O‘ZBEKISTON ALOQA VA AXBOROTLASHTIRISH AGENTLIGI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

S. G‘ANIYEV, M. KARIMOV, K.TASHEV

AXBOROT XAVFSIZLIGI

(Axborot-kommunikatsion tizimlar xavfsizligi)

Texnika fanlari doktori, professor S.S. Qosimov umumiy tahriri ostida

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi tomonidan texnika oliy o‘quv yurtlari, bakalavriat bosqichi talabalari uchun o‘quv qo‘llanma sifatida tavsiya etilgan

«ALOQACHI» – 2008

analyzed. In particular, principles, algorithms and reports of modern cryptographic means of protection of the information are considered; various types of gateway screens are described and recommendations on their use are given; methods and means of formation cryptoprotection virtual tunnels through the open communications of the global open networks of type Internet are discussed; questions of maintenance of the removed access to information resources of the enterprise are considered; problems of protection of the information in networks of data transmission and a way of their decision are described; the concept of a wireless network, threat on safety of a wireless network, a problem of safety of a wireless network are stated; methods and control systems of network safety are analyzed.

On the basis of the analysis and management of risks, the methodology of construction of system of information safety of the enterprise is formulated.

The manual is calculated on students of higher educational institutions, and also to the persons who are engaged in the field of information technologies and computer systems.

Taqrizchilar: **akad. Bekmurodov T.F** – Zamonaviy axborot texnologiyalari ITM, «Algoritm-injeniring» ITI yetakchi ilmiy xodimi, t.f.d., prof; **prof. Aripov M.M** – Mirzo Ulug'bek nomli O'zbekiston milliy universiteti «Informatika va tatbiqiy dasturlash» kafedrasi mudiri, fizika-matematika fanlari doktori

ISBN 978-9943-326-20-0

атак. Особое внимание уделяется проблемам обеспечения информационной безопасности электронного бизнеса и электронной коммерции. Формулируется концепция информационной безопасности и определяется политика безопасности в сетях.

Анализируются технологии защиты данных, базовые технологии сетевой безопасности, обнаружения вторжений и управления сетевой безопасностью. В частности, рассматриваются принципы, алгоритмы и протоколы современных криптографических средств защиты информации; описываются различные типы межсетевых экранов и даются рекомендации по их использованию; обсуждаются методы и средства формирования криптозащищенных виртуальных туннелей через открытые коммуникации глобальных открытых сетей типа Internet; рассматриваются вопросы обеспечения удаленного доступа к информационным ресурсам предприятия; описываются задачи защиты информации в сетях передачи данных и пути их решения; излагаются концепция беспроводной сети, угрозы на безопасность беспроводной сети, проблемы безопасности беспроводной сети; анализируются методы и системы управления сетевой безопасностью.

На основе анализа и управления рисками, формулируется методология построения системы информационной безопасности предприятия.

Пособие рассчитано на студентов высших учебных заведений, а также лицам, занимающимся в области информационной технологий и компьютерных систем.

***

The given manual is devoted to actual problems of protection of the information at creation and use of computer networks and corporate information systems. Kinds of attacks to computer networks and systems, and also methods and means of protection of local and corporate networks from the removed Internet-attacks are discussed. The special attention is given problems of maintenance of information safety of electronic business and electronic commerce. The concept of information safety is formulated and the politics of safety in networks is determined.

Technologies of protection of data, base technologies of network safety, detection of intrusions and managements of network safety are

G'aniyev Salim Karimovich, Karimov Majid Malikovich, Tashev Komil Axmatovich. Axborot xavfsizligi. (Axborot-kommunikatsion tizimlar xavfsizligi). O'quv qo'llanma. –T., «ALOQACHI», 2008, 362 bet.

Ushbu qo'llanma kompyuter tarmoqlari va korporativ axborot tizimlarini yaratishda va ishlatishda axborotni himoyalashning dolzarb muammolariga bag'lshlangan. Kompyuter tarmoqlari va tizimlariga tahdid xillari hamda lokal va korporativ tarmoqlarni **Internet**-hujumlardan himoyalash usullari va vositalari muhokama etiladi. Elektron biznes va elektron tijoratda axborot xavfsizligini ta'minlash muammosiga alohida e'tibor beriladi. Axborot xavfsizligi konsepsiyasi ta'riflanadi va tarmoqlarda xavfsizlik siyosati aniqlanadi.

Ma'lumotlarni himoyalash texnologiyasi, tarmoq xavfsizligining bazaviy texnologiyasi, suqilib kirishlarni va tarmoq xavfsizligini boshqarish tahlillanadi. Xususan, axborotni zamonaviy kriptografik himoyalash vositalarining prinsiplari, algoritmlari va protokollari ko'riladi; tarmoqlararo ekranlarning turli xillari tavsiflanadi va ularni ishlatish bo'yicha tavsiyalar beriladi; **Internet** xilidagi global ochiq tarmoqlarning ochiq kommunikatsiyalari orqali kriptohimoyalangan virtual tunnellarni shakllantirish usullari va vositalari muhokama etiladi; korxona axborot resurslaridan masofadan xavfsiz foydalanishni ta'minlash masalalari ko'riladi; ma'lumotlarni uzatish tarmog'ida axborotni himoyalash masalalari va ularni yechish yo'llari tavsiflanadi: simsiz tarmoq konsepsiyasi, simsiz tarmoq xavfsizligiga tahdidlar, simsiz tarmoq xavfsizligi muammosi bayon etiladi; tarmoq xavfsizligini boshqarish usullari va vositalari tahlillanadi.

Xavf-xatarlarni tahlillash va boshqarish asosida korxona axborot xavfsizligi tizimini qurish metodologiyasi ta'riflanadi.

Qo'llanma oliy o'quv yurtlari talabalariga, axborot texnologiyalari, kompyuter tizimlari sohasida faoliyat ko'rsatuvchilarga mo'ljallangan.

***

Данное пособие посвящено актуальным проблемам защиты информации при создании и использовании компьютерных сетей и корпоративных информационных систем. Обсуждаются виды атак на компьютерные сети и системы, а также методы и средства защиты локальных и корпоративных сетей от удаленных Internet-

MUNDARIJA

XII bob. **XAVFSIZLIKNI BOSHQARISH VA HIMOYA TIZIMINI QURISH**

ОГЛАВЛЕНИЕ

CONTENTS

XII chapter. **MANAGEMENT OF SAFETY AND CONSTRUCTION SYSTEMS OF PROTECTION**

MUQADDIMA

Ildam qadamlar bilan rivojlanayotgan kompyuter axborot texnologiyalari hayotimizda sezilarli o'zgarishlarga sabab bo'lmoqda. «Axborot» tushunchasi sotib olish, sotish, biror narsaga almashish va h. mumkin bo'lgan maxsus tovarni belgilashda tez-tez ishlatila boshlandi. Bunda axborotning narxi ko'pincha u joylashgan kompyuter tizimi narxidan yuz va ming marta yuqori bo'ladi. Demak, axborotni ruxsatsiz foydalanishdan, atayin o'zgartirishdan, yo'q qilishdan va boshqa jinoiy harakatlardan himoyalash zaruriyatining paydo bo'lishi tabiiydir.

Axborotni himoyalash muammosi kompyuter tizimlari va tarmoqlari sohasida faoliyat ko'rsatuvchi mutaxassislar hamda zamonaviy kompyuter vositalaridan foydalanuvchilar e'tiborini jalb etmoqda. Ayni paytda kompyuter fani va amaliyotining ushbu dolzarb muammosi Davlat tilida yozilgan ilmiy-texnik va o'quv adabiyotlarda yetarlicha o'z aksini topmagan.

O'quvchi e'tiboriga havola etilayotgan kitob axborot-kommunikatsion tizimlar xavfsizligiga bag'ishlangan va 12 ta bobdan iborat.

Kitobning *birinchi bobida* axborot xavfsizligining hozirgi holatiga baho beriladi. Kompyuter jinoyatchiligi tahlil etilib, tarmoq axborotiga bo'ladigan namunaviy hujum usullari keltiriladi hamda axborot xavfsizligini buzuvchining modeli tavsiflanadi. Shuningdek, bu bobda **Internet** – xizmatlari va elektron biznes tizimlarida xavfsizlik muammolari ko'rilgan.

Axborot xavfsizligining asosiy tushunchalari, xavfsizlikni ta'minlashning amalda tekshirilgan prinsiplari hamda xavfsizlik siyosatini yaratish jarayoni tavsifi kitobning *ikkinchi* bobida keltirilgan. Shu bilan birga axborot-kommunikatsion tizimlar va tarmoqlar xavfsizligiga qo'yiladigan talablar va axborot xavfsizligini ta'minlovchi choralar xususida so'z yuritilgan.

Axborot xavfsizligining huquqiy va tashkiliy ta'minoti, xavfsizlikning xalqaro va milliy huquqiy me'yorlari kitobning *uchinchi* bobida bayon etilgan.

Kitobning *to'rtinchi bobi* axborotni himoyalashning kriptografik usullariga bag'ishlangan bo'lib, ma'lumotlarni shifrlashning blokli

simmetrik algoritmlari, jumladan, **AQSH**ning yangi standarti **AES** tahlil etilgan va milliy standartimiz yoritib o'tilgan. Zamonaviy asimmetrik kriptotizimlar muhokama etilib, xeshlash funksiyalarining asosiy xususiyatlari va ishlatilish sohalari aniqlangan. Raqamli imzoni generatsiyalash va tekshirish muolajalari ko'rilgan. Kalitlarni boshqarish – kalitlarni taqsimlash jarayoniga alohida e'tibor qilingan.

Tizimning foydalanuvchilar bilan o'zaro aloqasidagi asosiy jarayoniar – foydalanuvchi harakatini autentifikatsiyalash, avtorizatsiyalash va ma'murlash, ko'p va bir marotabali parollar hamda raqamli sertifikatlar asosidagi autentifikatsiyalash xususiyatlarining tahlili kitobning *beshinchi* bobida yoritilgan. Foydalanuvchini identifikatsiyalash va autentifikatsiyalashning namunaviy sxemalari ko'rilgan. Simmetrik va asimmetrik kriptoalgoritmlarga asoslangan qat'iy autentifikatsiyalashga alohida e'tibor be-rilgan. Autentifikatsiyalashning **Kerberos** protokoli muhokama etilgan. Biometrik identifikatsiyalash va autentifikatsiyalash vositalari tavsiflangan.

Tarmoqlararo ekranlarning funksiyalari tahlili, ularning **OSI** modeli-ning turli sathlarida ishlashi xususiyatlari muhokamasi, tarmoqlaro ekranlar asosida tarmoqni himoyalash sxemalari, shaxsiy va taqsimlangan tarmoq ekranlarining ishlatilishi *oltinchi* bobda ko'rilgan.

Himoyalangan virtual xususiy tarmoqlarni ko'rish konsepsiyasi va ularning asosiy xususiyati – tunnellash, virtual himoyalangan kanallarni qurish variantlari tahlili, himoyalangan virtual xususiy tarmoqlarning qator alomatlari bo'yicha turkumlanishi, **VPN** texnologiyaning korporativ axborot tizimlari va tarmoqlarida qo'llanilishining texnik va iqtisodiy afzalliklari, **OSI** ochiq tizimlar o'zaro aloqa etalon modelining kanal va seans sathlarida himoyalangan virtual kanallar qurilishining muammolari muhokamasi, **IPSec** protokoliar stekining arxitekturasi, ularning himoyalangan xususiy tarmoqlar qurishda ishlatilishi masalalari kitobning *yettinchi* bobidan o'rin olgan.

