NIGMATOV XIKMATULLA
RAXMANOV QURBON SODIQOVICH

OBYEKTLARDA AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMINI YARATISH METODOLOGIYASI

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

O‘ZBEKISTON XALQARO ISLOM AKADEMIYASI

NIGMATOV XIKMATULLA
RAXMANOV QURBON SODIKOVICH

OBYEKTLARDA AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMINI YARATISH METODOLOGIYASI

(Monografiya)

TOSHKENT - 2022

УДК: 621.395.12
КБК:56.147

"Obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasi" (monografiya). - X.Nigmatov, Q.S.Raxmanov – Toshkent: O'zbekiston xalqaro islom akademiyasi, 2022. – 144 bet.

***Taqrizchi*:**

Ismoilov M.A. - Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti Milliy tadqiqot universiteti professori, texnika fanlari doktori

Xodjaeva M.S. - O'zbekiston xalqaro islom akademiyasi "Zamonaviy AKT" kafedrasi dotsenti, t.f.n.

Nashr uchun muharrir:
Mansur Yunus,
Ozbekiston Jurnalistlari ijodiy uyushmasi a`zosi

O'zbekiston xalqaro Islom Akademiyasi Kengashida ko'rib chiqildi va nashr etishga ruxsat etildi. 2022-yil 31-mart 8-sonli bayonnoma.

Obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasi

Ushbu monografiyada har xil turdagi obyektlarning kompyuter tizimi va tarmoqlarida xosil bo'ladigan xavf-xatarlarni oldini olish, ruxsatsiz kirayotgan ma'lumotlarni aniqlash, obyektlarning ma'lumotlar bazasidagi axborotlarni himoyalash usullarini qo'llash, uzatilayotgan va qabul qilinayotgan xabarlarni xatosiz va aniq yetkazib berish usullarini amalga oshirish va umuman ushbu obyektning axborot xavfsizlik tizimini yaratib berish usullari va metodologiyasi taklif etilgan.

Bundan tashqari VPN – shaxsiy virtual tarmoq texnologiyasi, ekranlash texnologiyalari, ularning ta'sirini aniqlovchi texnologiyalari, telekomunikatsiya tizimlarida himoyalash modellari, elektron raqamli imzo va hozirgi zamonaviy intellektual texnikaviy vositalari obyektlarning kompyuter tizimi va tarmoqlarining aloqa kanallarida yuborilayotgan ma'lumotlarni himoyalash usullari keng yoritilib berilgan.

Ushbu monografiya 5220400 – "Axborot xavfsizligini boshqarish", 60610400 – "Axborot xavfsizligini boshqarish" ta'lim yo'nalishi hamda 70610401–"Axborot xavfsizligini boshqarish" va 5A220401–"Axborot xavfsizligini boshqarish" mutaxassisligi talabalari uchun mo'ljallangan.

Методология создания системы управления информационной безопасностью на объектах.

В данной монографии предложена методика предупреждения рисков, возникающих в компьютерных системах и сетях различных типов объектов, выявления несанкционированного доступа к информации, применения методов защиты информации в базах данных объектов, осуществления безошибочной и точной доставки передаваемых и принимаемых сообщений и создания системы информационной безопасности данного объекта в целом. Кроме того, широко освещены технологии VPN – персональных виртуальных сетей, технологии экранирования, технологии определения их воздействия, модели защиты в телекоммуникационных системах, электронные цифровые подписи и современные интеллектуальные технические средства защиты информации, передаваемой по каналам связи компьютерных систем и сетей объектов.

Данная монография предназначена для студентов направлений 5220400 - «Управление информационной безопасностью», 60610400 - «Управление информационной безопасностью» и специальностей 70610401 - «Управление информационной безопасностью» и 5A220401 - «Управление информационной безопасностью».

Methodology for creating an information security management system at facilities.

This monograph offers a methodology for preventing risks arising in computer systems and networks of various types of objects, identifying unauthorized access to information, using methods to protect information in databases of objects, carrying out error-free and accurate delivery of transmitted and received messages and creating an information security system for this object as a whole. In addition, VPN technologies – personal virtual networks, screening technologies, technologies for determining their impact, protection models in telecommunication systems, electronic digital signatures and modern intelligent technical means of protecting information transmitted through communication channels of computer systems and object networks are widely covered.

This monograph is intended for students of directions 5220400 - "Information Security Management", 60610400 - "Information Security Management" and specialties 70610401 - "Information Security Management" and 5A220401 - "Information Security Management".

SO'Z BOSHI

Hozirgi rivojlanish davrida barcha tashkilotlar, davlat yoki hususiy korxonalar, muassasalar, tijorat kompaniyalari va boshqa har xil obyektlarda raqamli elektron texnolodiyalari asosida faoliyat olib borilayotgan jarayonida kompyuter tizimlari va tarmoqlari orqali amalga oshirilayotgani barchaga ma'lum. Kompyuter tizimlari va telekommunikatsiya tarmoqlarida axborotlarni xavfsizligini ta'minlash masalasi hozirgi paytda eng dolzarb va mas'uliyatli hisoblanadi. Obyektlarda axborot xavfsizligini boshqarish va axborotni muhofaza qilishni ta'minlovchi har xil himoyalash vositalarini o'rnatish faqat markazlashtirilgan nazorat bo'lmasdan, balki bu jarayonlar samaradorligini ta'minlash va nafaqat taktik, balki strategik vazifalarni hal etish, butun tashkilotni boshqarishning muhim qismi hisoblanadi.

Axborot xavfsizligini boshqarish – ya'ni axborotni himoya qilish va vazifalarni belgilash zarurligini anglashni o'z ichiga olgan siklik jarayon hisoblanib obyektlardagi axborot xavfsizligi holati haqida ma'lumotlarni yig'ish va tahlil qilishdan, axborot xatarlarini baholashdan, xavfni boshqarish choralarini rejalashtirishdan, tegishli nazorat mexanizmlarini amalga oshirishdan va mas'uliyatni belgilashdan, xodimlarni tayyorlash va rag'batlantirishdan, himoya choralarini amalga oshirish bo'yicha tezkor ish va nazorat mexanizmlarining ishlashini kuzatishdan hamda ularning samaradorligini va tegishli tuzatuvchi ta'sirlarni baholashdan iborat bo'ladi.

Monografiyani yozishdan maqsad respublikamizdagi barcha tashkilotlar, davlat yoki hususiy korxonalar, muassasalar, tijorat jamiyatlari, aktsiyadorlik kompaniyalari, firmalar va boshqa har xil obyektlarda axborot xavfsizligini boshqarish tizimini yaratish uchun qanday himoyalash vositalaridan foydalanish yo'llarini va usullarini yoritib berishdan iborat edi.

Monografiyani yozishda biz asosan X.Nigmatovning Oliy va o'rta maxsus ta'lim vazirligi tomonidan tasdiqlangan "Axborot xavfsizligi", "Intellektual tizimlar". deb nomlangan o'quv qo'llanmalari asosida va bizga axborotlarni xavfsizligini boshqarishga bag'ishlangan Rossiyada chop etilgan B. Vasilkov va V.I.Vasilyevlarning har xil nomlar bilan chiqarilgan o'quv qo'llanmalari bizga juda katta yordam berdi. Biz ularning kitoblaridan foydalandik. Bu esa monografiyaning sifatli

chiqishiga katta yordam berdi va shuning uchun biz ularga o'zimizning katta minnatdorchiligimizni bildiramiz.

Taqdim etilayotgan ushbu "Obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasi" deb nomlangan monografiya barcha tashkilotlar, korxonalar, muassasalar, mas'uliyati cheklangan jamiyatlar va har xil tijorat firmalari uchun mo'ljallangan bo'lib, ular o'zlarining axborotlarini xavfsizligini ta'minlashda qo'lanma sifatida foydalansalar biz juda hursand bo'lgan bo'lar edik.

Mualliflar

KIRISH

Hozirgi paytda rivojlangan davlatlarda innovatsion jarayonlarni rivojlantirish asosan global tarmoqlar asosida amalga oshirilmoqda, shunday tarmoq turidagi innovatsion infrastrukturalar ham tashkil etilmoqda. Bularning barchasi bir tomondan raqamli iqtisodiyotga o'tayotganligi, ishlab chiqarish samaradorlik darajasini oshishiga va umuman hayot sifatini yaxshilanishiga mo'ljallangan bo'lsa, ikkinchi tomondan jamiyatni axborotlashtirish jarayonida yangi xavf va xatarlarni kelib chiqishiga sabab bo'lmoqda.

O'zbekiston xalqi o'zining diniy-ma'rifiy boyliklarini saqlagan holda katta ishlarni amalga oshirmoqda. Jumladan, mustaqillikka erishilgan davrdan boshlab respublikadagi barcha diniy majmualarni, mavzoleylarni, masjidlarni, madrasalarni, o'quv yurtlarni qayta ta'mirlash bilan birgalikda zamonaviy axborot-kommunikatsiya texnologiyalari asosida xalqaro kompyuter tarmog'i bo'lmish Internet bilan bog'lanish uchun o'zlarining mahalliy kompyuter tarmoqlarini yaratib va unda faoliyat olib borish uchun keng ma'lumotlar omborini yaratmoqdalar. Kelayotgan turistlar va mehmonlar uchun yangi dasturiy vositalar asosida mobil uyali aloqa telefonlariga barcha ma'lumotlarni joylab berish ishlari ham bajarilmoqda. Hozirgi zamonda har bir axborot o'z bahosiga ega bo'lib qolmoqda va ularning qiymati esa olinayotgan, saqlanayotgan, uzatilayotgan yoki qabul qilinayotgan axborotlarning butunligiga, o'zgartirilmaganligiga, xatosiz berilganligiga va talab qilingan vaqtda yetkazib berilganligiga bog'liq bo'ladi. Bu shartlarning buzilganligi esa axborotlardan foydalanuvchilariga juda katta ma'naviy, siyosiy, axloqiy va iqtisodiy zarar keltirishi barchaga ma'lum bo'lib qoldi.

Bizning O'zbekiston xalqaro islom akademiyamizda ham ushbu yo'nalishlar bo'yicha juda ko'p ilmiy, ijtimoiy-iqtisodiy, o'quv va uslubiy ishlar olib borilmoqda. Ayniqsa, akademiyaga "Axborotlar xavfsizligini boshqarish" yo'nalishi va mutaxassisligi O'zbekiston Oliy va maxsus ta'lim vazirligi tomonidan tasdiqlab berilgani iqtisodiyotni raqamlashtirish va zamonaviy innovatsion va pedagogik texnologiyalarini qo'llanilishini rivojlantirishga qaratilgan amaliy tadbirlarni qo'llashga turtki berdi. Jumladan, akademiyada talabalarga va magistrlarga ta'lim berish, o'zi tanlagan kasbini mukammal bilib olish uchun zamonaviy axborot-kommunikatsiya texnologiyalardan

keng foydalanishni o'rgatish jarayonida yangi pedagogik texnologiyalarni qo'llash asosida amalga oshirilmoqda.

Kompyuter texnikasi va axborot tizimlarining iqtisodda, boshqarishda, aloqada, ilmiy tadqiqotlarda, ta'limda, xizmat ko'rsatish sohasida, tijorat, moliya va inson faoliyatining boshqa sohalarida qo'llanilishining rivoji axborotlashtirish va umuman, jamiyat rivojini belgilovchi yo'nalish hisoblanadi. Shuning uchun ushbu monografiyaning asosiy maqsadi axborot xavfsizligini boshqarish yonalishi bo'yicha bilim olgan mutaxassislar har qanday obyektlarda axborotlarni himoyalash usullarini qo'llashni va amalda tadbiq etishlari uchun metodologik qo'llanma sifatida nash etilgan. Bundan tashqari ish faoliyatidan qat'iy nazar korxonalar, tashkilotlar, muassasalar, kompaniyalar, tijorat firmalari ham o'zlarining saqlanayotgan, uzatilayotgan va qabul qilinayotgan ma'lumotlarini xavfsizligini ta'minlash jarayonida foydalanishlari mumkin bo'ladi.

I BOB.
AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMI

1.1. Monografiyada ishlatilgan atamalar

Obyektlarda axborot xavfsizligini boshqarish (AXB, ingliz tilida: Information Security Management, ISM) tizimini yaratish metodologiyasi bo'yicha mavzuga taaluqli atamalar, terminlar va ta'riflarni keltiramiz, ular quyidagilardan iborat:

Obyekt – o'zining tasdiqlangan nizomi asosida faoliyat olib borayotgan tashkilotlar, davlat yoki hususiy korxonalar, muassasalar, tijorat jamiyatlari va boshqa har xil tuzilmalar:

Axborot tizimi - xizmatlar, IT aktivlari va axborotni qayta ishlashning boshqa komponentlari;

Axborot xavfsizligi - axborotning maxfiyligini, yaxlitligini va mavjudligini saqlash;

Mavjudlik - vakolatli shaxsning iltimosiga binoan foydalanish uchun qulay va tayyor bo'lish xususiyati;

Maxfiylik - axborotning mulki ruxsatsiz shaxslar uchun mavjud emas yoki yopiq bo'lishi;

Yaxlitlik - aniqlik va to'liqlik xususiyati;

Qaytarilmaslik - voqea yoki harakatning boshlanishini va ularni yaratadigan subyektlarni tasdiqlash qobiliyati;

Axborot xavfsizligining hodisasi - xavfsizlik bilan bog'iq bo'lishi mumkin bo'lgan siyosat yoki xavfsizlik choralarini yoki undan oldin noma'lum vaziyatni buzganligini ko'rsatuvchi tizim (xizmat yoki tarmoq) ning aniqlangan holati;

Axborot xavfsizligi hodisasi - bu biznes operatsiyalarining uzilishiga olib kelishi va axborot xavfsizligiga tahdid solishi ehtimoli yuqori bo'lgan bir yoki bir nechta axbotot tizimidagi voqealari;

Axborot xavfsizligi intsidentlarini boshqarish - axborot xavfsizligini intsidentlarini aniqlash, ogohlantirish, baholash, javob berish, ko'rib chiqish va o'rganish jarayonlari;

Boshqarish tizimi - ushbu maqsadlarga erishish uchun siyosat, maqsadlar va jarayonlarni o'rnatish uchun tashkilotning o'zaro bog'liq elementlari to'plami;

Monitoring - tizim, jarayon yoki harakatning holatini aniqlash;

Siyosat - boshqaruv tomonidan rasmiy ravishda ifodalangan umumiy maqsad va yo'nalish;

Xavf - maqsadlar uchun noaniqlikning ta'siri;

Tahdid - zarar etkazishi mumkin bo'lgan kiruvchi hodisaning mumkin bo'lgan sababi;

Xavfsizlik kamomadi - bir yoki bir nechta tahdidlar bilan ishlatilishi mumkin bo'lgan aktiv yoki himoya choralari.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

Maxfiylik - aniq bir axborotga faqat tegishli shaxslar doirasigina kirishi mumkinligi, ya'ni foydalanilishi qonuniy hujjatlarga muvofiq saqlab qo'yilib, hujjatlashtirilganligi kafolati. Bu bandning buzilishi o'g'rilik yoki axborotni oshkor qilish deyiladi;

Konfidensiallik - ishonchliligi, 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 haqiqattan ham axborotning egasi ekanligiga beriladigan kafolat. Bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi;

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

Yuqoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin:

Ishonchlilik - tizim me'yoriy va g'ayri tabiiy hollarda rejalashtirilganidek o'zini tutishlik kafolati;

Aniqlilik - hamma buyruqlarni aniq va to'liq bajarish kafolati;

Tizimga kirishni nazorat qilish - turli shaxs guruhlari axborot manbalariga har xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati;

Nazorat qilinishi - istalgan paytda dastur majmuasining hoxlagan qismini to'liq tekshirish mumkinligi kafolati;

Identifikatsiyalashni nazorat qilish - hozir tizimga ulangan mijoz aniq o'zini kim deb atagan bo'lsa, aniq o'sha ekanligining kafolati;

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

Obyektlarda axborotlarni xavfsizligini boshqarish tizimini yaratishning maqsadlari quyidagilardan iborat:

– axborotning kelishuvsiz chiqib ketishi, o'g'irlanishi, yo'qotilishi, o'zgartirilishi, soxtalashtirilishlarning oldini olish;

– shaxs, jamiyat, davlat xavfsizliligiga bo'lgan xavf-xatarning oldini olish;

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

– hujjatlashtirilgan axborotning miqdori sifatida huquqiy tartibini ta'minlovchi, axborot zaxirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko'rinishlarining oldini olish;

– axborot tizimida mavjud bo'lgan shaxsiy ma'lumotlarning maxfiyligini va konfidensialligini saqlovchi fuqarolarning konstitutsion huquqlarini himoyalash;

– davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidensialligini saqlash;

– axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chiqish va qo'llashda subyektlarning huquqlarini ta'minlashdan iborat bo'ladi.

Axborot-kommunikatsiya texnologiyalarining ommaviy ravishda qog'ozsiz avtomatlashtirilgan asosida boshqarilishi sababli axborot xavfsizligini ta'minlash murakkablashib va muhimlashib bormoqda. huning uchun, ham avtomatlashtirilgan axborot tizimlarida axborotni himoyalashning yangi zamonaviy texnologiyasi paydo bo'lmoqda.

1.2. Axborot xavfsizligini boshqarish tizimining tushunchasi va uning tarixi

Axborot xavfsizligini boshqarish - bu siklik jarayon hisoblanadi. Axborotni himoya qilish zarurati darajasini anglash va maqsadlarni belgilash, tashkilotdagi axborot xavfsizligi holati to'g'risidagi ma'lumotlarni yig'ish va tahlil qilish, axborot xavfini baholash, xavfni oldini olish choralarini rejalashtirish, tegishli nazorat mexanizmlarini joriy etish, ro'lini va ma'suliyatini taqsimlash, xodimlarni o'qitish va rag'batlantirish, himoya choralarini amalga oshirish bo'yicha tezkor ishlar, nazorat mexanizmlarining ishlashini kuzatish, ularning samaradorligini baholash va tegishli tuzatish harakatlarini amalga oshirishdan iboratdir.

Obyektlarda saqlanadigan va qayta ishlangan barcha ma'lumotlar hujum tahdidlari, xatolar, tabiat (masalan, yong'in yoki suv toshqini) va boshqalar va undan foydalanishga xos bo'lgan zaifliklarning predmetidir.

Odatda, axborot xavfsizligi tushunchasi aktivning qiymatiga ega bo'lgan va tegishli himoya qilishni talab qiladigan ma'lumotlarga asoslangan (masalan, mavjudlik, maxfiylik va yaxlitlikni yo'qotishdan). Vakolatli shaxslarning aniq va to'liq ma'lumotlariga o'z vaqtida kirish imkoniyatiga ega bo'lish biznes samaradorligining katalizatori hisoblanadi.

Axborot xavfsizligini boshqarish-turli xil ishlarni bajarish uchun ko'plab kichik toifalarni o'z ichiga olgan ko'p tomonlama, ko'p qirrali, davriy jarayon hisoblanadi:

- kibernetikani qayta ishlash choralarini yaratish;
- obyektlarda kiberxavfsizlikning hozirgi holati haqida ma'lumot to'plash, tahlil qilish;
- obyektning kiber xavfsizligini ta'minlashning zarur darajasini aniqlash, tegishli mutaxassislar uchun tegishli vazifalarni shakllantirish;
- axborot xavflarini baholash;
- rollarni va mas'uliyatni nazorat qilish, taqsimlash uchun zarur mexanizmlarni integratsiya qilish va shakllantirish;
- axborot xavfsizligi sohasida obyekt xodimlarining raqamli savodxonligini oshirish, o'qitish;
- axborotni himoya qilish bo'yicha zarur chora-tadbirlarni amalga oshirishning tezkorligi;
- obyektda ishlatiladigan nazorat mexanizmlarining ishlashini kuzatish, ularning samaradorligini baholash, agar kerak bo'lsa, ularning ishiga zarur o'zgarishlarni amalga oshirishdan iborat bo'ladi.

AXB bugungi kunda ko'pchilik tomonidan hal qilinishi kerak bo'lgan asosiy vazifa hisoblanadi.

Axborot xavfsizligi (AX)ni aniqlash, yaratish, qo'llab-quvvatlash va takomillashtirish orqali axborot aktivlarini samarali himoya qilish tashkilotning maqsadlariga erishish, shuningdek, huquqiy muvofiqlik va obro'sini saqlab qolish va yaxshilash uchun zarur shartdir. Tegishli himoya choralarini amalga oshirish va qabul qilinmaydigan AX xatarlarini qayta ishlashga qaratilgan ushbu muvofiqlashtirilgan tadbirlar AXB boshqaruvlari sifatida yaxshi ma'lum.

AX xavfi va himoya choralari samaradorligi o'zgarganligi sababli, tashkilotning o'zgaruvchan sharoitlariga qarab quyidagilar mavjud:

- amalga oshirilgan himoya choralari va protseduralarining samaradorligini nazorat qilish va baholash;
- qayta ishlash uchun yuzaga keladigan xavflarni aniqlash;
- tegishli himoya choralarini to'g'ri tanlash, amalga oshirish va takomillashtirish.

AX harakatlarining o'zaro aloqasi va muvofiqlashtirilishi uchun har bir tashkilot xavfsizlik siyosati va maqsadlarini shakllantirishi va boshqaruv tizimidan foydalangan holda ushbu maqsadlarga samarali erishishi kerak.

Xalqaro standart hisoblangan ISO 27001 ga binoan, axborot xavfsizligini boshqarish tizimi (AXBT) - bu "axborot xavfsizligini yaratadigan, amalga oshiradigan, boshqaradigan, kuzatib boradigan, ko'rib chiqadigan, saqlaydigan va takomillashtiradigan korxona tavakkalchiliklarini boshqarishning umumiy tizimining bir qismi". Boshqaruv tizimiga tashkiliy tuzilma, siyosat, rejalashtirish, lavozim majburiyatlari, amaliyot, protsedura, jarayon va resurslar kiradi.

AXBTni yaratish va ishlatish boshqa har qanday boshqaruv tizimi bilan bir xil yondashuvni talab qiladi. AXBT larni tasvirlash uchun ISO 27001 da qo'llaniladigan jarayon modeli uzluksiz faoliyat siklini ta'minlaydi, ya'ni rejalashtirish, amalga oshirish, tekshirish harakatlaridan iborat bo'ladi.

Uzluksiz takomillashtirish jarayoni, odatda, dastlabki investitsiyalarni talab qiladi: faoliyatni hujjatlashtirish, risklarni boshqarishga yondashuvni rasmiylashtirish, tahlil usullarini belgilash va resurslarni ajratishga qaratilgan bo'ladi. Bu chora-tadbirlar sikli faollashtirish uchun ishlatiladi. Ular qayta ko'rib chiqish bosqichlari faollashtirilgunga qadar bajarilishi shart emas.

Rejalashtirish bosqichida tizimlarning konteksti va ko'lamini to'g'ri belgilash ta'minlanadi, axborot xavfsizligi risklari baholanadi va bu xavf-xatarlarni boshqarish bo'yicha tegishli reja taklif etiladi. O'z navbatida, amalga oshirish bosqichida qabul qilingan qarorlar amalga oshirilib, ular rejalashtirish bosqichida belgilanadi. Tekshirish va harakat bosqichlarida ular belgilangan va amalga oshirilgan xavfsizlik yechimlarini mustahkamlaydi, tuzatadi va yaxshilaydi.

Cheklar aniq vaziyatga qarab istalgan vaqtda amalga oshirilishi mumkin. Ba'zi tizimlarda ular zudlik bilan bajarilishi va javob berishini

ta'minlash maqsadida avtomatlashtirilgan jarayonlarga singdirilishi kerak bo'ladi. Boshqa jarayonlar uchun himoya qilinayotgan axborot resurslariga o'zgartirish yoki qo'shimchalar kiritilgan, shuningdek tahdid va zaifliklar o'zgargan taqdirda faqat xavfsizlik hodisalari holatidagina javob berish talab etiladi. Yillik yoki boshqa davriy tekshiruvlar yoki auditlar butun boshqaruv tizimining o'z maqsadlariga erishishini ta'minlash kerak bo'ladi.

Ko'plab korxona, tashkilot, muassasa, firma va har xil kompaniyalar uchun axborot xavfsizligini boshqarish haqida o'ylash vaqti keldi. Ularning ko'pchiligining IT - infratuzilmasi yaxshi tashkil etilgan muvofiqlashtirishni talab qiladigan darajaga yetdi.

AXBTni qurishda ekspertlar ISO 27001/17799 Xalqaro standartlariga tayanishni tavsiya etadilar.

Menejer o'z tashkiloti, bo'limi, loyihasi va mijozlar bilan munosabatlarda vaziyatni nazorat qilishi shart. Bu sodir bo'layotgan voqealardan xabardor bo'lishi, barcha favqulodda vaziyatlarni o'z vaqtida o'rganishi va u yoki bu holatda qanday harakatlarni amalga oshirishi kerakligini tasavvur qilishi demakdir. Tashkilotda raxbariyatning bir necha darajalari mavjud bo'lib, katta raxbarlardan boshlanib, aniq ijrochilar bilan yakunlanadi va har bir darajada vaziyat nazorat ostida bo'lishi kerak. Boshqacha aytganda, boshqaruv vertikal va boshqaruv jarayonlari qurilishi lozim.

AXBT — bu nima? degan savolga quidagicha javob berish mumkin.

ISO 27001/17799 Xalqaro standartlari asosida ishlab chiqilgan axborot xavfsizligini boshqarish tizimi - tizim xavfsizligining zarur darajasiga erishish va axborot xavfsizligi tahdidlari xavfini sezilarli darajada kamaytirish imkonini beradi. AXBT axborot xavfsizligi vositalarining turli tarkibiy AXBT larini bog'lovchi va kompaniyangizning axborot xavfsizligi tizimini ishonchli va oshkora boshqarish imkonini beruvchi asosdir.

Har bir obyektning axborot xavfsizligini boshqarish tizimlarining rivojlanishi bir qator asosiy bosqichlarni o'z ichiga oladi:

– axborot xavfsizligi komponentlarining axborot xavfsizligi auditi;

– axborot xatarlarini chuqur tahlil qilish, ularning turli axborot xavfsizligi mezonlariga ta'sirini hisobga olish (mavjudlik, maxfiylik, yaxlitlik);

– AXBT larni loyihalash;

– AXBT larning Real axborot xavfsizligi komponentlarining talablarini amalga oshirish rejasi va mexanizmlarini ishlab chiqish;

– xodimlarning axborot xavfsizligi sohasidagi xabardorligi bo'yicha o'quv jarayonini ishlab chiqish;

– AXBT qurish, konsalting va amalga oshirish jarayonini qo'llab-quvvatlash va boshqalar kiradi.

Yuqorida keltirilganlar asosida har qanday obyektlarda (korxona, tashkilot, muassasa, mas'uliyati cheklangan jamiya, firma va x/z) axborot xavfsizligini boshqarish tizimini yaratish uchun ishlatiladigan, saqlanadigan, uzatiladigan va qabul qiladigan axborotlarni turkumlanishini aniq bilib olish lozim.

Axborot xavfsizligini boshqarish muammosi Windows NT va Internetning ommaviy mahsulot sifatida paydo bo'lishi davrida boshlangan edi. Yangi texnologiyalarga ega bo'lgan xakerlar ularni kredit karta va boshqa turdagi ma'lumotlarini o'g'irlash uchun firibgarliklarni qo'llasha boshlashdi [2].

Britaniya standartlari instituti (BSI) tijorat tashkilotlari ishtirokida axborot xavfsizligini boshqarish standartini ishlab chiqishga kirishdi. 1995 yilda BSI natijasi, milliy Britaniya standarti BS 7799 tashkilotning axborot xavfsizligini boshqarish standarti qabul qilingan edi. Standart ikki qismdan iborat bo'lib standartning birinchi qismi (BS 7799:1) tabiatda tavsiya etilgan, ikkinchisi (BS 7799:2) sertifikatlash uchun mo'ljallangan va birinchi qismga kiritilmagan bir qator majburiy talablarni o'z ichiga olgan edi

1999 - yilda ISO standartlashtirish bo'yicha xalqaro tashkilotda BS 7799:1 axborot xavfsizligi sohasidagi standartni asos qilib olishga qaror qilindi. Natijada, BS 17799: 7799 standartiga asoslangan ISO 1 standarti chiqarildi. Ushbu standartning eng yangi versiyasi ISO / IEC 17799: 2005 hisoblanadi.

ISO/IEC 17799: 2005 standarti kompaniyaning axborot xavfsizligini boshqarishning eng yaxshi global tajribasini birlashtiradi. Ushbu standart printsiplarni belgilaydi va axborot xavfsizligini boshqarish tizimini ishlab chiqish, amalga oshirish, qo'llab-quvvatlash va takomillashtirish bo'yicha qo'llanma hisoblanadi. Axborot xavfsizligini boshqarishning turli sohalarida nazorat qilish va nazorat qilish maqsadlarini belgilash mexanizmlarini tavsiflaydi.

ISO/IEC 27001: 2005 standarti korporativ axborot xavfsizligini boshqarish tizimiga talablarni belgilaydi. Ushbu standart axborotga duch kelishi mumkin bo'lgan xavf va tahdidlarni aniqlash, kamaytirish va boshqarish bo'yicha qo'llanma hisoblanadi. Iso/IEC 27001:2005 standarti samarali va etarli vositalarni tanlashda yordam berish va tashkilotning iste'molchilari va hamkorlarining axborotlarini to'g'ri himoyalanganligini ta'minlash uchun mo'ljallangan.

Ushbu standart faoliyati turidan qat'iy nazar, har qanday tashkilotlarda qo'llanilishi mumkin.

ISO/IEC 27001:2005 ni axborot xavfsizligini boshqarish tizimi uchun asos sifatida ishlatadigan tashkilot Britaniyaning BSI standartlari institutida (British Standard Institute) ro'yxatga olinishi mumkin, bu esa barcha manfaatdor tomonlarga kompaniyaning korporativ axborot xavfsizligini boshqarish tizimi xalqaro standartning barcha talablariga javob beradi [3].

2000-yillarning boshidan boshlab, davlat va yirik xalqaro korporatsiyalar allaqachon zarar ko'rgan daromadli biznesga aylana boshlaganda, IT-kompaniyalar nafaqat antivirus dasturlarini o'z ichiga olgan axborot xavfsizligini boshqarish bo'yicha aniq yechimlarni ishlab chiqa boshladilar, balki tizim jurnallarini (fayllar jurnallarini) monitoring qilish bilan shug'ullanadigan kommunal xizmatlar ham mavjud bo'la boshladi.

Sonya AQShda kiber hujumlardan so'ng, kiberfoydalanish bo'yicha ixtisoslashgan agentlik tashkil etildi, uning vazifalaridan biri axborot xavfsizligini boshqarishning yangi standartlarini ishlab chiqishga sabab bo'ldi [4].

Axborot xavfsizligini boshqarish tizimlarining asosiy funktsiyalari quyidagilardan iborat:

- axborot xavfsizligi xavfini aniqlash va tahlil qilish;
- axborot xavfsizligi xavfini minimallashtirishga qaratilgan jarayonlarni rejalashtirish va amalga oshirish hamda ularni nazorat qilish;
- axborot xavflarini minimallashtirish jarayonlariga zarur tuzatishlar kiritishdan iborat.

Axborot xavfsizligini sifatli boshqarish quyidagi printsiplarga asoslanadi:

- kompleks yondashuv – ya'ni axborot xavfsizligini boshqaruvi keng qamrovli bo'lishi kerak. uning barcha tarkibiy qismlarini qamrab

oladi va korxona axborot tizimida yoki davlat muassasasida va undan tashqarida faoliyat yuritadigan barcha dolzarb omillarni hisobga oladi;
- tashkilotning vazifalari va strategiyasi bilan muvofiqlikligi;
- yuqori darajada boshqaruv tizimi;
- foydalanilgan va ishlab chiqarilgan ma'lumotlarning yetarliligi;
- samaradorlik - imkoniyatlar, ishlash va xarajatlar o'rtasidagi optimal muvozanat bo'lishligi;
- boshqarishning uzluksizligi;
- jarayon yondashuvi - boshqaruv jarayonlarini rejalashtirish, amalga oshirish, tekshirish, audit va tuzatishning yopiq sikliga bog'lash va aylanish bosqichlari o'rtasida uzviy aloqani ta'minlash, bu esa o'z navbatida tizim sifatini saqlab qolish va doimiy ravishda oshirish imkonini beradi [5].

Axborot xavfsizligini boshqarish amaliyoti turli sohalarda katta ahamiyatga ega: tijorat, bank, davlat, tibbiy va boshqalar [6], chunki bu sohalarda odamlar sirli ma'lumotlar bilan ishlaydi.

Jamiyat uchun axborot xavfsizligini boshqarish texnologiyalaridan oqilona foydalanish har bir a'zoning maxfiyligini va identifikatsiyasini himoya qilishni to'g'ri ta'minlashni anglatadi.

Axborot xavfsizligi, axborot tizimlari va kommunikatsiyalarning maxfiyligi, mavjudligi va yaxlitligini buzishdan himoya qilish uchun mo'ljallangan.

1.3. Obyektlarning kompyuter tizimi va tarmoqlar strukturasini aniqlash

Obyektlarda foydalanayotgan kompyuter tizimlari va tarmoq strukturalarini aniqlash uchun avvalam bor bugungi kunda yer sharidagi davlatlarda qanday kompyuter strukturalari qo'llanilayotganligini tahlil qilish kerak bo'ladi.

Barchaga ma'lumki, kompyuter tizimi deb texnik va dasturiy vositalar yordamida har xil hisoblash jarayonlarini bajaradigan majmuaga aytiladi. Kompyuter tarmoqlari esa ikki va undan ortiq bo'lgan kompyuterlarning texnik va dasturiy vositalar bilan bog'langan majmua hisoblanadi. Ularning bir – biri bilan topologik bog'lanishi asosida har xil strukturalar hosil bo'ladi, ya'ni apparat qurilmalari va tarmoq dastur ta'minoti orqali o'zaro bir-biri bilan hamoxang ishlay oladigan kompyuterlar majmuiga tarmoq deyiladi.

Tarmoqlarni turli me'yorlarga ko'ra sinflarga ajratish mumkin.

Bular:

1) O'tkazish qobiliyati, ya'ni ma'lumotlarni tarmoqqa uzatish tezligiga muvofiq:

- past 100 - 1000 Kbit/s gacha;
- o'rta 10 - 100 Mbit/s gacha;
- yuqori 100 Mbit/s - 40 Ggbit/s;
- o'ta yuqori 40 Ggbit/s – 10 Tbit/s dan ortiq.

2) Uzoq kommunikatsiya tarmoqlari bilan ishlash tezligi, ularning fizik o'lchoviga muvofiq:

- LAN (Local Area Network) lokal tarmoq (LXT bir ofis, bino ichidagi aloqa);
- CAN (Campus Area Network) - kampus tarmoq, bir-biri bilan telefon yoki modemlar bilan ulanishi shart bo'lmagan, ammo yetarlicha bir-birlaridan uzoqda joylashgan kompyuter lokal tarmog'i;
- MAN (Metropolitan Area Network) katta tezlik bilan aloqa uzatish (100 Mbit/s) imkoniyatiga, katta radiusga (bir necha o'n km) axborot uzatuvchi kengaytirilgan tarmoq;
- WAN (Wide Area Network) keng masshtabli (mintaqaviy) maxsus qurilma va dasturlar bilan ta'minlangan aloxida tarmoqlarni birlashtiruvchi yirik tarmoq;
- GAN (Global Area Network) global (xalqaro, qit'alararo) tarmoq;

3) Tarmoq tugunlari turi bo'yicha (tugun - hisoblash tarmoqlari va ularning aloxida elementlari ulangan joyi). Boshqacha aytganda, tugunga shaxsiy, mini va katta kompyuterlar, aloxida tarmoq ham kiradi. Masalan, umumiy foydalanish tarmoqlaridagi aloxida kompyuterlar (boshqachasiga ularni stantsiyalar deb ham yuritishadi) tugunlarga misol bo'la oladi. Unchalik katta bo'lmagan aloxida tarmoqlar kampus tarmog'i uchun tugun bo'ladi.

4) Tugunlar munosabatiga ko'ra:

Yacheykalar oralig'i, satr va ustunlar bilan ishlashning asosiy usullari va tavsifi.

- bir hil rangli (peer-to-peer), uncha katta bo'lmagan, bir hil mavqega ega kompyuterlar (bu erda hamma kompyuterlar ham "mijoz", ya'ni tarmoqning oddiy foydalanuvchisi, ham "server", ya'ni tarmoq foydalanuvchilariga xizmat ko'rsatishni ta'minlovchi bo'lishi mumkin);

- tarqatilgan (Distributed) tarmoqlar. Bunda serverlar tarmoq foydalanuvchilariga xizmat ko'rsatadi, biroq tarmoqni boshqarmaydi;
- server (Server based) yoki markazlashgan boshqarishga ega tarmoqlar. Bu yerda tarmoqning bosh elementi serverdir. Qolgan tugunlar serverning resurslaridan foydalanishi mumkin (masalan, Novell NetWare, Microsoft LAN Manager va boshqalar).

5) Tarmoq operatsion sistemalarini ishlatish bo'yicha (tarmoq OS):

- gomogenli - hamma tugunlarda bir hil yoki yaqin operatsion sistemalardan foydalaniladi;
- geterogenli - bir vaqtning o'zida bir nechta tarmoq operatsion sistemalari ishlatiladi (masalan, Novell NetWare va WINDOWS).

