yicha tarmoq xavfsizligi masalasini yechishga jiddiy e'tiborni qaratish zarur.

2. Ma’ruza. Tarmoqdagi axborotga bo’ladigan na`munaviy hujumlar. Axborot xavfsizligi modellari

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

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

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

Sarguzasht qidiruvchi, odatda, yosh, ko’pincha talaba yoki yuqori sinf o’quvchisi va unda o’ylab qilingan xujum rejasi kamdan-kam bo’ladi. U nishonini tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi. Xavfsizlik tizimida nuqsonli joyni topib, u maxfiy axborotni yig’ishga tirishadi, ammo hech qachon uni yashirincha o’zgartirishga urinmaydi. Bunday sarguzasht qidiruvchi muvaffaqiyatlarini fakat yaqin do’stлari-kasbdoshlari bilan o’rtoqlashadi.

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

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

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

Yuqorida keltirilgan axborot xavfsizligini buzuvchilar kategoriylarini ularni malakalari bo’yicha guruhlash mumkin: xavaskor (sarguzasht qidiruvchi), mutaxassis (g’oyali xaker, ishonchsiz xodim), professional (xaker-professional). Agar bu guruhlar bilan xavfsizlikning buzilishi sabablari va har bir guruhning texnik qurollanganligi

taqqoslansa, axborot xavfsizligini buzuvchining umumlashtirilgan modelini olish mumkin.

Axborot xavfsizligini buzuvchi, odatda ma'lum malakali mutaxassis bo'lgan holda kompyuter tizimlari va tarmoqlari xususan, ularni himoyalash vositalari xususida barcha narsalarni bilishga urinadi. Shu sababli buzuvchi modeli quyidagilarni aniqlaydi:

- buzuvchi bo'lishi mumkin bo'lgan shaxslar kategoriysi;
- buzuvchining bo'lishi mumkin bo'lgan nishonlari va ularning muhimlik va xavfsizlik darajasi bo'yicha rutbalanishi;
- uning malakasi xususidagi taxminlar; uning texnik qurollanganligining baxosi;
- uning harakat harakteri bo'yicha cheklashlar va taxminlar.



1.3-расм. Ахборот хавфсизлигини бузувчининг модели

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

Yaqin vaqtgacha rahbarlardan norozi xizmatchilarning o'z mavqelarini suiiste'mol qilgan holda tizimni buzishlari, undan begonalarning foydalanishlariga yo'l o'yishlari yoki tizimni ish holatida qarovsiz qoldirishlari tashvishlantirar edi. Bunday harakatlarga majbur etish sababbrili quyidagilar:

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

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

Professional xakerlar-hisoblash texnikasini va aloka tizimini juda yaxshi biladigan kompyuter fanatlari (mутаассиблари) hisoblanadi. Tizimga kirish uchun professionallar omadga va farazga tayanmaydilar va qandaydir tartibni va tajribani ishlataladilar. Ularning maksadi-himoyani aniqlash va yo'qotish, hisoblash kurilmasining imkoniyatlarini o'rganish va maqsadiga erishish mumkinligi to'g'risida qarorga kelish.

Bunday professional xakerlar kategoriyasiga quyidagi shaxslar kiradi:

- siyosiy maqsadni ko'zlovchi jinoiy guruhlarga kiruvchilar;
- sanoat joususlik maqsadlarida axborotni olishga urinuvchilar;
- tekin daromadga intiluvchi xakerlar guruhi.

Umuman professional xakerlar xavf-xatarni minimallashtirishga urinadilar. Buning uchun ular birga ishlashga firmada ishlaydigan yoki firmadan yaqinda ishdan bo'shatilgan xodimlarni jalb etadilar, chunki begona uchun bank tizimiga kirishda oshkor bo'lish xavfi juda katta. Xaqiqatan, bank hisoblash tizimlarining murakkabligi va yuqori tezkorligi, xujjatlarni yurgizish va tekshirish usullarining muntazam takomillashtirilishi begona shaxs uchun xabarlarni ushlab kolish yoki ma'lumotlarni o'g'irlash maqsadida tizimga o'rashishiga imkon bermaydi. Professional xakerlar uchun yana bir qo'shimcha xavotir-tizimdagi bir komponentning o'zgarishi boshqa bir komponentning buzilishiga olib kelishi va xatardan darak beruvchi signalga sabab bo'lishi mumkin.

Xakerlar xavf-xatarni kamaytirish maqsadida odatda moliyaviy va oilaviy muammolarga ega bo'lган xodimlar bilan kontaktga kiradilar. Ko'pgina odamlar hayotida xakerlar bilan to'qnashmasliklari mumkin, ammo alkagolga yoki qimorga ruju qo'ygan xodimlar bilmasdan jinoiy guruh bi lan bog'langan qandaydir bir bukmekerdan qarzdor bo'lib qolishlari mumkin. Bunday xodim qandaydir o'yin-kulgi kechasida suhbatdoshining professional agent ekanligiga shubha qilmagan holda ortiqcha gapirib yuborishi mumkin.

3.Ma’ruza. Axborot xavfsizligini tahminlashning asosiy yo’llari. Axborot xavfsizligining huquqiy va tashkiliy tahminoti.

Kompyuter jinoyatchiligi statistikasi tahlil etilsa qayg’uli manzaraga ega bo’lamiz. Kompyuter jinoyatchiligi yetkazgan zararni narkotik moddalar va qurollarning noqonuniy aylanishidan olingan foydaga qiyoslash mumkin. Faqat AQSHda "elektron jinoyatchilar" yetkazgan har yilgi zarar qariyb 100 mld. dollarni tashkil etar ekan.

Yaqin kelajakda jinoiy faoliyatning bu turi daromadliligi, pul mablag’larining aylanishi va unda ishtirok etuvchi odamlar soni bo'yicha yaqin vaqtlargacha noqonuniy faoliyat orasida daromadligi bilan birinchi o'rinni egallagan noqonuniy biznesning uch turidan uzib ketish ehtimolligi katta. Bu noqonuniy bizneslar-narkotik moddalar, qurol va kam uchraydigan yovvoyi hayvonlar bilan savdo qilish.

Davlat va xususiy kompaniyalar faoliyatining sotsiologik tadqiqi ma'lumotlariga qaraganda XXI asrning birinchi yillarida iqtisodiy sohadagi jinoyatchilik bank va boshqa tizimlarning axborot- kommunikatsion komplekslariga bo'lishi mumkin bo'lgan g'arazli iqtisodiy harakatlarga qaratilgan bo'ladi.

Kredit-moliya sohasidagi kompyuter jinoyatchiligining soni muttasil o'sib bormoqda. Masalan onlayn magazinlarida 25%gacha qalloblik to'lov amallari qayd etilgan. SHunga qaramasdan G'arb davlatlarida elektron tijoratning-yuqori daromadli zamonaviy biznesning faol rivojlanishi ko'zga tashlanmoqda. Ma'lumki, bu soha rivojlanishi bilan parallel ravishda "virtual" qalloblarning ham daromadi oshadi. Qalloblar endi yakka holda harakat qilmaydilar, ular puxtalik bilan tayyorlangan, yaxshi texnik va dasturiy qurollangan jinoiy guruqlar bilan, bank xizmatchilarining o'zları ishtirokida ishlaydilar.

Xavfsizlik sohasidagi mutaxassislarning ko'rsatishicha bunday jinoyatchilarning ulushi 70%ni tashkil etadi. "Virtual" o'g'ri o'zining hamkasbi-oddiy bosqinchiga nisbatan ko'p topadi. Undan tashqari "virtual" jinoyatchilar uyidan chiqmasdan harakat qiladilar. Foydalanishning elektron vositalarini ishlatib qilingan o'g'rilik zararining o'rtacha ko'rsatkichi faqat AQSHda bankni qurolli bosqinchilikdan kelgan zararning o'rtacha statistik zararidan 6-7 marta katta.

Bank xizmati va moliya amallari sohasidagi turli xil qalloblik natijasida yo'qotishlar 1989 yili 800 mln. dollardan 1997 yili — 100 mlrd. dollarga yetgan. Bu ko'rsatkichlar o'sayapti, aslida yuqorida keltirilgan ma'lumotlardan bir tartibga oshishi mumkin. CHunki ko'p yo'qotishlar aniqlanmaydi yoki e'lon qilinmaydi. O'ziga xos "indamaslik siyosati"ni tizim ma'murlarining o'zining tarmog'idan ruxsatsiz foydalanganlik tafsilotini, bu noxush xodisaning takrorlanishidan qo'rqib va o'zining himoya usulini oshkor etmaslik vajida muhokama etishni xoxlamasliklari bilan tushunish mumkin.

Kompyuter ishlatiladigan inson faoliyatining boshqa sohalarida ham vaziyat yaxshi emas. Yildan-yilga xuquqni muhofaza qiluvchi organlariga kompyuter jinoyatchiligi xususidagi murojaatlar oshib bormoqda.

Barcha mutaxassislar viruslarning tarqalishi bilan bir qatorda tashqi xujumlarning keskin oshganligini e'tirof etmoqdalar. Ko'rinib turibdiki, kompyuter jinoyatchiligi

natijasida zarar qat'iy ortmoqda. Ammo kompyuter jinoyatchiligi ko'pincha "virtual" qalloblar tomonidan amalga oshiriladi deyish haqiqatga to'g'ri kelmaydi. Hozircha kompyuter tarmoqlariga suqilib kirish xavfi har biri o'zining usuliga ega bo'lgan xakerlar, krakerlar va kompyuter qaroqchilarini tomonidan kelmoqda.

Xakerlar, boshqa kompyuter qaroqchilaridan farqli holda, ba'zida, oldindan, maqtanish maqsadida kompyuter egalariga ularning tizimiga ki-rish niyatlarini bildirib qo'yadilar. Muvaffaqiyatlari xususida Internet saytlarida xabar beradilar. Bunda xaker musobaqalashuvni niyatida kirgan kompyuterlariga zarar yetkazmaydi.

Krakerlar (cracker) — elektron "o'g'rilar" manfaat maqsadida dasturlarni buzishga ixtisoslashganlar. Buning uchun ular Internet tarmog'i bo'yicha tarqatiluvchi buzishning tayyor dasturlaridan foydalanadilar.

Kompyuter qaroqchilarini — raqobat qiluvchi firmalar va xatto ajnabiy maxsus xizmatlari buyurtmasi bo'yicha axborotni o'g'irlovchi firma va kompaniyalarning yuqori malakali mutaxassislari. Undan tashqari ular begona bank schetidan pul mablag'larini o'g'irlash bilan ham shug'ullanadilar.

Ba'zi "mutaxassislar" jiddiy guruh tashkil qiladilar, chunki bunday kriminal biznes o'ta daromadlidir. Bu esa tez orada, "virtual" jinoyatning zarari jinoyat biznesining an'anaviy xilidagi zarardan bir tartibga (agar ko'p bo'lmasa) oshishiga sabab bo'ladi. Hozircha bunday tahdidni betaraflashtirishning samarali usullari mavjud emas.

Axborot xavfsizligining xizmatlari va mexanizmlari. Axborot-kommunikatsion tizimlar va tarmoqlar xavfsizligiga qo'yiladigan talablar

Axborot xavfsizligining siyosatini ishlab chiqishda, avvalo himoya qilinuvchi ob'ekt va uning vazifalari aniqlanadi. So'ngra dushmanning bu ob'ektga qiziqishi darajasi, hujumning ehtimolli turlari va ko'rildigan zarar baholanadi. Nihoyat, mavjud qarshi ta'sir vositalari yetarli himoyani ta'minlamaydigan ob'ektning zaif joylari aniqlanadi.

Samarali himoya uchun har bir ob'ekt mumkin bo'lgan tahidilar va xujum turlari, maxsus instrumentlar, quollar va portlovchi moddalarning ishlatalishi ehtimolligi nuqtai nazaridan baholanishi zarur. Ta'kidlash lozimki, niyati buzuq odam uchun eng qimmatli ob'ekt uning e'tiborini tortadi va ehtimolli nishon bo'lib xizmat qiladi va unga qarshi asosiy kuchlar ishlataladi. Bunda, xavfsizlik siyosatining ishlab chiqilishida yechimi berilgan ob'ektning real himoyasini ta'minlovchi masalalar hisobga olinishi lozim.

Qarshi ta'sir vositalari himoyaning to'liq va eshelonlangan kontseptsiyasiga mos kelishi shart. Bu degani, qarshi ta'sir vositalarini markazida himoyalanuvchi ob'ekt bo'lgan kontsentrik doiralarda joylashtirish lozim. Bu holda dushmanning istalgan ob'ektga yo'li himoyaning eshelonlangan tizimini kesib o'tadi. Mudofaaning har bir chegarasi shunday tashkil qilinadiki, qo'riqlash xodimining javob choralarini ko'rishiga yetarlicha vaqt mobaynida xujumchini ushlab turish imkonini bo'lsin.

So'nggi bosqichda qarshi ta'sir vositalari qabul qilingan himoya kontseptsiyasiga binoan birlashtiriladi. Butun tizim hayoti tsiklining boshlang'ich va kutiluvchi umumiy narxini dastlabki baholash amalga oshiriladi.

Agar bir binoning ichida turli himoyalash talablariga ega bo'lgan ob'ektlar joylashgan bo'lsa, bino otseklarga bo'linadi. SHu tariqa umumiy nazoratlanuvchi makon ichida ichki perimetrlar ajratiladi va ruxsatsiz foydalanishdan ichki himoya vositalari yaratiladi. Perimetr, odatda, fizik to'siqlar orqali aniqlanib, bu to'siqlardan o'tish elektron usul yoki qo'riqlash xodimlari tomonidan bajariluvchi maxsus muolajalar yordamida nazoratlanadi.