Kitobning *sakkizinchi bobida* ochiq kalitlarni boshqarish infratuzilmasi **PKI** ko'rilgan. Ochiq kalitlarning raqamli sertifikatlarini ishlatish zaruriyati asoslangan. **PKI** ning ishlash prinsiplari muhokama etilgan. Sertifikatsiyalashning bazaviy modellari, **PKI** ning mantiqiy tuzilmasi va komponentlari keltirilgan.

Axborot xavfsizligini adaptiv boshqarishning dolzarb muammolari, korporativ tarmoq xavfsizligini adaptiv boshqarish konsepsiyasi tavsifi, himoyalanishni tahlillash texnologiyalari va vositalarining batafsil muhokamasi, tarmoq axborotini tahlillash usullari, hujumlarni aniqlash

tizimlarining komponentlari va arxitekturasi kitobning *to'qqizinchi* bobida o'z aksini topgan. Shu bilan bir qatorda kompyuter viruslaridan himoyalanishning dolzarb muammolari ham ushbu bobdan o'rin olgan. Kompyuter viruslarining turkumlanishi keltirilgan, virus hayot sikli bosqichlari tahlillangan, viruslar va boshqa zarar keltiruvchi dasturlarning asosiy tarqalish kanallari ko'rilgan. Virusga qarshi dasturlarning asosiylari muhokama etilib, virusga qarshi himoya tizimini qurish masalasi yoritilgan.

Ma'lumotlarni uzatish tarmog'ida axborotni himoyalash muammosi, ma'lumotlarni uzatish tarmog'i komponentlariga va arxitekturasiga real ta'sir etuvchi funksional, arxitekturaviy va boshqarish (ma'muriy) talablari hamda aloqa kanallarida ma'lumotlarni himoyalash usullarining muhokamasi *o'ninchi* bobda yoritib o'tilgan.

Simsiz aloqa tizimlarida axborot himoyasining dolzarb masalalariga bag'ishlangan muammolar *o'n birinchi* bobda keltirilgan bo'lib, unda simsiz tarmoq konsepsiyasi va tuzilmasi ko'rilgan. Simsiz tarmoq xavfsizligiga tahdidlar batafsil tahlil etilib, simsiz tarmoq xavfsizligi protokollari muhokama etilgan. Simsiz qurilmalar xavfsizligi muammolari ham ushbu bobdan o'rin olgan.

Kitobning *o'n ikkinchi bobi* tarmoq xavfsizligi vositalarini boshqarish usullariga bag'ishlangan. Axborot tizimlarini boshqarishning keng tarqalgan metodologiyasi **ITIL** tavsiflangan. Korxona miqyosida axborotni himoyalash tizimini boshqarish masalasi ta'riflangan. Xavfsizlikni markazlashtirilgan boshqarishning global va lokal xavfsizlik siyosatiga asoslangan istiqbolli arxitekturasiga alohida e'tibor berilgan. Axborot tizimlari xavfsizligining auditi va monitoringi ko'rilgan. Xavf-xatarlarni tahlillash va boshqarish muammosi hamda tarmoq xavfsizlik tizimini qurish metodologiyasi tavsiflangan.

Qo'llanmani tayyorlashda yaqindan yordam bergan (VII va XI boblar) texnika fanlari nomzodi A.A. G'aniyevga, taqrizchilarga hamda o'quv qo'llanma haqidagi barcha fikr mulohazalari uchun hurmatli kitobxonlarga mualliflar o'z minnatdorchiliklarini izhor etadilar.

Mualliflar

I bob. AXBOROT XAVFSIZLIGIGA TAHDIDLAR

1.1. Axborot urushlar va kiberhujumlar

Xavfsizlik – har kuni biz to'qnashadigan hayotimizning jihati: eshikni qulflaymiz, qimmatbaho narsalarni begona ko'zlardan berkitamiz va ham-yonni duch kelgan joyda qoldirmaymiz. Bu «raqamli dunyoga» ham rasm bo'lishi shart, chunki har bir foydalanuvchining kompyuteri qaroqchi hujumi obyekti bo'lishi mumkin.

Tijorat tashkilotlari xavfsizlikni ta'minlash o'zining birinchi galdagi vazifasi emas, balki uni ta'minlashga sarf etiladigan xarajatlarni muqarrar balo deb hisoblab kelganlar. Qandaydir darajada bu «oqilona ish»: nihoyat, usiz ham ish bajarishda to'siqlar to'lib-toshib yotibdiku?! Ammo firmaning barcha korporativ binolariga kecha-kunduz kirishga ruxsat berishga jur'at etuvchi aqli joyida «sanoat kapitanlari»ni ko'rganmisiz? Albatta, yo'q! Hatto kichkina kompaniya binosining kirish yo'lida sizni qorovul, yoki kirishni chegaralovchi va nazoratlovchi tizimi qarshi oladi. Axborotni himoyalash esa hali ko'ngildagidek emas. Axborotni qanday yo'qotish mumkinligini va bu qanday oqibatlarga olib kelishini barcha ham tushunavermaydi.

Yirik o'yinchilar yaxshigina saboq oldilar: xakerlar **Yahoo.com, Amazon.com** kabi kompaniyalarga va hatto kosmik tadqiqot agentiligi **NASA**ga katta zarar yetkazdilar. Xavfsizlik xizmati bozorining eng yirik nomoyondalaridan biri **RSA Sesurity**, harqanday tahdidga qarshi chora borligi xususidagi o'ylamasdan qilgan bayonotidan bir necha kundan keyin, hujumga duchor bo'ldi.

Odatda, odamlardan yoki predmetlardan chiqadigan va zarar yetkazadigan tahdidlar quyidagi sinflarga bo'linadi: *ichki* yoki *tashqi* va *tuzilmalangan* (ma'lum obyektga qarshi) yoki *tuzilmalanmagan* («kimga Xudo beradi» qabilida adreslanuvchi). Masalan, kompyuter viruslari «tashqi tuzilmalanmagan tahdidlar» sifatida turkumlanadi va tamomila oddiy hisoblanadi. Qizig'i shundaki, foydalanuvchilar o'zining kompyuterini muayyan nishon deb hisoblamaydilar, ular o'zlarini yaxshigina himoyalangandek sezadilar. Kerakli himoya darajasi aksariyat hollarda ishingizning holatiga bog'liq. Agar tashkilotingiz yoki kompaniyangiz qandaydir tazyiq nishoni bo'lsa, agar siz milliy energetik resurslarni taqsimlovchi yoki milliy aloqa tarmoqlariga xizmat qiluvchi davlat infratuzilmasi tarkibida bo'lsangiz, oddiy terroristlar

bombalarini va pistoletlarini chetga qo'yib, turli-tuman dasturiy vositalar yordamida tashkilotingizga elektron hujumni amalga oshirish masalasini ko'radilar. Ikkinchi tomondan, savdo-sotiq va marketing bo'yicha oddiy tashkilot xususida so'z borsa, faqat mijozlar ro'yxatini o'g'rilovchi xizmatchilaringiz to'g'risida, qalbaki kredit kartochkalari bo'yicha tovar oluvchi firibgarlar, tarmog'ingizga preyskurantlardan foydalanish maqsadida kiruvchi raqiblar, Web-saytingizni ta'magirlik maqsadida buzuvchilar va shunga o'xshashlar to'g'risida qayg'urishingizga to'g'ri keladi.

Ammo vahimaga o'rin yo'q. Birinchi navbatda kundalik ehtiyoj choralari ko'rilishi lozim. Axborotga ega bo'lishning eng ommabop usuli oddiy o'g'rilik. Siz ish stolingizda kechaga mo'maygina pulni qoldirib ketmaysiz-u. Nima uchun boquvchingiz-shaxsiy kompyuter xavfsizligini ta'minlashga ozgina vaqt sarf qilmaysiz? Bu nafaqat apparat vositalariga, balki ma'lumotlarga ham taalluqli. Ma'lumotlarni o'g'irlatish yoki yo'qotish katta, ba'zida, tuzatib bo'lmaydigan zarar keltiradi.

Ma'lumki, tizim ma'murlari barcha maxfiy materiallardan foydalanish imkoniga ega va odatda, kompaniya foydasidan o'z ulushlariga ega emaslar. Shu sababli xuddi ular tashkilot xavfsizligiga tahdid sola oluvchilar ichida eng kattasi hisoblanadilar. Ta'kidlash lozimki, kompaniya ishga kiruvchilarni sinchiklab tekshiradi. Xuddi shunday, xavfsizlik xizmatini ta'minlovchilarga, ayniqsa, maslahat berish, rejalashtirish va mu'murlashni tavsiya etuvchilarga diqqat bilan qarash lozim.

Sivilizatsiya rivojining zamonaviy bosqichida axborot nafaqat jamoat va davlat institutlari faoliyatida, balki har bir inson hayotida hal qiluvchi rolni uynaydi. Ko'z oldimizda jamiyatning axborotlashishi shiddat bilan va ko'pincha oldindan bilib bo'lmaydigan tarzda rivojlanmoqda. Biz esa uning ijtimoiy, siyosiy, iqtisodiy va boshqa oqibatlarini tushunib yetishga boshlaymiz, xolos. Jamiyatimizning axborotlashishi yagona dunyo axborot makonining yaratilishiga olib keladiki, bu makon doirasida axborotni yig'ish, ishlash, saqlash va subyektlar – insonlar, tashkilotlar, davlatlar o'rtasida almashish amalga oshiriladi.

Ravshanki, siyosiy, iqtisodiy, ilmiy-texnikaviy va boshqa axborotlarni tezlikda almashish imkoniyati, jamiyat hayotining barcha sohalarida va ayniqsa, ishlab chiqarishda va boshqarishda yangi texnologiyalarning qo'llanilishi so'zsiz foydalidir. Ammo sanoatning tezlikda rifojlanishi Yer ekologiyasiga tahdid sola boshladi, yadro fizikasi sohasidagi yutuqlar yadro urushi xavfini tug'dirdi. Axborotlashtirish ham jiddiy muammolar manbaiga aylanishi mumkin.

Urushlar doimo bo'lgan. Vaqt o'tishi bilan urushni olib borish butun bir fanga aylandi. Har qanday fandagidek urushda o'zining tarixi, o'zining qoidasi, mashhur namoyondalari, o'zining metodologiyasi paydo bo'ldi.

Zamonaviy urush g'oyasi juda ildamlab ketdi. Endi uning makoni – butun yer shari. Urush lokal qaroqchi hujumidan bir necha davlatlarni vayron qiluvchi global muammoga aylandi.

Turli mamlakatlarning harbiy doktrinalarida elektron qurol rivoji rejalari va maxsus vazifalarga mo'ljallangan dasturiy ta'minot to'g'risida eslatishlar ko'zga tashlanmoqda. Turli razvedka manbalaridan kelayotgan axborotning tahlili natijasida xulosa qilish mumkinki, ba'zi bir davlatlarning rahbarlari hujumkor kiber-dasturlarni yaratishni moliyalamoqdalar.