Kompyuter tarmog'ida quyidagi texnik va dasturiy vositalari ishlatiladi:

- Kontsentratorlar (inglizchasiga HUB).
- Kommutatorlar (inglizchasiga SWITCH).
- Ko'priklar (inglizchasiga BRIDGE).
- Marshrutizatorlar (inglizchasiga ROUTER).
- Qaytargich kuchaytiruvchilar (inglizchasiga REPEATOR).
- Darboza yoki Shlyuzlar (inglizcha GATEWAY).
- Interfeyslar.
- Drayverlar.

Bog'lovchi aloqa liniyalari (Har xil turdagi kabellar, radio, radiorele va yerning sun'iy yuldoshlari).

Tarmoqda bir necha hil serverlar bo'lishi mumkin. Kompyuter tarmog'i o'z mijozlariga qanday xizmatlar turkumini taklif etishi, ularning servisi qanday bo'lishi juda muhimdir. Ular bilan tanishamiz:

- fayl-server-mijozga axborot saqlash qurilmalarida saqlanuvchi fayllardan foydalanish imkonini beradi. Bunda server barcha ishchi stantsiyalaridan fayllarga kirish ruxsatini berishi zarur. Bunda bir vaqtning o'zida turli stantsiyalardan bir hil so'rov kelganda, axborotlarni himoya qila olish vazifasi ijobiy xal etiladi;
- print-server umumiy xolda ko'pgina mijozlarga bir nechta printer orqali xizmat ko'rsatishni ta'minlaydi. Bunda server chop etiluvchi axborotlarni qabul qila olishi va ularni navbati bilan chop etishga chiqarishi kerak;
- faks-server-mijozlarga faks-modem telefon tarmoqlari bilan mujassam tarmoqli xizmat ko'rsatishni ta'minlaydi. Bu go'yo axborot

chiqarishga o'xshaydi (printer kabi). Faks-server olgan faksimil xabarlar aloxida tarmoqda qayta ishlanadi. Bundan tashqari, tarmoqda quyidagi xizmatlar bo'lishi mumkin:

- elektron pochta (E-mail)-mijozlar o'rtasida, ular bir-birlaridan qancha uzoqlikda joylashganligidan qat'iy nazar, axborot almashishni ta'minlaydi. Bu yerda jarayon xuddi oddiy pochta kabi kechadi. Elektron xat o'z adresiga ega. Uni jo'natuvchi desak, qabul qiluvchi ham o'z adresiga ega. "Xat" pochta qutisiga tashlanadi (ya'ni pochta serveri) va pochta serverlar sistemasi yordamida qabul qiluvchi pochta qutisiga yetkaziladi, ya'ni bu yerda uzatuvchi va qabul qiluvchining maxsus kataloglari mijozga xizmat qiluvchi kompyuterda joylashtirilgan bo'ladi. Shu tariqa xatlar fayllar sifatida uzatiladi. Oxang, tovush kartalari yoki ovozli modemlar xatto tovushlarni ham uzatish imkonini beradi;

- bevosita muloqot (Chat), bunda aniq vaqtda maxsus dastur ta'minoti yordamida ikki yoki undan ortiq mijozlar o'zaro axborot almashinishi tushuniladi, ya'ni bir kompyuter klaviaturasida terilgan axborotlar ayni vaqtning o'zida boshqa kompyuter ekranida paydo bo'laveradi. Raqamli videokameralar, tovushli kartalar, mikrofonlar, multimedia vositalarini qo'llaganda, videokonferentsiyalar o'tkazish imkoniyati tug'iladi. Bunday xolatlarda kompyuterlar yuksak unumdor va tarmoqning o'tkazish qobiliyati kuchli bo'lishi lozim.

Obyektlarda lokal kompyuter tarmoqlari yaratilgan bo'ladi. Lokal kompyuter tarmoqlari (LKT) - bu bir obyektga taalluqli bo'lgan va uning barcha binolarida joylashgan kompyuterlarining bir – biri bilan bog'langan majmuasi hisoblanadi. Har bir obyekt o'zining kompyuter tarmog'iga ega bo'lganligi uchun ularning xarakteristika va ko'rsatkichlari har xil bo'ladi. Bular asosan kompyuterlarning turlariga, texnik komponentalarining parametrlariga, bog'lanish uchun ishlatilgan aloqa kabellarining turlari va xarakteristikalariga bog'liq bo'ladi.

Yuqori darajada qulaylik, ma'lumotlarni uzatish va qabul qilishdagi har xil xatolarga yo'l qo'ymaslik maqsadida tarmoqning butun ishi tarmoq bayonnomasi deb nomlanuvchi qoida va kelishuvlar bilan muvofiqlashtirib boriladi. Tarmoq bayonnomasi qo'llaniladigan birikmalar, kabellar, uzatiladigan signallarni kodlashtirish usullari, ma'lumotlar yozuvi formati, xatolarni payqash va tuzatish hamda shu kabilardan iborat.

Aloxida tugunlarni tarmoqda ulash usullari tarmoq topologiyasi deyiladi. Odatda quyidagi topologiyalar qo'llaniladi:

Umumiy shina xolda lokal tarmoqdagi barcha kompyuterlar bitta aloqa chizig'iga parallel bog'lanadi. Bunday shinalarni boshqarish ham aloxida, ham markazlashgan bo'lishi mumkin. Markazlashgan boshqaruvda tarmoqqa maxsus kompyuter-xakam ulanadi, uning vazifasi tarmoqda axborotni uzatishni boshqarishdir. Aloxida boshqaruvda hamma kompyuterlar bir hil maqomga ega, ular mustaqil ma'lumotlarni uzatish kanalini boshqaradi.

Xalqasimon xolatda barcha kompyuterlar yopiq xalqasimon, ketma-ket bog'lanadilar. Bunda xabar birin-ketin kompyuterdan-kompyuterga uzatiladi. Xabarni uzatgan kompyuter yana o'sha xabarni qayta qabul qilmaguncha, jarayon davom etaveradi.

Yulduzcha topologiyaga ega tarmoqlar markaziy tugunga ega (kommutator yoki kontsentrator). Mazkur markaziy tugunga barcha qolgan kompyuterlar ulanadi. Dastlab uzatilgan xabar ana shu qurilmaga kelib tushadi, so'ng boshqa kompyuterlarga uzatiladi.

Lokal tarmoqlarning qo'llanish sohasi juda keng. Bunga ofis ishlarini avtomatlashtirish, korxona boshqaruv sistemalari, loyixalarni avtomatlashtirish texnologik jarayonlari va robototexnika komplekslari, bank va axborot sistemalari, elektron pochta sistemalarini boshqarish kiradi.

Bugungi kunda barcha obyektlarning lokal kompyuter tarmoqlari asosan shisha ya'ni optik kabellarda tuzilgan va juda katta tezlikda ishlaydigan bo'lganligi uchun biz ularni kengroq ko'rib chiqamiz.

FDDI - inglischa Fiber Distributed Data Interface ya'ni ma'lumotlarni optik tolada tarqatish interfeysi hisoblanib, lokal maxalliy tarmoqlarning yangi standarti bo'lib, Amerikaning milliy instituti tomonidan ANSI standarti taklif qilingan.

Ushbu tarmoqdagi ma'lumotlar uzatish tezligi 10 Ggbit/sek. mo'ljallangan.

Bundan tashqari, ushbu tarmoqning yutug'i bu juda yuqori darajada tashqi xalaqitlardan himoyalanganligi, uzatilayotgan ma'lumotlarni maksimal sirliligini saqlashdan iboratdir. Katta tezligining yutug'i bu video tasvirlarni real vaqtda yetkazib berish va uzatish kanallarining uzunligi bir necha kilometrgacha kuchaytirgichsiz ishlatilishi hisoblanadi.

FDDI standarti asosida IEEE 802.5 (Token-Ring) tarmog'i yaratilgan. Ushbu tarmoq xalqasimon topologiyasiga ega.

Ushbu IEEE 802.5 (Token-Ring) halqasimon strukturaga ega bo'lgan kompyuter tarmog'i 2 ta optik kabelda yaratilgan bo'lib, kabelning biri zahirada (rezerv) ya'ni ikki tomonlama dupleks rejimida ma'lumotlarni uzatishi mumkin. Shuning uchun uzatish tezligi 200 Mbit/sek.

Yulduzsimon va xalqa topologiyasi birgalikda ishlatilishi mumkin.

FDDI tarmog'ining asosiy texnik harakteristikalari quyidagicha:

- tarmoqdagi maksimal abonentlar soni– 1000ta;
- xalqasimon tarmoqning maksimal uzunligi – 20 km;
- tarmoqdagi abonentlarning maksimal oralig'i – 2 km;

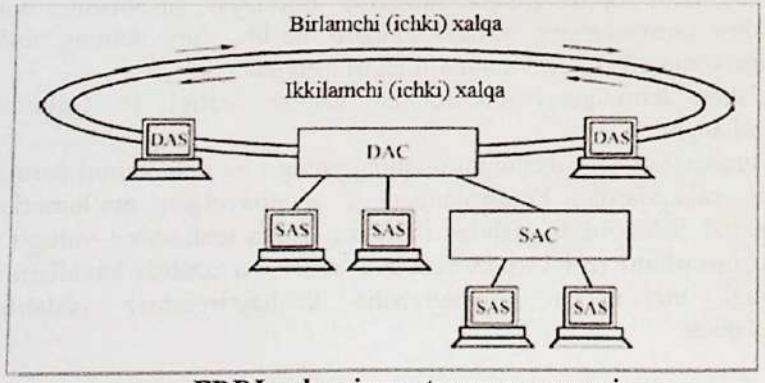
Ma'lumotlar uzatish aloqa kanallari sifatida ko'p modali optik tolali kabellari ishlatiladi.

Uzatish tezligi – 10 Ggbit/sek (dupleksda – 20 Ggbit/sek.)

FDDI tarmog'ining Fast Ethernet ga nisbatan yutug'i tarmoqning kattaligi va ulanish vaqtining juda kichikligi hisoblanadi, ya'ni tarmoqning umumiy uzunligi 20 km bo'lganligi bilan signalning so'nishligi farq o'ynamaydi, eng asosiysi tarmoqqa kirish va uzatish vaqtining kichikligi hisoblanadi.

Bir modali optik kabel ishlatilganda abonentlar orasidagi masofa 45 km gacha, umumiy masofa 200 km gacha bo'lishi mumkin.

Agar UTP elektr kabelining 5 kategoriyasini ishlatib RJ-45 konnektori orqali bog'langanda ham abonentlar orasidagi masofa 100 metrdan oshmaydi.



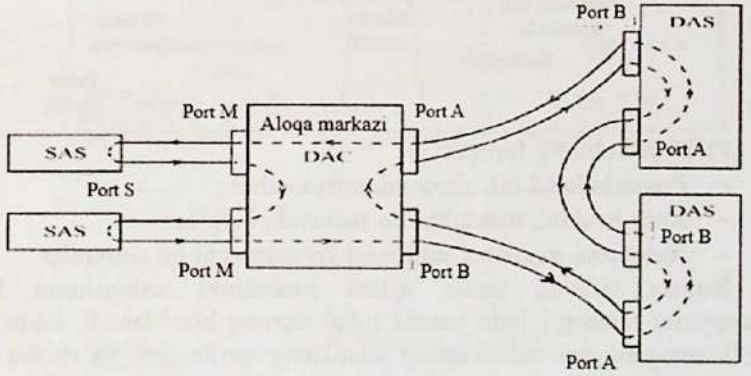
FDDI xalqasimon tarmoq sxemasi

FDDI tarmog'ining 4 xil porti bor:

- "A" porti ikki tomonlama ulanish uchun, ya'ni kirish qismi tashqi xalqaga ulanish uchun, chiqish qismi esa ichki xalqaga ulanish uchun mo'ljallangan.
- "V" porti ikki tomonlama ulanish uchun, ya'ni uning kirish tomoni ichki xalqaga, a chiqish tomoni tashqi halqaga (A-B ga), (B-A ga) ulanadi.
- "M" (Master) porti ikki konstentratorni bir biri bilan bog'lash uchun. "M" port "S" port bilan ulanadi.
- "S" (Stave) porti faqat bir tamonlama konstentrator bilan abonentni ulash uchun mo'ljallangan. "S" port "M" port bilan bog'lanadi.

Konstentratorlar ikki hil ulanishga mo'ljallangan bo'ladi. Ya'ni DAS - Dual-Attachment Concentrator – Ikkilamchi bog'lanish konstentratori va SAC- Single- Attachment Concentrator – Yagona (birlamchi) bog'lanish konstentratori bo'ladi.

Shuning uchun SAC konstentratori bitta S porti birlamchi xalqa uchun va bir nechta M portlari orqali abonentlarni DAS konstentratoriga ulashga mo'ljallangan bo'ladi.



FDDI tarmog'ida aloqa kontsentratori orqali bog'lanish sxemasi

FDDI tarmoq stanstiyasining abonentlari va konstentratorlaridan tashqari yonlab o'tish (bypass switch) konstentratorlari ishlatilishi mumkin.

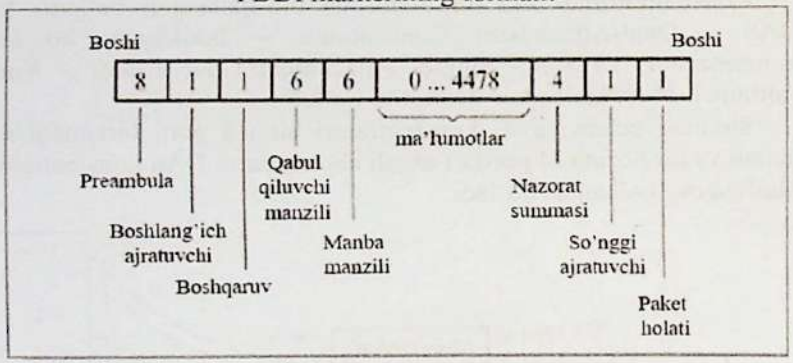
Ushbu kommutatorlar uzilgan abonentlarning elektr signallari orqali o'ziga ulatib tarmoqqa bog'lab qo'yadi.

Albatta, yonlab (aylanib) o'tish davrida qo'shimcha signallarni so'nish darajasi oshadi ya'ni 2,5 dB gacha bir kommutator uchun.

Tarmoqdagi markerning borib qaytish vaqtiga qarab asosiy ma'lumotni jo'natish kerak yoki kerak emasligi aniqlanadi. Ya'ni agar marker tez qaytib kelsa, demak tarmoq kanallari ancha bo'sh hisoblanib asosiy ma'lumot uzatilaboshlaydi. Agar kech vaqt ichida kelsa, demak kanallar band, asosiy ma'lumot uzatilmay kutib turadi.

Preambula (8 bayt)	Boshlang'ich ajratuvchi (1 bayt)	Boshqaruv (1 bayt)	So'nggi ajratuvchi (1 bayt)	Paket holati (1 bayt)

FDDI markerining formati:



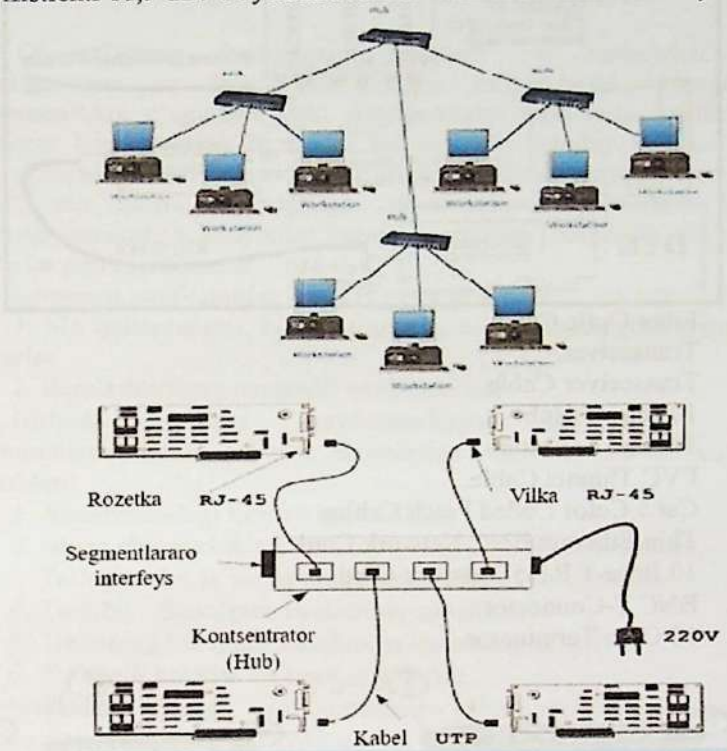
FDDI paketining formati:

- Preambula 64 bit. sinxronizastiya uchun;
- Kadr boshini, manzilini ko'rsatuvchi belgilar;
- Xatolarni, manzilni aniqligini ko'rsatuvchi bit simvollar.

Xulosa sifatida shuni aytish mumkinki xalqasimon FDDI kompyuter tarmog'i juda yaxshi lokal tarmoq hisoblanadi, lekin keng qo'llanmaganligiga sabab uning texnikaviy qurilmalari va shisha tolali optik kabellarining narxi xozirgi kunda ancha yuqori bo'lganligi sabab bo'lmoqda.

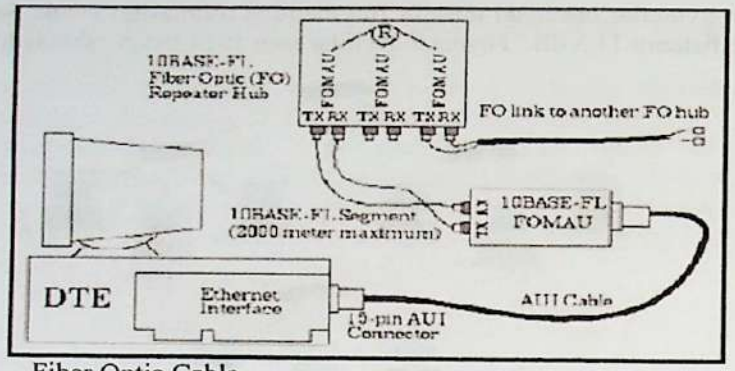
10Base-T yoki Ethernet tarmog'i ushbu yulduzsimon yoki daraxtsimon topologiyada bo'lishi mumkin va 2 ta para kabel ishlatiladi. HUB orqali ulanadi. Biri uzatishga, ikkinchisi qabul qilishga.

Kompyuterlar orasidagi masofa 100 metrdan oshmasligi kerak. So'nish koeffistienti 11,5 dB. Foydalanuvchilar soni 1024 tadan oshmaydi.

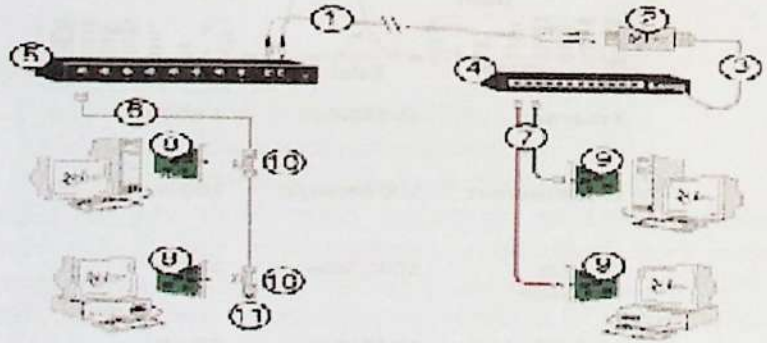


Ethernet	10 Мбит/с	2 500 м
Fast Ethernet	100 Мбит/с	200 м
Gigabit Ethernet	1000 Мбит/с	200 м
10G Ethernet	10 Гбит/с	40 км

10 Base-F standarti. Ushbu lokal kompyuter tarmog'i asosan shisha tolali optik kabellarda yaratilgan bo'ladi.



1. Fiber Optic Cable.
2. Transceiver.
3. Transceiver Cable.
4. 10 Base T Hub.
5. Thinnet Repeater.
6. PVC Thinnet Cable.
7. Cat 5 Color Coded Patch Cables.
8. Thin Ethernet BNC Network Card.
9. 10 Base-T RJ45 Network Card.
10. BNC T-Connector.
11. 50 Ohm Terminator.



Yuqorida keltirilganlar asosida obyektlarning himoya vositalarini aniqlash uchun ularning bog'lanish strukturasi katta ahamiyatga ega bo'ladi.

1.4. Obyektlarning kompyuter tizimi va tarmoqlarida hosil bo'ladigan xavf-xatar, risk va hujum turlari

Obyektlarning kompyuter tizimlari va tarmoqlari orqali uzatilayotgan va qabul qilanayotgan jarayonlarda axborotlarning mazmunining o'zgarishi yoki uzatilayotgan jarayonda uzilib qolishi axborot himoyasining buzulishi hisoblanadi. Bunday holatlar barcha obyektlarning ichki tarmoqlarida albatta bo'lish mumkin. Har qanday kompyuter tizimi (tarmog'i)ga ziyon yetkazishi mumkin bo'lgan sharoit, harakat va jarayonlar kompyuter tizimi (tarmog'i) uchun xavf-xatarlar deb hisoblanadi.

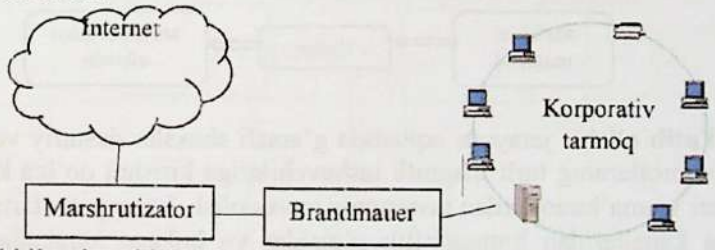
Umuman xavf-xatarlar 2 (ikki) turga bo'linadi:

1. Mo'ljallanmagan, ko'zda tutilmagan, maqsadsiz (tasodifiy) xavf-xatarlar.
2. Rejalashtirilgan maqsadli xavf-xatarlar.

Birinchi turdagi xavf-xatarlarga quyidagilar kiradi. Avtomatlashtirilgan axborot tizimlariga tasodifiy ta'sir ko'rsatish sabablari:

1. Apparaturadagi to'xtab qolishliklar.
2. Ishlab chiquvchining sxematik, texnik va tizimli xatolari.
3. Tashqi muhit ta'sirida aloqa kanallaridagi to'sqinliklar.
4. Tarkibiy, algoritmik va dasturiy xatoliklar.
5. Tizimning bir qismi sanaluvchi insonning xatosi.
6. Xalokatli holatlar va boshqa ta'sirlar.

Ikkinchi turdagi xavf-xatarlarga jinoyatchilar, buzuvchilar tomonidan tahdid asosida yoki qandaydir maqsad asosida bajariladigan harakatlar kiradi.



Tashkilotning himoyalash sistemasiga bo'lgan haqiqiy ehtiyojini aniqlash va xavfsizlikning mavjud barcha xilma-xil choralaridan kerakligini tanlashda turli yondashuvlardan foydalaniladi. Bunday

yondashuvlardan biri axborot himoyasining quyidagi uchta jihatiga asoslangan.

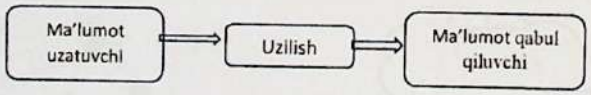
1. Himoyaning buzilishlari. Korxonaga tegishli axborotni saqlash va ishlatish xavfsizligiga zarar keltiruvchi har qanday harakatlar.

2. Himoya mexanizmi. Himoyaning buzilishlarini aniqlash va bartaraf etish hamda buzilishlar oqibatini yo'qotish mexanizmlari.

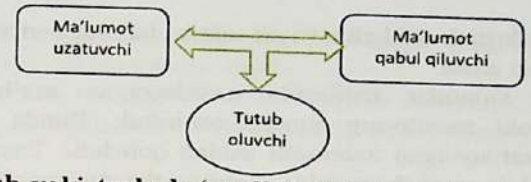
3. Himoya xizmati. Ma'lumotlarni ishlash sistemalari va korxonaga tegishli axborotni tashish xavfsizligi saviyasini ko'tarishga mo'ljallangan servis xizmati.

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

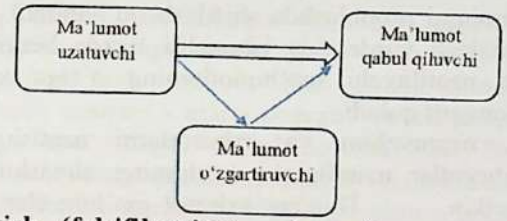
- uzilish - qandaydir tashqi harakatlar (ishlar, jarayonlar)ni bajarish uchun hozirgi ishlarni vaqtincha markaziy protsessor qurilmasi yordamida to'xtatishdir, ularni bajargandan so'ng protsessor oldingi holatga qaytadi va to'xtatib qo'yilgan ishni davom ettiradi. Har bir uzilish tartib raqamiga ega,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



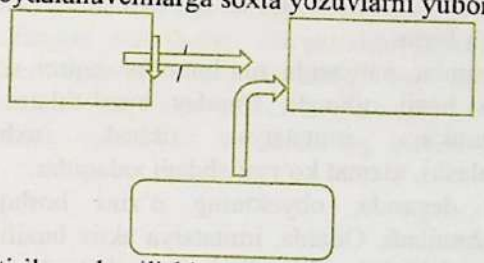
Tutib olish - jarayoni oqibatida g'arazli shaxslar dasturiy vositalar va axborotlarning turli magnitli tashuvchilariga kirishni qo'lga kiritadi. Dastur va ma'lumotlardan noqonuniy nusxa olish, kompyuter tarmoqlari aloqa kanallaridan nomualliflik o'qishlar va hokazo harakatlar tutib olish jarayonlariga misol bo'la oladi.



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



Soxtalashtirish (falsifikatsiya) - ham jarayon sanalib, uning yordamida g'arazli shaxslar tizimda hisobga olinmagan vaziyatlarni o'rganib, undagi kamchiliklarni aniqlab, keyinchalik o'ziga kerakli harakatlarni bajarish maqsadida tizimga qandaydir soxta jarayonni yoki tizim va boshqa foydalanuvchilarga soxta yozuvlarni yuboradi.



Yuqorida keltirilgan buzilishlar passiv va aktiv hujum atamalari bo'yicha klassifikatsiyalanganida passiv tahdidga ushlab qolish (perexvat) mansub bo'lsa, uzish (raz'edinenie), turlash (modifikatsiya)

va soxtalashtirish (falsifikatsiya) aktiv tahdidga mansub ekanligini ko'rish qiyin emas.

Passiv hujumlar natijasida uzatilayotgan ma'lumotlar ushlab qolinadi yoki monitoring amalga oshiriladi. Bunda buzg'unchining maqsadi uzatilayotgan axborotni ushlab qolishdir. Passiv buzilishlarni ikkita guruhga ajratish mumkin - axborotlar mazmunini fosh etish va ma'lumotlar oqimini tahlil etish.

Axborotlar mazmunini fosh etish nima ekanligi ma'lum. Telefon orqali suhbatda, elektron pochta axborotida yoki uzatilayotgan faylda muhim yoki maxfiy axborot bo'lishi mumkin. Tabiiyki, bunday axborot bilan bu axborot mo'ljallanmagan shaxslarning tanishishi maqbul emas. Ma'lumotlar oqimining tahlili mukammalroq hisoblanadi.

Faraz qilaylik, biz axborot yoki boshqa uzatiluvchi ma'lumotlar mazmunini shunday niqoblaylikki, buzuvchi axborotni o'z ixtiyoriga kiritganida ham undagi axborotni chiqarib ololmasin. Ko'pincha axborot mazmunini niqoblashda shifrlash qo'llaniladi. Ammo axborot mazmuni shifrlash yordamida ishonchli tarzda berkitilgan bo'lsada, buzg'unchida uzatiluvchi ma'lumotlarning o'ziga xos alomatlarini kuzatish imkoniyati qoladi.

Masalan, uzatuvchini va axborotlarni uzatishga ishlatiluvchi uzellarni, axborotlar uzunligini va ularning almashinuv chastotasini aniqlash mumkin. Bunday axborot ma'lumotlar almashinuvidan ko'zlangan maqsadni aniqlashda juda ham qo'l keladi. Himoyaning passiv buzilishlarini aniqlash juda qiyin, chunki ularda ma'lumotlarga qandaydir o'zgartirishlar kiritish ko'zda tutilmaydi. Ammo bunday xil buzilishlarning oldini olishni amalga oshirsa bo'ladi. Shu sababli passiv buzilishlar holida e'tiborni ularni aniqlashga emas, balki ularning oldini olishga qaratish lozim.

Aktiv hujumlar natijasida ma'lumotlar oqimi o'zgartiriladi yoki soxta oqimlar hosil qilinadi. Bunday buzilishlarni to'rtta guruhga ajratish mumkin: imitatsiya, tiklash, axborotni turlash (modifikatsiyalash), xizmat ko'rsatishdagi xalaqitlar.

Imitatsiya deganda, obyektning o'zini boshqa obyekt qilib ko'rsatishi tushuniladi. Odatda, imitatsiya aktiv buzilishlarning boshqa bir xilining urinishi bilan birgalikda bajariladi. Masalan, buzg'unchi sistemalar almashinayotgan autentifikatsiya ma'lumotlarining oqimini ushlab qolib so'ngra autentifikatsiya axborotlarining haqiqiy ketma-ketligini tiklashi mumkin. Bu esa vakolati chegaralangan obyektning

o'zini vakolati kengroq obyekt qilib ko'rsatishi (imitatsiya) orqali vakolatini kengaytirishiga imkon beradi.

Tiklash deganda, ma'lumotlar blokini passiv ushlab qolib, keyin uni ruxsat berilmagan natijani hosil qilish maqsadida retranslyasiya qilish tushuniladi.

Ma'lumotlarni modifikatsiyalash deganda, ruxsat berilmagan natijani hosil qilish maqsadida qonuniy axborot qismini o'zgartirish yoki axborot kelishi ketma-ketligini o'zgartirish tushuniladi.

Xizmat ko'rsatishdagi xalaqitlar aloqa yoki ularni boshqaruvchi vositalarning normal ishlashiga to'sqinlik qiladi. Bunday buzilishlarda muayyan maqsad ko'zlanadi: masalan, obyekt ma'lum adresatga yo'naltirilgan barcha axborotlarni to'xtatib qolishi mumkin. Yana bir misol, tarmoqni atayin axborotlar oqimi bilan ortiqcha yuklash orqali yoki tarmoqni ishdan chiqarish yo'li bilan barcha tarmoq ishini blokirovka qilish.

Himoyaning aktiv buzilishlarini butunlay oldini olish juda murakkab, chunki bunga faqat barcha aloqa vositalarini uzluksiz fizik himoyalash orqali erishish mumkin. Shu sababli himoyaning aktiv buzilishlarida asosiy maqsad - ularni operativ tarzda aniqlash va tezda sistemaning ishga layoqatliligini tiklash bo'lishi shart. Buzilishlarning o'z vaqtida aniqlanishi buzg'unchini to'xtatish vazifasini ham o'taydi va bu vazifani buzilishlardan ogohlantirish sistemasining qismi deb ko'rish mumkin.

I bob xulosasi

Ushbu bobda bizning monografiyamizda mavzuga taalluqli atamalar, terminlar, ta'riflar, hozirgu kunda axborot xavfsizligini boshqarish tizimining tushunchasi, uning tarixi, ushbu sohaga tegishli dunyoda qabul qilingan standartlar, obyektlarda ishlatilishi mumkin bo'lgan kompyuter tarmoqlarining umumiy har xil strukturalari keltirilgan hamda shu kompyuter tarmoqlarida xosil bo'lishi mumkin bo'lgan xavf-xatarlar, risklar va hujumlarning turlari keng yoritilib berilgan.

II BOB.
OBYEKTLARDA AXBOROT HIMOYASINING BUZILISHI, HIMOYA MEXANIZMI VA HIMOYA TURLARI

2.1. Obyektlardagi axborotlarni tashkiliy himoyalash vositalari

Bir necha yillar davomida o'tkazilgan ilmiy tadqiqotlar asosida barcha har xil turdagi va strukturali obyektlarning kompyuter tarmoqlarida saqlanayotgan, qayta ishlanayotgan, uzatilayotgan yoki qabul qilinayotgan axborotlani xavfsizligini ta'minlash uchun quyidagi 8 ta himoyalash vositalardan foydalanish mumkinligi aniqlandi:

1. Tashkiliy himoyalash vositalari.
2. Texnikaviy (uskunaviy) himoyalash vositalari.
3. Dasturiy himoyalash vositalari.
4. Huquqiy himoyalash vositalari.
5. Jismoniy (fizikaviy) himoyalash vositalari.
6. Kriptografik himoyalash vositalari.
7. Telekommunikatsiya tarmoqlarining aloqa liniyalarida axborotlarni himoyalash vositalari.
8. Kompyuter viruslaridan himoyalanish vositalari.

Ushbu axborotlarni havfsizligini ta'minlash vositalarini alohida alohida ko'rib chiqamiz.

Har bir obyekt uchun eng ko'p ishlatiladigan va juda katta samara beradigan tashkiliy himoyalash vositasi hisoblanar ekan. Umuman tashkiliy himoyalash vositasi 2 (ikki) turga bo'linadi:

1. Tashkiliy huquqiy himoyalash vositalari.
2. Tashkiliy texnikaviy himoyalash vositalari.

Tashkiliy huquqiy himoyalash vositalarga ushbu korxona, tashkilot, muassasa yoki firmaning o'ziga taalluqli binolari, xonalari va boshqa obyektlarining havfsizligini ta'minlash uchun ularning mas'ul xodimlarini aniqlab, buyruq yoki farmoyish asosida biriktirib qo'yadilar. Tasdiqlangan yo'riqnoma asosida nazorat olib boradilar va javobgar hisoblanadilar.

Tashkiliy texnikaviy (uskunaviy) vositalarga esa har bir obyekt xonadonining eshik, derazalariga qulflar, to'siq pardalar, kirish va chiqish eshiklari oldiga videokuzatuv qurilmalarini o'rnatishlar kiradi. Kompyuter xonalarining eshiklariga albatta elektron qulflar va signal beruvchi qurilmalar o'rnatilgan bo'lishi kerak.

Har bir korxona, tashkilot, muassasa yoki firmalarda yuqorida keltirilgan axborotlarni himoyalash vositalarining kamida 3 yoki 4 turlari albatta qo'llaniladi.

Axborotlarni tashkiliy himoyalash elementlari quyidagi keltirilgan.

Himoyalash texnologiyasi personali tashkilotning qimmatli axborotlarini himoyalash qoidalariga rioya qilishga undovchi boshqarish va cheklash xarakteriga ega bo'lgan chora-tadbirlarni o'z ichiga oladi. Tashkiliy himoyalash elementi boshqa barcha elementlarni yagona tizimga bog'lovchi omil bo'lib hisoblanadi. Ko'pchilik mutaxassislarning fikricha, axborotlarni himoyalash tizimlari tarkibida tashkiliy himoyalash 50—60 % ni tashkil qiladi. Bu hol ko'p omillarga bog'liq, jumladan, axborotlarni tashkiliy himoyalashning asosiy tomoni amalda himoyalashning prinsipi va usullarini bajaruvchi personalini tanlash, joylashtirish va o'rgatish hisoblanadi. Axborotlarni himoyalashning tashkiliy chora-tadbirlari tashkilot xavfsizligi xizmatining me'yoriy uslubiy hujjatlarida o'z aksini topadi.

Shu munosabat bilan ko'p hollarda yuqorida ko'rilgan tizim elementlarining yagona nomi — axborotni tashkiliy - huquqiy himoyalash elementini ishlatadilar.

Axborotlarni muxandis - texnik himoyalash elementi - texnik vositalar kompleksi yordamida hudud, bino va qurilmalarni qo'riqlashni tashkil qilish hamda texnik tekshirish vositalariga qarshi sust va faol kurash uchun mo'ljallangan. Texnik himoyalash vositalarining narxi baland bo'lsada, axborot tizimini himoyalashda bu element muhim ahamiyatga ega. Axborotni himoyalashning dasturiy-matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saqlanadigan qimmatli axborotlarni himoyalash uchun mo'ljallangan.

Shuning uchun quyidagilarni bilish kerak:

1. Axborotlarni uzatishda xavfsizlikni ta'minlashga qo'yiladigan talablarni bevosita quyidagi atamalardan aniqlash mumkin: konfidentsiallik, autentifikatsiya, yaxlitlikni saqlash, yolg'onning mumkin emasligi, foydalanuvchanlik, foydalanuvchanlikni boshqarish.

2. Ko'p xollarda yaratuvchi e'tiboridan chetda qolgan himoya sistemasining kamchiliklarini aniqlash maqsadida muammoga qarshi tomonning nuqtai nazaridan qarash lozim. Boshqacha aytganda, himoyaning u yoki bu mexanizmi yoki algoritmini yaratishda mumkin bo'lgan qarshi choralarni ham ko'rish lozim.

3. Himoya vositalaridan barcha qarshi choralar majmuasini hisobga olgan xolda foydalanish lozim.

4. Xavfsizlikni ta'minlash choralari sistemasi yaratilganidan so'ng bu choralarni qachon va qayerda qo'llash masalasini yechish lozim. Bu fizikaviy joy (ma'lum himoya vositasini qo'llash uchun tarmoq nuqtasini tanlash) yoki xavfsizlikni ta'minlovchi mantiqiy zanjirdagi joy (masalan, ma'lumot uzatuvchi protokol sathi yoki sathlarini tanlash) bo'lishi mumkin.

5. Himoya vositalari, odatda, ma'lum algoritm va protokoldan farqlanadi. Ularga binoan barcha himoyadan manfaatdor axborotning qandaydir qismi maxfiy bo'lib qolishi shart (masalan, shifr kaliti ko'rinishida). Bu esa, o'z navbatida, bunday maxfiy ma'lumotni yaratish, taqsimlash va himoyalash metodlarini ishlab chiqish zaruriyatini tug'diradi.