Umumiy chegaraga yoki perimetrga ega bo'lgan binolar guruhini himoyalashda nafaqat alohida ob'ekt yoki bino, balki uning joylanish joyi ham hisobga olinishi zarur. Ko'p sonli binolari bo'lgan yer uchastkalari xavfsizlikni ta'minlash bo'yicha umumiy yoki qisman mos keladigan talablarga ega bo'ladi, ba'zi uchastkalar esa perimetr bo'yicha to'siqqa va yagona yo'lakka ega. Umumiy perimetr tashkil etib, har bir binodagi himoya vositalarini kamaytirish va ularni faqat xujum qilinishi ehtimoli ko'proq bo'lgan muhim ob'ektlarga o'rnatish mumkin. Xuddi shu tariqa uchastkadagi har bir imorat yoki ob'ekt xujumchini ushlab qolish imkoniyati nuqtai nazaridan baholanadi.

Yuqoridagi keltirilgan talablar tahlili ko'rsatadiki, ularning barchasi axborotni ishslash va uzatish qurilmalaridan xuquqsiz foydalanish, axborot eltuvchilarini o'g'irlash va sabotaj imkoniyatini yo'l qo'ymaslikka olib keladi.

Binolar, imoratlar va axborot vositalarining xavfsizlik tizimini nazorat punktlarini bir zonadan ikkinchi zonaga o'tish yo'lida joylashtirgan holda kontsentrik halqa ko'rinishida tashkil etish maqsadiga muvofiq hisoblanadi.



- 1-зона. Компьютер тармоғи (КТ) хавфсизлигининг ташқи зонаси
Таъминланиши: - физик тусиқлар
- периметр бўйлаб ўтиш жойлари
- худудга кириш назоратининг ноавтоматик тизими
- 2- зона. КТ хавфсизлигининг ўртадаги зонаси
Таъминланиши: - эшиклари электрон ҳимояланган назорат пунктлари
- видеокузватиш
- бум буш зоналарни чиқариб ташлаш
- 3-зона. КТ хавфсизлигининг ички зонаси
Таъминлаш: - шахсий компьютерга фойдаланиш фақат назорат тизими орқали
- идентификациялашнинг биометрик тизими

3.3-расм. Бинодаги компьютер тизимининг хавфсизлик тизими

Axborot xizmati binolari va xonalariga kirishning nazorati masalasiga kelsak, asosiy chora-nafaqat bino va xonalarni, balki vositalar kompleksini, ularning funktional vazifalari bo'yicha ajratish va izolyatsiyalash. Bino va xonalarga kirishni nazoratlovchi avtomatik va noavtomatik tizimlar ishlataladi. Nazorat tizimi kunduzi va kechasi kuzatish vositalari bilan to'ldirilishi mumkin.

Xavfsizlikning fizik vositalarini tanlash himoyalanuvchi ob'ektning muhimligini, vositalarga ketadigan harajatni va nazorat tizimi ishonchliligi darajasini, ijtimoiy jihatlarni va inson nafsi buzuqligini oldindan o'rGANISHGA asoslanadi. Barmoq, kaftlar, ko'z to'r pardasi, qon tomirlari izlari yoki nutqni aniqlash kabi biometrik indentifikatsiyalash ishlatalishi mumkin. SHartnomaga asosida texnik vositalarga xizmat

ko'rsatuvchi xodimlarni ob'ektga kiritishning maxsus rejimi ko'zda tutilgan. Bu shaxslar identifikatsiyalanganlaridan so'ng ob'ektga kuzatuvchi hamrohligida kiritiladi. Undan tashqari ularga aniq kelish rejimi, makoniy chegaralanish, kelib-ketish vaqt, bajaradigan ish xarakteri o'rnatiladi.

Nihoyat, bino perimetri bo'yicha bostirib kirishni aniqlovchi turli datchiklar yordamida kompleks kuzatish o'rnatiladi. Bu datchiklar ob'ektni qo'riqlashning markaziy posti bilan bog'langan va bo'lisi mumkin bo'lgan bostirib kirish nuqtalarini, ayniqsa ishlanmaydigan vaqtarda, nazorat qiladi.

Vaqti-vaqt bilan eshiklar, romlar, tom, ventilyatsiya tuynuklari va boshqa chiqish yo'llarining fizik himoyalanish ishonchligini tekshirib turish lozim.

Har bir xonaga ichidagi narsaning muhimligiga bog'liq foydalanish tizimiga ega bo'lgan zona sifatida qaraladi. Kirish-chiqish xuquqi tizimi shaxs yoki ob'ekt muhimligiga bog'liq holda selektsiyali va darajalari bo'yicha rutbalangan bo'lisi shart. Kirish-chiqish xuquqi tizimi markazlashgan bo'lisi mumkin (ruxsatlarni boshqarish, jadval va kalendar rejalarining rejalashtirilishi, kirish-chiqish xuquqining yozma namunalari va h.).

Nazorat tizimini vaqt-vaqt bilan tekshirib turish va uni doimo ishga layoqatli holda saqlash lozim. Buni ixtisoslashgan bo'linmalar va nazorat organlari ta'minlaydi.

SHaxsiy kompyuter va fizikaviy himoya vositalari kabi o'lchamlari kichik asbob-uskunalarini ko'zda tutish mumkin.

Yuqorida keltirilganlarga xulosa qilib, kompyuter tarmoqlarini himoyalashda axborot xavfsizligi siyosati qanday aniqlanishi xususida so'z yuritamiz. Odatda ko'p sonli foydalanuvchilarga ega bo'lgan korporativ kompyuter tarmoqlari uchun maxsus "Xavfsizlik siyosati" deb ataluvchi, tarmoqda ishlashni ma'lum tartib va qoidalarga bo'y sindiruvchi (reglamentlovchi) hujjat tuziladi.

Siyosat odatda ikki qismdan iborat bo'ladi: umumiyl printsipler va ishslashning muayyan qoidalari. Umumiyl printsipler Internetda xavfsizlikka yondashishni aniqlasa, qoidalari nima ruxsat etilishini va nima ruxsat etilmasligini belgilaydi. Qoidalalar muayyan muolajalar va turli qo'llanmalar bilan to'ldirilishi mumkin.

Himoyaga qo'yiladigan talablarning asosini tahdidlar ro'yxati tashkil etadi. Bunday talablar o'z navbatida himoyaning zaruriy vazifalari va himoya vositalarini aniqlaydi.

Demak, kompyuter tarmog'ida axborotni samarali himoyasini ta'minlash uchun himoya tizimini loyihalash va amalga oshirish uch bosqichda amalga oshirilishi kerak.

- xavf-xatarni taxlillash;
- xavfsizlik siyosatini amalga oshirish;
- xavfsizlik siyosatini madadlash.

Birinchi bosqichda kompyuter tarmog'ining zaif elementlari taxlilanadi, tahdidlar aniqlanadi va baholanadi, himoyaning optimal vositalari tanlanadi. Xavf-xatarni taxlillash xavfsizlik siyosatini qabul qilish bilan tugallanadi.

Ikkinci bosqich — xavfsizlik siyosatini amalga oshirish moliyaviy xarajatlarni hisoblash va masalalarni yechish uchun mos vositalarni tanlash bilan boshlanadi. Bunda tanlangan vositalar ishslashining ixtilofli emasligi, vositalarni yetkazib beruvchilarining obro'si, himoya mexanizmlari va beriladigan kafolatlar xususidagi to'la axborot olish

imkoniyati kabi omillar hisobga olinishi zarur. Undan tashqari, axborot xavfsizligi bo'yicha asosiy qoidalar aks ettirilgan printsiplar hisobga olinishi kerak.

Uchinchi bosqich — xavfsizlik siyosatini madadlash bosqichi eng muhim hisoblanadi. Bu bosqichda o'tkaziladigan tadbirlar niyati buzuq odamlarning tarmoqqa bostirib kirishini doimo nazorat qilib turishni, axborot ob'ektini himoyalash tizimidagi "rahna"larni aniqlashni, konfidentsial ma'lumotlardan ruxsatsiz foydalanish hollarini hisobga olishni talab etadi. Tarmoq xavfsizligi siyosatini madadlashda asosiy javobgarlik tizim ma'muri bo'ynida bo'ladi. U xavfsizlikning muayyan tizimi buzilishining barcha xollariga operativ munosabat bildirishi, ularni taxlillashi va moliyaviy vositalarning maksimal tejalishini hisobga olgan holda himoyaning zaruriy apparat va dasturiy vositalaridan foydalanishi shart.

4. Ma’ruza. Axborotni himoyalashning kriptografik usullari. Elektron raqamli imzo.

Axborotning himoyalashning aksariyat mexanizmlari asosini shifrlash tashkil etadi. Axborotni shifrlash deganda ochiq axborotni (dastlabki matnni) shifrlangan axborotga o’zgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi.

Axborotni qayta akslantirish yordamida himoyalash muammosi inson ongini uzoq vaqtlardan buyon bezovta qilib kelgan. Kriptografiya tarixi – inson tili tarixi bilan tengdosh. Hatto dastlabki xat yozish ham o’z-o’zicha kriptografik tizim hisoblangan, chunki qadimgi jamiyatda faqat alohida shaxslargina xat yozishni bilganlar. Qadimgi Yegipet va Qadimgi Hindistonning ilohiy kitoblari bunga misol bo’la oladi.

Xat yozishning keng tarqalishi natijasida kriptografiya alohida fan sifatida vujudda keldi. Dastlabki kriptotizimlardan eramizning boshlaridayoq foydalilanigan. TSezar o’z xatlarida tizimli shifrlardan foydalangan.

Kriptografik tizimlar birinchi va ikkinchi jahon urushlarida jadal rivojlandi. Urush yillaridan so’ng va hozirga qadar hisoblash vositalarining jadal rivojlanishi kriptografik usullar yaratishni tezlashtirdi va ularning mukammalligini oshirdi.

Bir tomondan, kompyuter tarmoqlaridan foydalanish kengaydi, jumladan, Internet global tarmog’i. Bu tarmoqda begona shaxslardan himoyalanishi zarur bo’lgan hukumat, harbiy, tijorat va shaxsiy xarakterga ega bo’lgan axborotning katta hajmi harakatlanadi.

Boshqa tomondan, qudratli kompyuterlar, tarmoqli va nevronli hisoblash texnologiyalarining paydo bo’lishi ochish mumkin emas deb hisoblangan kriptografik tizimlarning obro’siga putur yetkazdi.

Kriptologiya – axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi (kryptos – maxfiy, sirli, logos - fan). Kriptologiya ikki yo’nalishga bo’linadi – kriptografiya va kriptoanaliz. Bu ikki yo’nalishning maqsadlari qarama-qarshi.

Kriptografiya – axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.

Kriptoanaliz – kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi.

Bu kitobda asosiy e’tibor kriptografik usullarga qaratilgan.

Zamonaviy kriptografiya quyidagi to’rtta bo’limlarni o’z ichiga oladi:

1. Simmetrik kriptotizimlar.
2. Ochiq kalitli kriptotizimlar.
3. Elektron imzo tizimlari.
4. Kalitlarni boshqarish.

Kriptografik usullardan foydalanishning asosiy yo’nalishi – maxfiy axborotning aloqa kanalidan uzatish (masalan, elektron pochta), uzatiladigan xabarning uzunligini o’rnatish, axborotni (hujjatlarni, ma’lumotlar bazasini) shifrlangan holda raqamli vositalarda saqlash.

SHunday qilib, kriptografiya axborotni shunday qayta ishlash imkonini beradiki, bunda uni qayta tiklash faqat kalitni bilgandagina mumkin.

Shifrlash va deshifrlashda qatnashadigan axborot sifatida biror alifbo asosida yozilgan matnlar qaraladi. Bu terminlar ostida quyidagilar tushuniladi.

Alifbo – axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam.

Matn – alifbo elementlarining tartiblangan to’plami.

Zamonaviy ATlarida qo’llaniladigan alifbolarga misol sifatida quyidagilarni keltirish mumkin:

- * Z_{33} alifbosi – rus alifbosining 32 harflari va bo’sh joy belgisi;
- * Z_{256} alifbosi – ASCII va KOI-8 standart kodlariga kiruvchi belgilar;
- * Binar alifbo - $Z_2 = \{0, 1\}$
- * Sakkizlik yoki o’n otilik alifbolar.

SHifrlash – akslantirish jarayoni: ochiq matn deb ham nomlanadigan matn shifrmatnga almashtiriladi.



Deshifrlash – shifrlashga teskari jarayon. Kalit asosida shifrmatn ochiq matnga akslantiriladi.

Kalit – matnni shifrlash va shifrni ochish uchun kerakli axborot.

Kriptografik tizim – ochiq matnni akslantirishning T oilasini o’zida mujassamlashtiradi. Bu oila a’zolari k bilan indekslanadi yoki belgilanadi. k parametr kalit hisoblanadi. K kalitlar fazosi – bu kalitning mumkin bo’lgan qiymatlari to’plami. Odatda kalit alifbo harflari ketma-ketligidan iborat bo’ladi.

Kriptotizimlar simmetrik va ochiq kalitli tizimlarga bo’linadi.

Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi.

Ochiq kalitli kriptotizimlarda bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan bo’ladi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi, yopiq kalit faqat qabul qiluvchigagina ma’lum.

Kalitlarni tarqatish va kalitlarni boshqarish terminlari axborotni akslantirish tizimlari jarayoniga tegishli. Bu iboralarning mohiyati foydalanuvchilar o’rasida kalit yaratish va tarqatishdir.

Elektron raqamli imzo deb – xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimchaga aytildi (elektron xujjatdagi mazkur elektron xujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan xolda maxsus o’zgartirish natijasida xosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron xujjatdagi axborotda xatolik yo’qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikasiya qilish imkoniyatini beradigan imzo).