Axborot urushiga oddiy vositalar yordamida harbiy harakatlar samara bermaydigan hollarga nisbatan strategik altemativ sifatida qaralmoqda.

Harbiylar tomonidan kiritilgan *axborot urushi* atamasi real, qirg'inli va yemiruvchi harbiy harakatlar bilan bog'liq shafqatsiz va xavfli faoliyatni anglatadi. Bu urushning alohida qirralari–shtab urushi, elektron urushi, psixologik amallar va h.

Har qanday urush, axborot urushi shu jumladan, zamonaviy qurol yordamida olib boriladi. Axborot quroli yordamida, urush olib boriluvchi barcha qurollardan farqli o'laroq, e'lon qilinmagan va ko'pincha dunyoga ko'rinmaydigan urushlarni olib borish mumkin (olib borilmoqda ham). Bu qurolning ta'sir obyektlari – iqtisodiy, siyosiy, ijtimoiy va h. kabi jamiyat va davlat institutlari. Ma'lumotlarni uzatish tarmoqlarining kelajak janglar maydoniga aylanishi allaqachon e'tirof etilgan.

Axborot quroli hujumda va mudofaada «elektron tezlik» bilan ishlatilishi mumkin. U eng ilg'or texnologiyalarga asoslangan bo'lib, harbiy nizolarni dastlabki bosqichida hal etilishini ta'minlaydi hamda umummaqsad kuchlarning qo'llanilishini istisno qiladi. Axborot quroli qo'llanishining strategiyasi hujumkor xarakterga ega. Ammo xususiy zaiflik nuqtai nazari mavjud, ayniqsa, fuqarolik sektorida. Shu sababli bunday quroldan va axborot terrorizmidan himoyalanish muammosi hozirda birinchi o'ringa chiqqan. Foydalanuvchilariga dunyo tarmoqlarida ishlashni ta'minlovchi mamlakatlarning milliy axborot resurslarining zaifligi – har ikki tomonga xavfli narsa.

Axborot quroli deganda axborot massivlarini yo'qotish, buzish yoki o'g'irlash vositalari, himoyalash tizimini yo'qotish, qonuniy foydalanuvchilar faoliyatini chegaralash asbob-uskunalar va butun kompyuter, tizimi ishlashi tartibini buzish vositalari tushuniladi.

Hozirda hujumkor axborot quroli sifatida quyidagilarni ko'rsatish mumkin:

– *kompyuter viruslari* – ko'payish, dasturlarda o'rnashish, aloqa liniyalari, ma'lumotlarni uzatish tarmoqlari bo'yicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga o'xshash qobiliyatlarga ega;

– *mantiqiy bombalar* – signal bo'yicha yoki o'rnatilgan vaqtda harakatga keltirish maqsadida harbiy yoki fuqaro infratuzilmalariga o'rnatiluvchi dasturlangan qurilmalar;

– *telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari*, davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish;

– *testli dasturlarni betaraflashtirish vositalari*;

– obyekt dasturiy ta'minotiga ayg'oqchilar tomonidan atayin kiritiluv-chi turli xil *xatoliklar*.

Universallik, maxfiylik, dasturiy-apparat amalga oshirilishining har xilligi, ta'sirining keskinligi, qo'llanilishining vaqti va joyini tanlash imkoniyati, nihoyat, foydaliligi axborot qurolini haddan tashqari xavfli qiladi. Bu qurolni, masalan, intellektual mulkni himoyalash vositasiga o'xshatib niqoblash mumkin. Undan tashqari, u hatto urush e'lon qilmasdan hujum harakatlarini avtonom tarzda olib borish imkonini beradi.

Zamonaviy jamiyatda axborot qurolini ishlatish harbiy strategiyasi fuqaro sektori bilan uzviy bog'langan. Axborot qurolining ta'siri, shakli va usullarining paydo bo'lishi va qo'llanishi xususiyatlarining turlitumanliligi undan himoyalanishning murakkab masalalarini vujudga keltirdi.

Axborot quroli qo'llanilishini oldini olish yoki qo'llanishi oqibatlarini bartaraf qilish uchun quyidagi choralarni ko'rish lozim:

– axborot resurslarining fizik asosini tashkil etuvchi moddiy-texnik obyektlarni himoyalash;

– ma'lumotlar bazalari va banklarining me'yoriy va muttasil ishlashini ta'minlash;

– axborotdan ruxsatsiz foydalanishdan, uni buzilishidan yoki yo'q qilinishidan himoyalash;

– axborot sifatini saqlash (o'z vaqtidaligi, aniqligi, to'laligi va foydalanuvchanligi).

Davlatning dunyo ochiq tarmog'iga ulanishining iqtisodiy va ilmiy-texnik siyosatini axborot xavfsizligi orqali ko'rish lozim. Bu ochiq, fuqarolarning axborotga va intellektual mulkka ega bo'lish qonuniy huquqini saqlashga mo'ljallangan siyosat mamlakat hududida tarmoq asbob-uskunalarini unga axborot quroli elementlarining kirishidan saqlashni

ko'zda tutish lozim. Bu muammo hozirda, chet el axborot texnologiyalarini ommaviy sotib olinayotgan paytda o'ta muhimdir.

Ma'lumki, dunyo axborot makoniga ulanmasdan mamlakat iqtisodini rivojlantirib bo'lmaydi. **Internet** tarmog'i tomonidan ta'minlangan axborot va hisoblash resurslaridan tezkor foydalanishni davlatchilikni, fuqarolik jamiyati institutlarini mustahkamlash, ijtimoiy infratuzilmalarining rivojla-nish shartlari sifatida talqin etish mumkin.

Ammo mamlakatning xalqaro telekommunikatsiya tizimida va axborot almashinuvida ishtirokining axborot xavfsizligi muammosini kompleks hal qilmasdan mumkin emasligini aniq tasavvur etish lozim. Ayniqsa, xususiy axborot resurslarini himoyalash muammosi axborot va telekommunikatsiya texnologiyalar sohasida rivojlangan mamlakatlardan texnologik orqada qolayotgan mamlakatlar uchun jiddiy hisoblanadi.

Axborot qurolini ishlab chiqishni va uni ishlatishni kimyoviy va bakteriologik qurol kabi taqiqlash ehtimoldan uzoq. Xuddi shu kabi ko'pgina mamlakatlarning yagona global axborot makonini shakllantirish bo'yicha urinishlarini chegaralab bo'lmaydi.

Tizim ma'muri uchun himoyaning maqbul darajasini ta'minlashning yagona usuli-axborotga ega bo'lishi, chunki hozircha axborot hujumiga eng tez reaksiya beradigan inson hisoblanadi. Demak, axborotni himoyalash ma'murlarining o'qitishga va professional o'sishiga sarf-xarajat axborot hujumlariga qarshi turuvchi eng samarali vosita hisoblanadi.

1.2. Axborot-kommunikatsion tizimlar va tarmoqlarda tahdidlar va zaifliklar

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

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

– kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot hajmining oshishi;

– ma'lumotlar bazasida muhimlik va maxfiylik darajasi turlicha bo'lgan axborotlarning to'planishi;

– ma'lumotlar bazasida saqlanayotgan axborotdan va hisoblash tarmoq resurslaridan foydalanuvchilar doirasining kengayishi;

– masofadagi ishchi joylar sonining oshishi;

– foydalanuvchilarni bog'lash uchun Internet global tarmog'ini va aloqaning turli kanallarini keng ishlatish;

– foydalanuvchilar kompyuterlari o'rtasida axborot almashinuvining avtomatlashtirilishi.

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

Zamonaviy korporativ tarmoqlar va tizimlar duchor bo'ladigan keng tarqalgan tahdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlikka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi manba) bo'lishi mumkin. Bunday ajratish to'g'ri, chunki bitta tahdid uchun (masalan, o'g'irlash) tashqi va ichki manbalarga qarshi harakat usullari turlicha bo'ladi. Bo'lishi mumkin bo'lgan tahdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta'minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi.

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

foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo'lishi mumkin, oxirgisi ayniqsa, xavfli.

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

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

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

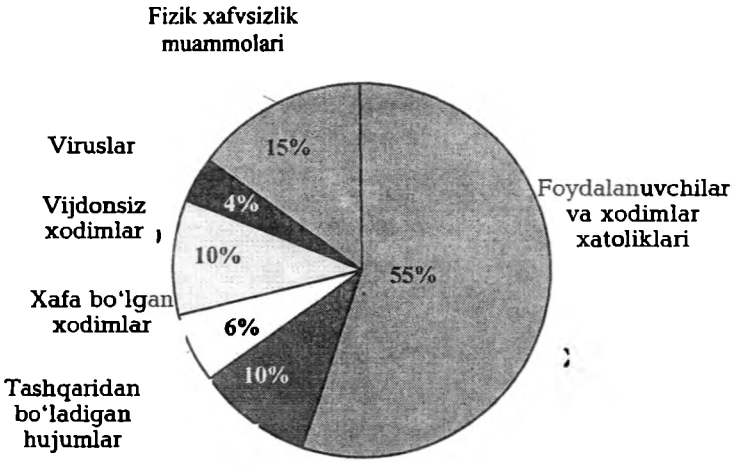
Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti duchor bo'ladigan xavf-xatar baholanishi va zarur choralar ko'rilishi zarur. Ravshanki, himoyaga tahdidni nazoratlash va zarur choralarni ko'rish uchun tashkilotning sarf-xarajati tashkilotda aktivlar va resurslarni himoyalash bo'yicha hech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

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

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

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

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



1.1-rasm. Xafvsizlikning buzilish manbalari.

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

1.3. Kompyuter jinoyatchiligining tahlili

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

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

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

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

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

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

Kompyuter ishlatiladigan inson faoliyatining boshqa sohalarida ham vaziyat yaxshi emas. Yildan-yilga huquqni muhofaza qiluvchi or-

ganlariga kompyuter jinoyatchiligi xususidagi murojaatlar oshib bormoqda.

Barcha mutaxassislar viruslarning tarqalishi bilan bir qatorda tashqi hujumlarning keskin oshganligini e'tirof etmoqdalar. Ko'rinib turibdiki, kompyuter jinoyatchiligi natijasida zarar qat'iy ortmoqda. Ammo kompyuter jinoyatchiligi ko'pincha «virtual» qalloblar tomonidan amalga oshiriladi deyish haqiqatga to'g'ri kelmaydi. Hozircha kompyuter tarmoqlariga suqilib kirish xavfi har biri o'zining usuliga ega bo'lgan xakerlar, krakerlar va kompyuter qaroqchilari tomonidan kelmoqda.

Xakerlar, boshqa kompyuter qaroqchilaridan farqli holda, ba'zida, ol-dindan, maqtanish maqsadida kompyuter egalariga ularning tizimiga kirish niyatlari borligini bildirib qo'yadilar. Muvaffaqiyatlari xususida Internet saytlarida xabar beradilar. Bunda xaker musobaqalashuv niyatida kirgan kompyuterlariga zarar yetkazmaydi.

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

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

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

1.4. Tarmoqdagi axborotga bo'ladigan namunaviy hujumlar

Barcha hujumlar Internet ishlashi prinsiplarining qandaydir chegaralangan soniga asoslanganligi sababli masofadan bo'ladigan namunaviy hujumlarni ajratish va ularga qarshi qandaydir kompleks choralarni tavsiya etish mumkin. Bu choralar, haqiqatan, tarmoq xavfsizligini ta'minlaydi.