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

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

2.2. Texnikaviy (uskunaviy) himoyalash vositalari

Apparat (texnik) himoya vositalari - bu apparat darajasida amalga oshiriladigan axborot va axborot tizimlarini himoya qilish vositalaridir. Ular turli xil qurilmalar (mexanik, elektromexanik, elektron va boshqalar) apparat bilan axborot xavfsizligi muammolarini hal qiladi. Apparatga quyidagilar kiradi shovqin generatorlari, tarmoq filtrlari, radiolarni skanerlash va axborot oqimining potentsial kanallarini blokirovka qiluvchi yoki ularni aniqlashga imkon beruvchi boshqa

qurilmalar kiradi. Texnik vositalarning afzalliklari ularning ishonchliligi, subyektiv omillardan mustaqilligi, modifikatsiyaga yuqori chidamliligi bilan bog'liqligi hisoblanadi. Zaif tomonlar esa bu moslashuvchanlikning yetishmasligi, nisbatan katta hajm va vaznligi, yuqori narxi. Ushbu vositalar axborot tizimi xavfsizligining zaruriy qismidir, garchi apparat ishlab chiquvchilar odatda axborot xavfsizligi muammosini hal qilishni dasturchilarga qoldiradilar. Bugungi kunda apparat qurilmalari turli maqsadlar uchun mo'ljallangan bo'lib, ular quyidagilarga bo'linadi:

- xavfsizlik ma'lumotlarini saqlash uchun maxsus registrlar;
- parollar, kodlarni, vulturalarni yoki maxfiylik darajasini aniqlash maqsadida insonning shaxsiy xususiyatlarini (ovoz, barmoq izlari) o'lchash qurilmalari;
- ma'lumotlar chiqishining manzilini vaqti-vaqti bilan tekshirib turish maqsadida aloqa liniyasida axborot uzatilishini to'xtatish sxemalari, axborotlarni shifrlash qurilmalari (kriptografik usullar asosida), ishonchli kompyuter yuklash modullari hisoblanadi.

Texnik axborotni muhofaza qilishning asosiy vazifasi axborotlarni chiqib ketish kanallarini ya'ni radio, akustik, optik kanallarini aniqlash va ularni bloklashdan iborat bo'ladi.

Axborotni texnik himoya qilish muammolarini hal qilish uchun, axborotni muhofaza qilish va tugunlardan chiqib ketish kanallarini aniqlash va blokirovkalash uchun maxsus uskunalar bilan jihozlash sohasidagi mutaxassislarning mavjudligi ham katta ro'l o'ynaydi. Axborotni texnik himoya qilish uchun maxsus jihozlarni tanlash, bo'lishi mumkin bo'lgan tahdidlarni aniqlashga, obyektning xavfsizlik darajasini tahlil qilishga asoslanadi. Axborot xavfsizligini ta'minlovchi apparatga ruxsatsiz kirishdan himoya qilish uchun identifikatori ya'ni foydalanuvchini tarmoq yoki mahalliy kompyuterda avtorizatsiya qilish, elektron pochtani himoya qilish, axborot resurslariga xavfsizlikni ta'minlovchi aloqa liniyalaridan kirishni, shuningdek, shaxsiy ma'lumotlarning ishonchli saqlanishini ta'minlash uchun ishlatiladigan texnikaviy qurilmalar kiradi.

Korporativ, mahalliy tarmoqlari va axborot tizimlarida foydalanuvchilarni ishonchli parolsiz autentifikatsiya qilish uchun ixcham elektron qurilmalar va elektron qulflar qo'llaniladi.

Akustik ya'ni nutqiy axborotlarni muhofaza qilishning texnik vositalarining vazifasi axborotni oqish (chiqib ketish) kanallarini

bartaraf etish yoki olingan axborot sifatini ko'tarishdan iborat bo'ladi. Tushunarlilik nutqiy axborot sifatining asosiy ko'rsatkichi bo'lib hisoblanadi. Akustik axborotning sifati 40% ga yaqin syujetli tushunarlilikni ta'minlansa kifoya bo'ladi. Agar suhbatni amalga oshirish deyarli imkonsiz bo'lsa, unda bo'g'inli tushunarli bo'lishi 1-2% ga to'g'ri keladi. Akustik kanallar orqali axborot oqishining oldini olish passiv va faol himoya usullariga tushiriladi. Shunga ko'ra, barcha axborot xavfsizligi qurilmalarini xavfsiz ravishda ikkita katta sinfga ajratish mumkin - passiv va faol. Passiv-tashqi muhitga hech narsa kiritmasdan, oqish kanallarini o'lchash, aniqlash, lokalizatsiya qilish asosida amalga oshiriladi. Faol - "sun'iy shovqin qilish" asosida maxfiy ma'lumot olishning barcha turdagi maxsus vositalarini yo'q qilishdan iborat bo'ladi.

Himoya qilishning passiv texnik vositalari-himoya obyektini uning nurlanishini yutish, aks ettirish yoki sochish yo'li bilan razvedka qilishning texnik usullaridan yashirishni ta'minlovchi qurilma. Bular ekranlovchi qurilmalar va inshootlar, elektr ta'minoti tarmoqlarida ajratish qurilmalari, himoya filtrlaridir. Passiv usulning maqsadi-akustik signalni tovush manbaidan iloji boricha zaiflashtirish. masalan, devorlarni tovush yutuvchi materiallar bilan bezash. Bo'limlar va devorlar, iloji bo'lsa, qatlamli bo'lishi kerak, qatlamlarning materiallari keskin farq qiladigan akustik xususiyatlarga ega (masalan, beton-ko'pikli kauchuk) tanlanadi. Membranani tashishni kamaytirish uchun ular massiv bo'lishi maqsadga muvofiqdir. Bundan tashqari, eshiklarni ular orasidagi havo bo'shlig'i va uy perimetri bo'ylab qistirmalarni yopish yanada to'g'ri bo'ladi. Axborotni oynadan chiqib ketishini himoya qilish uchun oynalarni ikki qavatli qilish kerak bo'ladi.

Demak, texnikaviy vositalar sifatida elektr, elektromexanik va elektron qurilmalar tushuniladi. Texnikaviy vositalar o'z navbatida, apparatli va fizikaviy bo'lishi mumkin.

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

Fizikaviy texnik vositalar — bu avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, oddiy eshik qulflari, derazada o'rnatilgan temir

panjaralar, qo'riqlash elektr uskunalari fizikaviy texnik vositalarga kiradi.

2.3. Dasturiy himoyalash vositalari

Bu axborotlarni himoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus dasturiy ta'minotdir. Axborotlarni himoyalashda birinchi navbatda eng keng qo'llanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parol tizimini keltirish mumkin.

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

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

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

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

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

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

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

Stoxastik testlarni tashkillashtirish vositalari — axborot tizimlarining sifati va ishonchliligini tekshirishda qo'llaniladigan vositadir.

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

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

Statistik tahlilgichlar — dasturlarning tuzilish tarkibidagi kamchiliklarni aniqlash, dasturlar kodida aniqlanmagan kirish va chiqish nuqtalarini topish, dasturdagi o'zgaruvchilarni to'g'ri aniqlanganligini va ko'zda tutilmagan ishlarni bajaruvchi qism dasturlarini aniqlashda foydalaniladi.

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

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

Misol sifatida quyidagi vositalarni keltirish mumkin:

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

Security Administrator Tool for ANALYZING Networks (SATAN) — dasturiy ta'minot bo'lib, bevosita tarmoqning zaif tomonlarini aniqlaydi va ularni bartaraf etish yo'llarini ko'rsatib beradi. Ushbu yo'nalish bo'yicha bir necha dasturlar ishlab chiqilgan, masalan: Internet Security Scanner, Net Scanner, Internet Scanner va boshqalar.

NBS tizimi — dasturiy-texnik vosita bo'lib, aloqa kanallaridagi ma'lumotlarni himoyalashda qo'llaniladi;

Free Space Communication System — tarmoqda ma'lumotlarning har xil nurlar orqali, masalan lazerli nurlar orqali almashuvini ta'minlaydi;

SDS tizimi — ushbu dasturiy tizim ma'lumotlarni nazorat qiladi va qaydnomada aks ettiradi. Asosiy vazifasi ma'lumotlarni uzatish vositalariga ruxsatsiz kirishni nazorat qilishdir;

Timekey — dasturiy-texnik uskunadir, bevosita EHMning parallel portiga o'rnatiladi va dasturlarni belgilangan vaqtda keng qo'llanilishini taqiqlaydi;

IDX — dasturiy-texnik vosita, foydalanuvchining barmoq izlarini «o'qib olish» va uni tahlil qiluvchi texnikalardan iborat bo'lib, yuqori sifatli axborot xavfsizligini ta'minlaydi. Barmoq izlarini o'qib olish va xotirada saqlash uchun 1 minutgacha, uni taqqoslash uchun esa 6 sekundgacha vaqt talab qilinadi.

2.4. Qonuniy himoyalash vositalari

Bu davlat tomonidan ishlab chiqilgan huquqiy hujjatlar sanaladi. Ular bevosita axborotlardan foydalanish, qayta ishlash va uzatishni tartiblashtiradi va ushbu qoidalarni buzuvchilarning mas'uliyatlarini aniqlab beradi. Bularga O'zbekiston Respublikasida ishlab chiqilib Oliy Kengash tamonidan tasdiqlangan axborot xavfsizligiga taalluqli qonunlar kiradi.

1994-yil 6 -mayda birinchi bo'lib "Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazalarining xuquqiy himoyasi to'g'risida"gi O'zbekiston RespublikaQonuni qabul qilingan edi[1].

1999-yildagi № 822-I raqamli "Telekommunikatsiyalar to'g'risida"gi, 2002-yildagi "Axborot erkinligi printsiplari va kafolatlari to'g'risida"gi[2], 2003-yildagi "Axborotlashtirish to'g'risida"gi[3] va shu yilda "Elektron raqamli imzo to'g'risida"gi[4], 2004-yildagi "Elektron nazorat to'g'risida" va "Elektron hujjat aylanishi to'g'risida"gi[5] va boshqa ko'p qonunlar qabul qilingan.

Yuqorida keltirilgan barcha Prezident Farmon, farmoyish va qarorlarni hamda O'zbekiston Respublikasi Vazirlar Mahkamasining axborotlarni xavfsisligini boshqarish yuzasidan chiqarilgan qarorlarini bajarish majburiy hisoblanadi.

2.5. Axborotni himoyalashning kriptografik usuli. Zamonaviy kompyuter stenografiyasi

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

Axborotni himoyalash uchun kodlashtirish va kriptografiya usullari qo'llaniladi.

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

Kriptografiya deb maxfiy xabar mazmunini shifrlash, ya'ni ma'lumotlarni maxsus algoritm bo'yicha o'zgartirib, shifrlangan matnni

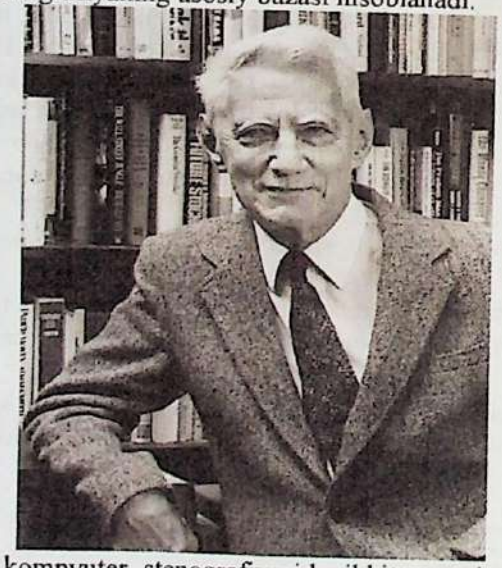
[1] https://lex.uz/uz/docs/-143983
[2] https://lex.uz/uz/docs/-52268
[3] https://lex.uz/uz/docs/-83472
[4] https://lex.uz/uz/docs/-64467
[5] https://lex.uz/uz/docs/-165079

yaratish yo'li bilan axborotga ruxsat etilmagan kirishga to'siq qo'yish usuliga aytiladi.

Kompyuter texnologiyalari stenografiyaning rivojlanishi va mukammallashuviga yangi turtki berdi. Natijada axborotni himoyalash sohasida yangi yo'nalish — kompyuter stenografiyasi paydo bo'lgan. Global kompyuter tarmoqlari va multimedia sohasidagi zamonaviy progress telekommunikatsiya kanallarida ma'lumotlarni uzatish havfsizligini ta'minlash uchun mo'ljallangan yangi usullarni yaratishga olib keldi. Bu usullar shifrlash qurilmalarining tabiiy noaniqligidan va analogli video yoki audio-signallarning serobligidan foydalanib, xabarlarni kompyuter fayllari (konteynerlar)da yashirish imkonini beradi.

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

Klod Élvud Shénnon (ingl. Claude Elwood Shannon; 1916-yil 30-aprel, Michigan, AQSh) sirli yozuvning umumiy nazariyasini yaratgan, u fan sifatida stenografiyaning asosiy bazasi hisoblanadi.



Zamonaviy kompyuter stenografiyasida ikkita asosiy fayl turlari mavjud: yashirish uchun mo'ljallangan xabar-fayl va konteyner-fayl, u

xabarni yashirish uchun ishlatilishi mumkin. Bunda konteynerlar ikki turda bo'ladi: konteyner-origanal (yoki «bo'sh» konteyner) - bu konteyner yashirin axborotni saqlamaydi; konteyner-natija (yoki «to'ldirilgan» konteyner) - bu konteyner yashirin axborotni saqlaydi. Kalit sifatida xabarni konteynerga kiritib qo'yish tartibini aniqlaydigan maxfiy element tushuniladi.

2.6. Kompyuter stenografiyasining istiqbollari

Kompyuter stenografiyasi rivojlanish tendentsiyasining tahlili shuni ko'rsatadiki, keyingi yillarda kompyuter stenografiyasi usullarini rivojlantirishga qiziqish kuchayib bormoqda. Jumladan, ma'lumki, axborot xavfsizligi muammosining dolzarbligi doim kuchayib bormoqda va axborotni himoyalashning yangi usullarini qidirishga rag'batlantirilayapti. Boshqa tomondan, axborot-kommunikatsiya texnologiyalari (AKT)ning jadal rivojlanishi ushbu axborotni himoyalashning yangi usullarini joriy qilish imkoniyatlari bilan ta'minlayapti, va albatta, bu jarayonning kuchli katalizatori bo'lib umumfoydalaniladigan Internet kompyuter tarmog'ining juda kuchli rivojlanishi hisoblanadi.

Hozirgi vaqtda axborotni himoyalash eng ko'p qo'llanilayotgan soha bu — kriptografik usullardir. Lekin, bu yo'lda kompyuter viruslari, «mantikiy bomba»lar kabi axborotiy qurollarning kriptovositalarni buzadigan ta'siriga bog'liq ko'p yechilmagan muammolar mavjud. Boshqa tomondan, kriptografik usullarni ishlatishda kalitlarni taqsimlash muammosi ham bor. Shuning uchun kompyuter stenografiyasi hozirgi kunda axborot havfsizligi bo'yicha asosiy texnologiyalardan biri bo'lib hisoblanadi.

Kompyuter stenografiyasining asosiy vazifalarini ko'rib chiqamiz.

Zamonaviy kompyuter stenografiyasining asosiy holatlari quyidagilardan iborat:

- yashirish usullari faylning autentifikatsiyalanishligini va yaxlitligini ta'minlashi kerak;
- yovuz niyatli shaxslarga qo'llaniluvchi steganografiya usullari to'liq ma'lum deb faraz qilinadi;
- usullarning axborotga nisbatan xavfsizlikni ta'minlashi ochiq uzatiladigan faylning asosiy xossalarini stenografik almashtirishlar bilan saklashga va boshqa shaxslarga noma'lum bo'lgan qandaydir axborot — kalitga asoslanadi;

- agar yovuz niyatli shaxslarga xabarni ochish vaqti ma'lum bo'lib qolgan bo'lsa, maxfiy xabarning o'zini chiqarib olish jarayoni murakkab hisoblash masalasi sifatida tasavvur qilinishi lozim.

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

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

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

II bob xulosasi

Ushbu bobda bugungi kunda obyektlarda eng ko'p ishlatilayotgan axborotlarni himoyalash vositalaridan tashkiliy, texnikaviy (uskunaviy) dasturiy, qonuniy hamda axborotlarni himoyalashning kriptografik usullari tahlil qilinib, obyektlarning faoliyatiga qarab tanlab olishlari taklif etilgan.

III BOB.
OBYEKTLARDA KONFIDENTSIAL AXBOROTLARNI RUXSATSIZ KIRISHDAN HIMOYALASH

3.1. Mualliflik huquqlarini himoyalash

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

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

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

Windows operatsiya muxitida ishlovchi dasturlar quyidagilardan iborat:

-Steganos for Windows dasturi ishlatishda juda yengil bo'lib, ayni paytda fayllarni shifrlash va ularni BMP, DIB, VOC, WAV, ASCII, HTML kengaytmali fayllar ichiga joylashtirib yashirishda juda qudratli hisoblanadi;

-Contraband dasturi 24-bitli BMP formatdagi grafik fayllar ichida har qanday faylni yashira olish imkoniyatiga ega.

DOS muhitida ishlovchi dasturlar:

-Jsteg dasturi ma'lumotni JPG formatli fayl lar ichiga yashirish uchun mo'ljallangan;

- FFEncode dasturi ma'lumotlarni matnli fayllar ichida yashirish imkoniyatiga ega;

- StegoDOS dasturlar paketining axborotni tasvirda yashirish imkoniyati mavjud;

- Winstorm dasturlar paketa PCX formatli fayllar ichiga xabarni shifrlab yashiradi.

OS/2 operatsion tizimida ishlovchi dasturlar:

- Texto dasturi ma'lumotlarni ingliz tilidagi matnga aylantiradi;

- Hide4PGP ver. 1.1 dasturi BMP, WAV, VOC formatli fayllar ichiga ma'lumotlarni yashirish imkoniyatiga ega.

Macintosh kompyuterlari uchun mo'ljallangan dasturlar:

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

Obyektlarda qo'llanilayotgan kompyuterlarining operatsion tizimlariga qarab tanlab olishlari mumkin.

3.2. Axborotlarni kriptografik himoyalash usullari

«Kriptografiya» atamasi dastlab «yashirish, yozuvni berkitib qo'ymoq» ma'nosini bildirgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya'ni diskda saqlanadigan sonlar ko'rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko'rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo'lgan har qanday axborotga nisbatan qo'llash mumkin.

Axborotning yaxlitligini tekshirishning bunday jarayoni, ko'p hollarda, axborotning haqiqiyligini ta'minlash deyiladi. Kriptografiyada qo'llaniladigan usullar ko'p bo'lmagan o'zgartirishlar bilan axborotlarning haqiqiyligini ta'minlashi mumkin. Nafakat axborotning kompyuter tarmog'idan ma'nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch hosil qilish juda muhim. Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiqlovchi turli usullar ma'lum. Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo'lmagan protsedura hisoblanadi. Chunki parolni qo'liga kiritgan har qanday shaxs axborotdan foydalanishi mumkin bo'ladi.

Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish va ularni kriptografik usullar bilan himoyalash mumkin, lekin kriptografiya bundan kuchliroq parolni uzluksiz o'zgartirish imkonini beradigan protseduralarni ham ta'minlaydi. Kriptografiya sohasidagi oxirgi yutuqlaridan biri — raqamli signatura — maxsus xossa bilan axborotni to'ldirish yordamida yaxlitlikni ta'minlovchi usul, bunda axborot uning muallifi bergan ochiq kalit ma'lum bo'lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik tekshiriladigan ma'lum usullardan ko'proq afzalliklarga ega.

Kriptografiya usullarini qo'llashning ba'zi birlarini ko'rib chiqamiz. Uzatiladigan axborotning ma'nosini yashirish uchun ikki xil o'zgartirishlar qo'llaniladi: kodlashtirish va shifrlash. Kodlashtirish uchun tez-tez ishlatiladigan iboralar to'plamini o'z ichiga oluvchi kitob yoki jadvallardan foydalaniladi. Bu iboralardan har biriga, ko'p hollarda, raqamlar to'plami bilan beriladigan ixtiyoriy tanlangan kodli so'z to'g'ri keladi. Axborotni kodlash uchun xuddi shunday kitob yoki jadval talab qilinadi.

Kodlashtiruvchi kitob yoki jadval ixtiyoriy kriptografik o'zgartirishga misol bo'ladi.

Kodlashtirishning axborot texnologiyasiga to'g'ri keladigan talablar — qatorli ma'lumotlarni sonli ma'lumotlarga aylantirish va aksincha o'zgartirishlarni bajara bilish. Kodlashtirish kitobini tezkor hamda tashqi xotira qurilmalarida amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik tizimni muvaffaqiyatli deb bo'lmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, u holda maxsus kodlarning yangi kitobini yaratish va uni hamma foydalanuvchilarga tarqatish zaruriyati paydo bo'ladi.

Kriptografik o'zgartirishning ikkinchi turi shifrlash o'z ichiga — boshlang'ich matn belgilarini anglab olish mumkin bo'lmagan shaklga o'zgartirish algoritmlarini qamrab oladi. O'zgartirishlarning bu turi axborot-kommunikatsiyalar texnologiyalariga mos keladi. Bu yerda algoritmni himoyalash muhim ahamiyat kasb etadi. Kriptografik kalitni qo'llab, shifrlash algoritmining o'zida himoyalashga bo'lgan talablarni kamaytirish mumkin.

Himoyalash obyekti sifatida faqat kalit xizmat kiladi. Agar kalitdan nusxa olingan bo'lsa, uni almashtirish mumkin va bu kodlashtiruvchi kitob yoki jadvalni almashtirishdan yengildir. Shuning uchun ham kodlashtirish emas, balki shifrlash axborot-kommunikatsiyalar texnologiyalarida keng ko'lamda qo'llanilmoqda. Sirli (maxfiy) aloqalar sohasi kriptologiyafiya deb aytiladi.

Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta'minlaydi. Masalan, to'lov varaqlarini elektron pochta orqali uzatishda uning o'zgartirilishi yoki soxta yozuvlarning qo'shilishi mumkin. Bunday hollarda axborotning yaxlitligini ta'minlash zaruriyati paydo bo'ladi. Umuman olganda kompyuter tarmog'iga ruxsatsiz kirishning mutlaqo oldini olish mumkin emas, lekin ularni aniqlash

mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko'p hollarda, axborotning haqiqiyligini ta'minlash deyiladi.

Ushbu kriptografiya so'z yunoncha «kripto» — sirli va «logus» — xabar ma'nosini bildiruvchi so'zlardan iborat. Kriptologiya ikki yo'nalish, ya'ni kriptografiya va kriptotahlildan iborat.

Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta'minlashdan iborat.

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

Hozirgi kunda kriptotizimni ikki sinfga ajratish mumkin:

- simmetriyali bir kalitlilik (maxfiy kalitli);
- asimmetriyali ikki kalitlilik (ochiq kalitli).

Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

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

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

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

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

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

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

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

Kriptografiya - ma'lumotlarni o'zgartirish usullarining to'plami bo'lib, ma'lumotlarni himoyalash bo'yicha quyidagi ikkita asosiy

muammolarni hal qilishga yo'naltirilgan: maxfiylik; yaxlitlilik. Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o'zgartira olmaslik haqida dalolat beradi. Bu yerda kalit qandaydir ximoyalangan kanal orqali jo'natiladi. Umuman olganda, ushbu mexanizm simmetriyali bir kalitlik tizimiga taalluqlidir.

3.3. Asimmetriyali ikki kalitlik kriptografiya tizimi

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

Yovuz niyatli shaxslar o'z maqsadlariga erisha olmasa va kriptotahlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u holda kriptotizim kriptomustahkam tizim deb aytiladi. Kriptotizimning mustahkamligi uning kaliti bilan aniqlanadi va bu kriptotahlilning asosiy qoidalaridan biri bo'lib hisoblanadi. Ushbu ta'rifning asosiy ma'nosi shundan iboratki, kriptotizim barchalarga ma'lum tizim hisoblanib, uning o'zgartirilishi ko'p vaqt va mablag' talab qiladi, shu bois ham faqatgina kalitni o'zgartirib turish bilan axborotni himoyalash talab qilinadi.

Simmetriyali kriptotizimda asosan bitta kalit ishlatiladi va himoyashda shifrlarga nisbatan quyidagi talablar qo'yiladi:

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

Ushbu talablarga quyidagi tizimlar javob beradi:

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

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

Almashtirish shifrlash usuli bo'yicha boshlang'ich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtiriladi.

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

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

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

— shifrlovchi jadval;

— sehrli kvadrat.

Shifrlovchi jadval usulida kalit sifatida quyidagilar qo'llaniladi:

- jadval o'lchovlari;
- so'z yoki so'zlar ketma-ketligi;
- jadval tarkibi xususiyatlari.

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

Hozirgi vaqtda kompyuter tarmoqlarida tijorat axborotlari bilan almashishda uchta asosiy algoritmlar, ya'ni DES, CLIPPER va PGP algoritmlari qo'llanilmoqda. DES va CLIPPER algoritmlari integral sxemalarda amalga oshiriladi.

PGP orqali shifrlangan axborotlarni ochish uchun, superkompyuterlar ishlatilganda bir asr ham kamlik qilishi mumkin. Bulardan tashqari, axborotlarni tasvirlarda va tovushlarda yashirish dasturlari ham mavjud. Masalan, S-tools dasturi axborotlarni BMP, GIF, WAV kengaytmali fayllarda saqlash uchun qo'llaniladi. Ba'zi hollarda yashirilgan axborotning hajmi rasmning hajmidan ko'p bo'lishi ham mumkin, ya'ni olingan natija faqatgina tanlangan rasmga bog'liq bo'ladi.

Kundalik jarayonda foydalanuvchilar ofis dasturlari va arxivatorlarni qo'llab kelishadi. Arxivatorlar, masalan PkZip dasturida ma'lumotlarni parol yordamida shifrlash mumkin. Ushbu fayllarni ochishda ikkita, ya'ni lug'atli va to'g'ridan-to'g'ri usuldan foydalanishadi. Lug'atli usulda bevosita maxsus fayldan so'zlar parol o'rniga qo'yib tekshiriladi, to'g'ridan-to'g'ri usulda esa bevosita belgilar kombinatsiyasi tuzilib, parol o'rniga qo'yib tekshiriladi.

Ofis dasturlari (Word, Excel, Access) orqali himoyalash umuman taklif etilmaydi. Bu borada mavjud dasturlar Internet da to'siqsiz tarqatiladi.

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

- elektron nurlarni chetdan turib o'qib olish;
- aloqa kabellarini elektromagnit to'lqinlar bilan nurlatish;
- yashirin tinglash qurilmalarini qo'llash;
- masofadan rasmga tushirish;
- printerdan chiqadigan akustik to'lqinlarni o'qib olish;
- ma'lumot tashuvchilarni va ishlab chiqarish chiqindilarini o'g'irlash;
- tizim xotirasida saklanib qolgan ma'lumotlarni o'qib olish;
- ximoyani yengib ma'lumotlarni nusxalash;
- qayd qilingan foydalanuvchi niqobida tizimga kirish;
- dasturiy tuzoqlarni qo'llash;
- dasturlash tillari va operatsion tizimlarning kamchiliklarida foydalanish;
- dasturlarda maxsus belgilangan sharoitlarda ishga tushishi mumkin bo'lgan qism dasturlarning mavjud bo'lishi;
- aloqa va apparatlarga noqonuniy ulanish;
- himoyalash vositalarini qasddan ishdan chiqarish va boshqalar.

3.4. Ma'lumotlarga ruxsatsiz kirishning dasturiy va texnik vositalari

Ma'lumki, hisoblash texnikasi vositalari ishi elektromagnit nurlanishi orqali bajariladi, bu esa, o'z navbatida, ma'lumotlarni tarqatish uchun zarur bo'lgan signallarning zaxirasidir. Bunday qismlarga kompyuterlarning platalari, elektron ta'minot manbalari, printerlar, plotterlar, aloqa aparatlari va h.k. kiradi. Lekin, statistik ma'lumotlardan asosiy yuqori chastotali elektromagnit nurlanish manbai sifatida displeyning rol o'ynashi ma'lum bo'ldi.

Bu displeylarda elektron nurli trubkalar o'rnatilgan bo'ladi. Displey ekranida tasvir xuddi televizordagidek tashkil etiladi. Bu esa videosignallarga egalik qilish va o'z navbatida, axborotlarga egalik kilish imkoniyatini yaratadi. Displey ekranidagi ko'rsatuv nusxasi televizorda hosil bo'ladi. Yuqorida keltirilgan kompyuter qismlaridan boshqa axborotga ruxsatsiz egalik qilish maqsadida tarmoq kabellari

hamda serverlardan ham foydalanilmoqda. Kompyuter tizimlari zaxiralariga ruxsatsiz kirish sifatida mazkur tizim ma'lumotlaridan foydalanish, ularni o'zgartirish va o'chirib tashlash harakatlari tushuniladi.

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

— himoyalash mexanizmini olib tashlash yoki ko'rinishini o'zgartirish;

— tizimga biror-bir foydalanuvchining nomi va paroli bilan kirish.

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

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

- kompyuter tizimlari zaxiralariga ruxsatsiz egalik qilish;
- kompyuter tarmog'i aloqa kanallaridagi xabar almashuvi jarayoniga ruxsatsiz aralashuv;
- virus ko'rinishidagi dasturiy kamchiliklar (defektlar)ni kiritish.

Ko'pincha kompyuter tizimida mavjud zaif qismlarni «teshik»lar, «lyuk»lar deb atashadi. Ba'zan dasturchilarning o'zi dastur tuzish paytida bu «teshik» larni qolririshadi. Masalan:

— natijaviy dasturiy mahsulotni yengil yig'ish maqsadida;

—dastur tayyor bo'lgandan keyin yashirincha dasturga kirish vositasiga ega bo'lish maqsadida.

Mavjud «teshik»ka zaruriy buyruqlar qo'yiladi va bu buyruqlar kerakli paytda o'z ishini bajarib boradi. Virus ko'rinishidagi dasturlar esa ma'lumotlarni yo'qotish yoki qisman o'zgartirish, ish seanslarini buzish uchun ishlatiladi.Yuqorida keltirilganlardan xulosa qilib, ma'lumotlarga ruxsatsiz egalik qilish uchun dasturiy moslamalar eng kuchli va samarali instrument bo'lib, kompyuter axborot zaxiralariga katta xavf tug'dirishi va bularga qarshi kurash eng dolzarb muammolardan biri ekanligini ta'kidlash mumkin.

3.5. Obyektlarning kompyuter tarmoqlarida ma'lumotlarning tarqalish kanallari

Hozirgi vaqtda lokal hisoblash tarmoqlari (LAN) va koorporativ tarmoqlari orasidagi farqlar yo'qolib bormoqda. Masalan, Netware 4x yoki Vines 4.11. operatsion tizimlari faoliyatini hududiy darajasiga chiqarmoqda. Bu esa, ya'ni LAN imkoniyatlarining ortishi, ma'lumotlarni himoyalash usullarini yanada takomillashtirishni talab qilmoqda.

Himoyalash vositalarini tashkil etishda quyidagilarni e'tiborga olish lozim:

- tizim bilan aloqada bo'lgan subyektlar sonining ko'pligi. ko'pgina hollarda esa ba'zi bir foydalanuvchilarning nazoratda bo'lmasligi;
- foydalanuvchiga zarur bo'lgan ma'lumotlarning tarmoada mavjudligi;
- tarmoqlarda turli firmalar ishlab chiqargan shaxsiy kompyuterlarning ishlatilishi;
- tarmoq tizimida turli dasturlarning ishlatish imkoniyati;
- tarmoq elementlari turli mamlakatlarda joylashganligi sababli, bu davlatlarga tortilgan aloqa kabellarining uzunligi va ularni to'liq nazorat qilishning qariyb mumkin emasligi;
- axborot zaxiralaridan bir vaqtning o'zida bir qancha foydalanuvchilarning foydalanishi;
- tarmoqqa bir qancha tizimlarning qo'shilishi;
- tarmoqning yengilgina kengayishi, ya'ni tizim chegarasining noaniqligi va unda ishlovchilarning kim ekanligining noma'lumligi;
- hujum nuqtalarining ko'pligi;
- tizimga kirishni nazorat qilishning qiyinligi.

Tarmoqni himoyalash zarurligi quyidagi hollardan kelib chiqadi:

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

Tarmoq muhofazasini tashkil etishda quyidagilarni e'tiborga olish lozim:

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

Maxfiy axborotni qayta ishlash uchun kerakli tekshiruvdan o'tgan kompyuterlarni ishlatish lozim bo'ladi. Muhofaza vositalarining funktsional to'liq bo'lishi muhim hisoblanadi. Bunda tizim administratorining ishi va olib borayotgan nazorat katta ahamiyatga egadir. Masalan, foydalanuvchilarning tez-tez parollarini almashtirib turishlari va parollarning juda uzunligi ularni aniqlashni qiyinlashtiradi. Shuning uchun ham yangi foydalanuvchini qayd etishni cheklash (masalan, faqat ish vaqtida yoki faqat ishlayotgan korxonasida) muhimdir.

Foydalanuvchining haqiqiyligini tekshirish uchun teskari aloqa qilib turish lozim (masalan, modem yordamida). Axborot zaxiralariga kirish huquqini chegaralash mexanizmini ishlatish va uning ta'sirini LAN obyektlariga to'laligicha o'tkazish mumkin.

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

- ma'lumotlarni aniqlab olishga yo'l qo'ymaslik;
- axborot almashishni tahlil qildlishga yo'l qo'ymaslik;
- xabarlarni o'zgartirishga yo'l qo'ymaslik;
- yashirincha ulanishga yo'l qo'ymaslik va bu hollarni tezda aniqlash lozim.

Ma'lumotlarni tarmoqda uzatish paytida kriptografik himoyalash usullaridan foydalaniladi. Qayd etish jurnaliga ruxsat etilmagan kirishlar amalga oshirilganligi haqida ma'lumotlar yozilib turilishi kerak. Bu jurnalga kirishni chegaralash ham himoya vositalari yordamida amalga oshirilishi lozim.

Kompyuter tarmog'ida nazoratni olib borish murakkabligining asosiy sababi - dasturiy ta'minot ustidan nazorat olib borishning murakkabligidir. Bundan tashqari kompyuter viruslarining ko'pligi ham tarmoqda nazoratni olib borishni qiyinlashtiradi. Hozirgi vaqtgacha muhofazalash dasturiy ta'minoti xilma-xil bo'lsa ham, operatsiyey

tizimlar zaruriy muhofazaning kerakli darajasini ta'minlamas edi. Netware 4.1, Windows NT operatsiyey tizimlari yetarli darajada muhofazani ta'minlay olishi mumkin.

Jinoyatlarni kamaytirish uchun quydagilarni bajarish lozim:

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

Stoxastik testlarni tashkillashtirish vositalari — axborot tizimlarining sifati va ishonchliligini tekshirishda qo'llaniladigan vositadir.

Aniq yo'naltirilgan testlar — AKTning sifati va ishonchliligini tekshirishda qo'llaniladi.

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

Statistik tahlilgichlar — dasturlarning tuzilish tarkibidagi kamchiliklarni aniqlash, dasturlar kodida aniqlanmagan kirish va chikish nuqtalarini topish, dasturdagi o'zgaruvchilarni to'g'ri aniqlanganligini va ko'zda tutilmagan ishlarni bajaruvchi kiyem dasturlarini anikdashda foydalaniladi.

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

Kompyuter tarmoqlarida ma'lumotlarni himoyalashning asosiy yo'nalishlari quyidagilar:

— axborotlarni himoyalash asosiy funksiyalarining texnik jixatdan amalga oshirilishi;

— bir nechta xavfsizlik funktsiyalarini bajaruvchi himoyalashning birgalikdagi vositalarini yaratish;

— algoritm va texnik vositalarni unifikatsiya qilish va standartlashtirish.

— foydalanuvchining anonimligini ta'minlovchi vositalar;

— serverga kirishni ta'minlash. Server faqatgina bitta foydalanuvchiga emas, balki keng miqyosdagi foydalanuvchilarga uz zaxiralaridan foydalanishga ruxsat berishi kerak;

- ruxsatsiz kirishdan tarmoqni himoyalash vositalari. Internet tarmog'ida ruxsatsiz kirishni taqiqlovchi tarmoqlararo ekran - Fire Wall vositalarini keng tarqalganligi hisoblanadi.

III bob xulosasi

Ushbu bobda har bir obyektning mualliflik huquqlarini himoyalashda stenografiyadan foydalanishi jarayonida kompyuterli grafik tasvirlarga maxsus belgi asosida dasturiy ta'minot bilan aniqlanishi, axborotlarni kriptografik himoyalash usullaridan asimmetriyali ikki kalitlik kriptografiya tizimini ishlash jarayoni, ma'lumotlarga ruxsatsiz kirishning dasturiy va texnik vositalari hamda obyektlarning kompyuter tarmoqlarida ma'lumotlarning tarqalish kanallari tahlil qilinib berilgan.

IV BOB.
OBYEKTNING KOMPYUTER TARMOG'IGA ALOQA KANALLARI ORQALI KIRAYOTGAN MA'LUMOTLARNI ANIQLASH

4.1. Identifikatsiya, autentifikatsiy va avtorizatsiya

Ma'lumotlarni uzatish kanallarini himoyalashda subyektlarning o'zaro autentifikatsiyasi, ya'ni aloqa kanallari orqali bog'lanadigan subyektlar haqiqiyligining o'zaro tasdig'i bajarilishi shart. Haqiqiylikning tasdig'i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. "Ulash" atamasi orqali tarmoqning ikkita subyekti o'rtasida mantiqiy bog'lanish tushuniladi. Ushbu muolajaning maqsadi - ulash qonuniy subyekt bilan amalga oshirilganligiga va barcha axborot mo'ljallangan manzilga borishligiga ishonchni ta'minlashdir.