Kriptobardoshlilik deb kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifiga aytildi.

Kriptobardoshlilikning bir necha ko’rsatkichlari bo’lib, ular:

- barcha mumkin bo’lgan kalitlar soni;
- kriptoanaliz uchun zarur bo’lgan o’rtacha vaqt.

Tk akslantirish unga mos keluvchi algoritm va k kalit qiymati bilan aniqlanadi. Axborotni himoyalash maqsadida samarali shifrlash kalitni yashirin saqlashga va shifrnning kriptobardoshliliga bog'liq.

Deyarli tub son – tub bo'lism ehtimoli 1 ga yaqin.

Belgi – axborotni fiksirlangan uzunlikdagi ko'rinishi

SHA – Secure Hash Algorithm ma'lumotni xeshlash algoritmi

vaqtinchalik shtempel - vaqtni belgilab qo'yish mexanizmi

Diffi - Xellman algoritmi – ikki abonent o'rtasida o'zaro kalit almashinish algoritmi

Autentifikatsiya – shaxsini haqqoniyligini tasdiqlash.

Kriptotizimlarga qo'yilgan talablar

Ma'lumotlarni kriptografik akslantirish jarayoni dasturiy va apparatli amalga oshirilishi mumkin. Apparatli ta'minot qimmat, ammo u sermahsullik, oddiylik, himoyalanganlik kabi afzalliliklarga ega. Dasturiy ta'minot foydalanishga qulayligi uchun ko'proq amaliy hisoblanadi.

Amalga oshirish usullariga bog'liq bo'limgan holda axborotni himoyalashning zamonaviy kriptografik tizimlariga quyidagi umumiyl talablar qo'yiladi:

- shifrlash algoritmini bilish shifrmattin kriptobardoshliligin tushirib yubormasligi lozim. Barcha kriptotizimlar bu talabga javob berishi kerak;
- shifrlangan xabarining biror qismi va unga mos ochiq matn asosida kalitni aniqlash uchun zarur bo'lgan amallar soni mumkin bo'lgan umumiyl kalitlarga sarflanadigan amallar sonidan kam bo'lmasligi kerak;
- shifrlangan matndan ochiq matnni hosil qilish uchun mumkin bo'lgan kalitlar to'plamini to'la ko'rib chiqish amallari soni qat'iy past ko'rsatkichga ega bo'lishi va zamonaviy kompyuterlar imkoniyatlari chegarasidan chiqib ketishi kerak;
- shifrlash algoritmini bilish himoyaga ta'sir qilmasligi kerak;
- kalitdagi yoki boshlang'ich ochiq matndagi kichik o'zgarishlar shifrlangan matnni tubdan o'zgartirib yuborishi kerak;
- shifrlash algoritmining tarkibiy elementlari o'zgarmas bo'lisi lozim;
- shifrlash jarayonida qo'shilgan qo'shimcha bitlar shifrmattnda bir butunligini saqlashi va yetarlicha yashirilgan bo'lisi talab etiladi;
- shifrmattin uzunligi ochiq matn uzunligiga teng bo'lisi kerak;
- shifrlash jarayonida ketma-ket qo'llaniladigan kalitlar o'rtasida o'zaro oddiy va oson bog'liqlik bo'lmasligi kerak;
- mumkin bo'lgan kalitlar to'plamidagi ixtiyoriy kalit, shifrmattning kriptobardoshliligin ta'minlashi kerak;
- algoritm ham dasturiy, ham apparatli realizatsiyaga qulay, va kalit uzunligining o'zgarishi, shifrlash algoritmining sifatini pasaytirmasligi kerak.

Axborotni simmetrik algoritmlar asosida kriptografik ximoyalash tamoyillari

Shifrlash kriptotizimining umumlashtirilgan sxemasi



Uzatiluvchi axborot matni M kriptografik o'zgartirish Yekl yordamida shifrlanadi, natijada shifrmattn C olinadi:

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

Kriptotizimlarning ikkita sinfi farqlanadi:

1. simmetrik kriptotizim (bir kalitli);
2. asimmetrik kriptotizim (ikkita kalitli).

SHifrlashning simmetrik kriptotizimida shifrlash va rasshifrovka qilish uchun bitta kalitning o'zi ishlatiladi. Demak, shifrlash kalitidan foydalanish xuquqiga ega bo'lgan har qanday odam axborotni rasshifrovka qilishi mumkin. SHu sababli, simmetrik kriptotizimlar mahfiy kalitli kriptotizimlar deb yuritiladi. Ya'ni shifrlash kalitidan faqat axborot atalgina foydalana olishi mumkin.

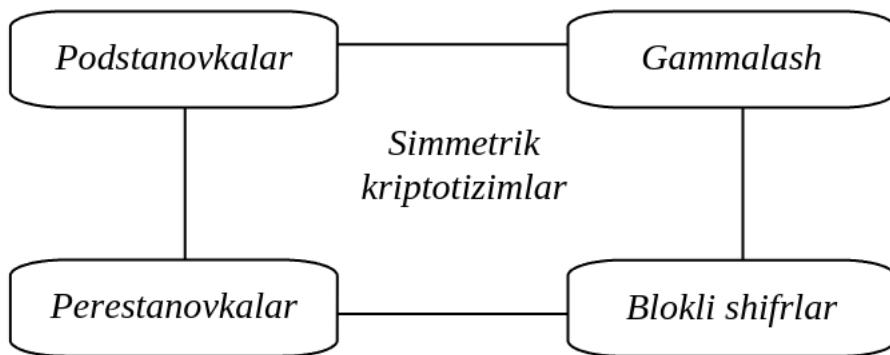


Elektron xujjatlarni uzatishning konfidentsialligini simmetrik kriptotizim yordamida ta'minlash masalasi shifrlash kaliti konfidentsialligini ta'minlashga keltiriladi. Odatda, shifrlash kaliti ma'lumotlar fayli va massividan iborat bo'ladi va shaxsiy kalit eltuvchisidan masalan, disketda yoki smart-kartada saqlanadi. SHaxsiy kalit eltuvchisi egasidan boshqa odamlarning foydalanishiga qarshi choralar ko'riliishi shart.

Simmetrik shifrlash axborotni "o'zi uchun", masalan, egasi yo'qligida undan ruxsatsiz foydalanishni oldini olish maqsadida, shifrlashda juda qulay xisoblanadi. Bu tanlangan fayllarni arxivli shifrlash va butun bir mantiqiy yoki fizik disklarni shaffof(avtomatik) shifrlash bo'lishi mumkin.

Simmetrik shifrlashning noqulayligi - axborot almashinushi boshlanmasdan oldin barcha adresatlar bilan maxfiy kalitlar bilan ayriboshlash zaruriyatidir. Simmetrik kriptotizimda maxfiy kalitni aloqaning umumfoydalanuvchi kanallari orqali uzatish mumkin emas. Maxfiy kalit jo'natuvchiga va qabul qiluvchiga kalitlar tarqatiluvchi himoyalangan kanallar orqali uzatilishi kerak.

Mavjud barcha kriptografik usullar quyidagi sinflarga ajratiladi:



Mono- va ko'p alifboli o'rniغا qo'yishlar (**podstanovkalar**).

Bir xil alifboden foydalangan holda ochiq matnni boshqa matnga murakkab yoki qiyin qoida bo'yicha almashtirish o'rniغا qo'yish hisoblanadi. Yuqori kriptobardoshlilikni ta'minlash uchun katta kalitlardan foydalanishga to'g'ri keladi.

O'rin almashtirishlar (**perestanovkalar**)

Bu ham uncha murakkab bo'limgan kriptografik akslantirish hisoblanadi, odatda boshqa usullar bilan birgalikda foydalaniladi.

Gamma qo'shish (**Gammalash**)

Bu usulda kalit asosida generatsiya qilinadigan psevdotasodifiy sonlar ketma-ketligi ochiq matn ustiga qo'yiladi.

Blokli shifrlar shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish usullarini (mumkin bo'lgan takrorlashlar va navbatlar bilan) tasvirlaydi. Blokli shifrlar yuqori kriptobardoshlilikka ega ekanligidan amalda u yoki bu sinf akslantirishidan ko'proq uchraydi. Amerika va Rossiyaning shifrlash standartlari aynan shu sinf shifrlariga asoslangan.

Axborotni nosimmetrik algoritmlar asosida kriptografik ximoyalash tamoyillari

Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilishda turli kalitlardan foydalaniladi:

- ochiq kalit K axborotni shifrlashda ishlataladi, maxfiy kalit k dan hisoblab chiqariladi;
- maxfiy kalit k , uning jufti bo'lgan ochiq kalit yordamida shifrlangan axborotni rasshifrovka qilishda ishlataladi.

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



Asimmetrik kriptotizimda shifrlangan axborotni uzatish quyidagicha amalga oshiriladi:

1. Tayyorgarlik bosqichi:

- abonent V juft kalitni generatsiyalaydi: maxfiy kalit k_V va ochiq kalit K_V ;
- ochiq kalit K_V abonent A ga va qolgan abonentlarga jo'natiladi.

2. A va V abonentlar o'rtasida axborot almashish:

- abonent A abonent Vning ochiq kaliti K_V yordamida axborotni shifrlaydi va shifrmatnni abonent Vga jo'natadi;
- abonent V o'zining maxfiy kaliti k_V yordamida axborotni rasshifrovka qiladi. Hech kim (shu jumladan abonent A ham) ushbu axborotni rasshifrovka qilaolmaydi, chunki abonent Vning mahfiy kaliti unda yo'q.

Asimmetrik kriptotizimda axborotni ximoyalash axborot qabul qiluvchi kaliti k_V ning mahfiyligiga asoslangan.

Asimmetrik kriptotizimlarning asosiy hususiyatlari quyidagilar:

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

2. SHifrlash $Y_{E_V} : M \rightarrow C$ va rasshifrovka qilish $D_B : S \rightarrow M$ algoritmlari ochiq.

Shifrlash standartlari. Kriptografik kalitlarni boshqarish. Xeshlash funksiyasi

O'zbekistonning axborotni shifrlash standarti. Ushbu "Ma'lumotlarni shifrlash algoritmi" standarti O'zbekiston aloqa va axborotlashtirish agentligining ilmiy-texnik va marketing tadqiqotlari markazi tomonidan ishlab chiqilgan va unda O'zbekiston Respublikasining "Elektron raqamlı imzo xususida"gi va "Elektron xujjat almashinuv xususida"gi qonunlarining me'yorlari amalga oshirilgan.

Ushbu standart — kriptografik algoritm, elektron ma'lumotlarni himoyalashga mo'ljallangan. Ma'lumotlarni shifrlash algoritmi simmetrik blokli shifr bo'lib, axborotni shifrlash va rasshifrovka qilish uchun ishlataladi. Algoritm 128 yoki 256 bit uzunligidagi ma'lumotlarni shifrlashda va rasshifrovka qilishda 128, 256, 512 bitli kalitlardan foydalanishi mumkin.

Rossiyaning axborotni shifrlash standarti. Rossiya Federatsiyasida hisoblash mashinalari, komplekslari va tarmoqlarida axborotni kriptografik o'zgartirish algoritmlariga davlat standarti (GOST 2814-89) joriy etilgan. Bu algoritmlar maxfiyliy

darjasiga ixtiyoriy bo'lgan axborotni hech qanday cheklovsiz shifrlash imkonini beradi. Algoritmlar apparat va dasturiy usullarida amalga oshirilishi mumkin.

Standartda axborotni kriptografik o'zgartirishning quyidagi algoritmlari mavjud:

- oddiy almashtirish;
- gammalash;
- teskari bog'lanishli gammalash;
- imitovstavka.

AQSHning axborotni shifrlash standarti. AQSHda davlat standarti sifatida DES(Data Encryption Standart) standarti ishlataligan. Bu standart asosini tashkil etuvchi shifrlash algoritmi IBM firmasi tomonidan ishlab chiqilgan bo'lib, AQSH Milliy Xavfsizlik Agentligining mutaxasislari tomonidan tekshirilgandan so'ng davlat standarti maqomini olgan. DES standartidan nafaqat federal departamentlar, balki nodavlat tashkilotlar, nafaqat AQSHda, balki butun dunyoda foydalanib kelingan.

Kriptografik kalitlarni boshqarish

Har qanday kriptografik tizim kriptografik kalitlardan foydalanishga asoslangan. Kalit axboroti deganda axborot tarmoqlari va tizimlarida ishlataluvchi barcha kalitlar majmui tushuniladi. Agar kalit axborotlarining yetarlicha ishonchli boshqarilishi ta'minlanmasa, niyati buzuq odam unga ega bo'lib olib tarmoq va tizimdagi barcha axborotdan hohlaganicha foydalanishi mumkin. Kalitlarni boshqarish kalitlarni generatsiyalash, saqlash va taqsimlash kabi vazifalarni bajaradi. Kalitlarni taqsimlash kalitlarni boshqarish jarayonidagi eng ma'suliyatlari jarayon hisoblanadi.

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

Asimmetrik kriptotizimda ikkita kalit-ochiq va yopiq (maxfiy) kalit ishlataladi. Ochiq kalitni oshkor etish mumkin, yopiq kalitni yashi-rish lozim. Xabar almashinuvida faqat ochiq kalitni uning haqiqiyligini ta'milagan holda jo'natish lozim.

Kalitlarni taqsimlashga quyidagi talablar qo'yiladi:

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

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

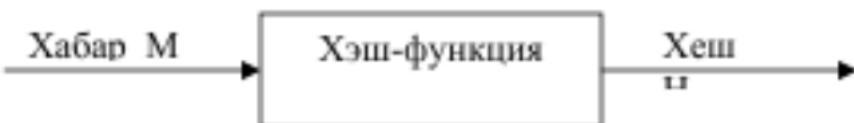
1. Kalitlarni taqsimlovchi bitta yoki bir nechta markazlardan foydalanish.