Internet protokollarining mukammal emasligi sababali tarmoqdagi axborotga masofadan bo'ladigan asosiy namunaviy hujumlar quyidagilar:

- tarmoq grafigini tahlillash;
- tarmoqning yolg'on obyektini kiritish;
- yolg'on marshrutni kiritish;
- xizmat qilishdan voz kechishga undaydigan hujumlar.

Tarmoq trafigini tahlillash. Serverdan Internet tarmog'i bazaviy protokollari **FTP (File Transfer Protocol)** va **TELNET** (Virtual terminal protokoli) bo'yicha foydalanish uchun foydalanuvchi *identifikatsiya* va *autentifikatsiya* muolajalarini o'tishi lozim. Foyda-lanuvchini 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. Demak, Internet xostlaridan foydalanish uchun foydalanuvchining ismi va parolini bilish kifoya.

Axborot almashinuvida Internetning masofadagi ikkita uzeli almashinuv axborotini *paketlarga* bo'lishadi. Paketlar aloqa kanallari orqali uzatiladi va shu paytda ushlab qolinishi mumkin.

FTP va **TELNET** protokollarining tahlili ko'rsatadiki, **TELNET** parolni simvollarga ajratadi va parolning har bir simvolini mos paketga joylashtirib bittalab uzatadi, **FTP** esa aksincha, parolni butunlayicha bitta paketda uzatadi. Parollar shifrlanmaganligi sababli paketlarning maxsus skaner-dasturlari yordamida foydalanuvchining ismi va paroli bo'lgan paketni ajratib olish mumkin. Xuddi shu sababli, hozirda ommaviy tus olgan **ICQ** dasturi ham ishonchli emas. **ICQ**ning protokollari va axborotlarni saqlash, uzatish formatlari ma'lum va demak, uning trafigi ushlab qolinishi va ochilishi mumkin.

Asosiy muammo almashinuv protokolida. Bazaviy tatbiqiy prokollarning **TCP/IP** oilasi ancha oldin (60-yillarning oxiri va 80-yillarning boshi) ishlab chiqilgan va undan beri umuman o'zgartirilmagan. O'tgan davr mobaynida taqsimlangan tarmoq xavfsizligini ta'minlashga yondashish jiddiy o'zgardi. Tarmoq ulanishlarini himoyalashga va trafikni shifrlashga imkon beruvchi axborot almashinuvining turli protokollari ishlab chiqildi. Ammo bu protokollar eskilarining o'rnini olmadi (SSL bundan istisno) va standart maqomiga ega bo'lmadi. Bu protokollarning standart bo'lishi uchun esa tarmoqdan foydalanuvchilarning barchasi ularga o'tishlari lozim. Ammo Internetda tarmoqni markazlashgan boshqarish bo'lmaganligi sababli bu jarayon yana ko'p yillar davom etishi mumkin.

Tarmoqning yolg'on obyektini kiritish. 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 hatto undan shubhalanmasdan o'zingiz barcha elektron pochtangizni jo'natgan bo'lar edingiz.

Qandaydir xostga murojaat etilganida adreslarni maxsus o'zgartirishlar amalga oshiriladi (IP-adresdan tarmoq adapteri yoki marshrutizatorining fizik adresi aniqlanadi). Internetda bu muammoni yechishda ARP(Adress Resolution Protocol) protokolidan foydalaniladi. Bu quyidagicha amalga oshiriladi: tarmoq resurslariga birinchi murojaat etilganida xost keng ko'lamli ARP-so'rovni jo'natadi. Bu so'rovni tarmoqning berilgan segmentidagi barcha stansiyalar qabul qiladi. So'rovni qabul qilib, xost so'rov yuborgan xost xususidagi axborotni o'zining ARP-jadvaliga kiritadi, so'ngra unga o'zining Ethernet-adresi bo'lgan ARP-javobni jo'natadi. Agar bu segmentda bunday xost bo'lmasa, tarmoqning boshqa segmentlariga murojaatga imkon beruvchi marshrutizatorga murojaat qilinadi. Agar foydala-nuvchi va niyati buzuq odam bir segmentda bo'lsa, ARP-so'rovni ushlab qolish va yolg'on ARP-javobni yo'llash mumkin bo'ladi. Bu usulning ta'siri faqat bitta segment bilan chegaralanganligi tasalli sifatida xizmat qilishi mumkin.

ARP bilan bo'lgan holga o'xshab DNS-so'rovni ushlab qolish yo'li bilan Internet tarmog'iga yolg'on DNS-serverni kiritish mumkin.

Bu quyidagi algoritm bo'yicha amalga oshiriladi:

1. DNS-so'rovni kutish.
2. Olingan so'rovdan kerakli ma'lumotni chiqarib olish va tarmoq bo'yicha so'rov yuborgan xostga yolg'on DNS-javobni haqiqiy DNS-server nomidan uzatish. Bu javobda yolg'on DNS-serverning IP-adresi ko'rsatilgan bo'ladi.
3. Xostdan paket olinganida paketning IP-sarlavhasidagi IP-adresni yolg'on DNS serverning IP-adresiga o'zgartirish va paketni serverga uzatish (ya'ni yolg'on DNS-server o'zining nomidan server bilan ish olib boradi).

4. Serverdan paketni olishda paketning IP-sarlavhasidagi IP-adresni yolg'on DNS-serverning IP-adresiga o'zgartirish va paketni xostga uzatish (yolg'on DNS serverni xost haqiqiy hisoblaydi).

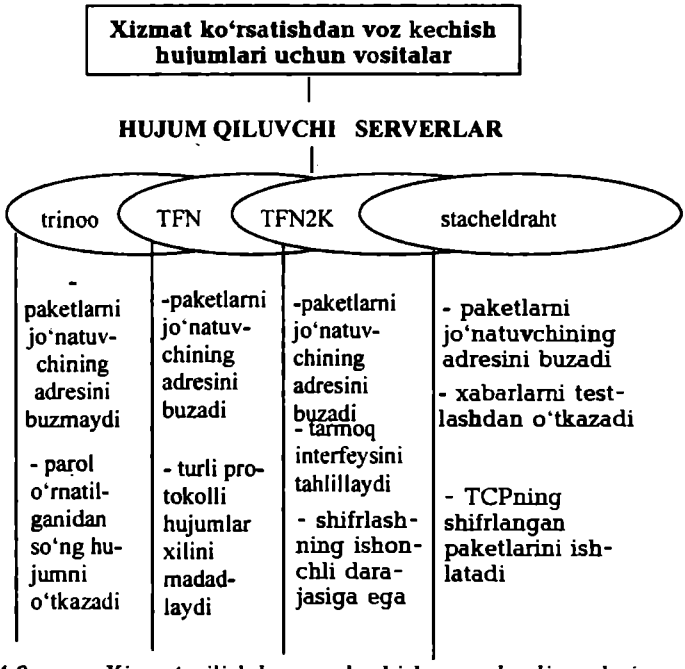
Yolg'on marshrutni kiritish. Ma'lumki, zamonaviy global tarmoqlari bir-biri bilan *tarmoq uzellari* yordamida ulangan tarmoq segmentlarining majmuidir. Bunda *marshrut* deganda ma'lumotlarni manbadan qabul qiluvchiga uzatishga xizmat qiluvchi tarmoq uzellarining ketma-ketligi tushuniladi. Marshrutlar xususidagi axborotni almashishni unifikatsiyalash uchun marshrutlarni boshqaruvchi maxsus protokollar mavjud. Internetdagi bunday protokollarga yangi marshrutlar xususida xabarlar almashish protokoli – **ICMP (Internet Control Message Protocol)** va marshrutizatorlarni masofadan boshqarish protokoli **SNMP (Simple Network Manegment Protocol)** misol bo'la oladi. Marshrutni o'zgartirish hujum qiluvchi yolg'on xostni kiritishdan bo'lak narsa emas. Hatto oxirgi obyekt haqiqiy bo'lsa ham, marshrutni axborot baribir yolg'on xostdan o'tadigan qilib qurish mumkin.

Marshrutni o'zgartirish uchun hujum qiluvchi tarmoqqa tarmoqni boshqaruvchi qurilmalar (masalan, marshrutizatorlar) nomidan berilgan tarmoqni boshqaruvchi protokollar orqali aniqlangan maxsus xizmatchi xabarlarni jo'natishi lozim. Marshrutni muvaffaqiyatli o'zgartirish natijasida hujum qiluvchi taqsimlangan tarmoqdagi ikkita obyekt almashadigan axborot oqimi ustidan to'la nazoratga ega bo'ladi, so'ngra axborotni ushlab qolishi, tahlillashi, modifikatsiyalashi yoki oddiygina yo'qotishi mumkin. Boshqacha aytganda tahdidlarning barcha turlarini amalga oshirish imkoniyati tug'iladi.

Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujumlar – DdoS (Distributed Denial of Service) kompyuter jinoyatchiligining nisbatan yangi xili bo'lsa-da, qo'rqinchli tezlik bilan tarqalmoqda. Bu hujumlarning o'zi anchagina yoqimsiz bo'lgani etmaganidek, 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, Tribe FloodNet (TFN) va TFN2K. Yaqinda TFN va trinooning eng yoqimsiz sifatlarini uyg'unlashtirgan yana bittasi stacheldraht («tikon simlar») paydo bo'ldi.

1.2-rasmda xizmat qilishdan voz kechishga undaydigan hujum vositalarining xarakteristikalari keltirilgan.



1.2-rasm. Xizmat qilishdan voz kechishga undaydigan hujum vositalarining xarakteristikalari.

Xizmat qilishdan voz kechishga undaydigan oddiy tarmoq hujumida xaker tanlagan tizimiga paketlarni junatuvchi instrumentidan foydalanadi. Bu paketlar nishon tizimining to'lib toshishi va buzilishiga sabab bo'lishi kerak. Ko'pincha bunday paketlarni junatuvchilar adresi buzib ko'rsatiladi. Shu sababli hujumning haqiqiy manbasini aniqlash juda qiyin.

DDoS hujumlarini tashkil etish bitta xakerning qo'lidan keladi, ammo bunday hujumning ta'siri *agentlar* deb ataluvchi hujum qiluvchi serverlarning ishlatilishi hisobiga anchagina kuchayadi. TFNda *serverlar* (server), a trinooda *demonlar* (daemon) deb ataluvchi bu agentlar xaker tomonidan masofadan boshqariladi.

1.5. Axborot xavfsizligini buzuvchining modeli

Bo'lishi mumkin bo'lgan tahdidlarni oldini olish uchun nafaqat operatsion tizimlarni, dasturiy ta'minotni himoyalash va foydalanishni na-

zorat qilish, balki buzuvchilar turkumini va ular foydalanadigan usullarni aniqlash lozim.

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

– sarguzasht qidiruvchilar;
– g'oyaviy xakerlar;
– xakerlar-professionallar;
– ishonchsiz xodimlar.