O'zining haqiqiyligining tasdiqlash uchun subyekt tizimga turli asoslarni ko'rsatishi mumkin. Subyekt ko'rsatadigan asoslarga bog'liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo'linishi mumkin:

– biror narsani bilish asosida. Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda "so'rov javob" xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko'rsatish mumkin;

– biror narsaga egaligi asosida. Odatda bular magnit kartalar, smart- kartalar, sertifikatlar va touch memory qurilmalari;

– qandaydir daxlsiz xarakteristikalar asosida. Ushbu kategoriya o'z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko'zining rangdor pardasi va to'r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. Bu kategoriyada kriptografik usullar va vositalar ishlatilmaydi.

Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

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

Masofadagi foydalanuvchi tarmoqdan foydalanishga uringanida undan shaxsiy identifikatsiya nomeri PINni kiritish taklif etiladi. PIN to'rtta o'nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server foydalanuvchi tomonidan kiritilgan PIN-koddan foydalanib ma'lumotlar bazasidagi foydalanuvchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni generatsiyalash algoritmini bajaradi. So'ngra server generatsiyalangan son bilan foydalanuvchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server foydalanuvchiga tizimdan foydalanishga ruxsat beradi.

Autentifikatsiyaning bu sxemasidan foydalanishda apparat kalit va serverning qat'iy vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda Security Dynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

– apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me'yoridan chetlashishi aniq o'lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;

– server muayyan apparat kalit generatsiyalangan kodlarni kuzatadi va zaruriyat tug'ilganida ushbu kalitga moslashadi.

Autentifikatsiyaning bu sxemasi bilan bir muammo bog'liq. Apparat kalit generatsiyalagan tasodifiy son katta bo'lmagan vaqt oralig'i mobaynida haqiqiy parol hisoblanadi. Shu sababli, umuman, qisqa muddatli vaziyat sodir bo'lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

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

Autentifikatsiya (Authentication) - ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatdan aynan o'zi ekanligiga ishonch xosil qilishiga imkon beradi. Autentifikatsiya o'tkazishda tekshiruvchi taraf tekshiriluvchi tarafning haqiqiy 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 subyektlarning (foydalanuvchi obyektlarning) haqiqiy ekanligini aniqlash va tekshirishning o'zaro bog'langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog'liq. Subyektni identifikatsiyalash va autentifikatsiyalashdan so'ng uni avtorizatsiyalash boshlanadi.

Avtorizatsiya (Authorization) - subyektga tizimda ma'lum vakolat va resurslarni berish muolajasi, ya'ni avtorizatsiya subyekt 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, tahlillash va ularga mos reaksiya ko'rsatish uchun juda muhimdir.

Ma'lumotlarni uzatish kanallarini himoyalashda subyektlarning o'zaro autentifikatsiyasi, ya'ni aloqa kanallari orqali bog'lanadigan subyektlar haqiqiyligining o'zaro tasdig'i bajarilishi shart. Haqiqiylikning tasdig'i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. "Ulash" atamasi orqali tarmoqning ikkita subyekti o'rtasida mantiqiy bog'lanish tushuniladi. Ushbu muolajaning maqsadi - ulash qonuniy subyekt bilan amalga oshirilganligiga va barcha axborot mo'ljallangan manzilga borishligiga ishonchni ta'minlash hisoblanadi.

O'zining haqiqiyligining tasdiqlash uchun subyekt tizimga turli asoslarni ko'rsatishi mumkin. Subyekt 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 boshqalar bo'lishi mumkin;

– qandaydir daxlsiz xarakteristikalar asosida. Ushbu kategoriya o'z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko'zining rangdor pardasi va to'r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. 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 maxfiy qiymati faqat karta egasiga ma'lum bo'lishi shart.

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

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

Sertifikatlar va raqamli imzolar - agar autentifikatsiya uchun sertifikatlar ishlatilsa, bu sertifikatlarda raqamli imzoning ishlatilishi talab etiladi. Sertifikatlar foydalanuvchi tashkilotining mas'ul shaxsi, sertifikatlar serveri yoki tashqi ishonchli tashkilot tomonidan beriladi. Internet doirasida ochiq kalit sertifikatlarini tarqatish uchun ochiq kalitlarni boshqaruvchi qator tijorat infrastrukturalari PKI (Public Key Infrastrusture) paydo bo'ldi. Foydalanuvchilar turli daraja sertifikatlarini olishlari mumkin.

Autentifikatsiya jarayonlarini ta'minlanuvchi xavfsizlik darajasi bo'yicha ham turkumlash mumkin. Ushbu yondashishga binoan autentifikatsiya jarayonlari quyidagi turlarga bo'linadi:

– parollar va raqamli sertifikatlardan foydalanuvchi autentifikatsiya;

– kriptografik usullar va vositalar asosidagi qatiy autentifikatsiya;

– nullik bilim bilan isbotlash xususiyatiga ega bo'lgan autentifikatsiya jarayonlari (protokollari);

– foydalanuvchilarni biometrik autentifikatsiyasi.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o'ziga xos masalalarni yechishga imkon beradi. Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi. Intellektual tizimlarni qo'llanganligi esa samaradorlikni oshiradi.

Autentifikatsiya protokollariga bo'ladigan asosiy hujumlar quyidagilar:

- maskarad (impersonation). Foydalanuvchi o'zini boshqa shaxs deb ko'rsatishga urinib, u shaxs tarafidan xarakatlarning imkoniyatlariga va imtiyozlariga ega bo'lishni mo'ljallaydi;

- autentifikatsiya almashinuvi tarafini almashtirib qo'yish (interleaving attack). Niyati buzuq odam ushbu hujum mobaynida ikki taraf orasidagi autenfikatsion almashinish jarayonida trafikni modifikatsiyalash niyatida qatnashadi. Almashtirib qo'yishning quyidagi xili mavjud: ikkita foydalanuvchi o'rtasidagi autentifikatsiya muvaffaqiyatli o'tib, ulanish o'rnatilganidan so'ng buzg'unchi foydalanuvchilardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;

- takroriy uzatish (replay attack). Foydalanuvchilarning biri tomonidan autentifikatsiya ma'lumotlari takroran uzatiladi;

- uzatishni qaytarish (reflection attak). Oldingi hujum variantlaridan biri bo'lib, hujum mobaynida niyati buzuq odam protokolning ushbu sessiya doirasida ushlab qolingan axborotni orqaga qaytaradi.

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

- matn tanlashli hujum (chosen text attack). Niyati buzuq odam autentifikatsiya trafigini ushlab qolib, uzoq muddatli kriptografik kalitlar xususidagi axborotni olishga urinadi.

Yuqorida keltirilgan hujumlarni bartaraf qilish uchun autentifikatsiya protokollarini qurishda quyidagi usullardan foydalaniladi:

- "so'rov-javob", vaqt belgilari, tasodifiy sonlar, identifikatorlar, raqamli imzolar kabi mexanizmlardan foydalanish;

- autentifikatsiya natijasini foydalanuvchilarning tizim doirasidagi keyingi xarakatlariga bog'lash. Bunday misol yondashish tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyinga o'zaro

aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko'rsatish mumkin;

- aloqaning o'rnatilgan seansi doirasida autentifikatsiya muolajasini vaqti-vaqti bilan bajarib turish va hokazo.

4.2. Obyektlarga kirayotgan ma'lumotlarni tekshirish vositalari va usullari. Real Secury va boshqa texnikaviy qurilmalar Aktiv va passiv nurlanish usullari

Kanal kirish yo'liga dastlabki signal ko'rinishidagi axborot qabul qilinadi.

Dastlabki signal - axborot manbaidan olinadigan axborot eltuvchisidir. Quyidagi signal manbalarini ko'rsatish mumkin:

– elektromagnit va akustik to'lqinlarini qaytaruvchi kuzatuv obyekti;

– o'zidan optik va radio diapazonlaridagi elektromagnit to'lqinlarini tarqatuvchi kuzatuv obyekti;

– funktsional aloqa kanalining uzatuvchi qurilmasi;

– yashirincha o'rnatilgan qurilmalar;

– xavfli signal manbai;

– axborot bilan modulyatsiyalangan akustik to'lqinlar manbai va boshqalar.

Kanal kirish yo'liga manbadan axborot signali manba tilida (xarf, raqam, matn, simvollar, belgilar, tovush signallari va h. ko'rinishida) qabul qilinganligi sababli uzatuvchi qurilma axborotning ushbu ifodalanish shaklini tarqalish muxitiga mos axborot eltuvchisiga yozishni ta'minlovchi shaklga o'zgartiradi.

Axborot eltuvchining fizik tabiati bo'yicha quyidagi axborot sirqib chiqadigan texnik kanallar farqlanadi:

– radioelektron;

– akustik;

– optik;

– moddiy.

Moddiy kanalda axborotning sirqib chiqishi himoyalanuvchi axborotli eltuvchilarning nazoratlanuvchi zona tashqarisiga ruxsatsiz tarqalishi hisobiga ro'y beradi. Eltuvchi sifatida ko'pincha hujjatlar qo'l yozmasi va ishlatilgan nusxalash qog'ozlari ishlatiladi.

Informativligi bo'yicha axborot sirqib chiqadigan kanallar informativ, informativligi kam va informativ emaslarga bo'linadi. Kanal

informativligi kanal bo'yicha uzatiluvchi axborot qiymati orqali baxolanadi.

Faollik vaqti bo'yicha kanallar doimiy, davriy va tasodifiylarga bo'linadi. Doimiy kanalda axborot sirqib chiqishi yetarlicha muntazam xarakterga ega. Tasodifiy kanallarga axborot sirqib chiqishi tasodifiy, bir martalik xarakterga ega bo'lgan kanallar tegishli bo'ladi.

Axborot sirqib chiqadigan kanallarning amalga oshirilishi natijasida quyidagi xavflar paydo bo'lishi mumkin:

– akustik axborotning sirqib chiqishi xavfi;

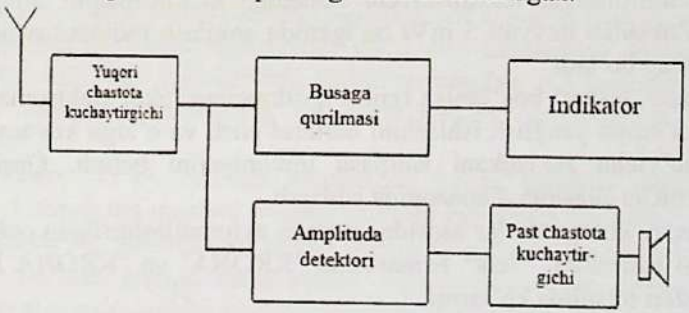
– tasviriy axborotning sirqib chiqishi xavfi;

– axborotning qo'shimcha elektromagnit nurlanishlar va navodkalar bo'yicha sirqib chiqishi xavfi.

Strukturalari bo'yicha axborot sirqib chiqadigan kanallar bir kanalli va ko'p kanalli bo'lishi mumkin. Ko'p kanallilarda axborot sirqib chiqishi bir qancha ketma-ket yoki parallel kanallar bo'yicha bo'ladi.

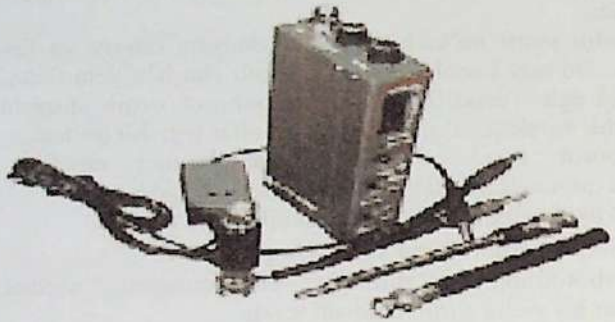
4.3. Axborot sirqib chiqadigan texnik kanallarni aniqlash usullari va vositalari

Elektromagnit nurlanish indikatorlari qo'shimcha elektromagnit nurlanishlarni aniqlash va nazoratlash uchun ishlatiladi. Indikatorning soddalashtirilgan sxemasi pastdagi rasmda keltirilgan.



Indikatorning soddalashtirilgan sxemasi.

Asbob fazoning ma'lum nuqtasidagi elektromagnit nurlanishlarni qaydlaydi. Agar ushbu nurlanishlarning sathi bo'sag'a nurlanishdan oshib ketsa tovush yoki nur yordamida ishlovchi ogohlantiruvchi qurilma ishga tushadi. Demak, ushbu joyda yashirincha o'rnatilgan radio qurilmasi (radiozakladka) mavjud.



Zamonaviy indikator D-008

Ushbu indikator ishlashining ikkita rejimi mavjud:

– radionurlantiruvchi zakladkani qidirishga mo'ljallangan maydonni aniqlash;

– yashirincha tinglovchi qurilmalarni qidirishga mo'ljallangan simli liniyalarni tahlillash.

Ushbu asbob modulyatsiya xiliga bog'liq bo'lmagan holda zakladkalarni aniqlaydi. Aniqlash radiusi nurlanish quvvatiga, zakladka ishlashi chastotasiga, tekshiriluvchi xonadagi elektromagnit ahvolga bog'liq. Zakladka quvvati 5 mVt bo'lganida aniqlash radiusi taxminan 1metrga teng bo'ladi.

Akustik teskari bog'lanish rejimi qurilmaning lokal elektromagnit maydon ta'sirida yanglish ishlashini bartaraf etish va o'ziga xos tovush signali bo'yicha zakladkani aniqlash imkoniyatini beradi. Qurilma 50–1500 mGts chastota diapazonida ishlaydi.

Shaxsiy kompyuterlar asosida qurilgan avtomatlashtirilgan qidiruv kompleksi ishlashini "Nelk" firmasining "KRONA" va "KRONA Pro" komplekslari misolida ko'ramiz.

"KRONA" kompleksi quyidagi muolajalarni bajarishga mo'ljallangan: hozirgi kunda ma'lum barcha niqoblash vositalaridan foydalanuvchi radiozakladkalarni aniqlash va lokalizatsiyalash. Z GGts gacha diapazonda ishlaydi (qo'shimcha konvertor bilan 18 GGts gacha). Ma'lumotlarni uzatuvchi raqamli kanallarni va axborotni radiokanal bo'yicha uzatuvchi yashirin videokameralarni avtomatik tarzda aniqlash imkoniyatiga ega. Mavjud dasturiy ta'minot radiozakladkalarni yuqori darajada ishonchlilikda aniqlashga imkon beradi.

"KRONA" kompleksi

Yuqorida ko'rilgan avtomatlashtirilgan qidiruv komplekslari standart kompyuterlarda va oddiy ko'chmas skanerlovchi priyemniklar asosida qurilgan.

Axborotlarni himoyalashda texnik vositalarga maxsus ishlab chiqilgan texnikaviy qurilmalar kiradi. Birinchilar qatorida kompyuter tarmoqlarida hujum qiluvchilarni aniqlab beruvchi, texnikaviy va dasturiy vosita sifatida, Real Secure tizimi Amerika Qo'shma shtatidagi Internet Security System kompaniyasi tomonidan 1998 yilda ishlab chiqilgan. Ushbu tizim (qurilma)-intellektual analizatordan iborat bo'lib kelayotgan ma'lumot paketlarini tahlil etib hujumlarni aniqlaydi. Bu sistema real vaqt masshtabida ishlab tarmoqdagi ma'lumot paketlarini tahlil etadi va tarmoqning bir segmentidagi ma'lumotlarni himoya qiladi.

Hujum bo'layotganligi aniqlangan holda elektron pochta yoki konsol orqali ma'muriyat boshqaruvchiga ma'lumot beriladi. Shu bilan birgalikda ma'lumotlar ba'zasiga hujum to'g'risida yozib qo'yiladi va kerak bo'lgan paytda tahlil etiladi. Agar qilinayotgan hujum sizning kompyuter tizimingizni ishdan chiqarishi mumkinligi aniqlansa, u holda avtomatik ravishda hujum etuvchi bilan aloqa uziladi va marshrutizator keyingi bog'lanishlikni taqiqlaydi. Ushbu Real Secure sistemasi kompyuter tarmog'ining ichidagi hamda tashqarida kelayotgan havfni aniqlaydi va himoya qiladi.

Real Secure sistemasi tarqalgan arxitektura asosida ishlaydi va 2 ta asosiy kompanentdan iboratdir, ya'ni Real Secure Detector va Real Secure Manager. Birinchi kompanent kompyuter tarmog'ida xosil

bo‘layotgan hujumlarni aniqlaydi. U moduldan ya’ni tarmoq va sistemali agentlardan tashkil topgan. Tarmoq agenti kompyuter ma`lumotlarining almashuvida bo‘layotgan xodisalar asosida xavf borligini aniqlab beradi. Sistemali agent esa tekshirilayotgan tarmoq tuguniga ulanib, hujum bo‘layotganligi to‘g‘risida xabar beradi. Ikkinchi komponent, ya’ni Real Secure Manager komponenti ma`lumotlarni detektordan yig‘ish va sozlash ishlariga javob beradi.

Real Secure sistemasining qobiliyati quyidagicha:

a) Aniqlovchi hujumlarning sonini ko‘pligi;

b) Nazorat etish modullarini markazlashgan holda boshqarish;

c) Juda ko‘p tarmoq protokollarini filtrlash va tahlil qilish (TEP, UDP, IEMP);

d) Hujumlarga har xil variantlar asosida ta’sir etish;

e) Hujum qilayotgan tugun bilan aloqani uzish;

f) Tarmok ekranlari va marshrutizatorlarni boshqarish;

g) Har bir hujumni qayta ko‘rib chiqish va tahlil etish uchun yozib olish;

h) Ethernet, Fast Ethernet va Token Ring tarmoq interfeyslarida ishlashni ta’minlash;

i) Maxsus uskunalar talab etmasligi;

j) Tarmoq unumdorligini pasaytirmaslik;

k) Hisobot tarmoqlarining har xilligi;

l) Uskunaviy va dasturiy ta’minotlarga talablarning balandmasligi va hokazo.

Hujumlarga e’tiroz etishning har xil variantlari aniqlangan va ular quyidagicha:

A). Hujum xaqida qayd etish va ro‘yxatga olish;

B). Ma’muriyatni elektron pochta yoki boshqaruv konsuli orqali ogoxlantirish;

C). Hujum qilayotgan tarmoq tugunini avariya sifatida uzib qo‘yish;

D). Qilingan hujumlarini ko‘rib chiqish va tahlil etish uchun yozib olish;

E). Tarmoqlararo ekranlarni va marshrutizatorlarni tarmoq ko‘rinishini o‘zgartirish va hokazolar.

Uskunaviy va dasturiy ta’minotlarga qo‘yilgan asosiy talablar:

- Protsessor - Pentium Pro 200 MGts (yoki Pentium II 300 MGts);
- OZU - 64 MB yeki 128 MB;

- NJMT (kattik) disk - 100 MB kam bo‘lmagan xotira (ma’lumotlar bazasi va ro‘yxat turlari uchun);
- Tarmoq interfeysi - Ethernet, Fast Ethernet, Token Ring, FDDI.

Internet Scanner qurilmasi esa kompyuter tarmoqlarini hujum qiluvchilarga qanday bardosh beraolishligini aniqlab beruvchi texnikaviy tizim hisoblanadi. U ham amerikadagi Internet Security System kompaniyasi tomonidan 1992 yilda ishlab chiqilib 1998 yilda Rossiya sertifikatini olgan. Ushbu tizim bir paytni o‘zida 128 ta tarmoq uzellarini tekshirib, 996 tagacha tekshiruv o‘tkazib, tarmoqni zaif tamonlarini aniqlab beradi.

Secret Net qurilmasi ham texnikaviy dasturiy qurilma hisoblanib tarmoqqa ruxsatsiz ulangan modemlarni aniqlab beradi. Bundan tashqari juda ko‘p uskunaviy - dasturiy qurilmalar xozirgi kunda ishlab chiqilmoqda.

Bugungi kunda kompyuter tizim va tarmoqlariga tashqaridan qilnayotgan hujumlarni aniqlovchi texnikaviy va dasturiy vositalardan IPS va IDS kabi yangi tizimlar qo‘llanilish boshlandi. Tarmoq infratuzilmasida ular serverlarga mumkin bo'lgan hujumlarni aniqlash va oldini olish orqali bir xil nazorat rolini bajaradilar.

IPS/IDS nima? IDS intrusion Detection System — obyektga ruxsatsiz kirishni aniqlovchi tizimni anglatadi. IPS, yoki ruxsatsiz kirishni oldini olish tizimi. An'anaviy himoya vositalari bilan taqqoslaganda — antivirus spam-filtrlar — xavfsizlik devorlari - IDS / IPS tarmoq muhofazasining ancha yuqori darajasini ta'minlaydi.

Antivirus fayllarni tahlil qiladi, spam-filtr xatlar, IP orqali xavfsizlik devori ulanishlarini tahlil qiladi. IDS / IPS ma'lumotlarni va tarmoq xatti-harakatlarini tahlil qiladi. Huquqni muhofaza qilish organlari, xavfsizlik devori, pochta filtrlari va antivirus bilan taqqoslashni davom ettirish "sohada" ishlaydigan oddiy xodimlardir va hujumni aniqlash va oldini olish tizimlari ofisda ishlaydigan yuqori lavozimlixodimlardir.

IDS arxitekturasi va texnologiyasi

IDS printsipi trafikni tahlil qilish asosida tahdidlarni aniqlashdan iborat, ammo keyingi harakatlar administratorning orqasida qoladi. IDS tizimlari o'rnatish joyi va operatsion printsipi bo'yicha turlarga bo'linadi.

IDS larni tizimga o‘rnatish bo‘yicha ikkita turga bo‘lish mumkin:

–Network Intrusion Detection System (NIDS),

–Host-based Intrusion Detection System (HIDS).

Birinchisi tarmoq darajasida ishlaydi, ikkinchisi esa faqat bitta xost darajasida.

Tarmoq hujumlarini aniqlash tizimlari (NIDS)

NIDS texnologiyasi tizimni strategik muhim tarmoq joylarida o'rnatish va barcha tarmoq qurilmalarining kirish/chiqish trafigini tahlil qilish imkonini beradi. NIDS, OSI modelining kanal darajasidan ilovalar darajasiga qadar har bir paketga "qarash" orqali chuqur darajadagi trafikni tahlil qiladi.

IDS xavfsizlik devori faqat tarmoqdan tashqarida keladigan hujumlarni aniqlaydi, NIDS esa ichki tahdidni aniqlay oladi.

Tarmoq hujumlarini aniqlash tizimlari butun tarmoqni nazorat qiladi, bu esa qo'shimcha echimlarga pul sarflamaslikka imkon beradi. Biroq, kamchiliklar mavjud: NIDS ko'plab resurslarni iste'mol qilib, barcha tarmoq trafigini kuzatib boradi. Trafik miqdori qanchalik ko'p bo'lsa, CPU va RAM resurslariga bo'lgan ehtiyoj shunchalik baland bo'ladi. Bu ma'lumotlar almashinuvining sezilarli kechikishiga va tarmoq tezligini pasayishiga olib keladi. Katta miqdordagi ma'lumot, shuningdek, tizimni ba'zi paketlarni o'tkazib yuborishga majbur qilib, NIDSNI "bezovta qilishi" mumkin bo‘ladi, bu esa tarmoqni zaiflashtiradi.

Host intrusion Detection tizimi (HIDS)

Tarmoq tizimlariga muqobil-host. Bunday tizimlar tarmoq ichida bitta maxalliy tarmoqga o'rnatiladi va faqat uni himoya qiladi. HIDS shuningdek, barcha kiruvchi va chiquvchi paketlarni tahlil qiladi, lekin faqat bitta qurilma uchun. HIDS tizimi fayl snapshotlarini yaratish tamoyiliga asoslangan: joriy versiyaning rasmini oladi va uni avvalgisi bilan taqqoslaydi, shu bilan mumkin bo'lgan tahdidlarni aniqlaydi.

O'rnatish joyidagi boshqa IDS turlari quyidagilardan iborat:

- NIDS va hidlardan tashqari, butun tarmoqni emas, balki faqat chegaralarni qo'riqlaydigan va ularning buzilishini bildiradigan PIDS (Perimeter Intrusion Detection Systems) ham mavjud. Signal yoki "Trump devori" kabi.
- VMIDS (Virtual Machine-based Intrusion Detection Systems). Bu virtualizatsiya texnologiyasiga asoslangan tahdidlarni aniqlash tizimlarining bir turi hisoblanadi. Bunday IDS alohida qurilmalarda

aniqlash tizimida ishlatish mumkin. Har qanday shubhali faoliyatni kuzatadigan virtual mashinada himoyani kengaytirish mumkin.

Faoliyat printsipi bo'yicha IDS turlari quyidagilarga bo‘linadi:

Barcha IDS hujumlarini aniqlash tizimlari bir xil printsip asosida ishlaydi — trafikni tahlil qilish orqali tahdidlarni topish. Farqlar tahlil jarayonida yotadi. Uchta asosiy turi mavjud: imzo, anomaliyalarga va qoidalarga asoslangan.

Imzo IDS

Ushbu turdagi IDS antivirus dasturiy ta'minotiga o'xshash printsip asosida ishlaydi. Ular imzolarni tahlil qilishadi va ularni to'g'ri ishlashni ta'minlash uchun doimiy ravishda yangilanishi kerak bo'lgan bazaga mos keladi. Shunga ko'ra, bu imzo identifikatorlarining asosiy kamchiliklari quyidagilardan iborat: agar biron sababga ko'ra ma'lumotlar bazasi mavjud bo'lmasa, tarmoq zaiflashadi. Bundan tashqari, agar hujum yangi bo'lsa va uning imzosi noma'lum bo'lsa, tahdid aniqlanmasligi xavfi tug'iladi.

Imzo identifikatorlari naqsh yoki holatlarni kuzatish imkoniyatiga ega. Shablonlar doimiy yangilanib turadigan ma'lumotlar bazasida saqlanadigan imzolardir. Tizimning boshlang'ich holati oddiy bo‘lib, hujumning yo'qligi hisoblanadi. Hujum boshlangandan so'ng tizim buzilgan holatga o'tadi. Har bir harakat (masalan, obyektning xavfsizlik siyosatiga mos kelmaydigan protokol orqali ulanishni o'rnatish, dasturiy ta'minotni faollashtirish va h.k.) obyektni o'zgartirishi mumkin. Shuning uchun imzo identifikatorlari xatti-harakatlarni emas, balki tizimning holatini kuzatadi.

Yuqoridagi tavsifdan tushunilgandek, NIDS ko'pincha taxdidlarni kuzatib boradi.

Anomaliyalarga asoslangan IDS

Anomaliyalarga asoslangan IDS tizimni o'rganishdan boshlaydi. Har xil tahdidlarni aniqlash tizimlarini to'g'ri ishlashi uchun sinov muddati talab qilinadi. Administratorlarga dastlabki bir necha oy ichida tizimni o'qitish uchun signallarni butunlay o'chirib qo'yish tavsiya etiladi. Sinov davridan keyin u ishlashga tayyor bo‘ladi.

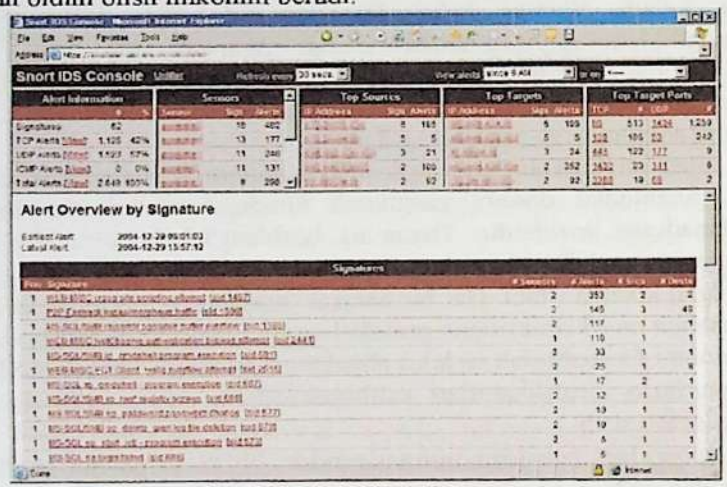
Tizim hozirgi vaqtda tarmoq ishini tahlil qiladi, shu davr bilan taqqoslanadi va anomaliyalarni aniqlaydi. Anomaliyalar uch toifaga bo'linadi:

- statistik;
- protokollarning anomaliyalari;

–trafik anomaliyalari.

IDS tizimi muntazam faoliyat profilini (kiruvchi/chiquvchi trafik hajmi, ishga tushirilgan ilovalar va boshqalar) tashkil etganda va uni joriy Profil bilan taqqoslaganida statistik anomaliyalar aniqlanadi.

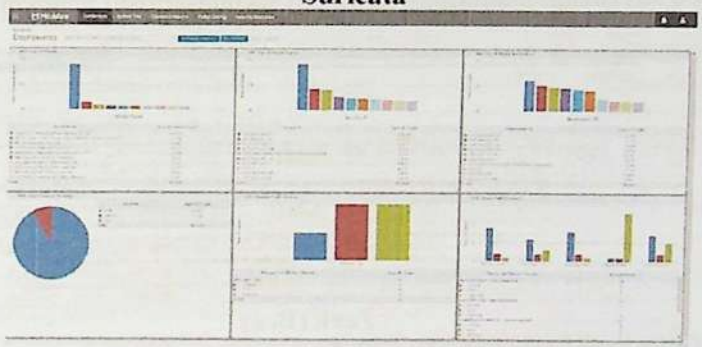
IDS protokollarining anomaliyalarini aniqlash uchun tizim aloqa protokollarini, ularning foydalanuvchilar, ilovalar bilan aloqalarini tahlil qiladi va profillar hosil qiladi. Bundan tashqari, IDS anomaliyalarni, tarmoq trafikidagi har qanday xavfli yoki hatto xavfli faoliyatni aniqlay oladi. Misol uchun, DoS hujumining holatini aniqlash. IDS texnologiyalari tarmoq trafigini tahlil qilish va shu kabi hujumlarni oldindan oldini olish imkonini beradi.



Klassik NIDS-Snort

Bu 1998 yilda yaratilgan ochiq kodli tizim. Snort tizimi mustaqil dasturiy ta'minot sifatida ishlab chiqilgan va 2008 yilda Cisco tomonidan sotib olingan bo'lib, u endi hamkor va ishlab chiquvchi hisoblanadi. Snort kichik va o'rta kompaniyalarga yaxshi mos keladi. Yordamchi dastur sniffer paketlarini o'z ichiga oladi, qoidalarni sozlashni qo'llab-quvvatlaydi. Snort - aniq va funktsional tahdidlarni oldini olish tizimini qidiruvchilar uchun vosita hisoblanadi.

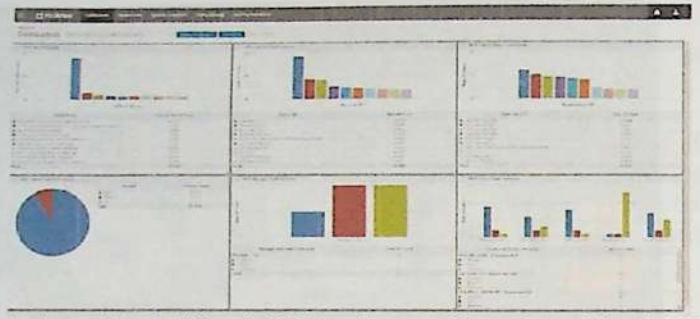
Suricata



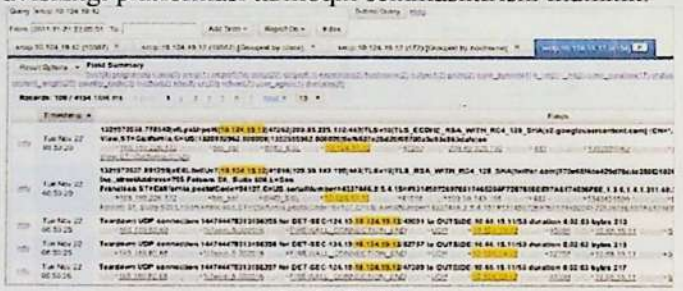
McAfee Network Security Platform

O'rta biznes bozorida snort raqobatchisi-ochiq manba Suricata tizimi, birinchi 2010 yilda joriy etildi. Suricata juda yosh tizim bo'lib, uning afzalligi juda katta. Suricatada juda ko'p legacy kodi yo'q, shuningdek, tizim raqobatchilardan ko'ra yangi ishlanmalardan foydalanadi. Buning natijasida Suricata tezroq ishlaydi. Bundan tashqari, ishlab chiquvchilar standart natijalarni tahlil qilish vositalari bilan muvofiqligi haqida g'amxo'rlik qildilar.

Bu shuni anglatadiki, Suricata Snort bilan bir xil modullarni qo'llab-quvvatlaydi. Imzo tahdidlarini aniqlashga qodir va o'rta va katta obyektlarga mos keladi.



IDS ko'p sonli tahdidlarni bloklaydi, zararli saytlarga kiradi, DDoS hujumlarini oldini oladi va hokazo. Monumentallik tufayli McAfee tarmoq xavfsizligi platformasi tarmoqni sekinlashtirishi mumkin.



Zeek (Bro)

To'liq bepul ochiq manba IDS. Standart intrusion Detection rejimida va zararli imzolarni aniqlash rejimida ishlashni qo'llab-quvvatlaydi. Zeek shuningdek, hodisalarni aniqlay oladi va o'z siyosat skriptlarini o'rnatishga imkon beradi. Zeekning kamchiliklari - bu vosita bilan aloqa qilishning murakkabligi, chunki rivojlanish grafik interfeysga emas, balki funksionallikka qaratilgan bo'ladi.

Obyektning axborot xavfsizligini buzuvchilarining modellari

Tizimdan ruxsatsiz foydalanishga majbur etish sabablarining diapazoni yetarlicha keng: kompyuter bilan o'ynaganidagi hayajon ko'tarinkiligidan to jirkanch menedjer ustidan hokimlik hissiyotigacha. Bu bilan nafaqat ko'ngil ochishni xoxlovchi havaskorlar, balki professional dasturchilar ham shug'ullanadi. Ular parolni tanlash, faraz qilish natijasida yoki 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 sho'xlikni yomon niyat bilan qilingan harakatdan ajratish qiyin bo'ladi. Yaqin vaqtgacha rahbarlardan norozi hizmatchilarning o'z mavqelarini suiste'mol qilgan xolda tizimni buzishlari, undan begonalarning foydalanishlariga yo'l qo'yishlari yoki tizimni ish holatida qarovsiz qoldirishlari tashvishlantirar edi. Bunday harakatlarga majbur etish sabablari quyidagilar:

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

Xarrison-Ruzzo-Ulmanning diskretsion modeli

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

Himoyalangan axborot tizimlarini ishlab chiqaruvchilar xavfsizlik modelidan quyidagi hollarda foydalanishadi:

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

Iste'molchilar xavfsizlikning formal modellarini tuzish yo'li bilan ishlab chiqaruvchilarga o'zlarining talablarini aniq va ziddiyatli bo'lmagan shaklda yetkazish hamda himoyalangan tizimlarning o'zlarining ehtiyojlariga mosligini baholash imkoniyatiga ega bo'ladilar. Kvalifikatsiya (Malaka) bo'yicha ekspertlar himoyalangan tizimlarda xavfsizlik siyosatining amalga oshirilish adekvatligini tahlillash mobaynida xavfsizlik modelidan etalon sifatida foydalanadilar.

Xavfsizlik modeli quyidagi bazaviy tasavvurlarga asoslangan.

Tizim o'zaro harakatdagi "subyektlar" va "obyektlar" majmuasidan iborat. Obyektlarni intuitiv ravishda axborotli konteynerlar ko'rinishida tasavvur etish mumkin, subyektlarni esa obyektlarga turli usullar bilan ta'sir etuvchi bajariluvchi dasturlar deb hisoblash mumkin.

1. Agar subyektlar xavfsizlik siyosati qoidalarini buzish imkoniyatiga ega bo'lmasa, tizim xavfsiz hisoblanadi. Ta'kidlash lozimki, "obyekt" va "subyekt" tushunchalarining tavsifi turli modellarda jiddiy farqlanishi mumkin.

2. Tizimdagi barcha o'zaro harakatlar subyektlar va obyektlar orasida ma'lum xildagi munosabatlarni o'rnatish orqali modellashtiriladi.

3. Barcha amallar o'zaro harakat monitori yordamida nazoratlanadi va xavfsizlik siyosati qoidalariga muvofiq ma'n etiladi yoki ruxsat beriladi.

4. Xavfsizlik siyosati qoidalar ko'rinishida beriladi, bu qoidalarga mos holda subyektlar va obyektlar orasida barcha o'zaro harakatlar amalga oshirilishi shart. Ushbu qoidalarni buzilishiga olib keluvchi o'zaro harakatlar foydalanishni nazoratlovchi vositalar yordamida to'sib qo'yiladi va amalga oshirilishi mumkin emas bo'ladi.

5. Subyektlar, obyektlar va ular orasidagi munosabatlar (o'rnatilgan o'zaro harakat) to'plami tizim "holatini" belgilaydi. Tizimning har bir xolati modelda taklif etilgan xavfsizlik mezoniga muvofiq xavfsiz yoki taxlikali bo'ladi.