2. Tarmoq foydalanuvchilari o'rtasida kalitlarni to'g'ridan-to'g'ri almashish.

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

Xeshlash funktsiyasi

Xeshlash funktsiyasi (xesh-funktsiyasi) shunday o'zgartirishki, kirish yo'liga uzunligi o'zgaruvchan xabar M berilganida chişish yo'lida belgilangan uzunlikdagi şator $h(M)$ kósil bo'ladi. Boshşacha aytganda, xesh-funktsiya $h(\cdot)$ argument sifatida uzunligi ixtiyoriy xabar (xujjat) M ni šabul šiladi va belgilangan uzunlikdagi xesh-şiyamat (xesh) $H=h(M)$ ni şaytaradi.



Xeshlash funktsiyasi šuyidagi xususiyatlarga ega bo'lishi lozim:

1. Xesh-funktsiya ixtiyoriy o'lchamli argumentga šo'llanishi mumkin.
2. Xesh-funktsiya chişish yo'lining şiymati belgilangan o'lchamga ega.
3. Xesh-funktsiya $h(x)$ ni ixtiyoriy "x" uchun yetarlicha oson kisoblanadi. Xesh-funktsiyani kisoblash tezligi shunday bo'lishi kerakki, xesh-funktsiya ishlatilganida elektron rašamli imzoni tuzish va tekshirish tezligi xabarning o'zidan foydalanilganiga şaraganda anchagina katta bo'lsin.
4. Xesh-funktsiya matn M dagi orasiga šo'yishlar (vstavki), chişarib tashlashlar (vlybrosy), joyini o'zgartirishlar va kabi o'zgarishlarga sezgir bo'lishi lozim.
5. Xesh-funktsiya şaytarilmaslik xususiyatiga ega bo'lishi lozim.
6. Ikkita turli xujjatlar (ularning uzunligiga bojhliš bo'lмаган кolda) xesh-funktsiyalari şiymatlarining mos kelishi ektimolligi juda kichkina bo'lishi shart, ya'ni kisoblash nuştai nazaridan $h(x')=h(x)$ bo'ladigan $x' \neq x$ ni topish mumkin emas.

Elektron raqamli imzo va uning zamonaviy turlari

Elektron xujjatlarni tarmoq orqali almashishda ularni ishslash va saqlash xarajatlari kamayadi, qidirish tezlashadi. Ammo, elektron xujjat muallifini va xujjatning o'zini autentifikatsiyalash, ya'ni muallifning xaqiqiyligini va olingan elektron xujjatda o'zgarishlarning yo'qligini aniqlash muammosi paydo bo'ladi.

Elektron xujjatlarni autentifikatsiyalashdan maqsad ularni mumkin bo'lgan jinoyatkorona xarakatlardan himoyalashdir. Bunday xarakatlarga quyidagilar kiradi:

- faol ushlab qolish - tarmoqqa ulangan buzg'unchi xujjatlarni (fayllarni) ushlab qoladi va o'zgartiradi;
- Maskarad-abonent S xujjatlarni abonent V ga abonent A nomidan yuboradi;
- renegatlik-abonent A abonent V ga xabar yuborgan bo'lsada, yubormaganman deydi;
- almashtirish-abonent V xujjatni o'zgartiradi, yoki yangisini shakillantiradiva uni abonent A dan olganman deydi;

- takrorlash - abonent A abonent V ga yuborgan xujjatni abonent S takrorlaydi. Jinoyatkorona xarakatlarning bu turlari o'z faoliyatida kompyuter axborot texnologiyalaridan foydalanuvchi bank va tijorat tuzilmalariga, davlat korxona va tashkilotlariga xususiy shaxslarga ancha- muncha zarar yetkazishi mumkin.

Elektron raqamli imzo metodologiyasi xabar yaxlitligini va xabar muallifining xaqiqiyligini tekshirish muammosini samarali hal etishga imkon beradi.

Elektron raqamli imzo telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. Raqamli imzo ishlashi bo'yicha oddiy qo'lyozma imzoga o'xshash bo'lib, quyidagi afzalliklarga ega:

- imzo chekilgan matn imzo qo'ygan shaxsga tegishli ekanligini tasdiqlaydi;
- bu shaxsga imzo chekilgan matnga bog'liq majburiyatlaridan tonish imkoniyatini bermaydi;
- imzo chekilgan matn yaxlitligini kafolatlaydi.

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

Elektron raqamli imzo asimmetrik shifrlarning qaytaruvchanligiga hamda xabar tarkibi, imzoning o'zi va kalitlar juftining o'zaro bog'liqligiga asoslanadi. Bu elementlarning xatto birining o'zgarishi raqamli imzoning haqiqiyligini tasdiqlashga imkon bermaydi. Elektron raqamli imzo shifrlashning asimmetrik algoritmlari va xesh-funksiyalari yordamida amalga oshiriladi.

Elektron raqamli imzo tizimining qo'llanishida bir- biriga imzo chekilgan elektron xujjatlarni jo'natuvchi abonent tarmog'ining mavjudligi faraz qilinadi. Har bir abonent uchun juft - mahfiy va ochiq kalit generatsiyalarini. Mahfiy kalit abonentda sir saqlanadi va undan abonent elektron raqamli imzoni shakllantirishda foydalanadi.

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

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

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

Imzoni shakllantirish muolajasida xabar jo'natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo'natuvchining ochiq kalitidan foydalaniladi.



Elektron raqamli imzo tizimining printsipial jihat— foydalanuvchining elektron raqamli imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirishning mumkin emasligidir. SHuning uchun imzo chekishdagi maxfiy kalitni ruxsatsiz foydalanishdan ximoyalash zarur. Elektron raqamli imzoning maxfiy kalitini, simmetrik shifrlash kalitiga o'xshab, shaxsiy kalit elituvchisida, himoyalangan holda saqlash tavfsiya etiladi.

Imzo chekiluvchi faylga joylashtiriluvchi elektron raqamli imzo imzo chekilgan xujjat muallifini identifikatsiyalovchi qo'shimcha axborot-ga ega. Bu axborot xujjatga elektron raqamli imzo hisoblanmasidan oldin qo'shiladi. Har bir imzo quyidagi axborotni o'z ichiga oladi:

- imzo chekilgan sana;
- ushbu imzo kaliti ta'sirining tugashi muddati;
- faylga imzo chekuvchi shaxs xususidagi axborot (F.I.SH., mansabi, ish joyi);
- imzo chekuvchining indentifikatori (ochiq kalit nomi);
- raqamli imzoning o'zi.

Elektron raqamli imzoning qator algoritmlari ishlab chiqilgan. 1977 yilda AQSH da yaratilgan RSA tizimi birinchi va dunyoda mashhur elektron raqamli imzo tizimi hisoblanadi va yuqorida keltirilgan printsiplarni amalga oshiradi. Ammo raqamli imzo algoritmi RSA jiddiy kamchilikka ega. U niyati buzuq odamga maxfiy kalitni bilmasdan, xesh-lash natijasini imzo chekib bo'lingan xujjatlarning xeshlash natijalarini ko'paytirish orkali hisoblash mumkin bo'lgan xujjatlar imzosini shakllantirishga imkon beradi.

Ishonchliligining yuqoriligi va shaxsiy kompyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmlri 1984 yilda El Gamal tomonidan ishlab chiqildi. El Gamalning raqamli imzo algoritmi (EGSA) RSA raqamli imzo algoritmidagi kamchiliklardan holi bo'lib, AQSH ning standartlar va texnologiyalarning Milliy universiteti tomonidan raqamli imzoning milliy standartiga asos kabi qabul qilindi.

5. Ma’ruza. Axborot xavfsizligida identifikatsiya va autentifikatsiya. Tarmoqlararo ekran texnologiyasi.

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

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

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

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

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

Avtorizatsiya (Authorization) — subektga tizimda ma'lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya sub’ekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli ajrata olmasa bu tizimda axborotning konfidentsialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma'murlash muolajasi uzviy bog'langan.

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

Ma'lumotlarni uzatish kanallarini himoyalashda sub’ektlarning o'zaro autentifikatsiyasi, ya’ni aloqa kanallari orqali bog’lanadigan sub’ektlar xaqiqiyligining o'zaro tasdig’i bajarilishi shart. Xaqiqiylikning tasdig’i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. “Ulash” atamasi orqali

tarmoqning ikkita sub'ekti o'rtasida mantiqiy bog'lanish tushuniladi. Ushbu muolajaning maqsadi — ulash qonuniy sub'ekt bilan amalga oshirilganligiga va barcha axborot mo'ljallangan manzilga borishligiga ishonchni ta'minlashdir.

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

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

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

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

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

6. Kompyuter viruslari va ularga qarshi kurashish mexanizmlari.

Bu nima va unga qarshi qanday kurashish kerak? Bu mavzuga o'nlab kitoblar va yuzlab maqolalar yozilgan. Kompyuter viruslariga qarshi minglab professional mutaxassislar ko'plab kompaniyalarda ish olib borishmoqda. Bu mavzu o'ta qiyin va muhimki ko'p e`tiborni talab qilmoqda. Kompyuter virusi ma'lumotni yo'qotish sabablaridan biri va asosiysi bo'lib qolmoqda. Viruslar ko'plab tashkilot va kompaniyalarni ishlarini buzishga olib kelganligi ma'lum. Shunday ma'lumotlar mavjudki, Niderlandiya gospitallaridan birida bemorga kompyuter qo'ygan tashxis bo'yicha iste'mol qilingan dori oqibatida bemor olamdan o'tgan. Bu kompyuter virusining ishi bo'lgan.

E`tiborsizlik bilan qilingan ishdan kompyuter tezda virus bilan zararlanadi. Inson kasallik virusi bilan zararlansa issiqligi o'zgarishi, vazni o'zgarishi, xolsizlanish va og'riqning paydo bo'lishi ko'zda tutiladi. Kompyuter virusi bilan zararlangan kompyuterlarda quyidagilar kuzatiladi: dasturlarning ishlashining sekinlashishi, fayllarni hajmi o'zgaradi, g'ayritabiyy va ba`zi bir noma'lum xatoliklar, ma'lumotlar va sistema fayllari yo'qotilishi. Ba`zi viruslar zararsiz ko'payadi, lekin qo'rinchli emas. Bu viruslar ekranga xato ma'lumot chiqaradi. Ammo, bir turdag'i viruslar hujum qiluvchi, ya`ni, yomon asoratlar qoldiruvchi hisoblanadi. Masalan, viruslar qattik diskdagi ma'lumotlarni o'chirib tashlaydi.

Virus nima?

Virus(Virus) inglizcha "yuqumli boshlanish", "yomon boshlanish – buzuvchi boshlanish", "yuqumli kasal" degan ma'nolarni anglatadi.

Mashxur «doktor» lardan biri D.N.Lozinskiy virusni kotibaga o'xshatadi. Tartibli kotibani faraz qilsak, u ishga keladi va stolidagi bir kunda qilishi kerak bo'lgan ishlarni - qog'ozlar qatlamini ko'radi. U bir varog'ni ko'paytirib bir nusxasini o'ziga ikkinchisini keyingi qo'shni stolga qo'yadi. Keyingi stoldagi kotiba ham kamida ikki nusxada ko'paytirib, yana bir kotibaga o'tkazadi. Natijada kontoradagi birinchi nusxa bir necha nusxalarga aylanadi. Ba`zi nusxalar yana ko'payib boshqa stollarga ham o'tishi mumkin.

Kompyuter viruslari taxminan shunday ishlaydi, Faqat qog'ozlar o'rnida endi dasturlar, kotiba bu - kompyuter. Birinchi buyruq «ko'chirish-nusxa olish» bo'lsa, kompyuter buni bajaradi va virus boshqa dasturlarga o'tib oladi. Agar kompyuter biror zararlangan dasturni ishga tushirsa virus boshqa dasturlarga tarqalib borib butun kompyuterni egallashi mumkin.

Agar bir dona virusning ko'payishiga 30 sekund vaqt ketsa, bir soatdan keyin bu 1000000000 dan ortib ketishi mumkin. Aniqrog'i kompyuter xotirasidagi bo'sh joylarni band qilishi mumkin.

Xuddi shunday voqeа 1988 yili Amerikada sodir bo'lgan. Global tarmoq orqali uzatilayotgan ma'lumot orqali virus bir kompyuterdan boshqasiga o'tib yurgen. Bu virus Morris virusi deb atalgan.

Ma'lumotlarni virus qanday yo'q qilishi mumkin degan savolga shunday javob berish mumkin:

Virus nusxalari boshqa dasturlarga tez ko'payib o'tib oladi;

Kalendar bo'yicha 13-sana juma kunga to'g'ri kelsa hamma xujjatlarni yo'q qiladi.

Buni hammaga ma'lum «Jerusalem» («Time» virusi ham deb ataladi) virusi juda «yaxshi» amalgalashadi.

Ko'p xollarda bilib bo'lmaydi, virus qayerdan paydo bo'ldi.

Virusni aniqlanishi shundaki, u kompyuter sistemasida joylashib va ko'payib borishiga bog'lik. Misol uchun, nazariy jihatdan operatsion sistemada virus davolab bo'lmaydi. Bajaruvchi kodning sohasini tuzish va o'zgartirish ta'qiqlangan sistema misol bo'lishi mumkin.