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

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

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

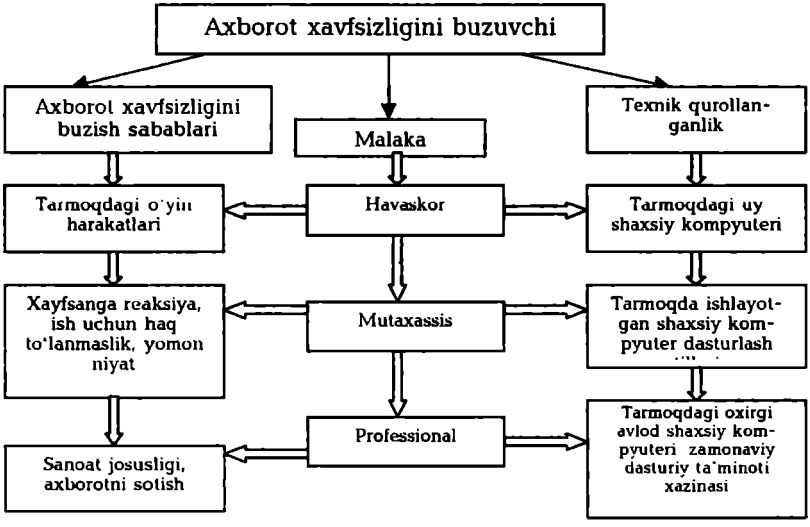
Ishonchsiz xodim o'zining harakatlari bilan sanoat josusi yetkazadigan muammoga teng (undan ham ko'p bo'lishi mumkin) muammoni tug'diradi. Buning ustiga uning borligini aniqlash murakkabroq. Undan tashqari unga tarmoqning tashqi himoyasini emas, balki faqat, odatda unchalik qatiy bo'lmagan tarmoqning ichki himoyasini bartaraf qilishiga to'g'ri keladi. Ammo bu holda, uning korporativ ma'lumotlardan ruxsat-

siz foydalanishi xavfi boshqa har qanday niyati buzuq odamnikidan yuqori bo'ladi.

Yuqorida keltirilgan axborot xavfsizligini buzuvchilar kategoriyalarini ularni malakalari bo'yicha guruhlash mumkin: havaskor (sarguzasht qidi-ruvchi), mutaxassis (g'oyali xaker, ishonchsiz xodim), professional (xaker-professional). Agar bu guruhlar bilan xavfsizlikning buzilishi sabablari va har bir guruhning texnik qurollanganligi taqqoslansa, axborot xavfsizligini buzuvchining umumlashtirilgan modelini olish mumkin (1.3-rasm).

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

- buzuvchi bo'lishi mumkin bo'lgan shaxslar kategoriyasi;
- buzuvchining bo'lishi mumkin bo'lgan nishonlari va ularning muhimlik va xavfsizlik darajasi bo'yicha rutbalanishi;
- uning malakasi xususidagi taxminlar; uning texnik qurollanganligi-ning bahosi;
- uning harakat xarakteri bo'yicha cheklashlar va taxminlar.



1.3-rasm. Axborot xavfsizligini buzuvchining modeli.

Tizimdan ruxsatsiz foydalanishga majbur etish sabablarining diapazoni yetarlicha keng: kompyuter bilan o'ynaganidagi hayajon ko'tarinkiligidan to jirkanch menejer ustidan hokimlik hissiyotigacha. Bu bilan nafaqat ko'ngil ochishni xohlovchi havaskorlar, balki professional dasturchilar ham shug'ullanadi. Ular parolni tanlash, faraz qilish natijasida yoki boshqa xa-kerlar 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 xizmatchilarning o'z mavqelarini suiiste'mol qilgan holda tizimni buzishlari, undan begonalarning foydala-nishlariga yo'l qo'yishlari yoki tizimni ish holatida qarovsiz qoldirishlari tashvishlantirar edi. Bunday harakatlarga majbur etish sabablari quyidagilar:

– xayfsanga yoki rahbar tomonidan tanbehga reaksiya;

– ish vaqtidan tashqari bajarilgan ishga firma haq to'lamaganidan norozilik;

– firmani qandaydir yangi tuzilayotgan firmaga raqib sifatida zaiflashtirish maqsadida qasos olish kabi yomon niyat.

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

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

Bunday professional xakerlar kategoriyasiga quyidagi shaxslar kiradi:

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

Umuman professional xakerlar xavf-xatarni minimallashtirishga urinadilar. Buning uchun ular birga ishlashga firmada ishlaydigan yoki firmadan yaqinda ishdan bo'shatilgan xodimlarni jalb etadilar, chunki begona uchun bank tizimiga kirishda oshkor bo'lish xavfi juda katta.

Haqiqatan, bank hisoblash tizimlarining murakkabligi va yuqori tezkorligi, hujjatlarni yurgizish va tekshirish usullarining muntazam takomillashtirilishi begona shaxs uchun xabarlarni ushlab qolish yoki ma'lumotlarni o'g'irlash maqsadida tizimga o'rnashishiga imkon bermaydi. Professional xakerlar uchun yana bir qo'shimcha xavotir-tizimdagi bir komponentning o'zgarishi boshqa bir komponentning buzilishiga olib kelishi va xatardan darak beruvchi signalga sabab bo'lishi mumkin.

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

1.6. Internet – xizmatlar va elektron biznes tizimlarida xavfsizlik muammolari

Hozirda Internet-xizmatining quyidagi tijorat shakllari keng tarqalgan:

- Internet-banking;
- Internet-treyding;
- Internet-sug'urta;
- ASP ilovalarini ijaraga berish bo'yicha xizmat ko'rsatish.

Internet-banking. Zamonaviy Internet-texnologiyalar banklarga xizmatlarining bir qismini yangi saviyaga o'tkazishga va shu orqali yangi mijozlarni jalb etishga va ularga xizmat qilish xarajatlarini pasaytirishga imkon yaratadi. An'anaviy banklarning aksariyati o'z mijozlariga elektron xizmat qilish va schet to'lovining qo'shimcha shakllarini tavsiya etadi. Faqat Internetda ish yurituvchi banklar nisbatan yaqinda paydo bo'ldi. Ular Web-banklar deb ataladi. Eng yirik Web-banklar sirasiga First Internet Bank, Net-Bank, CompuBank va qator boshqa banklar taalluqli.

Internet-banking deganda, odatda, mijozga oddiy kompyuter yordamida standart brauzerni ishlatib bank schyotidan Internet orqali to'g'ridan-to'g'ri foydalanish imkoniyatining berilishi tushuniladi. Internet-banking tizimining namunali varianti mijozlarga bank ofislaridagi

fizik shaxslarga (tabiiyki, naqd pul bilan bajariladigan amallar bundan istisno) taqdim etiluvchi bank xizmatining to'liq to'plamini o'z ichiga oladi.

Hozirda Internet-banking xizmati har biri Internet orqali amalga oshiri- luvchi quyidagi imkoniyatlarga ega:

– naqd pulsiz hisob-kitoblarni bajarish;

– kommunal xizmatlar uchun to'lovi;

– Internetdan foydalanish uchun to'lovi;

– uyali va peydjing aloqa operatorlari schyotlarini to'lash;

– ichki va banklararo hujjat asosidagi to'lovlarni bajarish;

– o'z schyotlari bo'yicha mablag'larni o'tkazish;

– istalgan vaqt oralig'i uchun o'z schyotlari bo'yicha barcha bank amallarini kuzatish.

Internet-banking tizimidan foydalanish mijozlarga qator imtiyozlar beradi:

– foizli stavkalari nisbatan yuqori;

– shaxsan bankka borish zaruriyati yo'qligi hisobidan mijozning vaqti jiddiy tejaladi;

– mijoz sutkada 24 soat shaxsiy schyotini nazoratlash va moliya bozoridagi vaziyatning o'zgarishiga tezdan reaksiya ko'rsatish imkoniyatiga ega.

Internet-banking tizimlari plastik kartalar bo'yicha amalga oshiriladigan amallarni kuzatishda juda asqotadi-karta hisobidan mablag'ni chiqarish tizimlar tomonidan tayyorlangan hisoblar bo'yicha ko'chirmada darhol akslantiriladi. Bu mijozga o'z amallarini nazoratlashda qulaylik tug'diradi.

Internet-treyding. Internet-texnologiyalar fond bozori uchun juda istiqbolli. Internet-texnologiyalar tufayli, dunyoda bo'sh kapitalni qo'yishning eng yaxshi usuli sifatida tan olingan qimmatbaho qog'ozlarni sotib olish, hozirda barcha xohlovchilar uchun oson. Internet-treyding investorlarni bitimlarni tuzishning soddaligi va onlayn-brokerlarning xizmatiga ta'riflarning pastligi bilan o'ziga jalb qiladi.

Internetning zamonaviy imkoniyatlari ko'chmas mulk bilan bo'ladigan amallarni (sotib olish, sotish, almashtirish, meros bo'yicha berish, ijaraga berish va h.) an'anaviy shakllariga nisbatan aytarlicha yengillashtirish va tezlashtirishga imkon beradi. Mijoz uyidan chiqmasdan ko'chmas mulkni sotib olishi va sotishi, mutaxassis maslahatini olishi mumkin. Bu amallarni bajarish uchun kompyuteri, Internetdan foydalana olishi va bankda schyoti bo'lishi kifoya.

Internet-sug'urta. Sug'urtalash deganda sug'urtalanuvchi-mijoz (sug'urta xizmatlarini sotib oluvchi) bilan sug'urtalovchi (bunday xizmatlarni taqdim etuvchi) o'rtasida shartnoma munosabatlarini o'rnatish va madadlash tushuniladi. Sug'urtalovchi sug'urta dasturini ishlab chiqadi va aniqlaydi, mijozga taklif etadi, agar sug'urtalanuvchi rozi bo'lsa, ikkala tomon shartnoma tuzadi. Mijoz birdaniga va muntazam to'lovlarni amalga oshiradi, sug'urtalovchi, o'z navbatida, so'g'urta holat kelishi bilan sug'urtalanuvchiga sug'urta shartnomasi shartlari bo'yicha kompensatsiya pulini to'lashga majburiyat oladi.

Bitimga kelishish jarayonida sug'urta polisi deb ataluvchi hujjat shakllantiriladi. Bu hujjat sug'urtalovchi va sug'urta kompaniyasi uchun yuridik hujjat hisoblanadi. Unda sug'urta obyekti (mol-mulk, odam, mas'uliyat), sug'urtalanuvchi holat, sug'urta muddatining boshlanishi va nihoyasi, sug'urta summasi, sug'urta mukofoti kabi muhim tomonlari oldindan aytib o'tiladi.

Rivojlangan mamlakatlar sug'urta kompaniyalarida sug'urta polislarini amalga oshiruvchi Internet-kanallar mavjud.

ASP ilovalarini ijaraga berish bo'yicha xizmat ko'rsatish. Yangi iqtisodiyot rivojining istiqbolli yo'nalishlaridan biri ASP (Applications Service Providing) ilovalarini ijaraga berish bo'yicha xizmat ko'rsatishdir. Internet yoki xususiy tarmoq orqali foydalanuvchidan uzoqdagi serverda joylashgan ilovalardan foydalanishni ASP ilovalari amalga oshiradi.

ASP ilovalarining provayderi o'zining serverlariga ilovalarning dasturiy ta'minotini o'rnatadi va ulardan mijozlarning foydalanishini ta'minlaydi. Mijoz kompyuteriga bunday dasturiy ta'minotni o'rnatishi, uni yangilashi, zaxira nusxalashi va h. shart emas. Barcha ishlarni ASP provayderi bajaradi. Mijoz provayderga ilovalardan foydalangani uchun ijara haqini to'laydi.