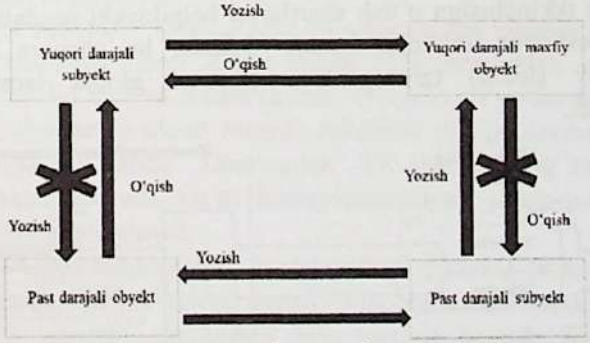
6. Xavfsizlik modelining asosiy elementi - xavfsiz xolatidagi tizim barcha o'rnatilgan qoida va cheklashlarga rioya qilinganida taxlikali holatga o'tish mumkin emasligi tasdig'ining (teoremasining) isboti.

Xarrison-Ruzzo-Ulmanning diskretsion modeli klassik (mumtoz) diskretsion model hisoblanib, subyektlarning obyektlardan foydalanishni ixtiyoriy boshqarishni va foydalanish xuquqlarining tarqalishi nazoratini amalga oshiradi. Ushbu model doirasida axborotni ishlash sistemasi axborotdan foydalanuvchi subyektlar, himoyalanuvchi axborotga ega bo'lgan obyektlar va mos harakatlarni, (masalan o'qish (R). yozish (W), dasturni bajarish(E)) vakolatini anglatuvchi foydalanish xuquqlarining chekli to'plam majmui ko'rinishida ifodalanadi.

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

3. Bella - La Padulaning mandatli modeli foydalanishni boshqarishning mandatli modeli ko'pgina mamlakaltlarning davlat va hukumat muassasalarida qabul qilingan maxfiy hujjat almashish qoidalariga asoslangan.

Bella La Padula siyosatining asosiy mazmuni amaliy hayotdan olingan bo'lib, himoyalanuvchi axborotni ishlashda qatnashuvchilarga va bu axborot mavjud bo'lgan hujjatlarga xavfsizlik sathi nomini olgan maxsus belgi, masalan "maxfiy", "mutlaqo maxfiy" va h. kabilarni tayinlashdan iborat. Xavfsizlikning barcha sathlari o'rnatilgan ustunlik munosabati asosida tartiblanadi, masalan, "mutlaqo maxfiy" sathi "maxfiy" sathidan yuqori yoki undan ustun turadi.



Foydalanishni nazoratlash o'zaro harakatdagi tomonlarning xavfsizlik sathlariga bog'liq holda quyidagi ikkita oddiy qoida asosida amalga oshiriladi:

1. Vakolatli shaxs (subyekt) faqat xavfsizlik sathi o‘zining xavfsizlik sathidan yuqori bo‘lmagan hujjatlardan axborotni o‘qishga haqli.

2. Vakolatli shaxs (subyekt) xavfsizlik sathi o‘zining xavfsizlik sathidan past bo‘lmagan hujjatlarga axborot kiritishga xaqli. Birinchi qoida yuqori sath shaxslari tomonidan ishlanadigan axborotdan past sath shaxslari tomonidan foydalanishdan himoyalashni ta’minlaydi.

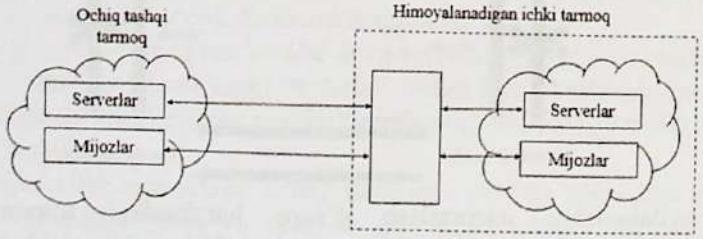
Xavfsizlikning rolli modeli

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

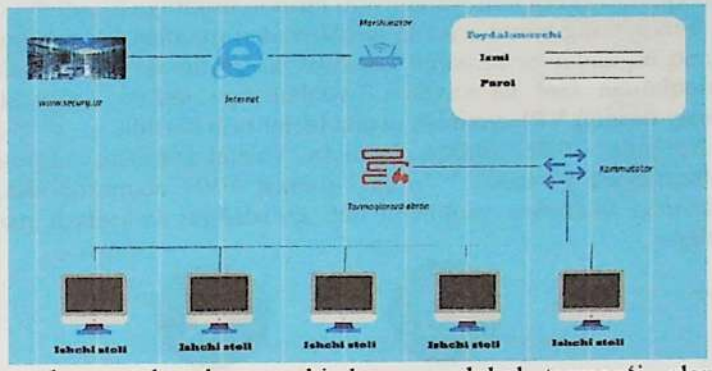
Rolli modelda “subyekt” tushunchasi “foydalanuvchi” va “rol” tushunchalari bilan almashtiriladi. Foydalanuvchi - tizim bilan ishlovchi va ma’lum xizmat vazifalarini bajaruvchi odam. Rol - tizimda faol ishtirok etuvchi abstrakt tushuncha bo‘lib, u bilan ma’lum faoliyatni amalga oshirish uchun zarur vakolatlarining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

4.4. Obyektlarda virtual korporativ tarmoqlarni tashkillashtirish uchun tarmoqlararo ekranlarni qo‘llash

Tarmoqlararo ekran (TE) - brandmauer yoki firewall sistemasi deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko‘p qismlarga ajratish va ma’lumot paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o‘tish shartlarini belgilovchi qoidalar to‘plamini amalga oshirish imkonini beradi. Odatda, bu chegara korxonaning korporativ (lokal) tarmog‘i va Internet global tarmoq orasida o‘tkaziladi.



Tarmoqlararo ekranni ulash sxemasi



Tarmoqlararo ekranlar garchi korxona lokal tarmog‘i ulangan korporativ intra tarmog‘idan qilinuvchi hujumlardan himoyalashda ishlatilishlari mumkin bo‘lsada, odatda ular korxona ichki tarmog‘ini Internet global tarmoqdan suqilib kirishdan himoyalaydi. Aksariyat tijorat tashkilotlari uchun tarmoqlararo ekranlarning o‘rnatilishi ichki tarmoq xavfsizligini ta’minlashning zaruriy sharti hisoblanadi.

Korporativ tarmoqlarda eshelon himoyaning asosiy elementlaridan biri tarmoqlararo ekrandir. Bundan tashqari tarmoqlararo ekran ichki va tashqi perimetrlarning birinchi himoya qurilmasi hisoblanadi. Tarmoqlararo ekran (TE) lokal (bir komponentli) yoki funktsional taqsimlangan vosita (kompleks) bo‘lib, u AKTlarida kiruvchi va chiquvchi ma’lumotlarni boshqaradi va ma’lumotlarni filtrlash orqali AKT himoyasini ta’minlaydi.

Belgilangan mezonlar asosida axborot tekshiruvini amalga oshirib, axborotlar tarqalishida qaror qabul qiladi. TE tarmoqdan o‘tuvchi barcha paketlarni ko‘radi va ikkala (kirish, chiqish) yo‘nalish bo‘yicha paketlarni belgilangan qoidalar asosida tekshirib ularga ruxsat berish yoki bermaslikni hal qiladi. Shuningdek, TE ikki tarmoq orasidagi himoyani amalga oshiradi, ya’ni himoyalanayotgan tarmoqni ochiq tashqi tarmoqdan himoyalaydi.

Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta’sir ko‘rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning himoyalanuvchi tarmog‘i va tashqi aniq tarmoq orasida joylanishi lozim. Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo

ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtai nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi.

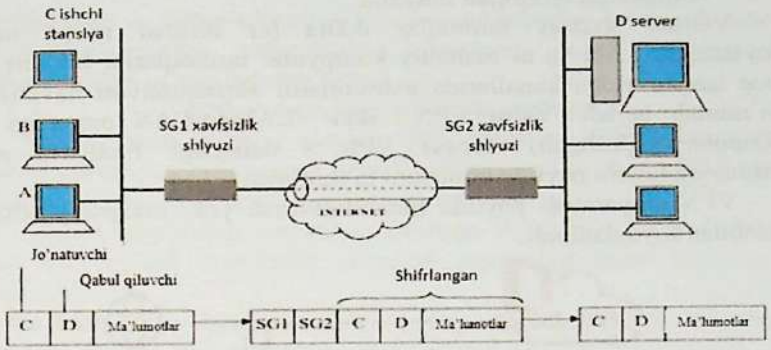
Internetning hamma yerda tarqalishidan manfaat ko'rish maqsadida tarmoq hujumlariga samarali qarshilik ko'rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq VPN yaratish ustida ishlar olib borildi.

Natijada 1990 yilning boshida virtual xususiy tarmoq VPN kontseptsiyasi yaratildi. "Virtual" iborasi VPN atamasiga ikkita uzel o'rtasidagi ulanishni vaqtincha deb ko'rilishini ta'kidlash maqsadida kiritilgan.

Haqiqattan, bu ulanish doimiy, qat'iy bo'lmay, faqat ochiq tarmoq bo'yicha trafik o'tganida mavjud bo'ladi. Axborotni VPN tunneli bo'yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

– o'zaro aloqadagi taraflarni autentifikatsiyalash;
– uzatiluvchi ma'lumotlarni kriptografik berkitish (shifrlash);
– yetkaziladigan axborotning haqiqiyligini va yaxlitligini tekshirish.

Virtual himoyalangan tunnel sxemasi 98 Intranet VPN Marshrutizatorlar asosidagi VPN. VPN qurishning ushbu usuliga binoan himoyalangan kanallarni yaratishda marshrutizatorlardan foydalaniladi.

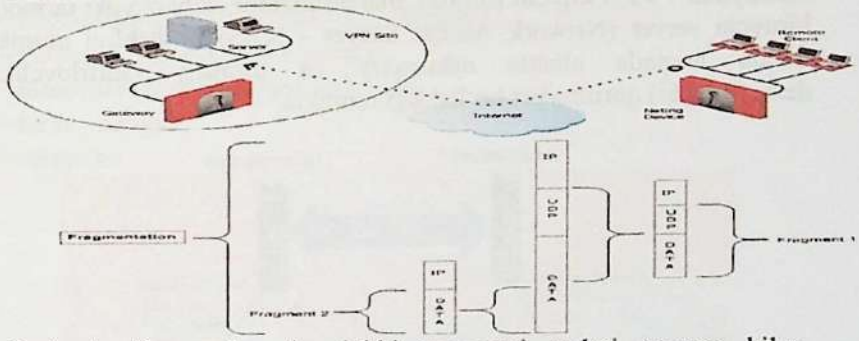


Virtual himoyalangan tunnel sxemasi

4.5. Tarmoqlararo ekranlash texnologiyalari. VPN texnologiyasi

Tarmoq perimetri - ichki sinalgan tarmoq bilan tashqi tarmoqlardan ajratib turuvchi chegara hisoblanadi. Perimetr - tashqi hujumlardan himoyalovchi birinchi liniya bo'ladi. Ushbu perimetrni himoyalovchi vositalar:

- Tarmoqlararo ekranlar (TE);
- Tarmoq qatlamidagi antivirus tizimlari;
- VPN (Virtual Private Network) - shaxsiy vertual tarmoq yaratish qurilmalari.



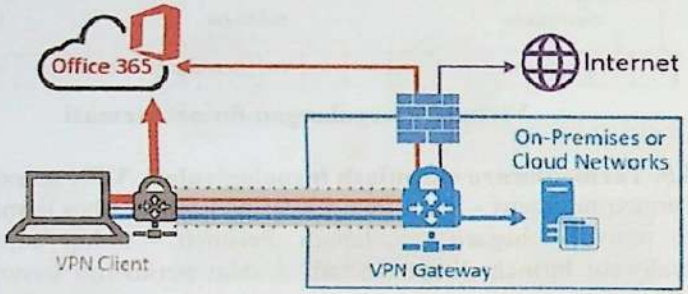
Perimetr himoyasi - bu ichki tarmoqni tashqi tarmoq bilan xarakatini nazorat etish, ya'ni:

- Internet tarmog'iga ulanish;
- Simsiz aloqa segmentlari;
- Uzoqdan kirish Serveri;

- Filiallarga ajratilgan liniyalar.

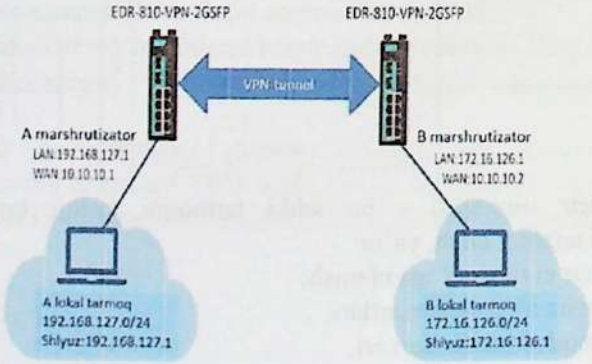
Vertual shaxsiy tarmoqlar ikkita bir biridan ancha uzoqda joylashgan LAN ya'ni mahalliy kompyuter tarmoqlarini bir biri bilan bog'langan aloqa kanallarida axborotlarni almashinuvini havfsizligini ta'minlab beradi. Ya'ni VPN ikki LAN-to-LAN orasidagi yoki Remote(uzoqlashgan) Access VPN - uzoqdagi filiallarni asosiy tarmoqqa kirishi paytida himoyani ta'minlaydi.

VPN ni yaratish paytida tunnellashtirish yoki inkapsulyatsiyalash usulidan foydalaniladi.



Ushbu texnologiya aloqa kanali orqali bir tarmoqdan ikkinchi tarmoqqa paketlarni uzatadi. Shu paytda birinchi tarmoq paketi inkapsulyatsiyalanadi va ko'rinadi.

Tunnel - bu ochiq virtual kanal hisoblanadi, bosh nuqtasi sifatida kompyuter - VPN kliyent (mijoz), marshrutizator, shlyuz yoki tarmoqqa kiruvchi server (Nrtwork Access Server - NAS) bo'lishligi mumkin. Ikkala nuqtada albatta uskunaviy va dasturiy (shifrlovchi / deshifrlovchi) qurilmalari bo'lishligi mumkin.



Shifrlangan va inkapsulyatsiya qilingan paketlar har xil marshrutlar orqali oxirgi nuqtaga yetkaziladi. Tunnelning asosiy vazifasi - konfidentsiallikni ta'minlashdan iborat.

VPNlarni amalga oshirish usullari

1. Tarmoqlararo ekranlar asosida VPN yaratish. Ushbu variantda ma'lumot paketlarini himoyalash uchun barcha lokal tarmoqlarida faqat bir dona texnikaviy-dasturiy kompleks ishlatiladi.

2. Tarmoq tugunining operatsion tizimiga o'rnatilgan VPN. Ushbu variant eng ma'qul hisoblanib, standart operatsion tizim vositalari asosida bajariladi.

3. Ichki tarmoq bilan umumiy tashqi tarmoq orasida maxsus kriptografik shlyuz asosida VPN tashkil etiladi.

4. VPN kriptografik himoyalash marshrutizatori asosida tuzilgan bo'ladi. Ushbu usul yuqori samarali hisoblanadi, ammo ancha narxi baland bo'ladi.

VPN tasnishlanishi quyidagicha:

–amalga oshirish usuliga ko'ra;
–dasturiy kompleks;
–apparat-dasturiy kompleks;
–integrasiyalashgan yechim.
–o'rnatilishiga ko'ra;
–korporatsiya ichidagi VPN tarmoq;
–masofadan foydalanuvchi VPN tarmoq;
–korporatsiyalararo VPN tarmoq.
–himoyalanganlik darajasiga ko'ra;
–himoyalangan;
–ishonchli.

Marshrutizatorlar asosidagi VPN

VPN qurishning ushbu usuliga binoan himoyalangan kanallarni yaratishda marshrutizatorlardan foydalaniladi. Lokal tarmoqdan chiquvchi barcha axborot marshrutizator orqali o'tganligi sababli, unga

shifrlash vazifasini yuklash tabiiy. Marshrutizator asosidagi VPN asbob-uskunalariga misol tariqasida Cisco-Systems kompaniyasining qurilmalarini ko'rsatish mumkin.

Tarmoqlararo ekranlar asosidagi VPN

Aksariyat ishlab chiqaruvchilarning tarmoqlararo ekrani tunnellash va ma'lumotlarni shifrlash vazifalarini madadlaydi. Tarmoqlararo ekranlar asosidagi yechimga misol tariqasida Check Point Software Technologies kompaniyasining Fire Wall-1 mahsulotini ko'rsatish mumkin. Shaxsiy kompyuter asosidagi tarmoqlararo ekranlar faqat uzatiluvchi axborot hajmi nisbatan kichik bo'lgan tarmoqlarda qo'llaniladi. Ushbu usulning kamchiligi bitta ishchi o'rniga hisoblanganda yechim narhining yuqoriligi va unumdorlikning tarmoqlararo ekran ishlaydigan apparat ta'minotiga bog'liqligi.

Dasturiy ta'minot asosidagi VPN

Dasturiy usul bo'yicha amalga oshirilgan VPN mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan qurilmadan qolishsada, VPN-tarmoqlarni amalga oshirilishida yetarli quvvatga ega. Ta'kidlash lozimki, masofadan foydalanishda zaruriy o'tkazish polosasiga talablar katta emas. Shu sababli, dasturiy mahsulotlarning o'zi masofadan foydalanish uchun yetarli unumdorlikni ta'minlaydi. Dasturiy mahsulotlarning shubhasiz afzalligi—qo'llanilishining moslanuvchanligi va qulayligi, hamda narxining nisbatan yuqori emasligi.

Ixtisoslashtirilgan apparat vositalari asosidagi VPN

Ixtisoslashtirilgan apparat vositalari asosidagi VPNlarning eng muhim afzalligi unumdorligining yuqoriligidir. Ixtisoslashtirilgan VPN tizimlarda shifrlashning mikrosxemalarda amalga oshirilishi tezkorlikning ta'minlanishiga sabab bo'ladi. Ixtisoslashtirilgan VPN-qurilmalar xavfsizlikning yuqori darajasini ta'minlaydi, ammo ularning narhi anchagina yuqori.

Kanal sathidagi VPN

OSI modelining kanal sathida ishlatiluvchi VPN vositalari uchinchi (va yuqoriroq) sathning turli xil trafigini inkapsulatsiyalashni ta'minlashga va "nuqta-nuqta" tilidagi virtual tunnellarni (marshrutizatordan marshrutizatorga yoki shaxsiy kompterdan lokal hisoblash tarmog'ining shlyuzigacha) qurishga imkon beradi.

Tarmoq sathidagi VPN

Tarmoq sathidagi VPN-mahsulotlar IPni IPga inkapsulyatsiyalashni bajaradi. Bu sathdagi keng tarqalgan protokollardan biri SKIP protokolidir. Ammo bu protokolni autentifikatsiyalash, tunnellash va IP-paketlarni shifrlash uchun atalgan IPSec(IPSecurity) protokoli asta-sekin surib chiqarmoqda.

Seans sathidagi VPN

Ba'zi VPNlar "kanal vositachilari" (circuit proxy) deb ataluvchi usuldan foydalanadi. Bu usul transport sathi ustida ishlaydi va har bir soket uchun alohida trafikni himoyalangan tarmoqdan umumfoydanuvchi Internet tarmog'iga retranslyatsiyalaydi. (IP soketi TCP-ulanishning va muayyan port yoki berilgan port UDP kombinatsiyasi orqali identifikatsiyalanadi. TCP/IP stekida beshinchi-seans sathi bo'lmaydi, ammo soketlarga mo'ljallangan amallarni ko'pincha seans sathi amallari deb yuritishadi.)

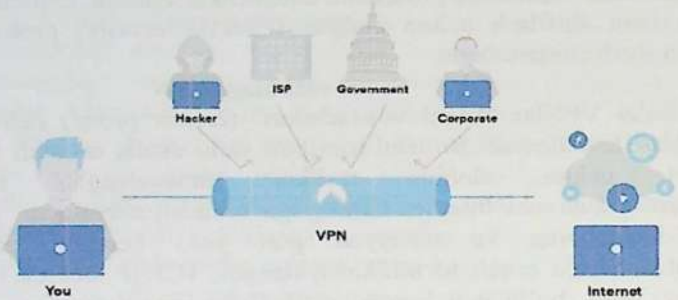
Lokal tarmoqdan chiquvchi barcha axborot marshrutizator orqali o'tganligi sababli, unga shifrlash vazifasini yuklash tabiiy. Marshrutizator asosidagi VPN asbob-uskunalariga misol tariqasida Cisco-Systems kompaniyasining qurilmalarini ko'rsatish mumkin.

Shaxsiy kompyuter asosidagi tarmoqlararo ekranlar faqat uzatiluvchi axborot hajmi nisbatan kichik bo'lgan tarmoqlarda qo'llaniladi. Ushbu usulning kamchiligi bitta ishchi o'rniga hisoblanganda yechim narhining yuqoriligi va unumdorlikning tarmoqlararo ekran ishlaydigan apparat ta'minotiga bog'liqligi. Dasturiy ta'minot asosidagi VPN. Dasturiy usul bo'yicha amalga oshirilgan VPN mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan qurilmadan qolishsada, VPN-tarmoqlarni amalga oshirilishida yetarli quvvatga ega.

Ta'kidlash lozimki, masofadan foydalanishda zaruriy o'tkazish polosasiga talablar katta emas. Shu sababli, dasturiy mahsulotlarning o'zi masofadan foydalanish uchun yetarli unumdorlikni ta'minlaydi. Dasturiy mahsulotlarning shubhasiz afzalligi—qo'llanilishining moslanuvchanligi va qulayligi, hamda narxining nisbatan yuqori emasligi.

Ixtisoslashtirilgan VPN qurilmalar xavfsizlikning yuqori darajasini ta'minlaydi, ammo ularning narhi anchagina yuqori. OSI modelining ish sathi bo'yicha VPNning turkumlanishi Kanal sathidagi VPN OSI modelining kanal sathida ishlatiluvchi VPN vositalari uchinchi (va yuqoriroq) sathning turli xil trafigini inkapsulatsiyalashni ta'minlashga

va "nuqta-nuqta" tilidagi virtual tunnellarni (marshrutizatordan marshrutizatorga yoki shaxsiy kompterdan lokal hisoblash tarmog'ining shlyuzigacha) qurishga imkon beradi. Tarmoq sathidagi VPN.



Tarmoq sathidagi VPN-mahsulotlar IPni Ipga inkapsulyatsiyalashni bajaradi. Bu sathdagi keng tarqalgan protokollardan biri SKIP protokolidir. Ammo bu protokolni autentifikatsiyalash, tunnellash va IPpaketlarni shifrlash uchun atalgan IPSec(IPSecurity) protokoli asta-sekin surib chiqarmoqda. Seans sathidagi VPN ba'zi VPNlar "kanal vositachilari" (circuit proxy) deb ataluvchi usuldan foydalanadi. Bu usul transport sathi ustida ishlaydi va har bir soket uchun alohida trafikni himoyalangan tarmoqdan umumfoydanuvchi Internet tarmog'iga retranslyatsiyalaydi. (IP soketi TCP-ulanishning va muayyan port yoki berilgan port UDP kombinatsiyasi orqali identifikatsiyalanadi. TCP/IP stekida beshinchi-seans sathi bo'lmaydi, ammo soketlarga mo'ljallangan amallarni ko'pincha seans sathi amallari deb yuritishadi.)

Zamonaviy telekommunikatsion tarmoqlarida axborot havfsizligini ta'minlash texnologiyalari obyektlarda qo'lanilishini ko'rib chiqamiz.

4.6. Obyektlarning tizimiga ruxsatsiz kirishning oldini olish

Elektron kommunikatsiyalarning zamonaviy texnologiyalari keyingi yillarda ishbilarmonlarga aloqa kanallari bo'yicha axborotning turlicha ko'rinishlari (masalan: faks, video, kompyuterli, nutqli axborotlar)ni uzatishda ko'pgina imkoniyatlar yaratib bermoqda. Zamonaviy ofis bugungi kunda aloqa vositalari va tashkiliy texnika bilan haddan tashqari to'ldirib yuborilgan va ularga telefon, faks, avtojavob apparati, modem, skaner, shaxsiy kompyuter va h.k. kiradi.

Zamonaviy texnika uchun axborot-kommunikatsiyalar texnologiyasi kompyuterlar telefoniyasi rivojlanishi bilan katta turtki

berildi. Bor-yo'g'i o'n yil ilgari sotuvga CANON firmasining narxi 6000 AQSh dollari bo'lgan «Navigator» nomli mahsuloti chiqarilgan edi va u birinchi tizimlardan hisoblanadi. Kompyuter telefoniyasi oxirgi o'n yil ichida juda tez sur'atlar bilan rivojlandi.

Hozirgi paytda sotuvda mavjud bo'lgan «PC Phone» (Export Industries Ltd, Israel) mahsulotining narxi bor-yo'gi 1000 Germaniya markasi turadi. «Powerline-II» (Talking Technology, ShA)ning narxi esa 800 AQSh dollari turadi. Keyingi paytlarda kompyuter telefoniyasi yunalishida 70% apparat vositalarini Dialogue (USA) firmasi ishlab chikarmoqda. Kompyuter telefoniyasida axborotlarning xavfsizligini ta'minlash katta ahamiyatga ega.

Kompyuter telefoniyasining himoyasini yetarli darajada ta'minlash uchun Pretty Good Privacy Inc. firmasining PC Phone 1.0 dasturiy paketi ishlab chiqarilgan. U kompyuter telefoniyasi orqali uzatilayotgan axborotlarni himoyalash uchun axborotlarni raqamli ko'rinishga o'tkazadi va qabul paytida esa dasturiy-texnik vositalar yordamida qayta ishlaydi. Zamonaviy kompyuter telefoniyasi vositalarining shifrlash tezligi ham juda yuqoridir, xato qilish ehtimoli esa juda kichikdir.

Bevosita telekommunikatsiya kanallarida axborot xavfsizlikni ta'minlash usul va vositalarini quyidagicha tasniflash mumkin. To'sqinlik apparatlarga, ma'lumot tashuvchilarga va boshqalarga kirishga fizikaviy usullar bilan qarshilik ko'rsatish deb aytiladi.

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

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

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

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

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

Undamoq — axloqiy va odobiy qoidalarga binoan qabul qilingan tartiblarni bajarishga yo'naltirilgan.

Yuqorida keltirilgan usullarni amalga oshirishda quyidagicha tasniflangan vositalarni tadbiq etishadi.

Rasmiy vositalar — shaxslarni ishtirokisiz axborotlarni himoyalash funksiyalarini bajaradigan vositalardir.

Norasmiy vositalar — bevosita shaxslarni faoliyati yoki uning faoliyatini aniqlab beruvchi reglamentlardir.

Dasturiy vositalar — bu axborotlarni himoyalash funksiyalarini bajarish uchun mo'ljallangan maxsus dasturiy ta'minotdir. Axborotlarni himoyalashda birinchi navbatda eng keng qo'llanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parol tizimini keltirish mumkin.

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

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

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

Havfsizlikni ta'minlash usullari va vositalarining rivojlanishini uch bosqichga ajratish mumkin:

1) dasturiy vositalarni rivojlanishi;

2) barcha yo'nalishlar bo'yicha rivojlanishi;

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

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

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

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

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

— uzatiladigan ma'lumotlarni ochib o'qishdan saqlanish;

— uzatiladigan ma'lumotlarni tahlil qilishdan saqlanish;

—uzatiladigan ma'lumotlarni o'zgartirishga yo'l qo'ymaslik va o'zgartirishga urinishlarni aniqlash;

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

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

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

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

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

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

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

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

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

Stoxastik testlarni tashkillashtirish vositalari — axborot tizimlarining sifati va ishonchliligini tekshirishda qo'llaniladigan vositadir.

Aniq yo'naltirilgan testlar — AKTning sifati va ishonchliligini tekshirishda qo'llaniladi.

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

Statistik tahlilgichlar — dasturlarning tuzilish tarkibidagi kamchiliklarni aniqlash, dasturlar kodida aniqlanmagan kirish va chikish nuqtalarini topish, dasturdagi o'zgaruvchilarni to'g'ri aniqlanganligini va ko'zda tutilmagan ishlarni bajaruvchi kiyem dasturlarini aniqlashda foydalaniladi.

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

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

Misol sifatida quyidagi vositalarni keltirish mumkin:

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

- Security Administrator Tool for ANALYZING Networks (SATAN) — dasturiy ta'minot bo'lib, bevosita tarmoqning zaif tomonlarini aniqlaydi va ularni bartaraf etish yo'llarini ko'rsatib beradi. Ushbu yo'nalish bo'yicha bir necha dasturlar ishlab chiqilgan, masalan: Internet Security Scanner, Net Scanner, Internet Scanner va boshqalar.

- NBS tizimi - - dasturiy-texnik vosita bo'lib, aloqa kanallaridagi ma'lumotlarni himoyalashda qo'llaniladi;

- Free Space Communication System — tarmoqda ma'lumotlarning har xil nurlar orqali, masalan lazerli nurlar orqali almashuvini ta'minlaydi;

- SDS tizimi — ushbu dasturiy tizim ma'lumotlarini nazorat qiladi va qaydnomada aks ettiradi. Asosiy vazifasi ma'lumotlarni uzatish vositalariga ruxsatsiz kirishni nazorat qilishdir;

- Timekey — dasturiy-texnik uskunadir, bevosita EHMning parallel portiga o'rnatiladi va dasturlarni belgilangan vaqtda keng qo'llanilishini taqiqlaydi;

- IDX — dasturiy-texnik vosita, foydalanuvchining barmoq izlarini «o'qib olish» va uni tahlil qiluvchi texnikalardan iborat bo'lib, yuqori sifatli axborot xavfsizligini ta'minlaydi. Barmoq izlarini o'qib olish va xotirada saqlash uchun 1 minutgacha, uni taqqoslash uchun esa 6 sekundgacha vaqt talab qilinadi.

4.7. Obyektlarning kompyuter tarmoqlaridagi ma'lumotlarni himoyalashning asosiy yo'nalishlari

Axborotlarni himoyalashning mavjud usul va vositalari hamda kompyuter tarmoqlari kanallaridagi aloqaning xavfsizligini ta'minlash texnologiyasi evolyutsiyasini solishtirish shuni ko'rsatmoqdaki, bu texnologiya rivojlanishining birinchi bosqichida dasturiy vositalar afzal topildi va rivojlanishga ega bo'ldi, ikkinchi bosqichida himoyaning hamma asosiy usullari va vositalari intensiv rivojlanishi bilan xarakterlandi.

Uchinchi bosqichida esa quyidagi tendentsiyalar ravshan bo'lmoqda:

— axborotlarni himoyalash asosiy funksiyalarining texnik jixatdan amalga oshirilishi;

—bir nechta xavfsizlik funksiyalarini bajaruvchi himoyalashning birgalikdagi vositalarini yaratish;

— algoritm va texnik vositalarni unifikatsiya qilish va standartlashtirish.

Kompyuter tarmoqlarida xavfsizlikni ta'minlashda hujumlar yuqori darajada malakaga ega bo'lgan mutaxassislar tomonidan amalga oshirishini doim esda tutish lozim. Bunda ularning harakat modellaridan doimo ustun turuvchi modellar yaratish talab etiladi. Bundan tashqari, avtomatlashtirilgan axborot tizimlarida inson eng ta'sirchan qismlardan biridir. Shuning uchun, yovuz niyatli shaxsga axborot tizimi personalidan foydalana olmaslik chora-tadbirlarini o'tkazib turish ham katta ahamiyatga ega.

Internet tarmoqda mavjud aloqaning himoyasini (xavfsizligini) ta'minlash asoslari ma'lumotlarni uzatish tizimlarining rivojlanishi va ular asosida yaratilgan telekommunikatsiya xizmat kursatish vositalarining yaratilishi bevosita foydalanuvchilarga tarmoq zaxiralaridan foydalanish tartiblarini ishlab chiqarish zaruriyatini paydo qildi:

- foydalanuvchining anonimligini ta'minlovchi vositalar;
- serverga kirishni ta'minlash.
- Server faqatgina bitta foydalanuvchiga emas, balki keng miqyosdagi foydalanuvchilarga o'z zaxiralaridan foydalanishga ruxsat berishi kerak;
- ruxsatsiz kirishdan tarmoqni himoyalash vositalari. Internet tarmogida ruxsatsiz kirishni taqiqlovchi tarmoqlararo ekran - Fire Wall vositalari keng tarqalgan. Ushbu vosita asosan UNIX operatsion tizimlarida qo'llanilib, bevosita tarmoqlar orasida aloqa o'rnatish jarayonida xavfsizlikni ta'minlaydi.

IV bob xulosasi

Ushbu bobda identifikatsiya, autentifikatsiya va avtotizatsiya jarayonlarini obyekrlarda qo'llanish davrlarini, ma'lumotlarni obyektga kirayotgan va ularni tekshirish vositalari va usullari ko'rib chiqilgan. Ruhsatsiz kirayotgan va obyektlarga qilinayotgan hujumlarni aniqlovchi texnikaviy qurilmalari tahlil qilingan va ularnin xarakteristikalarini keltirilgan. Hozirgi kunda eng dolzarb bo'lgan virtual korporativ tarmoqlarni tashkillashtirish masalalari keng yoritilib berilgani uchun tarmoqlararo ekranlarni qo'llash natijasida va obyektlarning tizimiga ruxsatsiz kirishning oldini olish uchun himoyalashning asosiy yo'nalishlari keltirilgan.

V BOB.
OBYEKTLARNING AXBOROTLARINI UZATISH VA QABUL QILISHDA KRIPTOTIZIMDAN FOYDALANISH

5.1. Obyektlarlar orasida axborotlarni uzatish va qabul qilishda ishlatiladigan telekommunikatsiya aloqa kanallari

Tadqiqot obyekti simli va simsiz radio kanallariga ega telekommunikatsiya tarmog'i va axborot jo'natuvchilar va oluvchilar (AJO) o'rtasida ishonchli va xavfsiz aloqani ta'minlash uchun mo'ljallangan vaqtni o'zgartiruvchi tuzilmadir.

Ma'lumki, har qanday telekommunikatsiya tarmog'i axborotni belgilangan vaqt, ishonchlilik, uzatish va himoyalash ishonchliligi uchun belgilangan talablarga javob berish uchun tegishli iste'mol obyektlariga axborot olib kelish vazifasini bajaradi.

Axborotni himoya qilish mas'uliyati asosan telekommunikatsiya vositalari bilan bog'liq.

XXI asr jamiyatning barcha sohalarini axborotlashtirish, globallashtirish va texnologiyalashtirish bilan ajralib turadi, bu esa fan, ta'lim, ishlab chiqarish va boshqaruv rivojlanishining yanada global tendensiyalarini belgilab beradi. Har qanday mamlakat iqtisodiyotini rivojlantirish, turli sohalarda kompaniyalar faoliyatini kengaytirish, ma'lumotlarni saqlash, qayta ishlash, uzatish va himoya qilish, samaradorlikni oshirish istagini yaxshilash zarurati-ijtimoiy voqelikning turli sohalarini axborotlashtirish va axborot-kommunikatsiya texnologiyalarini joriy etishda davlat ehtiyojlarini belgilovchi omillar hisoblanadi.

Obyektlar orasidagi axborot tizimlariga qo'yiladigan asosiy talablar axborot resurslarining mavjudligi, yaxlitligi va maxfiyligini ta'minlash va infratuzilmani qo'llab-quvvatlashdan iborat bo'ladi.

Ovozli xabarlar, video tasvirli axborot, kompyuter ma'lumotlari va boshqalar telekommunikatsiya tarmog'i orqali turli rejimlarda va turli uzatish tezliklarida uzatiladi. Ayniqsa, hozirgi vaqtda xalqaro kompyuter tarmog'i Internet tarmog'iga ulanish juda tez bo'lib, telekommunikatsiya transport va abonent tarmoqlaridan foydalanadi.

Hozirgi vaqtda axborot texnologiyalari shu qadar tez o'zgarmoqdaki, xavfsizlik mexanizmlari tizimning to'liq himoyasini ta'minlamay qolmoqda.

Har qanday zamonaviy axborot tizimini qurishda, ba'zi himoya mexanizmlarini ishlab chiqish va amalga oshirmaslik deyarli mumkin emas. Bu oddiy mexanizmlar (masalan, paketli filtrlash) yoki juda

murakkab (masalan, xavfsizlik devorlarida Stateful tekshiruv texnologiyasidan foydalanish) bo'lishi mumkin. Bunday mexanizmlar bo'lmasligi ham mumkin. Bunday holda loyihalashtirilgan tizimning axborot xavfsizligi telekommunikatsiya tarmog'iga yoki biron-bir qo'shimcha himoya vositasiga beriladi. Bu vazifa esa axborot tizimining tarkibiy qismlarini o'zgartirish va yangilash, operatsion tizim konfiguratsiyasini o'zgartirish va hokazolarda vaqti-vaqti bilan sodir bo'lib turadi.

Obyektlar orasidagi telekommunikatsiya tarmoqlarida har xil turdagi aloqa kanallari va axborotni muhofaza qilish vositalariga ega bo'lgan tarmoqlarni qurishda optimallashtirish mezoni sifatida ularni qurishning umumiy xarajatlarini ham hisobga olish zarur.

Ko'rib chiqilayotgan subyektning o'ziga xos xarakteristikalari turli usullar va uzatish usullari uchun o'zgaruvchan xarakteristikalarga ega. Simli, optik-tolali, radio aloqa kanallari majmuasidan foydalanish, ya'ni mobil aloqa tayanch stantsiyalaridan xabarlarni bir vaqtning o'zida ushbu mobil kompaniya abonentlari to'plamiga uzatish, mobil uyali aloqa tarmog'i hisoblanadi.