Virus hosil bo'lishi uchun bajariluvchi kodlar ketma-ketligi ma'lum bir sharoitda shakllanishi kerak. Kompyuter virusining xossalardan biri o'z nusxalarini kompyuter tarmoqlari orqali bajariluvchi obyektlarga ko'chiradi. Bu nusxalar ham o'z-o'zidan ko'payish imkoniyatiga ega.

Kompyuter viruslari qanday hosil bo'ladi?

Biologik viruslardan farqli o'laroq, kompyuter viruslarini inson tomonidan tuziladi. Viruslar kompyuter foydalanuvchilariga katta zarar yetkazadi. Ular kompyuter ishini to'xtatadi yoki qattiq diskdagi ma'lumotlarni o'chiradi. Virus sistemaga bir necha yo'llar bilan tushishi mumkin: ma'lumot tashuvchi qurilmalar, dasturiy ta'minot yuklangan CD-ROM, tarmoq interfeysi yoki modemli bog'lanish, global Internet; tarmog'idagi elektron pochta.

Ma'lumot tashuvchi qurilma virusdan zararlanishi oson. Zararlangan kompyuterga ma'lumot tashuvchi qurilmani solib o'qitilganda diskning bosh sektoriga virus tushadi. Internet ma'lumotlar almashinishiga katta imkoniyat yaratadi. Lekin, kompyuter viruslari va zararli dasturlar tarqalishi uchun yaxshi muhit yaratadi. Albatta Internetdan olingan barcha ma'lumotlarda virus bor deb bo'lmaydi. Kompyuterda ishlovchi ko'pchilik mutaxassislar va operatorlar qabul qilinadigan ma'lumotlarni viruslardan tekshirishni doimo bajaradi. Internet da ishlayotgan har bir kishi uchun yaxshi antivirus himoya zarur. «Kasperskiy laboratoriysi» texnik ta'minot xizmati statistikasiga ko'ra, viruslardan zararlangan xolatlarning 85% i elektron pochta orqali sodir bo'lgan. 1999 yilga nisbatan xozirgi kunda bu ko'rsatkich 70 % tashkil etadi. «Kasperskiy laboratoriysi» elektron pochtalarga yaxshi antivirus himoyasi kerakligini ta'kidlaydi. Virus tuzuvchilarga elektron pochta juda qulay. Amaliyat shuni ko'rsatadiki, ommabop dasturlar, operatsion sistemalar, ma'lumotlarni uzatish texnologiyalari uchun viruslar ko'plab tuzilmoqda. Xozirda elektron pochta biznes va boshqa sohalarda muloqot uchun asosiy vosita bo'lib qolmoqda. Shuning uchun virus tuzuvchilari elektron pochtaga diqqatini qaratmoqda.

Kompyuter virusining ko'p ta'riflari mavjud. Birinchi ta'rifni 1984 yili Fred Koen bergen: "Kompyuter virusi - boshqa dasturlarni, ularga o'zini yoki o'zgartirilgan nusxasini kiritish orqali, ularni modifikatsiyalash bilan zaharlovchi dastur. Bunda kiritilgan dastur keyingi ko'payish qobiliyatini saqlaydi". Virusning o'z-o'zidan ko'payishi va hisoblash jarayonini modifikatsiyalash qibiliyati bu ta'rifdagi tayanch tushunchalar hisoblanadi. Kompyuter virusining ushbu xususiyatlari tirik tabiat organizmlarida biologik viruslarning parazitlanishiga o'hshash.

Hozirda kompyuter virusi deganda quyidagi xususiyatlarga ega bo'lgan dasturiy kod tushuniladi:

- asliga mos kelishi shart bo'lman, ammo aslining xususiyatlariga (o'z-o'zini tiklash) ega bo'lgan nusxalarni yaratish qibiliyati;
- hisoblash tizimining bajariluvchi ob'ektlariga yaratiluvchi nusxalarning kiritilishini ta'minlovchi mexanizmlarning mavjudligi.

Ta'kidlash lozimki, bu xususiyatlar zaruriy, ammo yetarli emas. Ko'rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta'sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to'ldirish lozim.

Viruslarni quyidagi asosiy alomatlari bo'yicha turkumlash mumkin:

- yashash makoni;
- operatsion tizim;
- ishslash algoritmi xususiyati;
- destruktiv imkoniyatlari.

Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo'yicha turkumlash asosiy va keng tarqalgan turkumlash hisoblanadi.



Yashash makoni bo'yicha kompyuter viruslarining turkumlanishi.

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko'p tarqalgan viruslar xili), yoki fayl-yo'l doshchlarni (kompanon viruslar) yaratadi yoki faylli tizimlarni (link-viruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o'zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (Master Boot Record) bo'lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan MicroSoft Word, MicroSoft Excel va h. kabi ommaviy muharrirlarning fayl-xujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o'zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba'zida tarmoq viruslarini "qurt" xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo'yicha tarqaladi), IRC-qurtlarga (chatlar, Internet Relay Chat) bo'linadi.

Kompyuter viruslarining bajarilish davri, odatda, beshta bosqichni o'z ichiga oladi:

1. Virusni xotiraga yuklash.
2. Qurban ni qidirish.
3. Topilgan qurban ni zaharlash.
4. Destruktiv funksiyalarni bajarish.
5. Boshqarishni virus dastur-eltuvchisiga o'tkazish.

Virusni xotiraga yuklash. Virusni xotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi ob'ekt bilan bir vaqtda amalga oshiriladi.

Qurban ni qidirish. Qurban ni qidirish usuli bo'yicha viruslar ikkita sinfga bo'linadi. Birinchi sinfga operatsion tizim funksiyalaridan foydalanib faol qidirishni amalga oshiruvchi viruslar kiradi. Ikkinci sinfga qidirishning passiv mexanizmlarini amalga oshiruvchi, ya'ni dasturiy fayllarga tuzoq qo'yuvchi viruslar taalluqli.

Topilgan qurban ni zaharlash. Oddiy holda zaharlash deganda qurban sifatida tanlangan ob'ektda virus kodining o'z-o'zini nusxalashi tushuniladi.

Destruktiv funksiyalarni bajarish. Destruktiv imkoniyatlari bo'yicha beziyon, xavfsiz, xavfli va juda xavfli viruslar farqlanadi.

Beziyon viruslar - o'z-o'zidan tarqalish mexanizmi amalga oshiriluvchi viruslar. Ular tizimga zarar keltirmaydi, faqat diskdagini bo'sh xotirani sarflaydi xolos.

Xavfsiz viruslar - tizimda mavjudligi turli taassurot (ovozi, video) bilan bog'liq viruslar, bo'sh xotirani kamaytirsada, dastur va ma'lumotlarga ziyon yetkazmaydi.

Xavfli viruslar - kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar. Natijada dastur va ma'lumotlar buzilishi mumkin.

Juda xavfli viruslar - dastur va ma'lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o'chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar.

Boshqarishni virus dastur — eltuvchisiga o'tkazish. Ta'kidlash lozimki, viruslar buzuvchilar va buzmaydiganlarga bo'linadi. Buzuvchi viruslar dasturlar zaharlanganida ularning ishga layoqatligini saqlash xususida qayg'urmaydilar, shu sababli ularga ushbu bosqichning ma'nosi yo'q.

Buzmaydigan viruslar uchun ushbu bosqich xotirada dasturni korrekt ishlanishi shart bo'lgan ko'rinishda tiklash va boshqarishni virus dastur-eltuvchisiga o'tqazish bilan bog'liq.

Virus paydo bo'lish belgilari.

Zararlangan kompyuterda eng muhimi virusni aniqlash. Buning uchun virusni asosiy belgilarni bilish kerak:

- 1.Funktional dasturlarni ishini to'xtatish yoki noto'g'ri ishlashi;
- 2.Kompyuterni sekin ishlashi;
- 3.OS ni yuklanmasligi;
- 4.Fayl va kataloglarni yo'qolishi yoki ulardagi ma'lumotlarni buzilishi;
- 5.Fayllar modifikatsiyasining sana va vaqtining o'zgarishi;
- 6.Fayl hajmining o'zgarishi;
- 7.Diskdagagi fayllar miqdorining keskin ko'payishi;
- 8.Bo'sh operativ xotira hajmining keskin kamayishi;
- 9.Kutilmagan ma'lumotlar va tasvirlarning ekranga chiqishi;
- 10.Kutilmagan tovushlarning paydo bo'lishi;
- 11.Kompyuterning tez-tez osilib kolishi.

Yuqoridagi belgilarni boshqa sabablarga ko'ra ham bo'lishi mumkinligini eslatib o'tamiz.

Virusga qarshi dasturlar

Kompyuter viruslarini aniqlash va ulardan himoyalanish uchun maxsus dasturlarning bir necha xillari ishlab chiqilgan bo'lib, bu dasturlar kompyuter viruslarini aniqlash va yo'qotishga imkon beradi. Bunday dasturlar virusga qarshi dasturlar deb yuritiladi. Umuman, barcha virusga qarshi dasturlar zaharlangan dasturlarning va yuklama sektorlarning avtomatik tarzda tiklanishini ta'minlaydi.

Viruslarga qarshi dasturlar foydalanadigan viruslarni aniqlashning asosiy usullari quyidagilar:

- etalon bilan taqqoslash usuli;
- evristik taxlil;
- virusga qarshi monitoring;
- o'zgarishlarni aniqlovchi usul;
- kompyuterning kiritish/chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o'rnatish va h.

Etalon bilan taqqoslash usuli eng oddiy usul bo'lib, ma'lum viruslarni qidirishda niqoblardan foydalanadi. Virusning niqobi-mana shu muayyan virusga xos kodning qandaydir o'zgarmas ketma-ketligidir. Virusga qarshi dastur ma'lum virus niqoblarini qidirishda tekshiriluvchi fayllarni ketma-ket ko'rib chiqadi (skannerlaydi).

Evristik tahsil. Kompyuter virusi ko'payishi uchun xotirada nusxalanish, sektorga yozilish kabi qandaydir muayyan xarakatlarni amalga oshirishi lozim.

Virusga qarshi monitoring. Ushbu usulning mohiyati shundan iboratki, kompyuter xotirasida boshqa dasturlar tomonidan bajariluvchi shubhali harakatlarni monitoringlovchi virusga qarshi dastur doimo bo'ladi. Virusga qarshi monitoring barcha ishga tushiriluvchi dasturlarni, yaratiluvchi, ochiluvchi va saqlanuvchi xujjatlarni, Internet orqali olingan yoki disketdan yoki har qanday kompakt-diskdan nushalangan dastur va xujjatlarning fayllarini tekshirishga imkon beradi. Agar qandaydir dastur xavfli harakatni qilishga urinmoqchi bo'lsa, virusga qarshi monitor foydalanuvchiga xabar beradi.

O'zgarishlarni aniqlovchi usul. Diskni taftish qiluvchi deb ataluvchi ushbu usulni amalga oshirishda virusga qarshi dastur diskning xujumga duchor bo'lishi mumkin bo'lgan barcha sohalarini oldindan xotirlaydi, so'ngra ularni vaqtি-vaqtি bilan tekshiradi. Virus kompyuterlarni zaharlaganida qattiq disk tarkibini o'zgartiradi: masalan, dastur yoki xujjat fayliga o'zining kodini qo'shib qo'yadi, Autoexec.bat fayliga dastur-virusni chaqirishni qo'shadi, yuklama sektorni o'zgartiradi, faylyo'ldosh yaratadi. Disk sohalari xarakteristikalarining qiymatlari solishtirilganida virusga qarshi dastur ma'lum va no'malum viruslar tomonidan qilingan o'zgarishlarni aniqlashi mumkin.

Kompyuterlarning kiritish/chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o'rnatish. Kompyuterlarning tizimli platasiga viruslardan himoyalashning oddiy vositalari o'rnatiladi. Bu vositalar qattiq diskarning bosh yuklama yozuviga hamda disklar va disketlarning yuklama sektorlariga barcha murojaatlarni nazoratlashga imkon beradi. Agar qandaydir dastur yuklama sektorlar tarkibini o'zgartirishga urinsa, himoya ishga tushadi va foydalanuvchi ogohlantiriladi. Ammo bu himoya juda ham ishonchli emas.

Virusga qarshi dasturlarning xillari. Virusga qarshi dasturlarning quyidagi xillari farqlanadi:

- dastur-faglar (virusga qarshi skanerlar);
- dastur-taftishchilar (CRC-skanerlar);
- dastur-blokirovka qiluvchilar;
- dastur-immunizatorlar.

Dr.Web — Rossiyaning virusga qarshi ommaviy dasturi, Windows 9x/NT/2000/XP/7/8 uchun mo'ljallangan bo'lib, faylli, yuklama, va fayl-yuklama viruslarni qidiradi va zararsizlantiradi.

AVP (Antivirus Kasperskogo Personal) — Rossiyaning virusga qarshi paketi.

Eset Nod32 Antivirus

Symantec Antivirus — Symantec kompaniyasining korporativ foydalanuvchilarga taklif etgan virusga qarshi mahsuloti to'plami.

7. Ma’ruza. Axborot-kommunikatsion tizimlarda suqilib kirishlarni aniqlash. Mahlumotlarni uzatish tarmog’ida axborotni himoyalash.

Himoyalanishni taxlillash vositalari zaifliklarni topib va o’z vaqtida yo’q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatalishiga bo’ladigan barcha sarf-harajatlar kamayadi.

Himoyalanishni taxlillash vositalari tarmoq sathida, operatsion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko’paytirish, axborot tizimiga “ichkarilab borish” va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin.