Kompaniyalarning ASP xizmatlaridan foydalanishining sababi quyidagilar:

– kompaniya ehtiyoj sezgan eng yangi texnologiyalardan xavf-xatarsiz, katta xarajatsiz va ma'muriy javobgarsiz foydalanish;

– ilovalardan tezda foydalanish zaruriyati;

– agar kompaniyani ilova qandaydir sabablarga to'la qoniqtirmasa, osongina voz kechish imkoniyati.

Yaqin yillarda ASP bozorining tez o'sishi kutilmoqda. Bu esa, o'z navbatida, barcha kompaniyalarga istalgan biznes-ilovalardan bir xilda foydalanishni taqdim etish orqali, biznes rivojida barqarorlikni

ta'minlaydi. Aksariyat analitiklarning fikricha, keyinchalik ASP modeli biznes ilovalardan foydalanish usullarining orasida ustunlik qilishi mumkin.

Elektron biznes xaridor va sotuvchi orasidagi aloqani tashkil etish, buyurtmani ifodalash, muhokama qilish, o'zgartirish, tovarlarni va xizmatlarni sotish usullarini hamda to'lovni amalga oshirish jarayonlarini o'zgartirish uchun yangi texnologiyalardan foydalanadi. Hozirda elektron tijorat va biznesning aksariyat muammolari axborot xavfsizligi bilan bog'liq, ya'ni xavfsizlik muammolari elektron tijorat va biznes rivojidagi jiddiy to'siq hisoblanadi.

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

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

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

Internet konfidensial axborotni dunyoning istalgan nuqtasiga yuborishi mumkin, ammo agar u yetarlicha himoyalanmagan bo'lsa, ushlab qolinishi, nusxalashtirilishi, o'zgartirilishi hamda har qanday chetdagi foydalanuvchilar – niyati buzuq odamlar, raqiblar va oddiy qiziquvchilar tomonidan o'qilishi mumkin. Masalan, yetarlicha himoyalanmagan to'lov topshirig'i yoki kredit kartochka nomerini jo'natayotganda esda tutish lozimki, jo'natish xususiy/shaxsiy tarmoq orqali amalga oshirilmayapti va chetdagi foydalanuvchilar xabaringizni manipulatsiya qilish

imkoniyatiga ega. Undan tashqari xabaringiz almashtirilib qo'yilishi mumkin: xabarlarni xuddi *B* foydalanuvchidan yuborilganidek *A* foydalanuvchidan yuborish usullari mavjud. Internet tarmog'i maxsus paket, tamomila qonuniy paketlar, sonining haddan tashqari ko'pligi uzatishdagi buzilishlar, tarmoq komponentlarining nosozligi tufayli ishga layoqat bo'lmasligi mumkin. Bunday hollar «xizmat qilishdan voz kechish» deb ataladi va elektron tijorat uchun eng jiddiy tahdid hisoblanadi. 1.1-jadvalda axborot xavfsizligi buzilishining statistikasi keltirilgan.

1.1-jadval

Axborot xavfsizligi buzilishining turlari	**Qayd etilganligi %**	**Yo'qotishlar %**
Korporativ tarmoqdan ruxsatsiz chetdan foydalanish	44	25
Xizmat qilishdan voz kechish	32	28
Uzatishda ma'lumotlarni almashtirish	17	18
Faol tinglab ko'rish	2	1
Tarmoqdan ruxsatsiz ichki foydalanish	97	62
Axborotdan ruxsatsiz ichki foydalanish	55	32

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

– konfidensiallikka kafolatning yo'qligi – kimdir ma'lumotlaringizni uzatilayotganida ushlab qolishi va qiymatli axborotni (masalan, kredit kartochkangizning nomerini, tovar yetkazib berish sanasi va adres) topishga urinishi mumkin;

– amalda ishtirok etuvchilarni tekshirish darajasining yetarli emasligi – tranzaksiya qatnashchilari tekshirilmaganida tomonlarning biri «maskarad» uyushtirishi mumkinki, uning oqibati ikkinchi tomonga ancha qimmatga tushadi. Masalan, xaridor saytga kirib undagi kompaniyaning haqiqiyligiga shubha qiladi, shunday hol ham ro'y berishi mum-

kinki, xaridor kredit kartochkasining nomerini yetarlicha vakolatga ega bo'lmagan shaxsga beradi;

– sotuvchida buyurtma bergan xaridor kredit kartochkasining qonuniy egasi ekanligining tekshirish imkoni yo'q;

– kredit kartochkasining bank–emitenti to'lovni bajarishga talab qo'ygan sotuvchini tekshirishni istab qolishi mumkin;

– ma'lumotlar yaxlitligiga kafolat yo'q – hatto ma'lumotlarni jo'natuvchi indentifikatsiyalangan bo'lsa-da, uchinchi tomon ma'lumotlarni, ular uzatilishi vaqtida, o'zgartirish imkoniyatiga ega.

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

1. Buyurtmachi Web-server orqali mahsulot yoki xizmatni tanlaydi va mos buyurtmani rasmiylashtiradi.

2. Buyurtma magazinning buyurtmalar ma'lumotlari bankiga kiritiladi.

3. Buyurtma berilgan mahsulot yoki xizmatni olish mumkinligini ma'lumotlarning markaziy bazasi orqali tekshiriladi.

4. Agar mahsulotning olinishi mumkin bo'lmasa, buyurtmachi u to'g'rida ogohlantiriladi va mahsulot yoki xizmatga ega bo'lish jarayoni to'xtatiladi. Mahsulotga so'rov boshqa skladga (buyurtmachi roziligida) yo'naltirilishi mumkin.

5. Agar mahsulot yoki xizmat mavjud bo'lsa, buyurtmachi to'lovni tasdiqlaydi va buyurtma mos ma'lumotlar bazasiga kiritiladi. Elektron magazin mijozga buyurtma tasdig'ini yuboradi. Ko'pgina hollarda (ayniqsa, endigina ish boshlagan kompaniyalarda) buyurtmalar, tovarlarning borligini tekshirish va h. uchun yagona ma'lumotlar bazasi mavjud.

6. Mijoz onlayn rejimida buyurtma haqini to'laydi.

7. Tovar buyurtmachiga yetkaziladi.

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

- elektron magazin Web-saytining sahifasini almashtirib qo'yish Bu tahdidni amalga oshirishning asosiy usuli – foydalanuvchi so'rovini boshqa serverga yo'llash. Bu tahdid oltincha bosqichda buyurtmachi kredit kartochkasining nomerini kiritganda kuchayadi;

• yolg'on buyurtmalar berish va elektron magazin xodimlari tomonidan firibgarlik qilish. Hozirda ichki-tashqi tahdidlar munosabati 60/40ni tashkil etadi;

• elektron tijorat tizimida uzatiladigan ma'lumotlarni ushlab qolish. Buyurtmachining kredit kartasi xususidagi axborotni ushlab qolish o'zgacha xavf-xatarni tug'diradi;

• kompaniyaning ichki tarmog'iga kirish va elektron magazin komponentlarini obro'sizlantirish;

• «xizmat qilishdan voz kechish» (denial of service) hujumini amalga oshirish va elektron tijorat ishlashini yoki uning uzelini buzish.

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

II bob. AXBOROT XAVFSIZLIGINI TA'MINLASHNING ASOSIY YO'LLARI

2.1. Axborotni himoyalash konsepsiyasi

Niyati buzuq odamlarni yolg'iz foydalanuvchilar emas, balki korporativ kompyuter tarmoqlari qiziqtiradi. Aynan bunday tarmoqlarda axborotning yo'qolishi, ruxsatsiz modifikatsiyalanishi jiddiy oqibatlarga olib kelishi mumkin.

Kompyuter tarmoqlarini himoyalash uyda foydalanuvchi kompyuter-larni himoyalashdan farqlanadi (garchi individual ishchi stansiyalarni himoyalash-tarmoq himoyasining ajralmas qismi). Chunki avvalo, bunday masala bilan savodli mutaxassislar shug'ullanadilar. Shu bilan birga korporativ tarmoq xavfsizligi tizimining asosini chetki foydalanuvchilar uchun ishlash qulayligi va texnik mutaxassislarga qo'yiladigan talablar o'rtasida murosaga kelishni tashkil etadi.

Kompyuter tizimiga ikki nuqtai nazardan qarash mumkin: unda faqat ishchi stansiyalardan foydalanuvchilarni ko'rish mumkin yoki faqat tarmoq operatsion tizimining ishlashini hisobga olish mumkin.

Simlar bo'yicha o'tuvchi axborotli paketlar majmuini ham kompyuter tarmog'i deyish mumkin. Tarmoqni ifodalashning bir necha sathlari mavjud. Xuddi shunday tarmoq xavfsizligi muammosiga turli sathlarda yondashish mumkin. Mos holda har bir sath uchun himoyalash usuli turlicha bo'ladi. Tizimning ishonchli himoyalanishi himoyalangan sathlar soni bilan belgilanadi.

Birinchi, ko'rinib turgan va amalda eng qiyin yo'l-xodimlarni tarmoq hujumlarini qiyinlashtiruvchi xatti-harakatga o'rgatish. Bu bir qarashda osonday tuyulsa-da, ammo mushkul ish. Internetdan foydalanishni chegaralash lozim. Aksariyat foydalanuvchilar chegaralanishlar sababini bilmaydilar. Shuning uchun taqiqlar aniq ifodalanishi lozim.

Tarmoqda axborotni himoyalashning zaruriy darajasini ishlab chiqishda xodimlar va rahbariyatning o'zaro javobgarligi, shaxs va tash-

kilot manfaatlariga rioya qilish, huquqni muhofaza qiluvchi organlar bilan o'zaro aloqa hisobga olinadi.

Kompyuter tarmoqlari axborotini himoyalashga himoyalash tadbirlarining yagona siyosatini hamda huquqiy, tashkiliy-ma'muriy va muhandis - texnik xarakterga ega choralar tizimini o'tkazish orqali erishiladi.

Raqobatli sharoitda xizmatlarning katta sonini taqdim etish va xizmat qilish vaqtini qisqartirish orqali yetakchi o'rinni saqlab qolish va yangi mijozlarni jalb etish mumkin. Bunga faqat barcha amallarni avtomatlashtirishning zaruriy darajasini ta'minlash evaziga erishish mumkin. Ayni zamonda hisoblash texnikasining ishlatilishi bilan nafaqat paydo bo'lgan muammolar hal etiladi, balki axborotni buzilishi va yo'qotilishi, tasodifan va atayin modifikatsiyalanishi hamda axborotni begonalar tarafidan ruxsatsiz olinishi bilan bog'liq yangi noan'anaviy tahdidlar paydo bo'ladi.

Mavjud holatning tahlili ko'rsatadiki, axborotni himoyalash uchun qilinadigan tadbirlar darajasi, odatda, avtomatlashtirish darajasidan past. Bunday orqada qolish jiddiy oqibatlarga olib kelishi mumkin.

Avtomatlashtirilgan komplekslarda axborotning zaifligiga hisoblash resurslarining konsentratsiyalanishi, ularning hududiy taqsimlanganligi, magnit eltuvchilarida ma'lumotlarning katta hajmini uzoq vaqt saqlanishi, ko'pgina foydalanuvchilarning resurslardan bir vaqtda foydalanishi sabab bo'ladi.