Telekommunikatsiya tarmoqlariga qo'yiladigan talablar va tarmoqning ishlash sifatini baholash ko'rsatkichlari boshqaruv tizimini yuritish manfaatlaridan kelib chiqib taqozo etiladi. Telekommunikatsiya tizimlariga qo'yiladigan barcha talablarni yagona ro'yxatda qamrab olish qiyin. Ayrim mutaxassislarning fikricha, hozirgi vaqtda kommunikatsiyalarning umumiy samaradorligini aniqlash usullari mavjud emas, biroq bu usullarni alohida aloqa tarmoqlari uchun topishga urinishlar mavjud.

Tarmoqning ish sifatini baholash uchun quyidagi asosiy xarakteristikalarini hisobga olish mumkin:

- axborotni yetkazib berish vaqti, ya'ni uni taqdim etish zarur bo'lgan vaqtdan boshlab, undan foydalanish nuqtasiga kelgunga qadar bo'lgan vaqt;
- xabar yetkazishning ishonchliligi, ya'ni adresatga to'g'ri xabar yetkazish ehtimoli, xatolik darajasi;
- qabul qilingan xabarning ishonchliligi, ya'ni uzatilayotgan xabarning qabul qilingan axborot himoyasiga muvofiqlik darajasi;
- uzatilayotgan xabarning foydalanuvchiga havfsizligini ta'minlash.

Ishonchlilik, yetkazib berish muddati va ishonchlilik standartlari har bir alohida xabar yoki xabarlarning ma'lum guruhlari (toifalari) uchun muhimlik, dolzarbligi va semantik mazmuni asosida birlashtirilgan holda farqlanadi.

Murakkab telekommunikatsiya tarmoqlarida quyidagi xarakteristikalar ham muhim rol o'ynaydi:

- javob vaqti - so'rov uzatishning oxiridan javob boshlanishigacha bo'lgan vaqt. Tizimning javob vaqti aloqa vositalari va kompyuterda axborotni qayta ishlash vaqtiga bog'liq;
- telekommunikatsiya tarmog'ining ishlashi - tarmoqdagi vaqt birligiga uzatiladigan axborotning maksimal yoki o'rtacha miqdori;
- jo'natuvchidan qabul qiluvchiga xabarlarning ayrim turlarini uzatishda axborotning maxfiyliyligi.

Shuningdek, tarmoqning bunday xarakteristikalarini telekommunikatsiya tarmog'i tuzilmasining tasodifiy buzilishiga qarshilik ko'rsatish va xabarlar hajmining funktsiyasi sifatida ishlatish xarajatlari, ularni uzatishdagi kechikishlar va boshqalarni ham aytib o'tish mumkin.

5.2. Ma'lumotlarni himoyalashda kriptosistemalardan foydalanish

Axborotni himoyalash uchun kodlashtirish va kriptografiya usullari qo'llaniladi.

«Kriptografiya» atamasi dastlab «yashirish, yozuvni berkitib qo'ymoq» ma'nosini bildirgan. Birinchi marta u yozuv paydo bo'lgan davrlardayoq aytib o'tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya'ni diskda sakdanadigan sonlar ko'rinishida yoki hisoblash tarmoklarida uzatiladigan xabarlar ko'rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo'lgan har qanday axborotga nisbatan qo'llash mumkin.

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

Axborotning yaxlitligini tekshirishning bunday jarayoni, ko'p hollarda, axborotning haqiqiyligini ta'minlash deyiladi. Kriptografiyada qo'llaniladigan usullar ko'p bo'lmagan o'zgartirishlar bilan axborotlarning haqiqiyligini ta'minlashi mumkin. Nafaqat axborotning kompyuter tarmog'idan ma'nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch hosil qilish juda muhim.

Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiklovchi turli usullar ma'lum.

Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo'lmagan protsedura. Chunki parolni qo'lga kiritgan har qanday shaxs axborotdan foydalanishi mumkin bo'ladi.

Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish va ularni kriptografik usullar bilan himoyalash mumkin, lekin kriptografiya bundan kuchliroq parolni uzluksiz o'zgartirish imkonini beradigan protseduralarni ham ta'minlaydi. Kriptografiya sohasidagi oxirgi yutuqlardan biri — raqamli signatura — maxsus xossa bilan axborotni to'ldirish yordamida yaxlitlikni ta'minlovchi usul, bunda axborot uning muallifi bergan ochiq kalit ma'lum bo'lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik tekshiriladigan ma'lum usullardan ko'proq afzalliklarga ega.

Kriptografiya usullarini qo'llashning ba'zi birlarini ko'rib chiqamiz. Uzatiladigan axborotning ma'nosini yashirish uchun ikki xil o'zgartirishlar qo'llaniladi: kodlashtirish va shifrlash. Kodlashtirish uchun tez-tez ishlatiladigan iboralar to'plamini o'z ichiga oluvchi kitob yoki jadvallardan foydalaniladi. Bu iboralardan har biriga, ko'p hollarda, raqamlar to'plami bilan beriladigan ixtiyoriy tanlangan kodli so'z to'g'ri keladi. Axborotni kodlash uchun xuddi shunday kitob yoki jadval talab qilinadi. Kodlashtiruvchi kitob yoki jadval ixtiyoriy kriptografik o'zgartirishga misol bo'ladi.

Kodlashtirishning axborot texnologiyasiga mos talablar — qatorli ma'lumotlarni sonli ma'lumotlarga aylantirish va aksincha o'zgartirishlarni bajara bilish. Kodlashtirish kitobini tezkor hamda tashqi xotira qurilmalarida amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik tizimni muvaffaqiyatli deb bo'lmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, koddarning yangi kitobini yaratish va uni hamma foydalanuvchilarga tarqatish zaruriyati paydo bo'ladi.

Kriptografik o'zgartirishning ikkinchi turi shifrlash o'z ichiga — boshlang'ich matn belgilarini anglab olish mumkin bo'lmagan shaklga o'zgartirish algoritmlarini qamrab oladi. O'zgartirishlarning bu turi axborot-kommunikatsiyalar texnologiyalariga mos keladi. Bu yerda algoritmni himoyalash muhim ahamiyat kasb etadi. Kriptografik kalitni qo'llab, shifrlash algoritmining o'zida himoyalashga bo'lgan talablarni kamaytirish mumkin.

Himoyalash obyekti sifatida faqat kalit xizmat qiladi. Agar kalitdan nusxa olingan bo'lsa, uni almashtirish mumkin va bu kodlashtiruvchi kitob yoki jadvalni almashtirishdan yengildir. Shuning uchun ham kodlashtirish emas, balki shifrlash axborot-kommunikatsiyalar texnologiyalarida keng ko'lamda qo'llanilmoqda. Sirli (maxfiy) aloqalar sohasi kriptologiya deb aytiladi.

Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta'minlaydi. Masalan, to'lov varaqlarini elektron pochta orqali uzatishda uning o'zgartirilishi yoki soxta yozuvlarning qo'shilishi mumkin. Bunday hollarda axborotning yaxlitligini ta'minlash zaruriyati paydo bo'ladi. Umuman olganda kompyuter tarmog'iga ruxsatsiz kirishning mutlako oldini olish mumkin emas, lekin ularni aniqlash mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko'p hollarda, axborotning haqiqiyligini ta'minlash deyiladi.

Demak, kriptografiya so'zi yunoncha «kripto» — sirli va «logus» — xabar ma'nosini bildiruvchi so'zlardan iborat ekan. Kriptologiya ikki yo'nalish, ya'ni kriptografiya va kriptotahlildan iborat.

Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta'minlashdan iborat.

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

Hozirgi kunda kriptotizimni ikki sinfga ajratish mumkin:

- simmetriyali bir kalitlilik (maxfiy kalitli);
- asimmetriyali ikki kalitlilik (ochiq kalitli).

Bir kalitli simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

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

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

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

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

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

– foydalanuvchini autentifikatsiyalash, ya'ni kompyuter tizimi zaxiralariga kirmoqchi bo'lgan foydalanuvchini aniqlash;

– tarmoq abonentlari aloqasini o'rnatish jarayonida ularni o'zaro autentifikatsiyalash.

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

Bu holda ximoyalangan kanal bo'yicha ochiq kalit jo'natilib, maxfiy kalit jo'natilmaydi.

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

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

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

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo'yiladi:

– yetarli darajada kriptomustaxkamlik;
– shifrlash va kaytarish jarayonining oddiyligi;
– axborotlarni shifrlash oqibatida ular hajmining ortib ketmasligi;
– shifrlashdagi kichik xatolarga ta'sirchan bo'lmasligi.

Ushbu talablarga quyidagi tizimlar javob beradi:

– o'rinlarini almashtirish;
– almashtirish;
– gammalashtirish;
– analitik o'zgartirish.

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

Almashtirish shifrlash usuli bo'yicha boshlang'ich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtiriladi.

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

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

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

- shifrlovchi jadval;
- sehrli kvadrat.

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

Hozirgi vaqtda kompyuter tarmoqlarida tijorat axborotlari bilan almashishda uchta asosiy algoritmlar, ya'ni DES, CLIPPER va PGP algoritmlari qo'llanilmoqda. DES va CLIPPER algoritmlari integral sxemalarda amalga oshiriladi.

PGP orqali shifrlangan axborotlarni ochish uchun, superkompyuterlar ishlatilganda bir asr ham kamlik qilishi mumkin. Bulardan tashqari, axborotlarni tasvirlarda va tovushlarda yashirish dasturlari ham mavjud. Masalan, S-tools dasturi axborotlarni BMP, GIF, WAV kengaytmali fayllarda saqlash uchun qo'llaniladi. Ba'zi hollarda yashirilgan axborotning hajmi rasmning hajmidan ko'p bo'lishi ham mumkin, ya'ni olingan natija faqatgina tanlangan rasmga bog'liq bo'ladi.

Kundalik jarayonda foydalanuvchilar ofis dasturlari va arxivatorlarni qo'llab kelishadi. Arxivatorlar, masalan PkZip dasturida ma'lumotlarni parol yordamida shifrlash mumkin. Ushbu fayllarni ochishda ikkita, ya'ni lug'atli va to'g'ridan-to'g'ri usuldan foydalanishadi. Lug'atli usulda bevosita maxsus fayldan so'zlar parol

o'rniga qo'yib tekshiriladi, to'g'ridan-to'g'ri usulda esa bevosita belgilar kombinatsiyasi tuzilib, parol o'rniga qo'yib tekshiriladi.

Ofis dasturlari (Word, Excel, Access) orqali himoyalash umuman taklif etilmaydi. Bu borada mavjud dasturlar internetda to'siqsiz tarqatiladi.

Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

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

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

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

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

Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

– foydalanuvchini autentifikatsiyalash, ya'ni kompyuter tizimi zaxiralariga kirmoqchi bo'lgan foydalanuvchini aniqlash:

– tarmoq abonentlari aloqasini o'rnatish jarayonida ularni o'zaro autentifikatsiyalash.

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

5.3. Ixtisoslashtirilgan kommunikatsion kompyuter tizimlarida axborot xavfsizligini ta'minlash

Brandmauer - bu tarmoqlararo ekran bo'lib tarmoqdan kirib kelayotgan ma'lumotlarni filtrlash funksiyasini bajaradi. Ko'pincha shunday tarmoqlararo ekran sifatida firewall (fayrvol) termini ishlatiladi, lekin brandmauer deyilganda tarmoqlararo Windows ekrani tushuniladi. Windows brandmaueri kompyuter bilan tarmoqni ulangan qismida operatsion tizimga kirishdan saqlaydi. Ushbu brandmauerda lokal kompyuter tarmog'idan kompyuterga tarmoq paketlarini kirishini yoki qo'ymaslikni qoidalari bo'ladi. Shu qoidalar protokol, port yoki

dasturlar asosida trafikni filtrlaydi. Windows brandmauerida o'zining mo'ljallangan qoidalari bo'lib, administrator ushbu qoidalarni o'zgartirishi yoki unga qo'shishi mumkin.

Demak, tarmoqlararo ekran (TE) - brandmauer yoki firewall sistemasi deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko'p qismlarga ajratish va ma'lumot paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o'tish shartlarini belgilovchi qoidalar to'plamini amalga oshirish imkonini berar ekan.

Odatda, bu chegara korxonaning korporativ (lokal) tarmog'i va internet global tarmoq orasida o'tkaziladi. Tarmoqlararo ekranlar garchi korxona lokal tarmog'i ulangan korporativ intratarmog'idan qilinuvchi hujumlardan himoyalashda ishlatilishlari mumkin bo'lsada, odatda ular korxona ichki tarmog'ini internet global tarmoqdan suqilib kirishdan himoyalaydi. Aksariyat tijorat tashkilotlari uchun tarmoqlararo ekranlarning o'rnatilishi ichki tarmoq xavfsizligini ta'minlashning zaruriy sharti hisoblanadi.

Korporativ tarmoqlarda eshelon himoyaning asosiy elementlaridan biri tarmoqlararo ekrandir. Bundan tashqari tarmoqlararo ekran ichki va tashqi perimetrlarning birinchi himoya qurilmasi hisoblanadi. Tarmoqlararo ekran (TE) lokal (bir komponentli) yoki funktsional taqsimlangan vosita (kompleks) bo'lib, u AKTlarida kiruvchi va chiquvchi ma'lumotlarni boshqaradi va ma'lumotlarni filtrlash orqali AKT himoyasini ta'minlaydi, belgilangan mezonlar asosida axborot tekshiruvini amalga oshirib, axborotlar tarqalishida qaror qabul qiladi.

TE tarmoqdan o'tuvchi barcha paketlarni ko'radi va ikkala (kirish, chiqish) yo'nalish bo'yicha paketlarni belgilangan qoidalar asosida tekshirib ularga ruxsat berish yoki bermaslikni hal qiladi. Shuningdek, TE ikki tarmoq orasidagi himoyani amalga oshiradi, ya'ni himoyalanayotgan tarmoqni ochiq tashqi tarmoqdan himoyalaydi.

Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta'sir ko'rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning himoyalanuvchi tarmog'i va tashqi anim tarmoq orasida joylanishi lozim. Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtai nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi.

Bunday texnologiya oldin faqat tarmoq sathida IP adres manbai va qabul qiluvchi manzillarini filtrlash orqali amalga oshirilganligi sababli faqat tarmoq sathida qo'llanilgan. Hozirgi vaqtda transport sathida ham paketlarni filtrlash orqali tarmoq trafigi tahlil qilinadi. Har bir IP-paket

ko'pgina qoidalarga muvofiq tekshiriladi. Bu qoidalar TSR/IP modeli tarmoq va transport sathida sarlavha tarkibiga asoslangan holda aloqa o'rnatadi, tahlil qiladi va paketlar harakatini yo'nalishlarini belgilaydi.

Paketlarni filtrlovchi TElar ko'pincha tarmoq paketlari adreslarini shunday o'zgartiradiki, bunda chiquvchi oqim boshqa IP manzil bilan tashqi tarmoqqa tarqaladi. Bu sxema tarmoq adreslarni translyatsiyalash (Network Address Translation, NAT) sxemasi deb ataladi. NAT sxemasi qo'llanilishi natijasida, birinchidan ichki tarmoq topologiyasi va manzillar sxemasini bekitib turadi, ikkinchidan tashkilot ichidagi foydalanilayotgan IP adreslar hajmini kamaytiradi.

Paketlarni filtrlash jarayonida paketlar agar qoidalarga muvofiq kelsa, u keyingi ishlov yoki uzatish uchun tarmoq stekiga o'tkaziladi. Barcha kiruvchi paketlar filtrlashning berilgan qoidasiga muvofiq tekshiriladi. Bunda paket yo'qotiladi yoki tarmoq stekiga uni yetkazib berish uchun uzatiladi. Paket filtrlari qanday amaliy protokollar qo'llanilishini hal qila olmaydi. Qoidalarning ikkita ro'yxati mavjud: ta'qiqlash ro'yxati (deny) va ruxsat etish ro'yxati (permit). Tarmoq paketlari ikkala ro'yxat tekshiruvidan o'tadi.

Paket filtrlari quyidagilarni nazorat qiladi:

- Fizik interfeys, paket qayerdan keladi;
- Manbaning IP manzili;
- Qabul qiluvchining IP manzili;
- Transport sathi turiga ko'ra (TCP, UDP, ICMP);
- Manba va qabul qiluvchi transport portlari.

Paketlar tekshiruvining umumiy sxemasi:

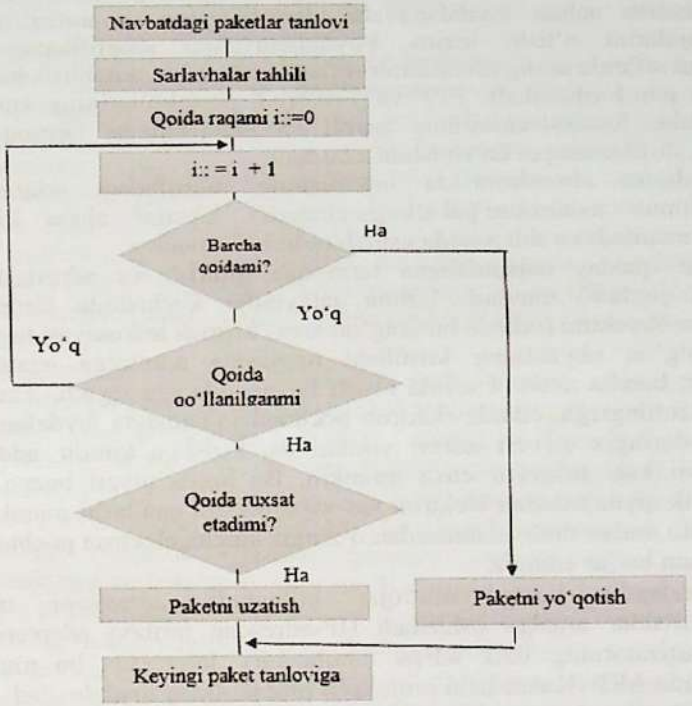
- agar qoidalar ruxsat bersa, paket uzatilishga ruxsat beriladi;
- agar qoidalar ta'qiqlasa, bu holatda paket yo'q qilinadi;
- agar bitta ham qoida qo'llanilmasa, paket yo'q qilinadi.

Ushbu TElar haqiqatan paket TSR bog'lanish so'rovi ekanligini yoki o'rnatilgan bog'lanish ma'lumotlarini taqdim etayotganligini yoki ikki transport sathi orasida virtual bog'lanishiga tegishli ekanligini tekshiradi.

Bog'lanish o'rnatilgandan so'ng jadval quyidagi ma'lumotlarni o'zida saqlaydi:

- seans identifikatori;
- bog'lanish holati(qo'l siqishish, o'rnatilgan, yopilgan);
- axborotlar ketma-ketligi(oldingi baytlarning raqam ketma-ketligi, bayroq holati va b.);
- Manba va qabul qiluvchining IP manzili;

- Portlar raqami, seans qatnashchilari;
- Fizik interfeys, paket qayerga kelib tushadi;
- Fizik interfeys, paket qayerga uzatiladi.



Paketlar tanlovi

Ushbu TElar bog'lanish o'rnatishdan oldin tarmoq paketlarini aynan amaliy sathga mosligini baholaydi. Ular amaliy sathdagi barcha tarmoq paketlari ma'lumotlarni tahlil qiladi va axborotlar ketma-ketligini hamda to'liq (tugatilgan) holdagi bog'lanishni o'rnatadi. Shu bilan birga, TElar xavfsizlikning boshqa parametrlari, ya'ni amaliy sathning ichki ma'lumotlarini tashkil etuvchilari (parollar, xizmat so'rovlari)ni ham tekshiradi. Amaliy sathning ko'pgina TElari maxsuslashtirilgan dasturiy ta'minot va proxy xizmatlarni o'z ichiga oladi. Funksiyalashgan proxy xizmat sxemasi quyidagi rasmda ko'rsatilgan.

5.4. O‘zaro aloqada bo‘lgan jarayonlarning va kommunikatsion qism orqali olinuvchi informatsiyani haqiqiy ekanligini tasdiqlash

Serverdan Internet tarmog‘i bazaviy protokollari FTP (Fayllarni uzatish protokoli) va TELNET (Virtual terminal protokoli) bo‘yicha foydalanish uchun foydalanuvchi identifikatsiya va autentifikatsiya muolajalarini o‘tishi lozim. Foydalanuvchini identifikatsiyalashda axborot sifatida uning identifikatori (ismi) ishlatilsa, autentifikatsiyalash uchun parol ishlatiladi. FTP va TELNET protokollarining xususiyati shundaki, foydaluvchilarning paroli va identifikatori tarmoq orqali ochiq, shifrlanmagan ko‘rinishda uzatiladi.

Axborot almashinuvida internetning masofadagi ikkita uzeli almashinuv axborotini paketlarga ajratadi. Paketlar aloqa kanallari orqali uzatiladi va shu paytda ushlab qolinishi mumkin.

Har qanday taqsimlangan tarmoqda qidirish va adreslash kabi “nozik joylari” mavjud. Ushbu jarayonlar kechishida tarmoqning yolg‘on obyektini (odatda bu yolg‘on xost) kiritish imkoniyati tug‘iladi.

Yolg‘on obyektning kiritilishi natijasida adresatga uzatmoqchi bo‘lgan barcha axborot aslida niyati buzuq odamga tegadi. Taxminan buni tizimingizga, odatda elektron pochtani jo‘natishda foydalanadigan provayderingiz serveri adresi yordamida, kirishga kimdir uddasidan chiqqani kabi tasavvur etish mumkin. Bu holda niyati buzuq odam unchalik qiynalmasdan elektron xat-xabaringizni egallashi mumkin, siz esa xatto undan shubxalanmasdan o‘zingiz barcha elektron pochtangizni jo‘natgan bo‘lar edingiz.

Qandaydir hostga murojat etilganida adreslarni maxsus o‘zgartirishlar amalga oshiriladi (IP-adresdan tarmoq adapteri yoki marshrutizatorning fizik adresi aniqlanadi). Internetda bu muamoni yechishda ARP (Kanal sathi protokoli) protokolidan foydalaniladi.

ARP (Kanal sathi protokoli) bilan bo‘lgan holda o‘xshab DNS-so‘rovni ushlab qolish yo‘li bilan internet tarmog‘iga yolg‘on DNS-serverni kiritish mumkin.

Ma’lumki, zamonaviy global tarmoqlari bir-biri bilan tarmoq uzellari yordamida ulangan tarmoq segmentlarining majmuidir. Bunda marshrut deganda ma’lumotlarni manbadan qabul qiluvchiga uzatishga xizmat qiluvchi tarmoq uzellarining ketma-ketligi tushuniladi. Marshrutlar xususidagi axborotni almashishni unifikatsiyalash uchun marshrutlarni boshqaruvchi maxsus protokollar mavjud.

Internetdagi bunday protokollarga yangi marshrutlar xususida habarlar almashish protokoli – ICMP (Tarmoqlararo boshqaruvchi habarlar protokoli) va marshrutizatorlarni masofadan boshqarish

protokoli SNMP (Tarmoqni boshqarishning oddiy protokoli) misol bo‘la oladi. Marshrutni o‘zgartirish hujum qiluvchi yolg‘on hostni kiritishidan bo‘lak narsa emas. Xatto oxirgi obyekt haqiqiy bo‘lsa ham marshrutni axborot baribir yolg‘on hostdan o‘tadigan qilib qo‘yish mumkin.

Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujumlar - DdoS (Xizmat qilishdan taqsimlangan voz kechish) kompyuter jinoyatchiligining nisbatan yangi xili bo‘lsada, qo‘rqinchli tezlik bilan tarqalmoqda. Bu hujumlarning o‘zi anchagina yoqimsiz bo‘lgani yetmaganidek, ular bir vaqtning o‘zida masofadan boshqariluvchi yuzlab hujum qiluvchi serverlar tomonidan boshlanishi mumkin. Xakerlar tomonidan tashkil etilgan uzellarda DDoS hujumlar uchun uchta instrumental vositani topish mumkin: trinoo, TribeFloodNet (TFN) va TFN2K. Yaqinda TFN va trinooning eng yoqimsiz sifatlarini uyg‘unlashtirgan yana bittasi stacheldraht (“tikon similar”) paydo bo‘ldi.

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

O‘zining haqiqiyligining tasdiqlash uchun subyekt tizimga turli asoslarni ko‘rsatishi mumkin. Subyekt ko‘rsatadigan asoslarga bog‘liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo‘linishi mumkin:

biror narsani bilish asosida. Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda “so‘rov javob” xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko‘rsatish mumkin;

biror narsaga egaligi asosida. Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va touch memory qurilmalari;

qandaydir daxlsiz xarakteristikalar asosida. Ushbu kategoriya o‘z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko‘zining rangdor pardasi va to‘r pardasi, barmoq izlari, kaft geometriyasi va x.) asoslangan usullarni oladi. Bu kategoriyada kriptografik usullar va vositalar ishlatilmaydi.

Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o'ziga xos masalalarni yechishga imkon beradi. Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi. Shu bilan bir qatorda ta'kidlash lozimki, no'llik bilim bilan isbotlash xususiyatiga ega bo'lgan autentifikatsiyaga qiziqish amaliy xarakterga nisbatan ko'proq nazariy xarakterga ega. Balkim, yaqin kelajakda ulardan axborot almashinuvini himoyalashda faol foydalanishlari mumkin.

Masofadagi foydalanuvchi tarmoqdan foydalanishga uringanida undan shaxsiy identifikatsiya nomeri PINni kiritish taklif etiladi. PIN to'rtta o'nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server foydalanuvchi tomonidan kiritilgan PIN-koddan foydalanib ma'lumotlar bazasidagi foydalanuvchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni generatsiyalash algoritmini bajaradi. So'ngra server generatsiyalangan son bilan foydalanuvchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server foydalanuvchiga tizimdan foydalanishga ruxsat beradi.

Autentifikatsiyaning bu sxemasidan foydalanishda apparat kalit va serverning qat'iy vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda Security Dynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me'yoridan chetlashishi aniq o'lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;

server muayyan apparat kalit generatsiyalagan kodlarni kuzatadi va zaruriyat tug'ilganida ushbu kalitga moslashadi.

Autentifikatsiyaning bu sxemasi bilan bir muammo bog'liq. Apparat kalit generatsiyalagan tasodifiy son katta bo'lmagan vaqt oralig'i mobaynida haqiqiy parol hisoblanadi. Shu sababli, umuman, qisqa muddatli vaziyat sodir bo'lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

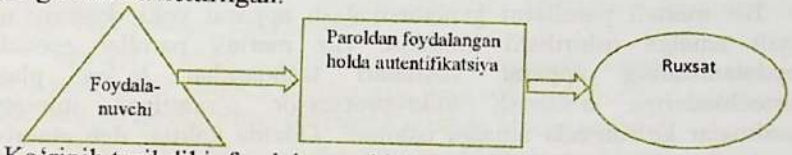
5.5. Identifikatsiya va autentifikatsiyalashda intellectual tizimlardan foydalanish

Parollar asosida autentifikatsiyalash

Autentifikatsiyaning keng tarqalgan sxemalaridan biri oddiy autentifikatsiyalash bo'lib, u an'anaviy ko'p martali parollarni ishlatishiga asoslangan. Tarmoqdagi foydalanuvchini oddiy autentifikatsiyalash muolajasini quyidagicha tasavvur etish mumkin. Tarmoqdan foydalanishga uringan foydalanuvchi kompyuter klaviaturasida o'zining identifikatori va parolini teradi. Bu ma'lumotlar autentifikatsiya serveriga ishlanish uchun tushadi.

Autentifikatsiya serverida saqlanayotgan foydalanuvchi identifikatori bo'yicha ma'lumotlar bazasidan mos yozuv topiladi, undan parolni topib foydalanuvchi kiritgan parol bilan taqqoslanadi. Agar ular mos kelsa, autentifikatsiya muvaffaqiyatli o'tgan hisoblanadi va foydalanuvchi legal (qonuniy) maqomini va avtorizatsiya tizimi orqali uning maqomi uchun aniqlangan xuquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Paroldan foydalangan holda oddiy autentifikatsiyalash sxemasi pastdagi rasmda keltirilgan.



Ko'rinib turibdiki, foydalanuvchining parolini shifrlamasdan uzatish orqali autentifikatsiyalash varianti xavfsizlikning xatto minimal darajasini kafolatlamaydi. Parolni himoyalash uchun uni himoyalanmagan kanal orqali uzatishdan oldin shifrlash zarur. Buning uchun sxemaga shifrlash Yek va rasshifrovka qilish Dk vositalari kiritilgan.

Bu vositalar bo'linuvchi maxfiy kalit K orqali boshqariladi. Foydalanuvchining haqiqiyligini tekshirish foydalanuvchi yuborgan parol PA bilan autentifikatsiya serverida saqlanuvchi dastlabki qiymat ni taqqoslashga asoslangan. Agar PA va qiymatlar mos kelsa, parol PA haqiqiy, foydalanuvchi A esa qonuniy hisoblanadi.

Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul - foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o'qish va yozishdan himoyalash atributlari o'rnatiladi (masalan, operatsion tizimdan foydalanishni

nazoratlash ro‘yxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funktsiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

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

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

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

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

Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.

Legal foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro‘yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish.

Foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

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

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

– joriy vaqt qiymati.

Masofadagi foydalanuvchi tarmoqdan foydalanishga uringanida undan shaxsiy identifikatsiya nomeri PINni kiritish taklif etiladi. PIN to‘rtta o‘nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server foydalanuvchi tomonidan kiritilgan PIN-koddan foydalanib ma’lumotlar bazasidagi foydalanuvchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni generatsiyalash algoritmini bajaradi. So‘ngra server generatsiyalangan son bilan foydalanuvchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server foydalanuvchiga tizimdan foydalanishga ruxsat beradi.

Autentifikatsiyaning bu sxemasidan foydalanishda apparat kalit va serverning qat’iy vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda Security Dynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

– apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me’yoridan chetlashishi aniq o‘lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;

– server muayyan apparat kalit generatsiyalagan kodlarni kuzatadi va zaruriyat tug‘ilganida ushbu kalitga moslashadi.

Autentifikatsiyaning bu sxemasi bilan bir muammo bog‘liq. Apparat kalit generatsiyalagan tasodifiy son katta bo‘lmagan vaqt oralig‘i mobaynida haqiqiy parol hisoblanadi. Shu sababli, umuman, qisqa muddatli vaziyat sodir bo‘lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

5.6. Obyektlarga kirishda insonlarning bioparametrlaridan foydalanish

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

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

- biometrik alomatlarning noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqori;
- biometrik alomatlarning sog'lom shaxsdan ajratib bo'lmasligi;
- biometrik alomatlarni soxtalashtirishning qiyinligi.

Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik algoritmlar quyidagilar:

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

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

- xatolik inkorlar koeffitsiyenti FRR (false-Rejection rate);
- xatolik tasdiqlar koeffitsiyenti FAR (false-Acceptance rate).

Xatolik inkor tizim qonuniy foydalanuvchi shaxsini tasdiqlamaganda paydo bo'ladi (odatda FRR qiymati taxminan 100 dan birni tashkil etadi). Xatolik tasdiq tizim noqonuniy foydalanuvchi shaxsini tasdiqlaganida paydo bo'ladi (odatda FAP qiymati taxminan 10000 dan birni tashkil etadi). Bu ikkala koeffitsiyent bir-biri bilan bog'liq: xatolik inkor koeffitsiyentining har biriga ma'lum xatolik tasdiq koeffitsiyenti mos keladi.

Mukammal biometrik tizimda ikkala xatolikning ikkala parametri no'lga teng bo'lishi shart. Afsuski, biometrik tizim ideal emas, shu sababli nimanidur qurbon qilishga to'g'ri keladi. Odatda tizimli parametrlar shunday sozlanadiki, mos xatolik inkorlar koeffitsiyentini aniqlovchi xatolik tasdiqlarning istalgan koeffitsiyentiga erishiladi.

Biometrik autentifikatsiyalashning daktiloskopik tizimi

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

Autentifikatsiyaning daktiloskopik tizimi quyidagicha ishlaydi. Avval foydalanuvchi ro'yxatga olinadi. Odatda, skanerda barmoqning

turli xolatlarida skanerlashning bir necha varianti amalga oshiriladi. Tabiiyki, namunalar bir-biridan biroz farqlanadi va qandaydir umumlashtirilgan namuna, «pasport» shakllantirilishi talab etiladi. Natijalar autentifikatsiyaning ma'lumotlar bazasida xotirlanadi. Autentifikatsiyalashda skanerlangan barmoq izi ma'lumotlar bazasidagi «pasportlar» bilan taqqoslanadi.

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

Bunday texnologiyalarni ishlab chiquvchi kompaniyalar barmoq izlarini olishda turli, xususan elektrik, elektromagnit va boshqa usullarni amalga oshiruvchi vositalardan foydalanadilar.

Skanerlardan biri barmoq izi tasvirini shakllantirish maqsadida teri qismlarining sig'im qarshiligini o'lchaydi. Masalan, Veridicom kompaniyasining daktiloskopik qurilmasi yarim-o'tkazgichli datchik yordamida sig'im qarshiligini aniqlash orqali axborotni yig'adi. Sensor ishlashining printsipi quyidagicha: ushbu asbobga quyilgan barmoq kondensator plastinalarining biri vazifasini o'taydi (2-rasm). Sensor sirtida joylashgan ikkinchi plastina kondensatorning 90000 sezgir plastinkali kremniy mikrosxemasidan iborat. Sezgir sig'im datchiklari barmoq sirti do'ngliklari va pastliklari orasidagi elektrik maydon kuchining o'zgarishini o'lchaydi. Natijada do'ngliklar va pastliklargacha bo'lgan masofa aniqlanib, barmoq izi tasviri olinadi.

Integral sxema asosidagi sensorli tekshirishda AuthenTec kompaniyasida ishlatiluvchi usul aniqlikni yana ham oshirishga imkon beradi. Qator ishlab chiqaruvchilar biometrik tizimlarni smart-kartalar va karta-kalitlar bilan kombinatsiyalaydilar. Integral sxemalar asosidagi barmoq izlari datchiklarining kichik o'lchamlari va yuqori bo'lmagan narxi ularni himoya tizimi uchun ideal interfeysga aylantiradi. Ularni kalitlar uchun breloklarga o'rnatish mumkin. Natijada foydalanuvchi kompyuterdan boshlab to kirish yo'li, avtomobillar va bankomatlar eshiklaridan himoyali foydalanishni ta'minlaydigan universal kalitga ega bo'ladi.

Qo‘l panjasining geometrik shakli bo‘yicha autentifikatsiyalash tizimlari

Qo‘l panjasi shaklini o‘quvchi qurilmalar barmoqlar uzunligini, qo‘l panja qalinligi va yuzasini o‘lchash orqali qo‘l panjasining hajmiy tasvirini yaratadi. Masalan, Recognition Systems kompaniyasining mahsulotlari 90 dan ortiq o‘lchamlarni amalga oshiradi. Natijada keyingi taqqoslash uchun 9-xonali namuna shakllantiriladi. Bu natija qo‘l panjasini individual skanerida yoki markazlashtirilgan ma’lumotlar bazasida saqlanishi mumkin. Qo‘l panjasini skanerlovchi qurilmalar narxining yuqoriligi va o‘lchamlarining kattaligi sababli tarmoq muhitida kamdan-kam ishlatilsada, ular qat’iy xavfsizlik rejimiga va shiddatli trafikka ega bo‘lgan hisoblash muhiti (server xonalari ham bunga kiradi) uchun qulay hisoblanadi. Ularning aniqligi yuqori va inkor koeffitsiyenti ya’ni inkor etilgan qonuniy foydalanuvchilar foizi kichik.

Yuzning tuzilishi va ovoz bo‘yicha autentifikatsiyalovchi tizimlar

Bu tizimlar arzonligi tufayli eng foydalanuvchan hisoblanadilar, chunki aksariyat zamonaviy kompyuterlar video va audeo vositalariga ega. Bu sinf tizimlari telekommunikatsiya tarmoqlarida masofadagi foydalanuvchi subyektni identifikatsiyalash uchun ishlatiladi. Yuz tuzilishini skanerlash texnologiyasi boshqa biometrik texnologiyalar yaroqsiz bo‘lgan ilovalar uchun to‘g‘ri keladi. Bu holda shaxsni identifikatsiyalash va verifikatsiyalash uchun ko‘z, burun va lab xususiyatlari ishlatiladi. Yuz tuzilishini aniqlovchi qurilmalarni ishlab chiqaruvchilar foydalanuvchini identifikatsiyalashda hususiy matematik algoritmlardan foydalanadilar.

Ma’lum bo‘lishicha, ko‘pgina tashkilotlarning hodimlari yuz tuzilishini skanerlovchi qurilmalarga ishonmaydilar. Ularning fikricha kamera ularni rasmga oladi, so‘ngra suratni monitor ekraniga chiqaradi. Kameraning sifati esa past bo‘lishi mumkin. Undan tashqari yuz tuzilishini skanerlash - biometrik autentifikatsiyalash usullari ichida yagona, tekshirishga ruxsatni talab qilmaydigan (yashiringan kamera yordamida amalga oshirilishi mumkin) usul hisoblanali.

Ta’kidlash lozimki, yuz tuzilishini aniqlash texnologiyasi yanada takomillashtirilishni talab etadi. Yuz tuzilishini aniqlovchi aksariyat algoritmlar quyosh yorug‘ligi jadalligining kun bo‘yicha tebranishi natijasidagi yorug‘lik o‘zgarishiga ta’sirchan bo‘ladilar. Yuz holatining o‘zgarishi ham aniqlash natijasiga ta’sir etadi. Yuz holatining 450 ga o‘zgarishi aniqlashni samarasiz bo‘lishiga olib keladi.