Tarmoq protokollari va servislari himoyalanishini tahlillash vositalari. Har qanday tarmoqda abonentlarning o’zaro aloqasi ikkita va undan ko’p uzellar orasida axborot almashinish muolajalarini belgilovchi tarmoq protokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislarini ishlab chiqishda ularga ishlanuvchi axborot xavfsizligini ta’minalash bo’yicha talablar (odatda shubxasiz yetarli bo’lmagan) qo’yilgan. SHu sababli, tarmoq protokollarida aniqlangan zaifliklar xususida axborotlar paydo bo’lmoqda. Natijada, korporativ tarmoqda foydalanadigan barcha protokol va servislarni doimo tekshirish zaruriyati tug’iladi.

Himoyalanishni taxlillash tizimi zaifliklarni aniqlash bo’yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga xujumlarida qo’llaniladiganiga o’xhash.

Zaifliklarni aniqlash maqsadida skanerlash tekshiruvchi tizim xususidagi dastlabki axborotni, xususan, ruxsat etilgan protokollar va ochiq portlar, operatsion tizimnnig ishlataluvchi versiyalari va h. xususidagi axborotni olish bilan boshlanadi. Skanerlash keng tarqagan xujumlar, masalan, to’liq saralash usuli bo’yicha parollarni tanlashdan foydalanib, suqilib kirishni imitatsiyalashga urinish bilan tugaydi.

Himoyalanishni taxlillash vositalari yordamida tarmoq sathida nafaqat Internetning korporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichki tarmog’ida tekshirishni amalga oshirish mumkin. Tarmoq sathida himoyalanishni taxlillash tizimi tashkilot xavfsizlik darajasini baholashga hamda tarmoq dasturiy va apparat ta’minotini sozlash samaradorligini nazoratlashga xizmat qiladi.

Xujumlarni aniqlash

Tarmoq axborotini taxlillash usullari. Mohiyati bo’yicha, xujumlarni aniqlash jarayoni korporativ tarmoqda bo’layotgan shubhali harakatlarni baholash jarayonidir. Boshqacha aytganda xujumlarni aniqlash- hisoblash yoki tarmoq resurslariga yo’naltirilgan shubhali harakatlarni identifikasiyalash va ularga reaktsiya ko’rsatish jarayoni. Hozirda xujumlarni aniqlash tizimida quyidagi usullar ishlataladi:

- statistik usul;
- ekspert tizimlari;

- neyron tarmoqlari.

Statistik usul. Statistik yondashishning asosiy afzalligi allaqachon ishlab chiqilgan va o'zini tanitgan matematik statistika apparatini ishlatish va sub'ekt xarakteriga moslash.

Avval tahlillanuvchi tizimning barcha sub'ektlari uchun profillar aniqlanadi. Ishlatiladigan profillarning etalondan har qanday chetlanishi ruxsat etilmagan foydalanish hisoblanadi. Statistik usullar universal hisoblanadi, chunki mumkin bo'lgan xujumlarni va ular foydalanadigan zaifliklarni bilish talab etilmaydi. Ammo bu usullardan foydalanishda bir qancha muammolar paydo bo'ladi:

1. Statistik tizimlar xodisalar kelishi tartibiga sezuvchanmaslar; ba'zi xollarda bir xodisaning o'zi, kelishi tartibiga ko'ra anomal yoki normal faoliyatni xarakterlashi mumkin.
2. Anomal faoliyatni adekvat identifikatsiyalash maqsadida xujumlarni aniqlash tizimi tomonidan kuzatiluvchi xarakteristikalar uchun chegaraviy (bo'sag'aviy) qiymatlarni berish juda qiyin.
3. Statistik usullar vaqt o'tishi bilan buzg'unchilar tomonidan shunday "o'rnatilishi" mumkinki, xujum harakatlari normal kabi qabul qilinadi.

Ekspert tizimlari. Ekspert tizimi odam-ekspert bilimlarini qamrab oluvchi qoidalar to'plamidan tashkil topgan. Ekspert tizimidan foydalanish xujumlarni aniqlashning keng tarqalgan usuli bo'lib, xujumlar xususidagi axborot qoidalar ko'rinishida ifodalanadi. Bu qoidalar harakatlar ketma-ketligi yoki signaturalar ko'rinishida yozilishi mumkin. Bu qoidalarning har birining bajarilishida ruxsatsiz faoliyat mavjudligi xususida qaror qabul qilinadi. Bunday yondashishning muhim afzalligi - yolg'on trevoganing umuman bo'lmasligi.

Ekspert tizimining ma'lumotlari bazasida hozirda ma'lum bo'lgan aksariyat xujumlar stsenariyasi bo'lishi lozim. Ekspert tizimlari, dol-zarblikni saqlash maqsadida, ma'lumotlar bazasini muttasil yangilashni talab etadi. Garchi ekspert tizimlari qaydash jurnallaridagi ma'lumotlarni ko'zdan kechirishga yaxshi imkoniyatni tavsiya qilsada, so'ralgan yangilanish e'tiborsiz qoldirilishi yoki ma'mur tomonidan qo'lda amalga oshirilishi mumkin. Bu eng kamida, ekspert tizimi imkoniyatlarining bo'shashiga olib keladi.

Ekspert tizimlarining kamchiliklari ichida eng asosiysi - noma'lum xujumlarni akslantira olmasligi. Bunda oldindan ma'lum xujumning xatto ozgina o'zgarishi xujumlarni aniqlash tizimining ishlashiga jiddiy to'siq bo'lishi mumkin.

Neyron tarmoqlari. Xujumlarni aniqlash usullarining aksariyati qoidalar yoki statistik yondashish asosida nazoratlanuvchi muhitni tahlillash shakllaridan foydalanadi. Nazoratlanuvchi muhit sifatida qaydash jurnallari yoki tarmoq trafigi ko'riliishi mumkin. Bunday taxlillash ma'mur yoki xujumlarni yaniqlash tizimi tomonidan yaratilgan, oldindan aniqlangan qoidalar to'plamiga tayanadi.

Xujumni vaqt bo'yicha yoki bir necha niyati buzuq odamlar o'rtasida har qanday bo'linishi ekspert tizimlar yordamida aniqlashga qiyinchilik tug'diradi. Xujumlar va ular usullarining turli-tumanligi tufayli, ekspert tizimlari qoidalarining ma'lumotlar bazasining hatto doimiy yangilanishi ham xujumlar diapazonini aniq identifikatsiyalashni kafolatlamaydi.

8. Ma’ruza. Virtual himoyalangan tarmoqlar. Simsiz aloqa tizimlarida axborot himoyasi.

Internet ning gurillab rivojlanishi natijasida dunyoda axborotni tarqatish va foydalanishda sifatiy o’zgarish sodir bo’ldi. Internet foydalanuvchilari arzon va qulay kommunikatsiyaga ega bo’ldilar. Korxonalar Internet kanallaridan jiddiy tijorat va boshqaruv axborotlarini uzatish imkoniyatlariga qiziqib qoldilar. Ammo Internetning qurilishi printsipi niyati buzuq odamlarga axborotni o’g’irlash yoki atayin buzish imkoniyatini yaratdi. Odatda TCP/IP protokollar va standart Internet-ilovalar (e-mail, Web, FTP) asosida qurilgan korporativ va idora tarmoqlari suqilib kirishdan kafolatlanmaganlar.

Internetning hamma yerda tarqalishidan manfaat ko’rish maqsadida tarmoq xujumlariga samarali qarshilik ko’rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq VPN yaratish ustida ishlar olib borildi. Natijada 1990 yilning boshida virtual xususiy tarmoq VPN kontseptsiyasi yaratildi. "Virtual" iborasi VPN atamasiga ikkita uzel o’rtasidagi ularishni vaqtincha deb ko’rlishini ta’kidlash maqsadida kiritilgan. Haqiqatan, bu ularish doimiy, qat’iy bo’lmay, faqat ochiq tarmoq bo’yicha trafik o’tganida mavjud bo’ladi.

Virtual tarmoq VPNlarni qurish kontseptsiyasi asosida yetarlicha oddiy g’oya yotadi: agal global tarmoqda axborot almashinuvchi ikkita uzel bo’lsa, bu uzellar orasida ochiq tarmoq orqali uzatilayotgan axborotning konfidentsialligini va yaxlitligini ta’minlovchi virtual himoyalangan tunnel qurish zarur va bu virtual tunneldan barcha mumkin bo’lgan tashqi faol va passiv kuzatuvchilarning foydalanishi xaddan tashqari qiyin bo’lishi lozim.

SHunday qilib, VPN tunneli ochiq tarmoq orqali o’tkazilgan ularish bo’lib, u orqali virtual tarmoqning kriptografik himoyalangan axborot paketlari uzatiladi. Axborotni VPN tunneli bo’yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

- o’zaro aloqadagi taraflarni autentifikatsiyalash;
- uzatiluvchi ma’lumotlarni kriptografik berkitish (shifrlash);
- etkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish.

Bu vazifalar bir biriga bog’liq bo’lib, ularni amalga oshirishda axborotni kriptografik himoyalash usullaridan foydalaniladi. Bunday himoyalashning samaradorligi simmetrik va asimmetrik kriptografik tizimlarning birgalikda ishlatalishi evaziga ta’milanadi. VPN qurilmalari tomonidan shakllantiriluvchi VPN tunneli himoyalangan ajratilgan liniya xususiyatlariga ega bo’lib, bu himoyalangan ajratilgan liniyalar umumfoydalanuvchi tarmoq, masalan Internet doirasida, saflanadi. VPN qurilmalari virtual xususiy tarmoqlarda VPN-mijoz, VPN-server yoki VPN xavfsizligi shlyuzi vazifasini o’tashi mumkin.

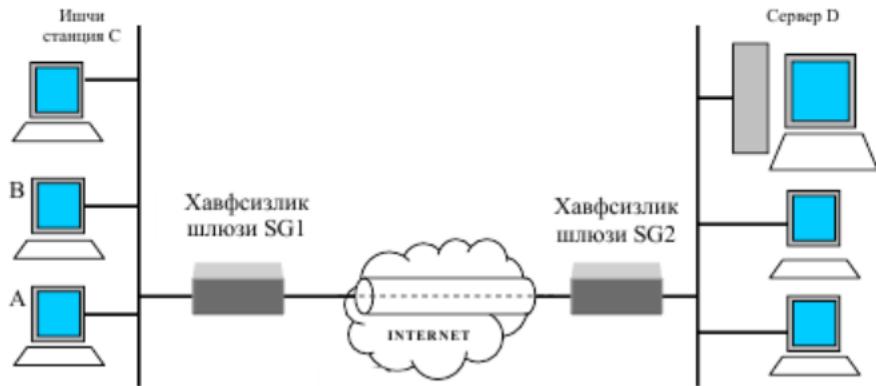
VPN-mijoz odatda shaxsiy kompyuter asosidagi dasturiy yoki dasturiy-apparat kompleksi bo’lib, uning tarmoq dasturiy ta’mnoti u boshqa VPN-mijoz, VPN-server yoki VPN xavfsizligi shlyuzlari bilan almashinadigan trafikni shifrlash va autentifikatsiyalash uchun modifikatsiyalanadi.

VPN-server server vazifasini o'tovchi, kompyuterga o'rnatiluvchi dasturiy yoki dasturiy-apparat kompleksidan iborat. VPN-server tashqi tarmoqlarning ruxsatsiz foydalanishidan serverlarni himoyalashni hamda alohida kompyuterlar va mos VPN-mahsulotlari orqali himoyalangan lokal tarmoq segmentlaridagi kompyuterlar bilan himoyalangan ulanishlarni tashkil etishni ta'minlaydi. VPN-server VPN-mijozning server platformalari uchun funktsional analog hisoblanadi. U avvalo VPN-mijozlar bilan ko'pgina ulanishlarni madadlovchi kengaytirilgan resurslari bilan ajralib turadi. VPN-server mobil foydalanuvchilar bilan ulanishlarni ham madadlashi mumkin.

VPN xavfsizlik shlyuzi. (Security gateway) ikkita tarmoqqa ulanuvchi tarmoq qurilmasi bo'lib, o'zidan keyin joylashgan ko'p sonli xostlar uchun shifrlash va autentifikatsiyalash vazifalarini bajaradi. VPN xavfsizligi shlyuzi shunday joylashtiriladiki, ichki korporativ tarmoqqa atalgan barcha trafik u orqali o'tadi. VPN xavfsizligi shlyuzining adresi kiruvchi tunnellanuvchi paketning tashqi adresi sifatida ko'rsatiladi, paketning ichki adresi esa shlyuz orqasidagi muayyan xost adresi hisoblanadi. VPN xavfsizligi shlyuzi alohida dasturiy yechim, alohida apparat qurilmasi, hamda VPN vazifalari bilan to'ldirilgan marshrutizatorlar yoki tarmoqlararo ekran ko'rinishida amalga oshirilishi mumkin.

Axborot uzatishning ochiq tashqi muhiti ma'lumot uzatishning tezkor kanallarini (Internet muhiti) va aloqaning sekin ishlaydigan umumfoydalanuvchi kanallarini (masalan, telefon tarmog'i kanallarini) o'z ichiga oladi. Virtual xususiy tarmoq VPNning samaradorligi aloqaning ochiq kanallari bo'yicha aylanuvchi axborotning himoyalanish darajasiga bog'liq. Ochiq tarmoq orqali ma'lumotlarni xavfsiz uzatish uchun inkapsulyatsiyalash va tunnellash keng ishlatiladi. Tunnellash usuli bo'yicha ma'lumotlar paketi umumfoydalanuvchi tarmoq orqali xuddi oddiy ikki nuqtali ulanish bo'yicha uzatilganidek uzatiladi. Har bir "jo'natuvchi-qabul qiluvchi" juftligi orasiga bir protokol ma'lumotlarini boshqasining paketiga inkapsulyatsiyalashga imkon beruvchi o'ziga xos tunnel-mantiqiy ulanish o'rnatiladi.