Bunday sharoitda himoyalash choralarini ko'rish zaruriyatiga shubha qilmasa bo'ladi. Ammo quyidagi qiyinchiliklar mavjud:

- hozirgi kunda himoyalangan tizimlarning yagona nazariyasi yo'q;
- himoya vositalarini ishlab chiqaruvchilar xususiy masalalarni yechish uchun asosan alohida komponentlarni tavsiya etadilar, himoyalash tizimini shakllantirish va bu vositalarning birga ishlatilishi masalalari esa iste'molchi ixtiyoriga qoldiriladi;
- ishonchli himoyani ta'minlash uchun texnik va tashkiliy muammolari kompleksini hal etish va mos hujjatlarni ishlab chiqish zarur.

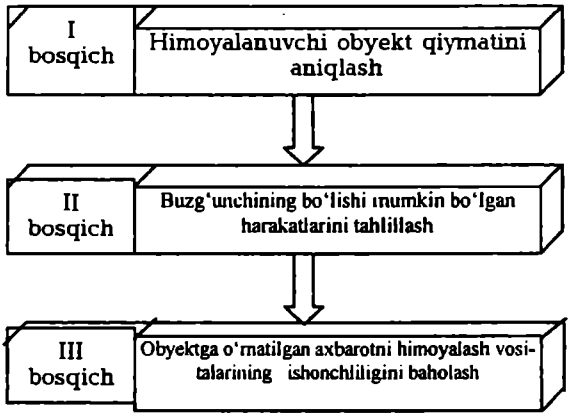
Yuqorida sanab o'tilgan qiyinchiliklarni bartaraf qilish uchun nafaqat alohida korxona, balki davlat darajasidagi axborot jarayonlarida ishtirok etuvchilari harakatining koordinatsiyasi zarur. Axborot xavfsizligini ta'minlash yetarlicha jiddiy masala. Shuning uchun avvalo axborot xavfsizligi konsepsiyasini ishlab chiqish zarur. Konsepsiyada milliy va korporativ manfaatlar, axborot xavfsizligini ta'minlash prinsiplari

va madadlash yo'llari aniqlanadi va ularni amalga oshirish bo'yicha masalalar ta'riflanadi.

Konsepsiya – axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yo'llari.

Konsepsiyada ifodalangan maqsadlar, masalalar va ularni bo'lishi mumkin bo'lgan yechish yo'llari asosida axborot xavfsizligini ta'minlashning muayyan rejalari shakllantiriladi.

Konsepsiyani ishlab chiqishni uch bosqichda amalga oshirish tavsiya etiladi (2.1-rasm).



2.1-rasm. Axborot himoyasi konsepsiyaini ishlab chiqish bosqichlari.

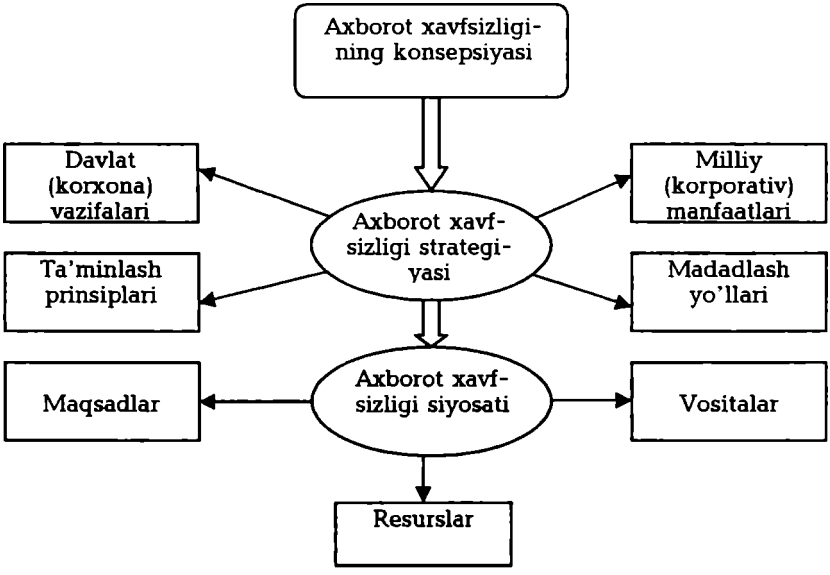
Birinchi bosqichda himoyaning maqsadli ko'rsatmasi, ya'ni qanday real boyliklar, ishlab chiqarish jarayonlari, dasturlar, ma'lumotlar bazasi himoyalanishi zarurligi aniqlanishi shart. Ushbu bosqichda himoyalanuvchi alohida obyektlarni ahamiyati bo'yicha tabaqalashtirish maqsadga muvofiq hisoblanadi.

Ikkinchi bosqichda himoyalanuvchi obyektga nisbatan bo'lishi mumkin bo'lgan jinoiy harakatlar tahlillanishi lozim. Iqtisodiy josuslik, terrorizm, sabotaj, buzish orqali o'g'Irlash kabi keng tarqalgan jinoyatchiliklarning real xavf-xatarlik darajasini aniqlash muhim hisoblanadi. So'ngra, niyati buzuq odamlarning himoyaga muhtoj asosiy obyektlarga nisbatan harakatlarining ehtimolligini tahlillash lozim.

Uchinchi bosqichning bosh masalasi–vaziyatni, xususan o'ziga xos mahalliy sharoitni, ishlab chiqarish jarayonlarini, o'rnatib qo'yilgan himo-yaning texnik vositalarini tahlillashdan iborat.

2.2. Axborot himoyasining strategiyasi va arxitekturasi

Axborot xavfsizligi strategiyasi va himoya tizimi arxitekturasi (2.2-rasm) axborot xavfsizligi konsepsiyasi asosida ishlab chiqiladi.



2.2-rasm. Axborot xavfsizligini ta'minlash ierarxiyasi.

Axborot xavfsizligi bo'yicha tadbirlar kompleksining asosini axborot himoyasining strategiyasi tashkil etishi lozim. Unda ishonchli himoya tizimini qurish uchun zaruriy maqsadlar, mezonlar, prinsiplar va muolajalar aniqlanadi. Yaxshi ishlab chiqilgan strategiyada nafaqat himoya darajasi, rahnalarni qidirish, brandmauerlar yoki proxy-serverlar o'rnatiladigan joy va h. o'z aksini topishi lozim, balki ishonchli himoyani kafolatlash uchun ularni ishlatish muolajalari va usullari ham aniqlanishi lozim.

Axborot himoyasi umumiy strategiyasining muhim xususiyati xavfsizlik tizimini taqiqlashdir. Ikkita asosiy yo'nalishni ajratish mumkin:

- himoya vositalarining tahlili;
- hujum bo'lganini aniqlash.

Axborot xavfsizligini ta'minlash ierarxiyasidagi ikkinchi masala siyosatni aniqlashdir. Uning mazmuni eng ratsional vositalar va resurslar, ko'rilayotgan masala maqsadi va unga yondashish tashkil etadi. Himoya siyosati-umumiy hujjat bo'lib, unda foydalanish qoidalari sanab o'tiladi, siyosatni amalga oshirish yo'llari aniqlanadi va himoya muhitining bazaviy arxitekturasi tavsiflanadi. Bu hujjat matnning bir nechta sahifalaridan iborat bo'lib, tarmoq fizik arxitekturasini shakllantiradi, undagi axborot esa himoya mahsulotini tanlashni aniqlaydi.

2.3. Axborot xavfsizligining siyosati

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

Samarali himoya uchun har bir obyekt mumkin bo'lgan tahdidlar va hujum turlari, maxsus instrumentlar, qurollar va portlovchi moddalarning ishlatilishi ehtimolligi nuqtai nazaridan baholanishi zarur. Ta'kidlash lozimki, niyati buzuq odam uchun eng qimmatli obyekt uning e'tiborini tortadi va ehtimolli nishon bo'lib xizmat qiladi va unga qarshi asosiy kuchlar ishlatiladi. Bunda, xavfsizlik siyosatining ishlab chiqilishida yechimi berilgan obyektning real himoyasini ta'minlovchi masalalar hisobga olinishi lozim.

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

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

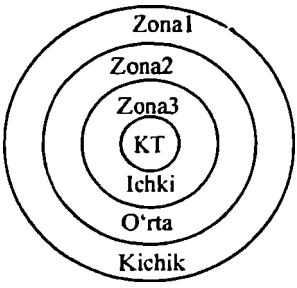
Agar bir binoning ichida turli himoyalash talablariga ega bo'lgan obyektlar joylashgan bo'lsa, bino otsekllarga bo'linadi. Shu tariqa umumiy nazoratlanuvchi makon ichida ichki perimetrlar ajratiladi va ruxsatsiz foydalanishdan ichki himoya vositalari yaratiladi. Perimetr, odatda, fizik to'siqlar orqali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

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

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

Binolar, imoratlar va axborot vositalarining xavfsizlik tizimini nazorat punktlarini bir zonadan ikkinchi zonaga o'tish yo'lida joylashtirgan holda konsentrik halqa ko'rinishida tashkil etish maqsadga muvofiq hisoblanadi (2.3-rasm).

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



1-zona. Kompyuter tarmog'i (KT) xavfsizligining tashqi zonasi
Ta'minlanishi: - fizik to'siqlar
- perimetr bo'ylab o'tish joylari
- hududga kirish nazoratining noavtomatik tizimi
2- zona. KT xavfsizligining o'rtadagi zonasi
Ta'minlanishi: - eshiklari elektron himoyalangan nazorat punktlari
- videokuzatish
- bo'm-bo'sh zonalarni chiqarib tashlash
3-zona. KT xavfsizligining ichki zonasi
Ta'minlash: - shaxsiy kompyuterga foydalanish faqat nazorat tizimi orqali
- identifikatsiyalashning biometrik tizimi

2.3-rasm. Binodagi kompyuter tarmog'ining xavfsizlik tizimi.

Xavfsizlikning fizik vositalarini tanlash himoyalanuvchi obyektning muhimligini, vositalarga ketadigan xarajatni va nazorat tizimi ishonchliligi darajasini, ijtimoiy jihatlarni va inson nafsi buzuqligini oldindan o'rganishga asoslanadi. Barmoq, kaftlar, ko'z to'r pardasi, qon tomirlari izlari yoki nutqni aniqlash kabi biometrik indentifikatsiyalash ishlatilishi mumkin. Shartnoma asosida texnik vositalarga xizmat ko'rsatuvchi xodimlarni obyektga kiritishning maxsus rejimi ko'zda tutilgan. Bu shaxslar identifikatsiyalanganlaridan so'ng obyektga kuzatuvchi hamrohligida kiritiladi. Undan tashqari ularga aniq kelish rejimi, makoniy chegaralanish, kelib-ketish vaqti, bajaradigan ish xarakteri o'rnatiladi.

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

Vaqti-vaqti bilan eshiklar, romlar, tom, ventilatsiya tuynuklari va boshqa chiqish yo'llarining fizik himoyalanish ishonchliligini tekshirib turish lozim.

Har bir xonaga ichidagi narsaning muhimliligiga bog'liq foydalanish tizimiga ega bo'lgan zona sifatida qaraladi. Kirish-chiqish huquqi tizimi shaxs yoki obyekt muhimligiga bog'liq holda seleksiyali va dara-

jalari bo'yicha rutbalangan bo'lishi shart. Kirish-chiqish huquqi tizimi markazlashgan bo'lishi mumkin (ruxsatlarni boshqarish, jadval va kalendar rejalarining tuzilishi kirish-chiqish huquqining yozma namunalari va h.).