Ovoz bo‘yicha autentifikatsiyalash tizimlari

Bu tizimlar arzonligi tufayli foydalanuvchan hisoblanadilar. Hususan ularni ko‘pgina shaxsiy kompyuterlar standart komplektidagi uskuna (masalan mikrofonlar) bilan birga o‘rnatish mumkin. Ovoz bo‘yicha autentifikatsiyalash tizimlari har bir odamga noyob bo‘lgan balandligi, modulyatsiyasi va tovush chastotasi kabi ovoz xususiyatlariga asoslanadi. Ovozni aniqlash nutqni aniqlashdan farqlanadi. Chunki nutqni aniqlovchi texnologiya abonent so‘zini izohlasa, ovozni aniqlash texnologiyasi so‘zlovchining shaxsini tasdiqlaydi.

So‘zlovchi shaxsini tasdiqlash ba’zi chegaralanishlarga ega. Turli odamlar o‘xshash ovozlar bilan gapirishi mumkin, har qanday odamning ovozi vaqt mobaynida kayfiyati, hissiyotlik holati va yoshiga bog‘liq holda o‘zgarishi mumkin. Uning ustiga telefon apparatlarning turli-tumanligi va telefon orqali bog‘lanishlarining sifati so‘zlovchi shaxsini aniqlashni qiyinlashtiradi. Shu sababli ovoz bo‘yicha aniqlashni yuz tuzilishini yoki barmoq izlarini aniqlash kabi boshqa biometriklar bilan birgalikda amalga oshirish maqsadga muvofiq hisoblanadi.

Ko‘z yoyi to‘r pardasining shakli bo‘yicha autentifikatsiyalash tizimi

Bu tizimlarni ikkita sinfga ajratish mumkin:

- ko‘z yoyi rasmidan foydalanish;
- ko‘z to‘r pardasi qon tomirlari rasmidan foydalanish.

Odam ko‘z pardasi autentifikatsiya uchun noyob obyekt hisoblanadi. Ko‘z tubi qon tomirlarining rasmi hatto egizaklarda ham farqlanadi. Identifikatsiyalashning bu vositalaridan xavfsizlikning yuqori darajasi talab etilganida (masalan harbiy va mudofaa obyektlarining rejimli zonalarida) foydalaniladi.

Biometrik yondashish “kim bu kim” ekanligini aniqlash jarayonini soddalashtirishga imkon beradi. Daktiloskopik skanerlar va ovozni aniqlovchi qurilmalardan foydalanish xodimlarni tarmoqqa kirishlarida murakkab parollarni eslab qolishdan xalos etadi. Qator kompaniyalar korxona masshtabidagi bir martali autentifikatsiya SSO (Single Sign-On) ga biometrik imkoniyatlarni integratsiyalaydilar. Bunday biriktirish tarmoq ma’murlariga parollarni bir martali autentifikatsiyalash xizmatini biometrik texnologiyalar bilan almashtirishga imkon beradi. Shaxsni biometrik autentifikatsiyalashning birinchilar qatorida keng tarqalgan sohalaridan biri mobil tizimlari bo‘ldi.

Muammo faqat kompyuter o‘g‘irlanishidagi yo‘qotishlarda emas, balki axborot tizimining buzilishi katta zararga olib kelishi mumkin. Undan tashqari, noutbuklar dasturiy bog‘lanish (mobil kompyuterlarda saqlanuvchi parollar yordamida) orqali korporativ tarmoqdan foydalanishni tez-tez amalga oshiradi. Bu muammolarni kichik, arzon va katta energiya talab etmaydigan barmoq izlari datchiklari yechishga imkon beradi. Bu qurilmalar mos dasturiy ta’minot yordamida axborotdan foydalanishning mobil kompyuterda saqlanayotgan to‘rtta sathi - ro‘yxatga olish, ekranni saqlash rejimidan chiqish, yuklash va fayllarni deshifratsiyalash uchun autentifikatsiyani bajarishga imkon beradi.

Foydalanuvchini biometrik autentifikatsiyalash maxfiy kalitdan foydalanishni modul ko‘rinishida shifrlashda jiddiy ahamiyatga ega bo‘lishi mumkin. Bu modul axborotdan faqat haqiqiy xususiy kalit egasining foydalanishiga imkon beradi. So‘ngra kalit egasi o‘zining maxfiy kalitini ishlatib xususiy tarmoqlar yoki internet orqali uzatilayotgan axborotni shifrlashi mumkin.

V bob xulosasi

Ushbu bob asosan obyektlarlar orasida axborotlarni uzatish va qabul qilish jarayonida qo‘llaniladigan aloqa kanallarining, turlari, xarakteristikalari va zamonaviy optik shisha tolali aloqa kabellerini ishlatish usullari chizmali ko‘rsatib berilgan. Obyektlar bir-birlari bilan ma’lumotlar ayirboshlash va himoyalash jarayonida kriptografik shifrlash va deshifrlash usullaridan foydalanish isbotlab berilgan. Obyektlarning axborotlarini himoyalashda eng asosiy me’zonlardan hisoblangan insonlarning bioparametrlaridan foydalanish taklif etilgan.

VI BOB.
OBYEKTLARNING AXBOROTLARINI XAVFSIZLIGINI BOSHQARISH JARAYONIDA INTELLEKTUAL TIZIMLARDAN FOYDALANISH

6.1. Avtomatlashtirilgan obyektlarning axborot xavfsizligini ta’minlashda intellektual tizimlarni qo‘llash

Tilga ishlov berish mexanizmi

Dunyodagi barcha rivojlangan davlatlarda avtomatlashtirilgan boshqaruv tizimlari taraqqiy etgan bo‘lib, axborotlarni xavfsizligini ta’milash uchun har xil turdagi intellektual tizimlardan foydalanilgan. Zamonaviy davrda, dasturchilarning ishlashi, kompyuterlar intellektual yukning ba’zi qismini egallagan hollarda, deyarli amalga oshiriladi. Ushbu sohada maksimal progressga erishishning yo‘llaridan biri “sun’iy aql” hisoblanadi, chunki kompyuter faqat bir xil turdagi, takrorlanadigan operatsiyalarni oladi va o‘rganishi mumkin. Bundan tashqari, to‘liq “sun’iy intellekt” yaratish insoniyat uchun yangi rivojlanish yo‘nalishlarini ochadi. Sun’iy razvedka sohasidagi maydonlardan biri - aqlli axborot tizimlari. Matnni axborot tizimlari an’anaviy axborot tizimlarining rivojlanishining tabiiy natijasidir. Ular o‘zlarini eng yuqori texnologiyali texnologiyalarni faqat qarorlarni qabul qilish uchun axborot tayyorlash jarayonlaridan emas, balki axborot tizimidan olingan ma’lumotlarga asoslangan yechimlarni ishlab chiqish jarayonlarini yuqori darajada avtomatlashtirish bilan birlashtirdi.

Intellektual tizim (IP, intellektual tizim - aql, razvedka, aql-idrok) an’anaviy ravishda yaratilgan, muayyan bir mavzuga tegishli bo‘lgan, bilimlari bunday tizim xotirasida saqlanadigan muammolarni yechishga yordam beradigan texnik yoki dasturiy tizimdir. Intellektual tizimning strukturasi uchta asosiy blokdan iborat: ma’lumot bazasi, qaror qabul qilish mexanizmi va aqlli interfeys.

Qaror qabul qilish texnologiyalarida intellektual tizim intellektual qo‘llab-quvvatlashga ega bo‘lgan axborot va hisoblash tizimi bo‘lib, u operatorning mavjud bo‘lgan intellektual tizimdan farqli o‘laroq, inson aralashuvisiz muammolarni hal qiladi. Shuning uchun obyektlarda axborotlarni xavfsizligini taq’minlashda intellektual tizimlardan foydalanish juda katta samara beradi.

Inson va kompyuter muloqoti bu ko‘pgina tadqiqotchilar ish olib borayotgan masaladir. Bu ishlardan yakuniy maqsad foydalanuvchi va

kompyuter o‘zaro tabiiy tilda suxbat qura olishidir misol uchun rus tilida yoki kompyuter ularga shu tilda javob bera olishi.

Tashqi ko‘ranishdan bu vazifa yengil tuyulishi mumkin, buning sababi biz yoshligimizdan inson muloqotini eshitib kelganligimizda. Kompyuterlarning aqli ularni ishlab chiqqan insonlarning maxorati bilan o‘lchanadi, shuning sababidan ular o‘z-o‘zidan fikrlashga qodir bo‘lmaganliklari uchun ularga o‘ta aniq yullanmalarni berish orqali nimani qilish kerakligini tushuntirish mumkin. Inson tug‘ilganidanoq tilni o‘rganishga moyillik bilan tug‘iladi, lekin kompyuter inson tilini tushunishi uchun tilni avvalo asosiy elementlarga bo‘lish va shu axborotlarni kompyuterga u tushunadigan tarzda kiritish zarur. Inson va kompyuter muloqoti tushunarli bo‘lishi uchun tabiiy tilni qayta ishlash tizimini ishlab chiqish zarur.

Keling, bu vazifa qanchalik mushkul ekanligini ko‘ramiz. Tasavvur qiling sun’iy tafakkurga ega bo‘lgan robot avtoulovlarni tamirlay oladi.

Unga quyidagi ikki topshiriqlarni berish mumkin.

1. G‘ildiragi teshilgan uy yonidagi avtoulovni tamirlash.
2. Uy yonidagi qizil pardali avtoulovni tamirlash.

Birinchi jumlani ikki xil izohlash mumkinligiga qaramay xar bir inson uyning yonida tushirilgan g‘ildirak bo‘lmasligini tushunadi. Inson bu jumladagi noaniqlikni darxol sezadi va undan ham muhimrog‘i ongida bu noto‘g‘ri jumlani to‘g‘rilaydi chunki malumki teshilgan g‘ildirak avtoulovda uy yonida emas. Robot so‘zlarni bog‘lashdan va ularni ma’nosini tushunishdan ko‘proq qila olishi kerak aks xolda u teshilgan g‘ildirakni qidirishiga to‘g‘ri kelar edi. Ikkala jumla ham bir xil tuzilishga ega bo‘lganligi uchun robot grammatikani va obyektlarni ularning manosini taqqoslay olishi kerak. Inson tilining qoidalari faqatgina inson uchun manogo ega, kompyuter uchun esa gap manosini anglash uchun maxsus qoidalar darkor.

Bizning robotimiz ega bo‘lgan sunniy intellekt jumlalar va ularning orasidagi bog‘liqlikni tahlil qila olishi kerak. Misol uchun quyidagi ikki gapni olamiz.

1. Sarvar sut ichmoqda.
2. So‘ngra u palto kiymoqda.

Ikkinchi gapdagi u so‘zi birinchi gapdagi Savarga taaluqli. Birinchi jumlasiz ikkinchi manosiz bo‘lar edi. Barcha tabiiy tillar kantekstual tillardir. Boshqacha qilib aytganda ikkinchi jumlani tushinish uchun birinchi jumlani bilish shart. Birgina jumla orqali izohlash mumkin

bo‘lgan tillar kontekstual mustaqil deyiladi. Kompyuter insonni tushina olishi uchun tabiiy til tavsilatorini ishlab chiqish zarur. Tahlilning asosiy funksiyalari quyidagicha:

1. Leksik tahlil (so‘zlar tahlili).
2. Sintaktik tahlil (grammatik qoidalar asosida so‘zlar tahlili).
3. Semantik tahlil.

Leksik tahlil

Leksik tahlil jumla so‘zlarning tovush yoki to‘xtash belgilari asosida bo‘lish. Bundan tashqari jumlada o‘zakni va qo‘shimchalarni ajratib olish mumkin. Misol uchun qo‘shimcha so‘z quyidagicha bo‘lish mumkin:

Qo‘shimcha (so‘z)

qo‘shish (o‘zak)

cha (qo‘shimcha)

So‘zlarni lug‘atdan olish mumkin lekin ularning umumiy manosini kompyuterga tushintirish qiyin masala.

Sintaktik tahlil

Inson tilini kompyuter tushinishi uchun avvalam bor komyuterni so‘zlarni ajrata olishni o‘rgatish kerak. Grammatika va sintaksiz qoidalarini kopmyuter tushunadigan shaklga keltirish kerak.

Odatda jumla (J) otlar gurixi (OG) va fellar gurixi (FG)dan tashkil topgan bo‘ladi va ularni quyidagi ko‘rinishda bo‘ladi:

J→OG, FG

Ot gurixi quyidagicha bo‘linishi mumkin: (atoqli ot, olmosh va x.k).

OG->AO.

Grafik tarzda jumlaning sintaksik ko‘rinishi “daraxt” shaklida bo‘lishi mumkin. Misol uchun: “qari o‘tinchi daraxt chopmoqda” jumlasi 1-rasm. da ko‘rsatilgandek tuzilishga ega. Jumla so‘zlarga bo‘linadi so‘zlar esa sinflarga bo‘linadi. Qari so‘zi - aniqlovchi (A), sifat orqali ifodalangan, o‘tinchi- so‘zi - ot (O), chopmoqda - fe’l (F) va daraxt -ot (O).

Semantik tahlil

So‘zni tarkibiy qismlarga bo‘lgandan so‘ng kompyuter uning semantik tahlil qilmoqda yani uning manosini tushinmoqchi. Sunniy aql tizimida jumlani manosini anglash uchun qoidalar umumiyligi ishlatiladi.

A O F O

Qari o‘tinchi daraxt chopmoqda

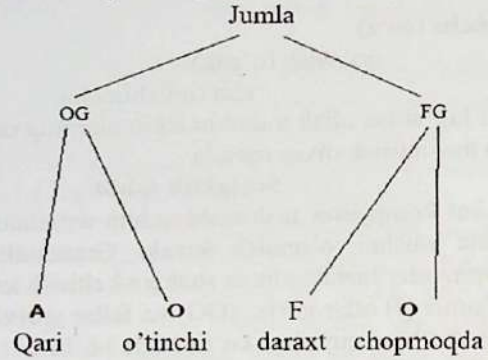
Jumlani izohlash uchun simantik tahlilchining bilimlar omborida quyidagi qoidalar mavjud bo‘lishi lozim.

1-qoida: AGAR aniqlovchi birinchi bo‘lib kelsa va undan keyin ot kelsa U XOLDA ot egadir.

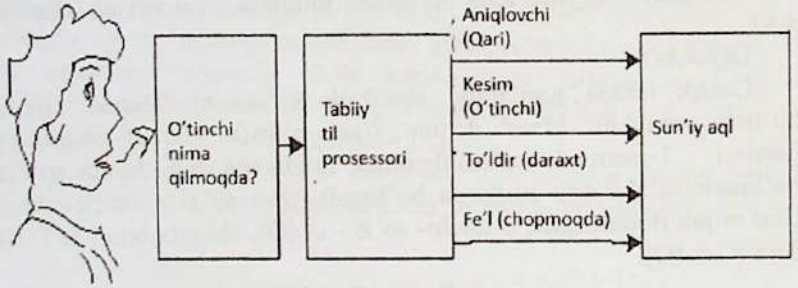
2-qoida: AGAR egadan keyin fe’l kelsa u xolda fe’l sifatdir va kesimdir.

3-qoida: AGAR egadan so‘ng kesim kelsa va undan so‘ng ot u xolda ot to‘ldiruvchidir.

4-qoida: AGAR jumla quyidagicha ketma-ketlikda bo‘lsa: ega, fe’l, to‘ldiruvchi u xolda butun jumla egasi to‘ldiruvchiga nisbatan kesimdir.



Jumlaning sintaksik daraxti



Tabiiy til protsessori

Yuqorida aytilganni misolda tushintiramiz. Faraz qilaylik sunniy aql tizimi quyidagi masalani yechishi kerak: qari o‘tinchi nima qilayotganini va uning faoliyat obyektini aniqlash. Semantik tahlilchi birinchi qoidaga murojat qiladi, uning yordamida u “o‘tinchi” so‘zi ega

ekanligini aniqlaydi. 2-qoida yordamida “chopmoq” kesimligini. Xarakat obyekti 3,4-qoidalar orqali “darax” so‘zi ekanligi. Quyidagi misol tabiiy til protsessorining semantik , leksik va sintaktik qoidalar orqali jumlani qanday qilib tushinishini ko‘rsatadi. Insonga kampyuter bilan og‘zaki muloqat uchun tabiiy til protsessori foydalanuvchi va sunniy aql tizimi orasidagi bog‘lovchi zanjir bo‘la oladi. Umuman olganda tabiiy tilni qayta ishlash foydalanuvchidan qiyin dasturlash tillarini o‘rganishdan ozod etadi. Agar kompyuter va inson tabiiy tilda so‘zlashishini vujudga keltira oladigan dastur ishlab chiqilsa bu haqiqiy sun’iy kompyuter bo‘ladi.

6.2. Obyektlarda axborot xavfsizligini boshqarish jarayonida o‘zini-o‘zi o‘qituvchi tizimlar yaratish

Neyronni asosiy xususiyat, tushuncha va modellari

Neyron bosh miyaning tarkibiy birligi bo‘lib, ularni o‘zaro xarakati axborotni qayta ishlash jarayonda elektr signallarni uzatish va ketma-ket-parallel: kuchaytirish-kamaytirish, nochiziqli qayta o‘zgartirish, jamlash kabi qayta o‘zgartirishlar yo‘li bilan bajariladi. Sun’iy neyron modeli tabiiy neyronni funksional xususiyat va xarakteristikalarini aks etadi. Neyron-elektr faolliklikka ega bo‘lgan va organizmni operativ boshqaradigan tirik organizmlarni nerv (asab) xujayralini alohida turi bo‘ladi. Neyron tarkibi: soma (tan), dendritlar - kirish axborotlarni o‘zatadigan o‘sitmalar va akson - chiqish axborotlarni o‘zatadigan o‘sitmalar. Xar bir neyron faqat bir akson va bir necha dendritlardan iborat. Neyronni chiqish signali (qo‘zg‘alishi, impulsi) boshqa neyronga nerv birikish (sinaps)lar orqali keladi. Bu holatda qo‘zg‘alish signallar kuchaytirilishi yoki kamaytirilishi mumkin. Shuning uchun neyron tanasi krishiga ikki turdagi - qo‘zg‘alishli va tormozlanishli signallar keladi. Neyron tanasi bu signallarni algebraik jamlab shu jamlangan signal o‘stida nochiziqli qayta o‘zgartirish amalni bajaradi. Jamlangan signal qiymati qandaydir chegarali qiymatidan oshgan holatda neyron qo‘zg‘aladi va chiqish signalni boshqa neyronlarga yuboradi.

Neyrotarmoqli hisoblashlar matematik asosi - har qanday ko‘p o‘zgaruvchanlardan bog‘lik bo‘lgan nochiziqli funksiyani oldindan belgilangan aniqligi bilan chiziqli amal va ketma-ket ulangan bir o‘zgaruvchandan bog‘lik bo‘lgan nochiziqli funksiyalar yordamida approksimatsiyalash (ifodalash) mumkin - qoidasi bo‘ladi.

Neyrotarmoqli hisoblashlarni asosiy xususiyatlari: a) konnektsiyanistlik - axborotni va qayta ishlash algoritmlarni eslash sifatida neyronlar orasidagi vaznlangan (o'lchangan) bog'lanish (aloqa)lardan foydalanish; b) o'rgatish - masalalarni berilgan sinfiga neyrotarmoqlarni sozlash jarayonda "dasturlash" funksiyani bajarish.

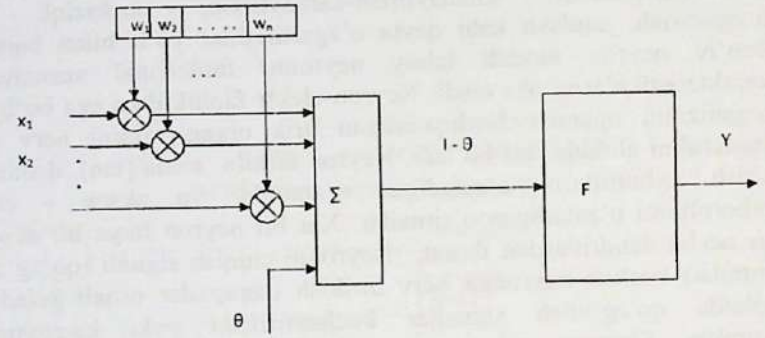
Mazkur xususiyatlar neyrotarmoqlarni - universallik, ommaviy parallellik va golografiklik (tuzilmani qisman buzilishida ishlash osoishtaligini saqlash) xarakteristikalar bilan ta'minlaydi.

Neyrotarmoqli hisoblashlar quyidagi holatlarda afzallikni ko'rsatadi:

– masalalarni matematik usullar yoradamida formallashtirish mumkin bo'lmaganda;

– mavjud formallashtiriladigan masalani yechish uchun matematik apparati mavjud bo'lmaganda,

– formallashtiriladigan masalani yechish matematik apparati juda katta resurs (vaqt, texnika, energiya va b.)larni talab qiladiganda.



Sun'iy neyronni tarkibiy modeli

Sun'iy neyron modeli ilk bor 1943y. Mak-Klokk va Pitts tomonidan tavsiflangan. Ular 13.1-rasmda ko'rsatilgan tuzilma ko'rinishdagi bir necha kirish (xi) va bir (Y) chiqishli chegara elementlari bilan ifodalangan. U ko'paytma-sinaps (⊗), jamlagich (∑) va nochiziqli o'zgartirish (F) operatorlardan iborat bo'lgan sun'iy neyron modelini tasvirlaydi. Neyronni kirish (x_i) signallar boshqa neyronlarning chiqish signallari bo'ladi. Har bir kirish signalga bog'lanish (aloqa) vazni (w_i) biriktiriladi. Uning qiymati musbat yoki manfiy bo'lishi mumkin. Kirish signal va bog'lanish vaznlar ko'paytmalari sinaps orqali jamlagich

elementga keladi. Uning chiqishida mazkur ko'paytmalar algebraik yig'indisi shakllanadi

$$I = \sum_{i=1}^{n} w_i x_i$$

Bu kattalik (I) neyronni qo'zg'alish darajasini ifodalaydi. Neyron kirish signalni F(I) aktivatsion yoki uzatma funktsiya bo'yicha nochiziq ravishda o'zgartiradi va, natijada, chiqish signalni quyidagi ifoda bo'yicha shakllantiradi

$$Y = F(I) = F(\sum_{i=1}^{n} w_i x_i)$$

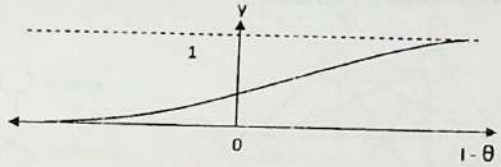
Agar neyron kirishida chegara (θ) o'rnatilgan bo'lsa, unda chiqish signal quyidagi ifoda bo'yicha shakllanadi

$$Y = F(I - \theta) = F(\sum_{i=1}^{n} x_i w_i - \theta)$$

Odatda F funktsiya sifatida quyidagi sodda nochiziq funksiyalar qo'llaniladi:

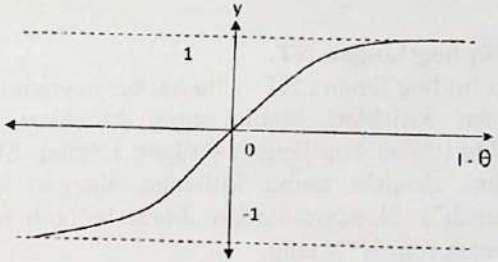
1) binarli (porogovaya)

$$Y = \begin{cases} 1, npuI > \theta, \\ 0, npuI \le \theta; \end{cases}$$



2) sigmoid

$$Y = \frac{1}{1+e^{-\sum w_i x_i}} = \frac{1}{1+e^{(I-\theta)}}$$



3) giperbolik tangens

$$Y = th(\sum w_i x_i) = th(I - \theta)$$

4) chiziqli

$$Y = k\sum_{i=1}^{n} w_i x_i$$

Shularni ichidan sigmoid funktsiyasi keng qo'llaniladi, chiziqli - deyarlik ishlatilmaydi.

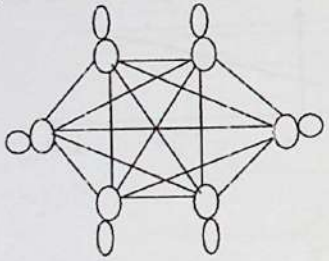
Neyron tarmoqlar turi

Neyron majmuini belgilangan ravishda bir-biri bilan hamda tashqi muxit bilan bog'lab, har xil turdagi neyron tarmoqlar modellarni qurish

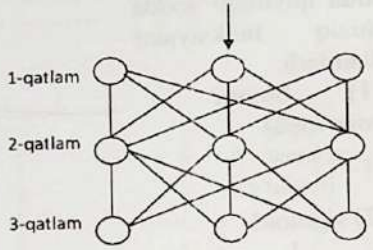
mumkin. Bu holda kirish signallar to'plami tarmoqni kirish vektorni tashkil qiladi, chiqish signallar to'plami esa - chiqish vektorni (chiqish faollik vektorni). Neyron tarmoqni bog'lanish vaznlari W matritsa ko'rinishda ifodalanadi. Bunda matritsani w i j elementi i va j neyronlar o'rtasidagi bog'lanish vazni bo'ladi. Neyron tarmog'i o'zining ishlash paytida kirish vektorni chiqish vetorga o'zgartiradi, ya'ni axborotni qayta ishlash (neyrotarmoqli hisoblash) jarayonni bajaradi. Bu qayta ishlashni aniq ko'rinishi (turi) neyron modeli turlari bilan hamda neyron tarmoqni arxitekturasi va xarakteristikalari bilan belgilanadi.

Neyron tarmoqlar arxitekturasi va turlari neyronlarni tarmoqdagi bog'lanish tartibi bilan belgilanadi. Shuning uchun ko'pincha neyron tarmoqlarni va tizimlarni konnektsionistik nomi bilan ataydi ("Connection" -"Bog'lanish" ingliz so'zidan).

Neyron tarmoq (NT)larini ikki asosiy: to'liq bog'langan va iyerarxik turlarini ajratadi.



To'liq bog'langan NT.

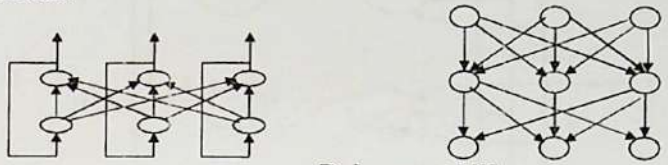


Iyerarxik NT.

To'liq bog'langan NT - bu har bir neyronni chiqishi barcha boshqa neyronlar kirishlari bilan, uning kirishlari esa qolgan neyronlar chiqishlari bilan bog'langan bo'lgan tarmoq. Shundan tashqari har bir neyronni chiqishi uning kirishiga ulangan bo'ladi ("o'z - o'ziga bog'lanish"). N neyronlardan iborat bo'lgan to'liq bog'langan NTda bog'lanish soni N*N teng.

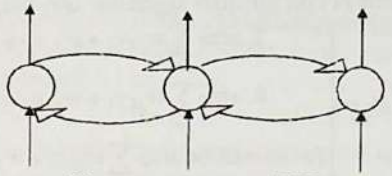
Iyerarxik NT - neyron guruxlari tegishli alohida qatlam va darajalarda joylashgan bo'lgan tarmoq. Bunday NT tegishli qatlamni har bir neyroni oldingi va keyingi qatlamlarni xar bir neyronlar bilan bog'langan. Uning kirish va chiqish qatlamlari tashqi muxit bilan bog'langan.

Bog'lanish yo'nalishlari bo'yicha teskari aloqasiz - norekurrent (feed - forward) va teskari aloqali - rekurrent (feed-back) NTlar ajratiladi.



Rekurrent NT

Agar rekurrent NTda o'zining bir qatlamni neyron o'rtasida tormozlaydigan (manfiy bog'lanish vaznlar bilan) aloqalari bo'lsa, unda bunday tarmoqni lateral yoki lateralli tormzlanishi bilan tarmoq deb ataydi.



Neyron tarmoq (NT)

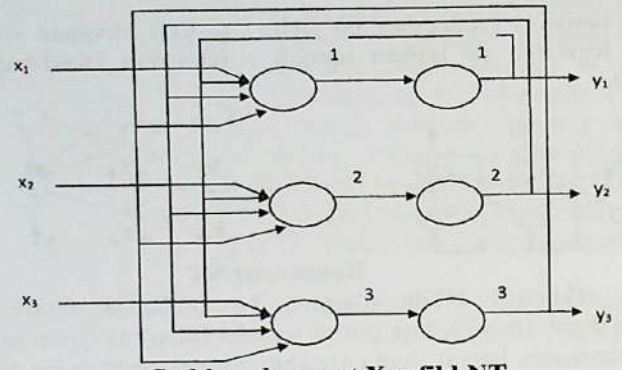
Bir qatlamli NT - bu sodda, iyerarxik, norekurrent turdagi tarmoq. Bunday tarmoqda tashqi muxit signallarni qabul qiladigan va taqsimlaydigan kirish neyronlar qatlami hamda hisoblashli neyronlar qatlami mavjud. Ularni har bittasini chiqish signallari uning kirishiga keladigan vaznlangan yig'indisi funksiyasi sifatida belgilanadi. Chiqish signallar majmuisi NT chiqish vektorni

$$Y=WX$$

tashkil qiladi. Bu yerda X - n o'lchamli kirish vektori; W - nm o'lchamli (m- chiqish qatlamni neyronlar soni) bog'lanish vaznlar matritsasi; Y - m o'lchamli chiqish vektori.

Ko'p qatlamli NT - bu bir necha hisoblashli neyronlar qatlamlardan iborat bo'lgan tarmoqlar. Bunday qatlamlar soni ko'payishi bilan tarmoqni hisoblash quvvati ham oshadi.

Xopfild neyron tarmog'i - bu aloxida turdagi rekurrent NT. Bunday tarmoqda har bir neyron kirishiga, X kirish vektorni tegishli komponentasidan tashqari, birinchi qatlamni taqsimlovchi neyronlar orqali boshqa neyronlar chiqish signallari ham keladi.



Sodda rekurrent Xopfild NT

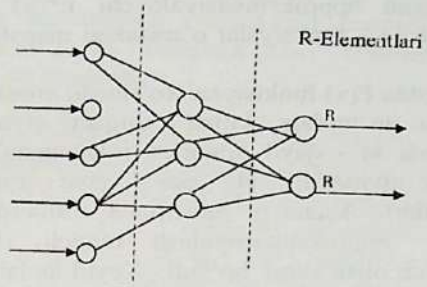
Bunday Xopfild NTda chiqish signallar quyidagi

$$y_i = \begin{cases} 1, \text{agar} \sum_{j \neq i} w_{ji} y_i + w_{j_0} x_j > \theta_j \\ 0, \text{agar} \sum_{j \neq i} w_{ji} y_i + w_{j_0} x_j < \theta_j \\ \text{ўзгармайди, agar} \sum_{j \neq i} w_{ji} y_i + w_{j_0} x_j = \theta_j \end{cases}$$

Perseptron turdagi NT

Bunday NTni 1958y. F. Rozenblat taklif qildi. Uni tasvir (timsol, obraz)larni aniqlash uchun ishlatgan. Bu ko'p qatlamli norekurrent tarmoq. Uning tuzilmasi uch qatlamlardan iborat.

qatlamda sezgirli retseptor (S- sensor) elementlar joylashgan. Ularga kirish tasvirlar signallari keladi. S- elementlar keyingi (ikkinchi) qatlamni assotsiativ A-elementlari bilan bog'langan. A-elementi faqat u bilan bog'langan yetarli miqdorda S-elementlar qo'zg'alishgandagina qo'zg'aladi. A-elementlar chiqish (uchinchi) qatlamni binar R-elementlar (yechuvchi elementlar) bilan o'zgaradigan qiymatlarga ega bo'lgan bog'lanish (aloqa) vaznli yoylar orqali bog'langan. R1 element chiqish qiymati R2 element chiqish qiymatidan oshsa unda perseptron aniqlaydigan obyektni birinchi sinfga kiritadi, aks holda - ikkinchi sinfga.



Perseptron sxemasi

Perseptronni o'rgatish jarayoni o'zgaruvchan bog'lanish koeffitsiyent (vazn)lar qiymatlarini sozlash yo'li bilan bajariladi.

Neyron tarmoqlar yordamida yechiladigan asosiy masalalar

Tasniflash. Bunday masalarda obyekt belgi (alomat)lar vektori Xn={x1,x2,...,xn} beriladi. Shularni asosida obyektni o'zaro kesishmaydigan m $C_i \cap C_j = 0, i \neq j, i, j = \overline{1,m}$ sinflardan biriga (Ci sinfga) kiritish kerak. Masalan, uchadigan obyektlar belgilari qanotlar, dvigatel, patlar va x.k. bo'lishi mumkin. Shunday obyektlar sinflari: Samolyot, Qush, Raketa, AUO va x.q. kabi sinflar bo'lishi mumkin. Belgilar majmui kirish vektorni tashkil qiladi, sinflar majmui esa - chiqish vektorni.

Mazkur masalani yechish uchun n kirish va m chiqish neyronlardan iborat bo'lgan perseptron turdagi NT quriladi. Aniq belgilar vektori kirishiga berilganda NT chiqish qatlamida eng darajadagi faollikli neyron tanlanadi. Shu neyron beriladigan belgilarga muvofiq bo'lgan sinfni belgilaydi. Masala to'g'ri yechilishi uchun NTni o'rgatish kerak. O'rgatish jarayonida bog'lanish vaznlarni tadqiq qilinayotgan obyektlar belgi va sinflarni aniq qiymatlariga munosib bo'lib sozlanadi.

Klasterlash. Bu masalarda belgi vektorlar majmuisi alohida gurux (klaster) larga ajratiladi. Shu klasterga kiradigan belgilar bir biriga yaqin bo'lgan xarakteristikalarga ega bo'lishi kerak. Turli klasterlar belgilari esa bir biridan uzoq bo'lishi kerak. Bu masalani yechish uchun dastlabki belgilar vektor komponentlariga teng bo'lgan kirish va klasterlar soniga teng bo'lgan chiqish neyronlardan iborat bo'lgan NT quriladi. Bunday NT vaznli koeffitsiyent qiymatlari ham o'rgatish jarayonda topiladi.

Approksimatsiyalash. Bunday masalada izlangan F(x) funksiyaga to'g'ri keladigan va quyidagi o'zaro nisbatga

$$d[F(x), F^*(x)] < \varepsilon$$

talab beradigan approksimatsiyalovchi F*(x) funksiyasi tanlab olinadi. Bu yerda ε - funksiyalar o'rtasidagi masofani berilgan kichik qiymati.

Umumiy holda F(x) funktsiyani ko'rinishi noma'lum bo'ladi. U x1 u1, x2 u2, ..., xn un turdagi "kirish - chiqish" qiymatlar juftlari bilan beriladi. Bu yerda xi - qayd qilingan (o'lchangan) argument (kirish o'zgaruvchan)lar qiymatlari, yi esa - qayd qilingan (o'lchangan) funksiya qiymatlari. Ananaviy matematik usullardan foydalanganda avval kerakli approksimatsiyalash modeli (F*(x) funktsiyani ko'rinishi)ni tanlab olish kerak bo'ladi. Keyin tanlab olingan mezonlar bo'yicha F*(x) funksiyani parametr (koeffitsiyent)lari topiladi.

NT lar universal approksimatorlar bo'lib, approksimatsiyalovchi F*(x) funksiyani tanlab olishini talab qilmaydi. Bu yerda NT ni o'rgatish uchun faqat qayd qilingan $\{x_i \rightarrow y_i\}$ juftlar ko'riladi. O'rgatish jarayonida NT chiqish yi* qiymatlari qayd qilingan yi qiymatlaridan berilgan ε qiymatidan kam bo'lganligini ta'minlaydigan bog'lanish vaznlar qimatlari topiladi.

Bu masala obyektlarni identifikatsiyalashda, ularni aniq matematik modellarini qurilishi murakkab bo'lgan holatda, keng qo'llaniladi.

Avtoassotsiatsiya. Bu masala assotsiativ xotira modellarni qurish masalasi bilan bog'liq.

Assotsiativ xotirani neyron modelida neyron guruxlar orqali tegishli timsol (tasvir, obraz)larni eslab olinishi ta'minlanadi. Bunday NT kirishiga timsolni qismi (tadqiq qilinadigan obyektni barcha belgilarining qandaydir o'ziga xos bo'lgan kirish vektorni tegishli majmuasi) berilganda uning chiqishida butun timsolni tavsiflaydigan neyronlarni hamnasi faollashtiriladi.

Shuni qayd qilish kerakki, bir qatlamli NT lar faqat sodda masalalarni yechish qobiliyatiga ega. Murakkab masalalarni yechish uchun har xil turdagi ko'p qatlamli NT ishlatiladi.

Neyron tarmoqlarni o'rgatish usullari

O'rgatish jarayonda vaznli bog'lanish koeffitsiyent, chegara va tuzilma kabi NT parametrlar qiymatlari sozlanadi (modifikatsiyalashadi). Shu holatda mazkur parametrlarni boshlang'ich qiymatlari odatda tasodifiy ravishda beriladi.

Tasnifni eng muhim belgisi (ko'rsatgichi) tashqi muxit bilan o'zaro xarakatlarini turi, xususiyati bo'ladi. O'rgatish jarayonda tashqi

muxitdan keladigan axborotni miqdori va sifati (semantikasi, ma'nosi)ga ko'ra supervizorli (supervised learning), nosupervizorli (unsupervised learning) va tasdiqlash bilan (reinforcement learning) o'rgatish algoritmlar ajratiladi.