Tunnellashga binoan, uzatiluvchi ma'lumotlar portsiyasi xizmatchi hoshiyalar bilan birga yangi "konvert"ga "joylash" amalga oshiriladi. Bunda pastroq sath protokoli paketi yuqoriqoq yoki xudi shunday sath protokoli paketi ma'lumotlari maydoniga joylashtiriladi. Ta'kidlash lozimki, tunnelashning o'zi ma'lumotlarni ruxsatsiz foydalanishdan yoki buzishdan himoyalamaydi, ammo tunnellash tufayli inkapsulyatsiyalananuvchi dastlabki paketlarni to'la kriptografik himoyalash imkoniyati paydo bo'ladi. Uzatiluvchi ma'lumotlar konfidentsialligini ta'minlash maqsadida jo'natuvchi dastlabki paketlarni shifrlaydi, ularni, yangi IP-sarlavha bilan tashqi paketga joylaydi va tranzit tarmoq bo'yicha jo'natadi



Simsiz aloqa tizimlarida axborot himoyasi. Simsiz qurilmalar xavfsizligi muammolari

Simsiz tarmoqlar odamlarga simli ulanishsiz o'zaro bog'lanishlariga imkon beradi. Bu siljish erkinligini va uy, shahar qismlaridagi yoki dunyoning olis burchaklaridagi ilovalardan foydalanish imkonini ta'minlaydi. Simsiz tarmoqlar odamlarga o'zlariga qulay va xoxlagan joylarida elektron pochtani olishlariga yoki Web-sahifalarni ko'zdan kechirishlariga imkon beradi.

Simsiz tarmoqlarning turli xillari mavjud, ammo ularning eng muhim xususiyati bog'lanishning kompyuter qurilmalari orasida amalga oshirilishidir. Kompyuter qurilmalariga shaxsiy raqamli yordamchilar (Personal digital assistance, PDA), noutbuklar, shaxsiy kompyuterlar, serverlar va printerlar taalluqli. Odatda uyali telefonlarni kompyuter qurilmalari qatoriga kiritishmaydi, ammo eng yangi telefonlar va hatto naushniklar ma'lum hisoblash imkoniyatlariga va tarmoq adapterlariga ega. Yaqin orada elektron qurilmalarning aksariyati simsiz tarmoqlarga ulanish imkoniyatini ta'minlaydi.

Bog'lanish ta'minlanadigan fizik xudud o'lchamlariga bog'liq holda simsiz tarmoqlarning quyidagi kategoriyalari farqlanadi:

- simsiz shaxsiy tarmoq (Wireless personal-area network, PAN);
- simsiz lokal tarmoq (Wireless local-area network, LAN);
- simsiz regional tarmoq (Wireless metropolitan-area network, MAN);
- simsiz global tarmoq (Wireless Wide-area network, WAN).

Simsiz shaxsiy tarmoqlari uzatishning katta bo'lмаган masofasi bilan (17 metrgacha) ajralib turadi va katta bo'lмаган binoda ishlatalidi. Bunday tarmoqlarning xarakteristikalari о'rtacha bo'lib, uzatish tezligi odatda 2Mb/s dan oshmaydi.

Bunday tarmoq, masalan, foydalanuvchi PDA sida va uning shaxsiy kompyuterida yoki noutbukida ma'lumotlarni simsiz sinxronlashni ta'minlashi mumkin. Xuddi shu tariqa printer bilan simsiz ulanish ta'minlanadi. Kompyuterni tashqi qurilmalar bilan ulovchi simlar chigalliklarining yo'qolishi yetarlicha jiddiy afzallik bo'lib, buning evaziga tashqi qurilmalarning boshlang'ich o'rnatilishi va keyingi, zaruriyat tug'ilganda, joyining o'zgartirilishi anchagina osonlashadi.

Simsiz lokal tarmoqlar ofislarning ichida va tashqarisida, ishlab chiqarish binolarida uzatishlarning yuqori xarakteristikalarini ta'minlaydi. Bunday tarmoqlardan foydalanuvchilar odatda noutbuklarni, shaxsiy kompyuterlarni va katta resurslarni talab etuvchi ilovalarni bajarishga qodir protsessorli va katta ekranli PDA larni ishlatalishadi. Xizmatchi tarmoq xizmatlaridan majlislar zalida yoki binoning boshqa xonalarida bo'la turib foydalanishi mumkin. Bu xizmatchiga o'z vazifalarini samarali bajarishga imkon beradi. Simsiz lokal tarmoqlar uzatishning 54Mbit/sgacha tezligida barcha ofis yoki maishiy ilovalar talablarini qondirish imkoniga ega. Xarakteristikalari, komponentlari, narxi va bajaradigan amallari bo'yicha bunday tarmoqlar Ethernet xilidagi an'anaviy simli lokal tarmoqlariga o'xshash.

Simsiz regional tarmoqlar yuzasi bo'yicha shaxarga teng bo'lган xududga xizmat qiladi. Aksariyat xollarda ilovalarni bajarishda belgilangan ulanish talab etiladi, ba'zida esa mobillik zarur bo'ladi. Masalan, kasalxonada bunday tarmoq asosiy bino va masofadagi klinikalar orasida ma'lumotlarni uzatishni ta'minlaydi. Yoki energetik kompaniya bunday tarmoqdan shaxar masshtabida foydalanib, turli tumanlardan beriladigan ish naryadlaridan foydalanishini ta'minlaydi. Natijada, simsiz regional tarmoqlar mavjud tarmoq infratuzilmalarini bir yerga to'playdi yoki mobil foydalanuvchilarga mavjud tarmoq infratuzilmalari bilan ulanishni o'rnatishga imkon beradi.

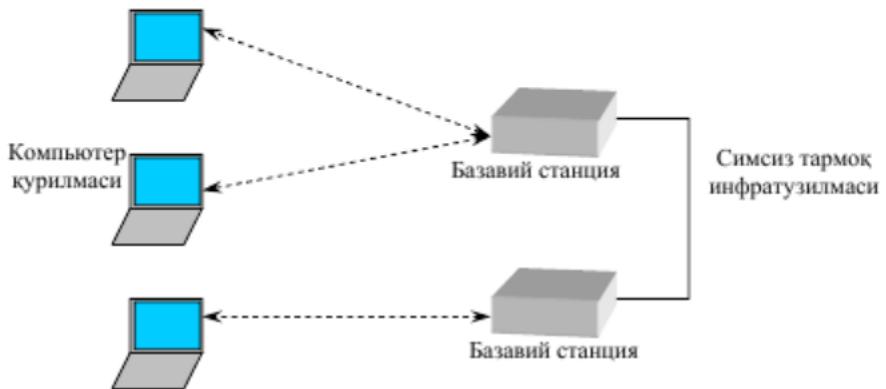
Simsiz regional tarmoqlarning xarakteristikalari turlicha. Ulanishlarda infraqizil texnologiyaning ishlatilishi ma'lumotlarni uzatish tezligining 100 Gbit/s va undan katta bo'lishini ta'minlaydi.

Simsiz global tarmoqlar mobil ilovalarning, ulardan mamlakat yoki xatto kontinent masshtabida foydalanishni ta'minlash bilan ishlanishini ta'minlaydi. Iqtisodiy mulohazalarga tayangan holda, telekommunikatsiya kompaniyalari ko'pgina foydalanuvchilar uchun uzoq masofadan ulanishni ta'minlovchi simsiz global tarmoqning nisbatan qimmat infratuzilmasini yaratadilar. Bunday yechimning xarajati barcha foydalanuvchilar o'rtasida taqsimlanadi, natijada abonent to'lovi unchalik yuqori bo'lmaydi.

Simsiz global tarmoq xarakteristikalari nisbatan yuqori emas, ma'lumotlarni uzatishning tezligi 56 Kbit/s ni, ba'zida 170 Kbit/s ni tashkil etadi.

Simsiz global tarmoqlarga xos ilovalar Internetdan foydalanishni, elektron pochta xabarlarini uzatish va qabul qilishni, foydalanuvchi uydan yoki ofisdan tashqarida bo'lganida korporativ ilovalardan foydalanishni ta'minlovchi ilovalardir. Abonentlar, masalan, taksida ketayotganlarida yoki shahar bo'yicha sayr qilinayotganlarida ulanishni o'rnatishlari mumkin. Umuman, simsiz global tarmoqdan foydalanuvchilar xududiy chegaralanmaganlar.

Simsiz tarmoq tuzilmasi. Simsiz tarmoqlarda simli tarmoqda ishlatiladigan komponentlar ishlatiladi. Ammo, simsiz tarmoqlarda axborot xavo muhiti (medium) orqali uzatishga yaroqli ko'rinishga o'zgartirilishi lozim.



Foydalanuvchilar. Simsiz tarmoq foydalanuvchiga xizmat qilishligi sababali, foydalanuvchiga simsiz tarmoqning muhim qismi sifatida qarash mumkin. Foydalanuvchi simsiz tarmoqdan foydalanish jarayonini boshlaydi va uning o'zi tugallaydi. SHu sababli unga "oxirgi foydalanuvchi" atamasi joiz hisoblanadi. Odatda, foydalanuvchi simsiz tarmoq bilan o'zaro aloqani ta'minlash bilan bir qatorda, muayyan ilovalar bilan bog'liq boshqa vazifalarni bajaruvchi kompyuter qurilmalari (computer device) bilan ish ko'radi.

Mobililik - simsiz tarmoqning eng sezilarli afzalliklaridan biridir. Masalan, mobillik xususiyatidan qandaydir bino bo'yicha xarakatlanuvchi va o'zining PDAsi yordamida elektron pochtani oluvchi yoki jo'natuvchi odam foydalanadi. Bu holda PDA simsiz tarmoq infratuzilmasiga uzlucksiz yoki tez-tez tiklanuvchi ulanishni ta'minlashi lozim.

Kompyuter qurilmalari. Kompyuter qurilmalarining (ba'zida ularni mijozlar deb atashadi) ko'pgina xillari simsiz tarmoq bilan ishlayoladi. Ba'zi kompyuter qurilmalari foydalanuvchilar uchun atayin qurilgan bo'lsa, boshqalari oxirgi tizim hisoblanadi.



Simsiz qurilmalar xavfsizligi muammolari

Simsiz qurilmalarni to'rtta kategoriya ajratish mumkin: noutbuklar, cho'ntak kompyuterlari (PDA), simsiz infratuzilma (ko'priklar, foydalanish nuqtalari va h.) va uyali telefonlar.

Noutbuklar — korporativ simsiz tarmoqlarda va SOHO (Small Office Home Office - kichik va uy ofislari) tarmoqlarida keng tarqalgan qurilma.

Fizik xavfsizlik noutbuklar uchun jiddiy muammo hisoblanadi. Bunday kompyuterlarni xarid qilishdagi parametrlardan biri-uning o'lchami. Noutbuk qanchalik kichkina bo'lsa, u shunchalik qimmat turadi. Boshqa tarafdan, noutbuk qanchalik kichkina bo'lsa, uni o'g'irlash shunchalik osonlashadi. SHifrlash kalitlarining, masalan, WEP-kalitlar (Wired Equivalent Privacy), dasturiy kalitlar, parollar yoki shaxsiy kalitlarning (PGP, Pretty Good Privacy kabilar) yo'qotilishi katta muammo hisoblanadi va uni ilovalar yaratilishi bosqichidayoq hisobga olish zarur. Niyati buzuq odam noutbukni o'z ixtiyoriga olganidan so'ng aksariyat xavfsizlik mexanizmlari buzilishi mumkin.

Noutbuklarning mobilligi ularning korporativ tarmoqlararo ekranlar (brandmauerlar) bilan himoyalanmagan boshqa tarmoqlar bilan ulanish ehtimolligini oshiradi. Bu Internet-ulanihlar, foydalanuvchi tarmoqlar, asbob-uskuna ishlab chiqaruvchilarining tarmog'i yoki raqiblar ham joylanuvchi mehmonxona yoki ko'rgazmalardagi umumfoydalanuvchi tarmoqlar bo'lishi mumkin. Bunday hollarda mobil kompyuterlarning axborot xavfsizligi xususida jiddiy o'ylanish lozim.

Noutbuklarning fizik saqlanishlarini ta'minlash usullaridan biri-xavfsizlik kabelidan foydalanish. Ushbu kabel noutbukni stolga yoki boshqa yirik predmetga "boylab" qo'yishga mo'ljallangan. Albatta, bu yuz foizlik kafolatni bermaydi, ammo har xolda o'g'rining anchagina kuch sarf qilishiga to'g'ri keladi.

Noutbuklarning tez-tez o'g'irlanishi sababli, axborotni arxivlashning xavfsizlikni ta'minlashga nisbatan muhimligi kam emas. SHifrlash dasturlari fayllar xavfsizligini ta'minlashda yoki qattiq disklarda shifrlangan ma'lumotlar xajmini yaratishda ishlatiladi. Bu ma'lumotlarni rasshifrovka qilish uchun, odatda, parolni kiritish yoki shaxsiy kalitlarni ishlatish talab etiladi. Barcha axborotlarni shifrlangan fayllarda yoki arxivlarda saqlanishi kerakli fayllar to'plamini arxiv uchun nusxalashni yengillashtiradi, chunki ular endi ma'lum joyda joylashgan bo'ladi.

O'g'rilar uchun noutbuklar "birinchi nomerli nishon" ekanligini foydalanuvchilar tushunib yetishlari va ularni qarovsiz qoldirmasliklari zarur. Hatto ofislarda noutbukni kechaga qoldirish mumkin emas, chunki ofisga ko'p kishilar (kompaniya xodimlari, farroshlar, mijozlar) tashrif buyuradilar.

Axborotning chiqib ketishi noutbuk egasining ko'p odamlar to'plangan joylarda ham sodir bo'lishi mumkin. Samolet - kompaniya menedjerlari foydalanadigan odatdag'i transport vositasidir. Samoletda qo'shni kreslodagi yo'lovchi noutbuk egasining yelkasi ustidan muhim axborotni o'qib olishi mumkin. Hatto "uy sharoitidagi" noutbuklar ham himoyalanishi zarur. Bu holda kompyuterning himoyasi server himoyasidan farqlanmaydi. Juda ham zarur bo'limgan servislarning o'chirilishi qurilma ishlashini yaxshilaydi.

O'zining dasturiy ta'minotini noutbukka o'rnatgan niyati buzuq odam xavfsizlikning barcha mexanizmlarini chetlab o'tish imkoniyatiga ega bo'ladi.

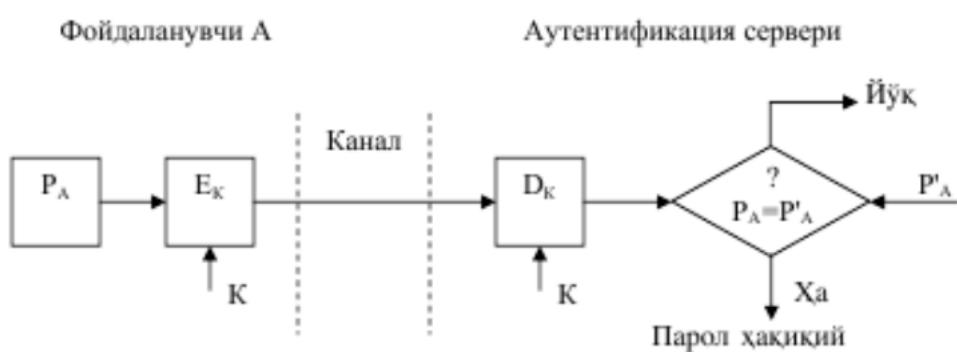
Kompyuterni o'z ixtiyoriga olgan o'g'ri unga o'zining dasturini o'rnatganida uni tuxtatib bo'lmaydi. BIOSda (Basic Input/Output System-kiritish/chiqarishning bazaviy tizimi) va qattiq diskda o'rnatilgan parollar o'g'rila noutbukdan foydalanishga to'sqinlik qilishi mumkin. Ushbu barcha vositalar, afsuski, tajribali xaker uchun to'siq bo'laolmaydi.

9. Ma'ruza. Xavfsizlikni boshqarish va himoya tizimini qurish.

Parolli himoya va ularning zamonaviy turlari. Parollar asosida autentifikatsiyalash

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

Eng keng tarqalgan usul — foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o'qish va yozishdan himoyalash atributlari o'rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ruyxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funktsiyalar kabi kriptografik mehanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma'mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.



Oddiy autentifikatsiyanı tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul — foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o'qish va yozishdan himoyalash atributlari o'rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ruyxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funktsiyalar kabi kriptografik mehanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma'mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funktsiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli uringa uning bir tomonlama funktsiya h(.) dan foydalanib olingen tasvirini yuborishi shart. Bu o'zgartirish g'anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki g'anim yechilmaydigan sonli masalaga duch keladi.

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

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

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

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

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

Birinchi usulni amalga oshirish misoli sifatida SecurID autentifikatsiyalash texnologiyasini ko'rsatish mumkin. Bu texnologiya Security Dynamics kompaniyasi tomonidan ishlab chiqilgan bo'lib, qator kompaniyalarning, xususan Cisco Systems kompaniyasining serverlarida amalga oshirilgan.

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

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

Autentifikatsiyaning bu sxemasi bilan yana bir muammo bog'liq. Apparat kalit generatsiyalagan tasodifiy son katta bo'limgan vaqt oralig'i mobaynida haqiqiy parol hisoblanadi. SHu sababli, umuman, qisqa muddatli vaziyat sodir bo'lishi mumkinki,

xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

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

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli foydalanuvchi va tekshiruvchi uchun umumiyo bo'lgan tasodifiy parollar ruyxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo'linuvchi ro'yxati maxfiy parollar ketma-ketligi yoki to'plami bo'lib, har bir parol faqat bir marta ishlatiladi. Ushbu ro'yxat autentifikatsion almashinuv taraflar o'rtasida oldindan taqsimplanishi shart. Ushbu usulning bir variantiga binoan so'rov-javob jadvali ishlatiladi. Bu jadvalda autentifikatsilash uchun taraflar tomonidan ishlatiluvchi so'rovlar va javoblar mavjud bo'lib, har bir juft faqat bir marta ishlatilishi shart.

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

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

Elektron biznes va uning xavfsizligi muammolari.

Elektron biznes xaridor va sotuvchi orasidagi aloqani tashkil etish, buyurtmani ifodalash, muxokama qilish, o'zgartirish, tovarlarni va xizmatlarni sotish usullarini hamda to'lojni amalga oshirish jarayonlarini o'zgartirish uchun yangi texnologiyalardan foydalanadi. Hozirda elektron tijorat va biznesning aksariyat

muammolari axborot xavfsizligi bilan bog'liq, ya'ni xavfsizlik muammolari elektron tijorat va biznes rivojidagi jiddiy to'siq xisoblanadi.

Har qanday tijorat kompaniyasining boshqa kompaniyalar bilan yoki ushbu kompaniyaning bo'limlari orasida aloqa o'rnatilishi zarur. Hozirda global Internet tarmog'i o'zining uzellari o'rtasida ishonchli va arzon axborot almashinuvini ta'minlaydi. Ochiq global Internet tarmog'i kanallaridan faol foydalanuvchi elektron biznesning ishlashi jarayonida ko'pgina xavf-xatarlar paydo bo'ladi.

Internetdan foydalanish kanallari kompaniyaning axborot resurslaridan chetdan foydalanishga imkon berishi mumkin. Kommunikatsion, xususan HTTP — protokol asosidagi dasturlardan extiyotsizlik bilan foydalanish axborot tizimining ishga layoqatligini buzuvchi va/yoki axborot tizimima'lumotlarini buzuvchi maxsus dastur — "Troyan otlarining" kirishiga olib kelishi mumkin. Bu xil dasturlarning ichida viruslar eng tarqagan. O'ziga xos malakali mutaxassislar korporativ axborot tarmoqlariga bilinmasdan kirish uchun ko'pincha umummaqsad tarmoqlardan foydalanadilar.

Elektron qutisining tez-tez ishlatalishi niyati buzuq odamlarga elektron biznes bilan shug'ullanuvchi tashkilot foydalanuvchilar nomlarini obro'sizlantirishga yordam berishi mumkin. Foydalanuvchilar ma'lumotlarini (ismlar, parollar, PIN — kodlar va h.) saqlovchi tizimining zaif joylarini qidirishdan tarmoqda keng ishlatiluvchi maxsus dasturlardan foydalanish mumkin.

Internet konfidentsial axborotni dunyoning istalgan nuqtasiga yuborishi mumkin, ammo agar u yetarlicha ximoyalanmagan bo'lsa, ushlab qolinishi, nusxalashtirilishi, o'zgartirilishi hamda har qanday chetdagi foydalanuvchilar -niyati buzuq odamlar, raqiblar va oddiy qiziquvchilar tomonidan o'qilishi mumkin. Masalan, yetarlicha himoyalanmagan to'lov topshirig'i yoki kredit kartochka nomerini jo'natayotganda esda tutish lozimki, jo'natish xususiy/shaxsiy tarmoq orqali amalga oshirilmayapti va chetdagi foydalanuvchilar xabaringizni manipulyatsiya qilish imkoniyatiga ega. Undan tashqari xabaringiz almashtirilib qo'yilishi mumkin: xabarlarni xuddi V foydalanuvchidan yuborilganidek A foydalanuvchidan yuborish usullari mavjud. Internet tarmog'i mahsus paket, tamomila qonuniy paketlar, sonining xaddan tashqari ko'pilgi uzatishdagi buzilishlar, tarmoq komponentlarining nosozligi tufayli ishga layoqat bo'imasligi mumkin. Bunday xollar "xizmat qilishdan voz kechish" deb ataladi va elek-tron tijorat uchun eng jiddiy tahdid hisoblanadi.

Axborot xavfsizligi elektron biznes tizimining eng muxim elementlaridan biri xisoblanadi va usullar va vositalarning butun bir to'plami yordamida ta'minlanishi shart. Elektron tijorat sohasidagi savdo ko'lami Internet xavfsizligi masalalaridan tashvishlangan xaridorlar, sotuvchilar va moliya institutlarining boshidan kechiruvchi qo'rquvlari bilan chegaralanadi. Bu qo'rquvlar, hususan, quyidagilarga asoslanadi:

- konfidentsiallikka kafolatning yo'qligi-kimdir ma'lumotlaringizni uzatilayotganida ushlab qolishi va qiymatli axborotni (masalan, kredit kartochkangizning nomerini, tovar yetqazib berish sanasi va adres) topishga urinishi mumkin;
- amalda ishtirok etuvchilarni tekshirish darajasining yetarli emasligi - tranzaktsiya qatnashchilari tekshirilmaganida tomonlarning biri "maskarad" uyuشتirishi mumkinki, uning oqibati ikkinchi tomonga ancha qimmatga tushadi. Masalan, xaridor saytga kirib undagi kompaniyaning haqiqiyligiga shubha qiladi, shunday hol ham ro'y berishi

mumkinki, xaridor kredit kartochkasining nomerini yetarlicha vakolatga ega bo'lмаган shaxsga beradi;

- sotuvchida buyurtma bergen xaridor kredit kartochkasining qonuniy egasi ekanliginining tekshirish imkoniy yo'q;
- kredit kartochkasining bank - emitenti to'lovniga bajarishga talab qo'ygan sotuvchini tekshirishni istab qolishi mumkin;
- ma'lumotlar yaxlitligiga kafolat yo'q - xatto ma'lumotlarni jo'natuvchi indentifikatsiyalangan bo'lsada, uchinchi tomon ma'lumotlarni, ular uzatilishi vaqtida, o'zgartirish imkoniyatiga ega.

Axborot xavfsizligini ta'minlash nuqtai nazaridan elektron tijoratning namunaviy qo'llanilishini — Internet orqali maxsulotga va xizmatlarga ega bo'lishni ko'raylik. Ushbu jarayon quyidagi bosqichlar orqali ifodalanishi mumkin.

1. Buyurtmachi Web-server orqali maxsulot yoki xizmatni tanlaydi va mos buyurtmani rasmiylashtiradi.
2. Buyurtma magazinning buyurtmalar ma'lumotlari bankiga kiritiladi.
3. Buyurtma berilgan maxsulot yoki xizmatni olish mumkinligini ma'lumotlarning markaziy bazasi orqali tekshiriladi.
4. Agar mahsulotning olinishi mumkin bo'lmasa, buyurmachi u to'g'rida ogohlantiriladi va mahsulot yoki xizmatga ega bo'lish jarayoni to'xtatiladi. Mahsulotga so'rov boshqa skladga (buyurtmachi roziligidagi) yo'naltirilishi mumkin.
5. Agar maxsulot yoki xizmat mavjud bo'lsa buyurtmachi to'lovniga tasdiqlaydi va buyurtma mos ma'lumotlar bazasiga kiritiladi. Elektron magazin mijozga buyurtma tasdig'ini yuboradi. Ko'pgina xollarda (ayniqsa endigina ish boshlagan kompaniyalarda) buyurtmalar, tavarlarning borligini tekshirish va h. uchun yagona ma'lumotlar bazasi mavjud.
6. Mijoz onlayn rejimida buyurtma xaqini to'laydi.
7. Tovar buyurtmachiga yetqaziladi.

Elektron tijorat bilan shug'ullanadigan kompaniyalar yuqorida keltirilgan bosqichlarda duch keladigan tahdidlar quyidagilar:

- elektron magazin Web-saytining sahifasini almashtirib quyish. Bu tahdidni amalga oshirishning asosiy usuli — foydalanuvchi so'rovini boshqa serverga yo'llash. Bu tahdid oltincha bosqichda buyurtmachi kredit kartochkasining nomerini kiritganda kuchayadi;
- yolg'on buyurtmalar berish va elektron magazin xodimlari tomonidan firibgarlik qilish. Hozirda ichki/tashqi tahdidlar munosabati 60/40ni tashkil etadi;
- elektron tijorat tizimida uzatiladigan ma'lumotlarni ushlab qolish. Buyurtmachining kredit kartasi xususidagi axborotni ushlab qolish o'zgacha xavf-xatarni tug'diradi;
- kompaniyaning ichki tarmog'iga kirish va elektron magazin komponentlarini obro'sizlantirish;
- "xizmat qilishdan voz kechish" (denial of service) xujumini amalga oshirish va elektron tijorat ishlashini yoki uning uzelini buzish.

Ushbu tahdidlar natijasida kompaniya - elektron bitim provayderi - mijozlar ishonchini yo'qotadi, moddiy zarar ko'radi. Ba'zi xollarda bu kompaniyalarga kredit kartochka nomeri fosh qilingani uchun da'vo qo'zg'atilishi mumkin. "Xizmat qilishdan voz kechish" xujumi natijasida elektron magazinning ishlashi buzilishi mumkin, uning ishga layoqatligini tiklashga inson, vaqt va material resurslari talab etiladi.

Asosiy adabiyotlar

1. S.K.G'aniev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil
2. Анин Б. "О шифровании и дешифровании". Конфидент, 1997.
3. Гайкович В. "Компьютерная безопасность", Банковская технология, 1997.
4. Балакирский Б.В. "Безопасност электронного платежа", Конидент, 1996.
5. Давидовский А.Н. "Зашита информасия в вичислителних платежей"