NT o'rgatish usullar tasnifi

Supervizoli usulda oldindan o'rgatish juftlarni hammasidan iborat bo'lgan o'rgatish to'plam shakllanadi. O'rgatish jufti X kirish vektori va unga muvofiq bo'lgan Y chiqish vektorlar qiymatlari bilan ifodalanadi. Shu holatda har bir xi kirish vektorni i- komponentasi i-kirish neyronga keladigan signalga muvofiq bo'ladi. Shunga o'xshash har bir y j chiqish vektorni j- komponentasi j-chiqish neyronda paydo bo'ladigan signalga muvofiq bo'ladi.

O'rgatish jarayonda chiqish vektorlarni berilgan kirish vektorlarni qiymatlarga muvofiq bo'lgan joriy haqiqiy qiymatlarini o'rgatish to'plamda oldindan berilgan chiqish qiymatlardan og'ishlari hisoblanadi. Bu og'ishni qiymatiga muvofiq NT parametrlari mazkur og'ishlar qiymatlarini minimum (berilgan) kattaligiga olib keltirish uchun to'g'irlanadi (sozlanadi, modifikatsiyalanadi). Supervizorli o'rgatish algoritmlarni ichida eng keng tarqalgan xatolarni (to'lqinlarni) orqaga traqatish algoritmi (error backpropagation) bo'ladi.

Nosupervizorli algoritm (usul)larda o'rgatish to'plami faqat kirish vektorlar majmuasini ichiga oladi. Qo'llaniladigan shu holatda raqobatli o'rgatish algoritmi (competitive learning) klasterlash masalalarni yechish uchun NT parametrlarni sozlaydi. O'rgatish paytda tegishli klasterga kiradigan faol bo'lgan kirish komponenta (neyron)lar va shu klasterni tavsiflaydigan (aks etadigan) faol bo'lgan chiqish neyron orasidagi bog'lanish vaznlar qiymatlari maksimal darajada ko'paytiriladi. Shu bilan birga ushbu chiqish neyronni faol bo'lmagan kirish neyronlar bilan bog'lanish vaznlar qiymatlari kamaytiriladi.

Tasdiqlash bilan o'rgatish usul (algoritm)lar ko'rib o'tilgan ikkisini o'rtasida turadi. Bu usulni asosiy printsipi tashqi muxitdan (o'qituvchidan) keladigan "tasdiqlash - rad qilish " yoki "rag'batlantirish - jazolash" (reward/penalty) signalni mavjudligi bo'ladi. Bunday o'rgatish jarayonda navbatdagi kirish vektori berilganda NT xarakati qoniqarli bo'lsa tasdiqlash («+1») signal, aks holda - rad qilish («0» yoki «-1») signal beriladi. Shu holatda tarmoq tasdiqlash signallarni olishini balandroq tezligini ta'minlash maqsadda

vaznli koeffitsiyent qiymatlarini tegishli ravishda o'zgartiradi. Shu tezlik qiymati maqbul darajasiga yetmaguncha o'rgatish jarayoni davom etadi.

Tuzilmali o'rgatish usullar endi rivojlana boshladi. Ular murakkab masalalarni yechish uchun mo'ljallangan NTni qurishga imkoniyat beradi.

Kirishlarga qo'yiladigan talablar bo'yicha misol (timsol, o'xshashlik)lar va yagona misol (buyruqqa asoslangan) bo'yicha o'rgatish usullar ajratiladi. Shu holatda tadqiq qilinadigan obyektlarni tavsiflaydigan etalon (misol, timsol) to'plami shakllanadi. NT parametrlari shunday qilib sozlanadiki, kirish belgilarni tegishli qiymatlarda faqat mazkur belgilarga ega bo'lgan berilgan etalonga muvofiq bo'lgan chiqish neyronlar aktivlanishi kerak.

Stoxastik o'rgatish usullar ehtimolli aktivlash qoidalarga, determinlik (aniq belgilangan) usullar - determinlik qoidalarga asoslangan.

6.3. Obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasini ishlab chiqish

Yuqorida aytganimizdek axborotning zaif tomonlarini kamaytiruvchi va axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qolishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi - axborotni himoyalash tizimi ekanligini aniqlab oldik.

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

Buning uchun boshidan shart belgilab olish kerak. Birinchidan, faraz qilaylik, bizda haqiqattan qandaydir qiymatga ega axborot bor bo'lishi kerak. Ikkinchidan, shu axborotga himoya sistemasini o'rnatish

uchun sarf-harajatni aniqlab olishimiz kerak. Bu maqsad uchun biz optimal himoyalash usullarini tanlashimiz lozim bo'ladi.

Zamonaviy obyektning hayoti mahalliy tarmoqsiz ishlashi mumkin emas, ya'ni, bu tarmoq qo'llanuvchi qayerda bo'lishidan qat'iy nazar axborot almashuvini ta'minlab beradi. Har bir obyektni ish faoliyatining xavfsizligini ta'minlash uchun himoyalash tizimi ishlab chiqiladi.

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

- kompyuterda saqlanayotgan, uzatilayotgan yoki ishlab chiqiladigan axborotlar hajmining kattaligi;
- ma'lumotlar bazasiga muhimligi va maxfiligi jihatidan har xil axborotlarning kiritilishi;
- axborotdan foydalanuvchilarning imkoniyat doirasining kengayishi;
- masofadagi ish joylarining soni ko'payishi;
- internet tarmog'ida ishlovchilarning sonini oshib borishi;
- kompyuter qo'llanuvchilari orasida axborot almashuvining avtomatlantirilishi.

Har bir himoya tizimini o'rnatganda quyidagi savollarga javob berish kerak:

1. Nimani himoyalash kerak?
2. Kimdan yoki nimadan himoyalanamiz kerak?
3. Qanday himoya o'rnatishni aniqlash kerak?

Birinchi savolga quyidagicha javob berish mumkin. Har bir mahalliy tarmoqning asosiy vazifasi, kerakli axborotni qisqa vaqt ichida qo'llanuvchiga yetqazishdir. Shuning uchun axborotni himoyalashni ta'minlash muammosini xal qilishda buni inobatga olish kerak. Axborotni himoyalash usullarini ishlab chiqqanda, himoya tizimi xalaqit bermasligi kerak, aksincha, asosiy funksiya - axborot almashuvini ta'minlashda yordam berishi shart. Shuning uchun, himoyalash tizimining modelini ishlab chiqishda, mahalliy tarmoqning modelini yaxshi bilish kerak.

Buning uchun, mahalliy tarmoqning modeli - ya'ni undagi bajariladigan asosiy funksiyalar va barcha elementlar yig'indisini aniqlab olinadi.

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

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

«Mahalliy tarmoq foydalanuvchisi» tushunchasi – bu belgilangan tartib bo'yicha ro'yxatdan o'tgan va tarmoqni foydalanishda aniq bir huquqga ega shaxsga (tashkilotga) aytiladi. Tarmoqdagi axborot tizimining administratori nazorati ostida ishlab chiqiladi, uning ish holatini saqlash uchun, amaliy dasturiy ta'minotni ishlab chiqish uchun mutaxassis – dasturchilar va texnik shaxslar jalb qilinadi. Ularda ham axborotga cheklangan huquqlari bor, lekin dasturiy ta'minotni o'zgartirishda va axborotni ishlab chiqish jarayoniga cheklanmagan ta'sir ko'rsatishi mumkin.

Mahalliy tarmoqni tizim ko'rinishda olish mumkin. Bu tizim quyidagi ichki tizimlardan – boshqaruvchining ish joyi, masofadagi ish joyi, xavfsizlik va tizim administratorlarining ish joylaridan tashkil topgan. Bularning har biri - mustaqil ichki tizimlar. Shuning uchun, axborotni himoyalashda – dekompozitsiya prinsipi qo'llaniladi.

Ikkinchi savol quyidagicha hal qilinishi mumkin. Axborotni himoyalash savollariga qaratilgan adabiyotlarda har xil variantli axborot xavfsizligining xavflari modelini topish mumkin. Bunda ixtiyoriy modeldan foydalanish mumkin, lekin u axborot xavfsizligiga ta'sir etish faktorlarining maksimal sonini ko'rsatishi kerak.

Axborot xavfsizligining xavflarini yuqorida mukammal ko'rib va tahli qilib bergan edik. Bunaqa taqsimlanish sababi, bir xil xavfga ichki va tashqi omillarga qarab har xil usul qo'llaniladi.

Korxonaning axborot xavfsizligi tizimining modeli tashqi va ichki omillarning jamiyati, ularning korxona axborot xavfsizligi holatiga ta'siri va resurslarning xavfsizligini ta'minlashdir. Har qanday obyektning axborot xavfsizligi tizimining modeli quyidagi omillar o'rtasidagi ta'sir yo'nalishlarini taqdim etadi:

– axborot xavfsizligi tahdidlari yuzaga kelishi va amalga oshirilishi ehtimoli bilan tavsiflanadi;

– tahdidni amalga oshirish ehtimoliga ta'sir qiluvchi axborot xavfsizligi tizimining zaifligi;

– axborot xavfsizligi tahdidini amalga oshirish natijasida yuzaga keladigan zararni aks ettiruvchi xavflar.

Himoya qilinishi kerak bo'lgan axborot va moddiy resurslar himoya obyektlari deb ataladi. Bunga quyidagilar kiradi:

– nutq ma'lumoti;

– turli xil tashuvchilar shaklida aloqa vositalari orqali saqlanadigan va qayta ishlangan ma'lumotlar;

– qog'oz tashuvchi hujjatlar;

– aloqa va axborotlashtirish texnik vositalari;

– axborotni muhokama qilish, qayta ishlash va saqlash uchun mo'ljallangan xonalar;

– umuman axborot tizimlari, jumladan, aloqa tizimlari;

– aloqa va axborotlashtirish texnik va dasturiy vositalari uchun hujjatlar;

– dasturiy vositalar va boshqalar.

Korxona yuzaga kelishi mumkin bo'lgan tahdidlar ularning kelib chiqishi tabiatiga ko'ra tasniflanadi, ya'ni tasodifiy yoki qasddan tabiat tahdidlari va ular himoyalangan obyektga, ya'ni tashqi va ichki tahdidlarga qanday munosabatda bo'lishlari hisoblanadi.

Tashqi tahdidlarning manbalari quyidagilar bo'lishi mumkin:

– muhim axborotni ushlashda raqobatchilarning faoliyati;

– axborotni yo'q qilish, yoki o'zgartirish bo'yicha qasddan qilingan harakatlar;

– tizim elementlarining ishdan chiqishiga olib keladigan uchinchi tomon xodimlarining noto'g'ri harakatlari;

– tabiiy ofatlar va falokatlar, baxtsiz hodisalar, ekstremal vaziyatlar.

Ichki tahdidlarning manbalari quyidagilardan iborat:

– axborotni muhofaza qilish sohasida korxona bo'linmalari faoliyatini muvofiqlashtirishning yo'qligi;

– axborotni yo'q qilish yoki o'zgartirish bo'yicha xodimlarning qasddan qilingan harakatlari;

– xodimlarning noto'g'ri xatolari, texnik vositalarning muvaffaqiyatsizligi va axborot tizimlarida uzilishlar;

– axborotni yig'ish, to'plash, saqlash, qayta ishlash, konvertatsiya qilish, ko'rsatish va uzatish bo'yicha belgilangan qoidalarni buzilishi.

Buzilishlar bir necha turdagi bo'lishi mumkin.

Tashkiliy-huquqiy buzilishlar - axborotni muhofaza qilish sohasida korxonaning yagona kelishilgan siyosati yo'qligi, normativ hujjatlar talablarini bajarmaslik, axborotni olish, saqlash va yo'q qilish tartibi bilan bog'liq qoida buzarliklar hisoblanadi.

Buzilishlarning tashkiliy turlari ma'lumotlar bazalari va massivlariga ruxsatsiz kirish, faol tarmoq uskunalariga, serverlarga ruxsatsiz kirish, ularni boshqarishda himoya vositalarini noto'g'ri joylashtirish va xatolar, axborot almashinuvida axborotni tarqatish manzilida buzilishlarni o'z ichiga oladi.

Jismoniy buzilishlar avtomatlashtirilgan tizimlar, aloqa liniyalari va aloqa uskunalari apparatlariga zarar etkazish, axborot vositalarining mazmuni bilan o'g'irlik yoki ruxsatsiz tanishish, ularni o'g'irlash degan ma'noni anglatadi.

Radioelektron buzilishlarning turlari orasida axborotni ushlash uchun elektron qurilmalarni joriy etish, axborot oqimlarini ushlash va parolini hal qilish, monitorlarni suratga olish, mahalliy hisoblash tarmoqlarida noto'g'ri ma'lumot olish, ma'umotlarni uzatish va aloqa liniyalari kiradi.

Tahdidlarga qarshi kurashish va buzilishlarni bartaraf etish uchun korxonalarda risklarni boshqarish jarayoni tashkil etilmoqda, bu esa korxonaning axborot xavfsizligi tizimining asosi hisoblanadi.

Samarali axborot xavfsizligi tizimini yaratish - resurslar va vaqt cheklovlarini hisobga olishda tashqi va ichki tahdidlarni minimallashtirishga qaratilgan keng qamrovli jarayon bo'lishi kerak.

Jarayon yondashuvi nuqtai nazaridan obyekt-korxona axborot xavfsizligi tizimi risklarni boshqarish jarayoni sifatida taqdim etilishi mumkin va ular quyidagi komponentlarni o'z ichiga oladi.

1. Obyekt faoliyati jarayonlarining tavsifi. Ishlash jarayonlarini tuzatish va tahlil qilish amalga oshiriladi. Xatarlar sohasida siyosatni

shakllantirish jarayonida aniqlangan mezonlarga ko'ra, kirish va chiqish jarayonlarida identifikatsiya qilishni amalga oshiriladi.

2. Xatarlarni yig'ish. Korxonaning jiddiy zarar yetkazishi mumkin bo'lgan tahdidlarga ta'sir qilish darajasini aniqlash uchun amalga oshiriladi. Buning uchun uning ishi tahlil qilinadi.

Axborot xavfsizligi tizimi uchun risklarni boshqarish jarayonining modeli va axborot xavfsizligining standart xatarlari quyidagilardan iborat bo'lishi mumkin:

– mahalliy joylardan maxfiy ma'lumotlarni olib qo'yish;
– yo'q qilish maqsadida axborotni qasddan o'zgartirish;
– muhim hujjatlarni nusxalash va raqibga topshirish;
– korporativ tarmoqqa noqonuniy kirish;
– texnik sabablarga ko'ra yo'q qilish va boshqalar.

3. Xatarlarni baholash. Axborot tizimining tavakkalchilik xususiyatlari va resurslari aniqlanadi. Ushbu jarayonning asosiy natijasi barcha mumkin bo'lgan xavflarning ro'yxati bo'lib, ularning miqdoriy va sifatli zararlari va amalga oshirish imkoniyatlari va qo'shimcha – korxonada kuzatilmaydigan xavflar ro'yxatidan iborat bo'ladi.

Xatarlarni baholash jarayoni quyidagi bosqichlardan iborat:

– obyektning tavsifi va himoya choralari;
– resursni aniqlash va uning miqdoriy ko'rsatkichlarini aniqlash;
– axborot xavfsizligi tahdidlarini tahlil qilish;
– zaifliklarni baholash;
– mavjud va taxmin qilingan axborot xavfsizligini ta'minlash vositalarini baholash.

4. Tadbirlarni rejalashtirish. Xatarlarni minimallashtirish bo'yicha chora-tadbirlarni rejalashtirishning maqsadi xavfni minimallashtirishda zararni bartaraf etish yoki kamaytirish bo'yicha ishlarning muddati va ro'yxatini aniqlashdan iborat bo'ladi.

Axborot xavfsizligi bo'yicha quyidagi tadbirlar ajratiladi:

- tashkiliy;
- huquqiy;
- tashkiliy-texnik;
- dasturiy ta'minot;
- muhandislik va texnik.

5. Tadbirlarni amalga oshirish. Xatarlarni minimallashtirish bo'yicha chora-tadbirlarni amalga oshirish rejalashtirilgan ishlarni bajarish, olingan natijalar va muddatlarning sifatini nazorat qilishni

nazarda tutadi. Ushbu jarayonning natijasi risklarni minimallashtirish va ularni amalga oshirish vaqti bo'yicha bajarilgan ishlardan iborat bo'ladi.

6. Ishlashni baholash. Axborot xavfsizligini boshqarish tizimining samaradorligini baholash - bu tizimning hozirgi holati, unda yuz beradigan harakatlar va hodisalar haqida obyektiv ma'lumotlarni olish va baholashning tizimli jarayoni bo'lib, ular muayyan mezonlarga muvofiqligini belgilaydi.

Jarayonning maqsadlari quyidagilardir:

- tizimning joriy ishlash darajasini baholash;
- tizimdagi "tor" joylarni mahalliylashtirish;
- korxona tizimining axborot xavfsizligi sohasidagi mavjud standartlarga muvofiqligini baholash;
- himoya obyektlarining xavfsizligini ta'minlash bo'yicha tavsiyalar va reglamentlarni ishlab chiqish hisoblanadi.

Jarayon natijalari obyektni ISO / IEC 27001: 2005 standartiga muvofiq sertifikatlash uchun audit maqsadida ishlatilishi mumkin.

Obyektlarni injener himoyalash va texnik qo'riqlash bo'icha takliflar

Axborot manbalarini fizik himoyalash tizimi niyati buzuqning himoyalanuvchi axborot manbalariga suqilib kirishini oldini oluvchi hamda tabiiy ofatdan, avvalo yong'indan, ogohlantiruvchi vositalarni o'z ichiga oladi.

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

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

Boshqarish quyidagilarni ta'minlashi lozim:

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

Fizik himoyalash tizimini boshqarish bo'yicha me'yoriy hujjatlar axborotni himoyalash bo'yicha yo'riqnomalarda o'z aksini topgan. Ammo yo'riqnomalarda barcha vaziyatlarni hisobga olish mumkin

emas. Fizik himoyalash tizimining vositalari vaqt tanqisligi sharoitida notipik vaziyatlar sodir bo'lganida to'g'ri xulosa qabul qilinishini ta'minlashi lozim.

Fizik ximoyalash tizimining tarkibi turli - tuman: oddiy qulfli yog'och eshikdan to qo'riqlashning avtomatlashtirilgan tizimigacha.

Obyektlarni injener himoyalash va texnik qo'riqlash zaruriyati statistika orqali tasdiqlanadi, ya'ni suqilib kirishlarning 50% dan ko'prog'i xodimlar va mijozlar tomonidan erkin foydalaniladigan obyektlarga amalga oshirilsa, faqat 5 % kuchli qo'riqlash rejimli obyektlarga amalga oshiriladi.

Axborotni injener himoyalashni quyidagilar ta'minlaydi:

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

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

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

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

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

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

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

Qabul qiluvchi - nazoratlovchi punkt datchiklardan keladigan signallarni qabul qilish va ishlashga, qo'riqlash xodimlarini tovush va

yorug'lik signali yordamida trevoga signallari kelganligi, datchiklar va shleyflar ishlashidagi nosozliklar xususida xabardor qilishga mo'ljallangan.

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

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

VI bob xulosasi

Hozirgi rivojlanish davrida barcha korxona. tashkilot, muassasa, kompaniya, jamiyat va firmalar avtomatlashtirilgan boshqaruv tizimlarini yaratib, o'z ish faoliyatlarini amalga oshirayotganlari natijasida saqlanayotgan, qabul qilinayotgan va uzatilayotgan ma'lumotlarini xavfsizligini ta'minlash jarayonlari ham ancha murakkablashib bormoqda. Shuning uchun ushbu bob asosan avtomatlashtirilgan obyektlarning axborot xavfsizligini ta'minlashda intellektual tizimlarni qo'llashga, obyektlarda axborot xavfsizligini boshqarish jarayonida o'zini-o'zi o'qituvchi tizimlar yaratishga va obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasini ishlab chiqishga asoslangan bo'lib, kerakli va zarur takliflar keltirilgan.

METODOLOGIK TAVSIYALAR

Bugungi kunda biz o'byekt deb nomlagan barcha vazirlik, qo'mita, agentlik, korxona, tashkilot, muassasa, kompaniya, tijorat firmalari va boshqa uyushmalar o'zlarining xizmat faoliyatlarida asosan kompyuterardan foydalanganlari uchun barcha ma'lumotlarini saqlash, qayta ishlash, uzatish va qabul qilish jarayonlarida ularning xavfsizligini ta'minlash masalasi asosiy ro'lni o'ynaydi. Shuning uchun yuqorida keltirilganlar asosida har bir obyekt ma'lumotlarini xavfsizligini ta'minlash jarayonida quyidagilarga e'tibor berishlari kerak:

Obyektdagi binolarning sonidan, har bir binodagi honalarida joylashgan va ularda o'rnatilgan kompyuterlarning sonidan qat'iy nazar ma'lumotlarni turlariga qarab xavfsizlik modellarini qo'llashni;

Kompyuterlar joylashgan xonalarga katta e'tibor berish, yaniy tashkiliy himoyalash vositalarini - tashkiliy texnikaviy va tashkiliy xuquqiy vositalarni qo'llashni;

Obyektning mahalliy kompyuter tarmog'i orqali chetga chiqib ketadigan aloqa liniyalariga brandmauer, FireWall ekranlashtirish qurulmalarini o'rnatishni;

Obyektni kompyuter tarmog'ining aloqa kanallari orqali ruxsatsiz kirmoqchi bo'lganlar uchun identifikatsiya, autentifikatsiya, avtorizatsiyalarni qo'llashni;

Obyektning iqtisodiy sharoyatiga qarab kirayotgan hujumlarni aniqlaydigan texnikaviy va dasturiy qurulmalarni o'rnatishni;

Ma'lumotlarni uzatish va qabul qilish jarayonlarida kriptografik shifrlash va deshifrlash usullaridan foydalanishni;

Avtomashtirilgan obyektlarda intellektual tizimlardan foydalanib axborot xavfsizligini ta'minlashni va ushbu monografiyada keltirilganlardan foydalanishliklari kerak bo'ladi.

Bulardan tashqari quyidagilarga e'tibor berishliklarini so'raymiz:

1. Tarmoqdagi kompyuterlarga ruxsatsiz kirish va uni masofadan turib boshqarish. Ularga obyektning manfaatiga zid bo'lgan dasturlarni joylashtirish mumkin.

2. Web sahifalarida joylashtirilgan «aktiv obyektlar» agressiv dastur kodlari bo'lib, obyekt uchun xavfli virus yoki josus dastur vazifasini o'tashi mumkin.

3. Internetda uzatilayotgan ma'lumotlar yo'l yo'lakay aloqa kanallari yoki tarmoq tugunlarida tutib olinishi ulardan nusxa ko'chirilishi, almashtirilishi mumkin.

4. Davlat muassasasi, korxona faoliyati, moliyaviy ahvoli va uning xodimlari haqidagi ma'lumotlarni razvedka qilinishi o'g'irlashi va shu orqali obyektning rivojiga tahdid solishi mumkin.

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

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

1. Shaxsiy kompyuterga va mahalliy kompyuter tarmog'iga hamda unda mavjud bo'lgan informatsion resurslarga tashqaridan internet orqali kirishni cheklovchi va ushbu jarayonni nazorat qilish imkonini beruvchi texnik va dasturviy usullardan foydalanish.

2. Tarmoqdagi informatsion muloqat ishtirokchilari va ular kuzatayotgan ma'lumotlarni asl nusxasiga mosligini tekshirish.

3. Ma'lumotlarni uzatish va qabul qilishda kiriptografiya usullaridan foydalanish.

4. Viruslarga qarshi nazoratchi va davolovchi dasturlardan foydalanish.

5. Shaxsiy kompyuter va mahalliy kompyuter tarmog'iga begona shaxslarni qo'ymaslik va ularda mavjud bo'lgan ma'lumotlardan nusxa olish imkoniyatlarini cheklovchi tashkiliy ishlarni amalga oshirish.

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

- hech qachon hech kimga internetdagi login va parolingizni aytmaslik;

- hech qachon hech kimga o'zingiz va oila a'zolaringiz haqidagi shaxsiy hamda obyektingizga oyid ma'lumotlarni internet orqali yubormlik.

- elektron manzilingiz (e-mail)dan maqsadli foydalanish. Internet orqali dasturlar almashmaslik.

Internet tizimidagi elektron pochta juda ko'p ishlatilayotgan axborot almashish kanallaridan biri hisoblanadi. Elektron pochta yordamida axborot almashuvi tarmoqdagi axborot almashuvining 30% ini tashkil

etadi. Bunda axborot almashuvi bor-yo'g'i ikkita protokol: SMTP (Simple Mal Transfer Protocol) va POP-3 larni ishlatish yordamida amalga oshiriladi.

Shuning uchun ham bu protokollarning hammaga ochiqligi sababli, elektron pochta resurslariga ruxsatsiz kirishga imkoniyatlar yaratilib berilmoqda:

— SMTP server — dasturlarining nokorrekt o'rnatilishi tufayli bu serverlardan ruxsatsiz foydalanilmoqda va bu texnologiya «spama» texnologiyasi nomi bilan ma'lum;

— elektron pochta xabarlariga ruxsatsiz egalik qilish uchun oddiygina va samarali usullardan foydalanilmoqda, ya'ni quyi qatlamlarda vinchesterdagi ma'lumotlarni o'qish, pochta resurslariga kirish parolini o'qib olish va hokazolar.

Internetda tarqatilayotgan duch kelgan dasturlardan foydalanish kerak emas. Dasturlarni faqat ishonchli egasi ma'lum bo'lgan serverlardan ko'chirish kerak.

Elektron pochta orqali yuborilgan «aktiv obyektlar» va dasturlarni ishlatish kerak emas, yoki qo'shimchali o'z-o'zidan ochiluvchi sizga noma'lum arxiv holidagi ma'lumotlarni ochish taqiqlanadi.

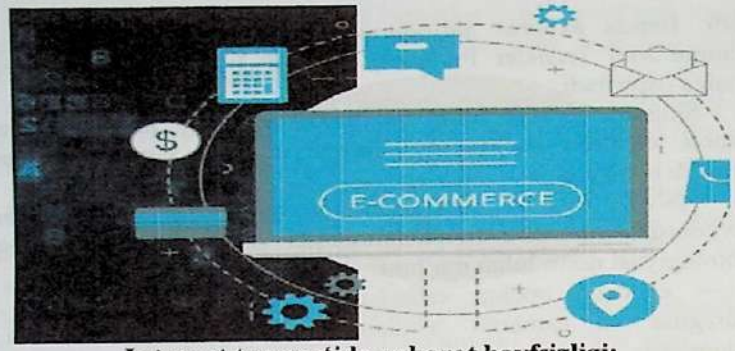
Elektron pochta xizmatidan foydalanayotgan davrda ma'lumotlarni shifrlash zarur, ya'ni kriptografiya usullaridan foydalanish kerak.

Egasi noma'lum bo'lgan xatlarni ochish kerak emas.

Egasi ma'lum bo'lgan va uning sifatiga kafolat beruvchi antivirus dasturlardan foydalanish va ularni muntazam yangilab borish zarur.

Internetda mavjud bo'lgan informatsion resurslar va dasturlardan ularning mualliflari ruxsatisiz foydalanish ham taqiqlanadi.

Tarmoqdagi begona kompyuter va serverlarning IP manzillarini aniqlash va shu orqali ruxsat etilmagan serverlar va informatsion resurslarga kirish nusxa ko'chirish, viruslar tarqatish kabi noqonuniy dasturlashtirish ishlari bilan shug'ullanish taqiqlanadi, bu esa jinoyat hisoblanadi.



Internet tarmog'ida axborot havfsizligi:

1. Har doim kirish manzillarini tekshirib borish kerak.

2. Brauzerning har bir kirish saytining yozuvini aniq o'qib tekshirib bo'lgandan so'ng kirish.

3. Noma'lum fayl yoki domen bo'lgan taqdirda ushbu faylni ochmaslik.

4. Har qanday ko'chirib olinadigan fayllarni aniq tekshirib keyin ko'chirish lozim.

Interanetda axborotlarni himoyalash

Intranet tarmog'i asosan "Mijoz-server" tizimi asosida faoliyat olib boriladi. Shuning uchun bosh rolni Web - servis o'ynaydi. Web - serverlar barcha himoyalash vositalari bilan ta'minlangan bo'lishligi kerak. Birinchi navbatda, barcha serverga kiruvchilarni autentifikatsiya asosida tekshirib ruhsat berish. Web serverning va kliyent (mijoz)ning dasturiy vositalari himoyalangan bo'lishligi kerak.

Intranetda asosan quyidagi himoyalash vositalari ishlatiladi:

1. Huquqiy himolash vositalari (qonunlar, normativ aktlar, standartlar va xakazo.

2. Tashkiliy ya'ni tashkiliy texnikaviy va tashkiliy huquqiy himolash vositalari.

3. Jismoniy yoki fizikaviy himoyalash vositalari.

4. Dasturiy va texnikaviy himoyalash vositalari va boshqalar.

UMUMIY XULOSA

Ushbu monografiya asosan 6 bobdan iborat bo'lib, har bir bobda konkret masalalar ko'rib, tahlil qilinib takliflar keltirilgan. Monografiyani o'qib chiqqan har bir inson o'ziga taaluqli bo'lgan ma'lumotlarga ega bo'ladi.

Birinchi bobda bizning monografiyamizda mavzuga taaluqli atamalar, terminlar, ta'riflar, hozirgi kunda axborot xavfsizligini boshqarish tizimining tushunchasi, uning tarixi, ushbu sohaga tegishli dunyoda qabul qilingan standartlar, obyektlarda ishlatilishi mumkin bo'lgan kompyuter tarmoqlarining umumiy har xil strukturalari keltirilgan hamda shu kompyuter tarmoqlarida xosil bo'lishi mumkin bo'lgan xavf-xatarlar, risklar va hujumlarning turlari keng yoritilib berilgan.

Ikkinchi bob bugungi kunda obyektlarda eng ko'p ishlatilayotgan axborotlarni himoyalash vositalaridan tashkiliy, texnikaviy (uskunaviy) dasturiy, qonuniy, hamda axborotlarni himoyalashning kriptografik usullari tahlil qilinib, obyektlarning faoliyatiga qarab tanlab olishlari taklif etilgan.

Uchinchi bobda har bir obyektning mualliflik huquqlarini himoyalashda stenografiyadan foydalanishi jarayonida kompyuterli grafik tasvirlarga maxsus belgi asosida dasturiy ta'minot bilan aniqlanishi, axborotlarni kriptografik himoyalash usullaridan asimmetriyali ikki kalitlik kriptografiya tizimini ishlash jarayoni, ma'lumotlarga ruxsatsiz kirishning dasturiy va texnik vositalari hamda obyektlarning kompyuter tarmoqlarida ma'lumotlarning tarqalish kanallari tahlil qilinib berilgan.

To'rtinchi bobda identifikatsiya, autentifikatsiya va avtotizatsiya jarayonlarini obyektlarda qo'llanish davrlarini, ma'lumotlarni obyektga kirayotgan va ularni tekshirish vositalari va usullari ko'rib chiqilgan. Ruhsatsiz kirayotgan va obyektlarga qilinayotgan hujumlarni aniqlovchi texnikaviy qurilmalari tahlil qilingan va ularnin xarakteristikalarini keltirilgan. Hozirgi kunda eng dolzarb bo'lgan virtual korporativ tarmoqlarni tashkillashtirish masalalari keng yoritilib berilgan. uchun tarmoqlararo ekranlarni qo'llash natijasida va obyektlarning tizimiga ruxsatsiz kirishning oldini olish uchun himoyalashning asosiy yo'nalishlari keltirilgan.

Beshinchi bob asosan obyektlarlar orasida axborotlarni uzatish va qabul qilish jarayonida qo'llaniladigan aloqa kanallarining, turlari, xarakteristikalari va zamonaviy optik shisha tolali aloqa kabellerini ishlatish usullari chizmali ko'rsatib berilgan. Obyektlar bir-birlari bilan ma'lumotlar ayirboshlash va himoyalash jarayonida kriptografik shifrlash va deshifrlash usullaridan foydalanish isbotlab berilgan. Obyektlarning axborotlarini himoyalashda eng asosiy me'zonlardan hisoblangan insonlarning bioparametrlaridan foydalanish taklif etilgan.

Oltinchi bob asosan avtomatlashtirilgan obyektlarning axborot xavfsizligini ta'minlashda intellektual tizimlarni qo'llashga, obyektlarda axborot xavfsizligini boshqarish jarayonida o'zini-o'zi o'qituvchi tizimlar yaratishga va obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasini ishlab chiqishga asoslangan bo'lib, kerakli va sarur takliflar keltirilgan.

Bulardan tashqari, ushbu monografiyada konkret obyektlar uchun olib borayotgan faoliyatiga qarab o'zlarida saqlanayotgan, qayta ishlanayotgan, kompyuter tarmoqlarining aloqa kanallari orqali qabul qilinayotgan va uzatilayotgan ma'lumotlarni xavfsizligini ta'minlash uchun qanday himoya vositalarini qo'llash, hamda obyekt xodimlari xalqaro kompyuter tarmoq'i bo'lmish Internetdan va Intranetdan foydalanganda nimalarga e'tibor berishlik qoidalari taklif sifatida berilgan.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Nigmatov H. Axborot xavfsizligi. O'quv qo'llanma (kirillda). "Fan va texnologiyalar nashriyot-matbaa uyi" bosmaxonasi. Toshkent. 2021. 176 bet.
2. Nigmatov H. Intellektual tizimlar. O'quv qo'llanma. "Fan va texnologiyalar markazining bosmaxonasi", Toshkent. 2020 y. 136 bet.
3. Nigmatov H., Tursunov N. Kompyuter tizimlari va tarmoqlari. O'quv qo'llanma. "Toshkent islom universiteti nashriyot-matbaa birlashmasi" nashriyoti. Toshkent shaxri. 2018 y. 184 bet.
4. Nigmatov H., Tursunov N. Axborot xavfsizligi. O'quv qo'llanma (lotinda). "Toshkent islom universiteti nashriot-matbaa birlashmasi" nashriyoti. Toshkent shaxri. 2018 y. 120 bet.
5. Nigmatov H. va boshqalar. Zamonaviy axborot texnologiyalari. O'quv qo'llanma. Toshkent sh. "Navro'z" nashriyoti. 2015 y.
6. Nigmatov H. va boshqalar. Axborot kommunikatsion texnologiyalarni transport va yo'l sohasida qo'llash. O'quv qo'llanma. Toshkent sh. "Adabiyot uchqunlari" nashriyoti 2017 y. 238 b.
7. Nigmatov X.. Системи и устройства спутниковой и мобилной радиосвязи. Учебное пособие. Шимкент. Izd."Jebe". 2013. 304 str.
8. Romantsev Yu.V., Timofeyev P.A., Shangin V.F. Зашита информатсии в компьютерних системах и сетях. Moskva: 2001. Radio i svyaz nashriyoti.
9. Ermatov Sh.T. Kompyuter tizimlarida axborotni himoya qilish. Elektron darslik. Toshkent, 2003.
10. Heglov A.Yu. Защита компьютерной информации от несанксинированного доступа. - SPb.: Nauka i texnika, 2004. - 384 s.
11. G'aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. " ALOQACHI" - 2008.
12. Vasilkov A. V. Vasilkov A. A. Vasilkov I. A. Информационные системы и их безопасность. Moskva-2011.
13. Nigmatov X.. Информационная безопасность. Защита информации в сетях телекоммуникации. Учебное пособие. Шимкент. 2013. Izd."Jebe". 188 стр.
14. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. Kompyuter tizimlarida axborotni himoyalash. Ma'ruza matnlari. TDIU Toshkent, 2003.
15. Zavgorodniy V.I. Комплексная зашита информации в компьютерних системах - M.: Logos, 2001.

16. Stepanov Ye.A., Korneyev I.K. Информационная безопасность и зашита информации. M.: Infra, 2002.
17. Partika T.L., Popov I.I. Информационная безопасность. Учебное пособие. — M.: Forum, 2010. — 432 c.
18. Melnikov V.P., Kleymenov S.A., Petrakov A.M. Информационная безопасность и зашита информации. Москва Издательский центр "Akademiya" -2009-331 c.

Internet resurslari

19. www.ziyonet.uz - Ziyonet axborot-ta'lim portali.
20. www.intuit.ru - Основы информационной безопасности.
21. www.osp.ru - Стандарты информационной безопасности.

MUNDARIJA

V BOB.
OBYEKTLARNING AXBOROTLARINI UZATISH VA QABUL QILISHDA KRIPTOTIZIMDAN FOYDALANISH

VI BOB.
OBYEKTLARNING AXBOROTLARINI XAVFSIZLIGINI BOSHQARISH JARAYONIDA INTELLEKTUAL TIZIMLARDAN FOYDALANISH

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

O‘ZBEKISTON XALQARO ISLOM AKADEMIYASI

NIGMATOV XIKMATULLA
RAXMANOV QURBON SODIKOVICH

OBYEKTLARDA AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMINI YARATISH METODOLOGIYASI

(Monografiya)

Taqrizchilar:
Ismoilov M.A.
- Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti Milliy tadqiqot universiteti professori, texnika fanlari doktori

Xodjaeva M.S.
- O‘zbekiston xalqaro islom akademiyasi “Zamonaviy AKT” kafedrasi dotsenti, t.f.n.

Nashr uchun muharrir:
Mansur Yunus,
O`zbekiston Jurnalistlari ijodiy uyushmasi a`zosi

Bosishga ruxsat etildi: 15.04.2022.
Ofset qog‘oz. Qag‘oz bichimi 84x108 1/16.
Times New Roman garniturasi. Shartli bosma tabog‘i 9,75
Nashr hisob tabog‘i 8,74. Adadi 50.

«ZAMON POLIGRAF» OK bosmaxonasida chop etildi.
Manzil: Toshkent shahri. Yunusobod tumani,
Bobodehqon mahallasi 45-uy.