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

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

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

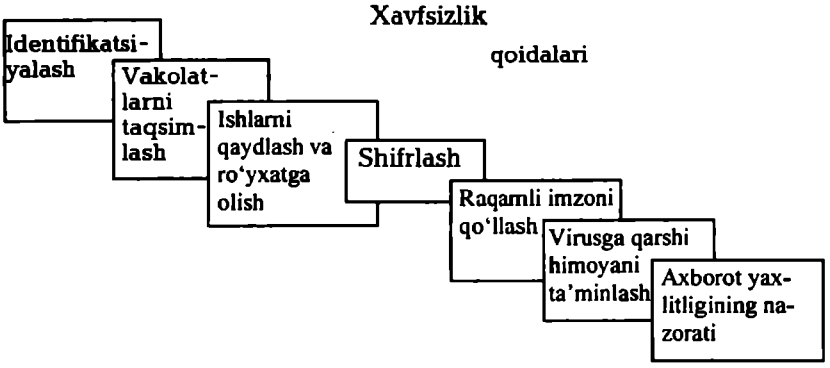
Siyosat odatda ikki qismdan iborat bo'ladi: umumiy prinsiplar va ishlashning muayyan qoidalari. Umumiy prinsiplar Internetda xavfsizlikka yondashishni aniqlasa, qoidalar nima ruxsat etilishini va nima ruxsat etilmasligini belgilaydi. Qoidalar muayyan muolajalar va turli qo'llanmalar bilan to'ldirilishi mumkin.

Odatda, xavfsizlik siyosati tarmoq asosiy servislaridan (elektron pochta, WWW va h.) foydalanishni reglamentlaydi hamda tarmoqdan foydalanuvchilarni ular qanday foydalanish huquqiga ega ekanliklari bilan tanishtiradi. Bu esa, o'z navbatida, foydalanuvchilarni autentifikatsiyalash muolajasini aniqlaydi.

Bu hujjatga jiddiy yondashish lozim. Himoyaning boshqa barcha strategiyasi xavfsizlik siyosatining qat'iy bajarilishi taxminiga asoslangan. Xavfsizlik siyosati foydalanuvchilar tomonidan ko'pgina malomat orttirilishiga sabab bo'ladi, chunki unda foydalanuvchiga ma'n etilgan narsalar ochiq-oydin yozilgan. Ammo xavfsizlik siyosati rasmiy hujjat, u bir tomondan Internet taqdim etuvchi servislarda ishlash zaruriyati, ikkinchi tomondan mos mutaxassis-professionallar tarafidan ifodalangan xavfsizlik talablari asosida tuziladi.

Avtomatlashtirilgan kompleks himoyalangan hisoblanadi, qachonki barcha amallar obyektlar, resurslar va muolajalarni bevosita himoyasini ta'minlovchi qat'iy aniqlangan qoidalar bo'yicha bajarilsa (2.4-rasm).

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



2.4-rasm. Axborot xavfsizligi siyosatini ta'minlashning asosiy qoidalari.

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

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

– xavf-xatarni tahlillash;

– xavfsizlik siyosatini amalga oshirish;

– xavfsizlik siyosatini madadlash.

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

Ikkinchi bosqich – xavfsizlik siyosatini amalga oshirishdagi moliyaviy xarajatlarni hisoblash va bu masalalarni yechish uchun mos vositalarni tanlash bilan boshlanadi. Bunda tanlangan vositalar ishlashining ixtilofli emasligi, vositalarni yetkazib beruvchilarning obro'si, himoya mexanizmlari va beriladigan kafolatlar xususidagi to'la axborot olish imkoniyati kabi omillar hisobga olinishi zarur. Undan tashqari, axborot

xavfsizligi bo'yicha asosiy qoidalar aks ettirilgan prinsiplar hisobga olinishi kerak.

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

2.4. Axborot-kommunikatsion tizimlar va tarmoqlar xavfsizligiga qo'yiladigan talablar

Qo'yida Rossiya Fedaratsiyasida ishlab chiqilgan kompyuter tarmoqlarida axborotni himoyalash sohasiga taalluqli hujjatlar xususida so'z yuritiladi. Hujjatlarda qo'yilgan talablar davlat sektorida yoki tarkibida davlat siri bo'lgan axborotni ishlovchi tijorat tashkilotlarida bajarilishi shart. Boshqa tijorat tuzilmalar uchun hujjatlar tavsiya xarakteriga ega.

Hujjatlardan biri axborotdan ruxsatsiz foydalanishdan himoyalash bo'yicha talablarni aks ettiradi va «avtomatlashtirilgan tizimlar. Axborotdan ruxsatsiz foydalanishdan himoyalash. Avtomatlashtirilgan tizimlarning turkumlanishi va axborotni himoyalash bo'yicha talablar» deb nomlanadi.

Bu hujjatda xavfsizlikning istalgan darajasiga erishish bo'yicha asoslangan choralarni ishlab chiqish va qo'llash maqsadida avtomatlashtirilgan tizimlarning axborotni himoyalash nuqtai nazaridan ishlashi sharoitlari bo'yicha turkumlanishi keltirilgan. Har bir himoyalash bo'yicha ma'lum minimal talablar majmui orqali xarakterlanuvchi himoyalanishning to'qqizta sinfi belgilanadi (2.1-jadval).

Kompyuter tarmoqlarining himoyalanish sinflari

2.1-jadval

Talablar	Sinflar								
	3B	3A	2B	2A	1D	1G	1V	1B	1A
Foydalanishni boshqarish qism tizimiga									
Identifikatsiyalash, haqiqiyligini tekshirish va subyektlar foydalanishining nazorati									
- tizimga	x	x	x	x	x	x	x	x	x
- terminallarga, EHMga, EHM tarmog'i uzellariga, aloqa kanallariga, EHMni tashqi qurilmalariga	-	-	-	x	-	x	x	x	x
- dasturlarga	-	-	-	x	-	x	x	x	x
- jildlarga, kataloglarga, fayllarga, qaydlarga	-	-	-	x	-	x	x	x	x
Axborot oqimlarini boshqarish	-	-	-	x	-	-	x	x	x
Ro'yxatga va hisobga olish qism tizimiga									
Ro'yxatga va hisobga olish									
- subyektlarning tizimga(dan) kirishini (chiqishini)	x	x	x	x	x	x	x	x	x
- bosma (grafik) hujjatlarni berishni	-	x	-	x	-	x	x	x	x
- dasturni va jarayonlarni (topshiriqlar, masala-lar)ishga tushirishni (tugal-lashni)	-	x	-	x	-	x	x	x	x
- subyekt dasturlaridan foydalanishni (himoyalanuvchi fayllardan foydalanish, ularni yaratish va yo'qotish, aloqa liniyalari va kanallari orqali uzatishni)	-	-	-	x	-	x	x	x	x
- subyekt dasturlaridan foydalanishni (termi-nallardan, EHMdan, EHM tarmog'i uzellaridan, aloqa kanallaridan, EHM tashqi qurilmalaridan, dasturli jildlardan, katloglardan, fayllardan, qaydlar hoshiyalaridan foydalanishni)	-	-	-	x	-	x	x	x	x
- foydalanuvchi subyektlar vakolatlarini o'zgartirishlarni	-	-	-	-	-	-	x	x	x

- himoyalanuvchi foydalanish obyektning yaratilishini	-	-	-	x	-	-	x	x	x
Axborot eltuvchilarini hisobga olish	x	x	x	x	x	x	x	x	x
Tezkor xotira va tashqi to'plagichlarni tozalash	-	x	-	x	-	x	x	x	x
Himoyani buzishga urinishni signalizatsiyasi	-	-	-	-	-	x	x	x	x
Kriptografik qism tizimiga									
Konfidensial axborotni shifrlash	-	-	-	-	-	-	x	x	x
Foydalanishni turli subyektlariga (subyektlar guruhiga) tegishli axborotni turli kalitlarda shifrlash	-	-	-	-	-	-	-	-	x
Attestatsiyadan o'tgan (sertifikatsiyalangan) kriptografik vositalardan foydalanish	-	-	-	-	-	-	-	x	x
Yaxlitlikni ta'minlovchi qism tizimiga									
Dasturiy vositalar va ishlanuvchi axborotning yaxlitligini ta'minlash	x	x	x	x	x	x	x	x	x
Hisoblash texnikasi vositalari va axborot eltuvchilarini qo'riqlash	x	x	x	x	x	x	x	x	x
Axborot himoyasi ma'muriyatining (xizmatining) mavjudligi	-	-	-	x	-	-	x	x	x
Axborot himoyasi tizimini vaqti-vaqti bilan testlash	x	x	x	x	x	x	x	x	x
Axborot himoyasi tizimini tiklash vositalarining mavjudligi	x	x	x	x	x	x	x	x	x
Sertifikatsiyalangan himoya vositalaridan foydalanish	-	x	-	x	-	-	x	x	x

Sinflar axborot ishlanishi xususiyatlari bilan bir-biridan farqlanuvchi uchta guruhga bo'linadi. Har bir guruh ichida axborotning qiymatligiga (konfidensialligiga) bog'liq holda himoya bo'yicha talablar ierarxiyasi va demak, himoyalanish sinflari saqlanadi. Har bir guruh ko'rsatkichlarini, oxirgisidan boshlab ko'rib chiqamiz.

Uchinchi guruh bir xil konfidensiallik darajasiga ega bo'lgan eltuvchilarda joylashtirilgan barcha axborotdan foydalanuvchi bitta foydalanuvchi ishlaydigan tizimlardan iborat. Guruhda ikkita – 3B va 3A sinflari mavjud.

Ikkinchi guruh har xil konfidensiallik darajasiga ega bo'lgan ishlanuvchi va yoki eltuvchilarda joylashtirilgan barcha axborotdan foydalanishga bir xil huquqli foydalanuvchilari bo'lgan tizimlardan iborat. Guruhda ikkita – 2B va 2A sinflari mavjud.

Birinchi guruh ko'pchilik foydalanuvchi tizimlardan iborat bo'lib, ularda bir vaqtning o'zida konfidensiallik darajasi turli axborot ishlanadi va/yoki saqlanadi. Guruhda beshta -1D, 1G, 1V, 1B va 1A sinflari mavjud.

Umumiy holda himoyalash tadbirlari 4 ta qism tizimni o'z ichiga oladi:

– foydalanishni boshqarish;
– ro'yxatga va hisobga olish;
– kriptografik;
– yaxlitlikni ta'minlash.

Hisoblash texnikasi vositalarini ruxsatsiz foydalanishdan himoyalanish ko'rsatkichlari «Hisoblash texnikasi vositalari. Axborotni ruxsatsiz foydalanishdan himoyalash. Himoyalash ko'rsatkichlari» deb ataluvchi hujjatda keltirilgan. Unda axborotdan ruxsatsiz foydalanishdan himoyalanishning 7 sinfi aniqlangan. Eng pastki sinf – yettinchi, eng yuqori sinf – birinchi. Har bir sinf himoyalanish talablarini oldingisidan meros qilib oladi. Himoyaning amalga oshirilgan modellari va ularni tekshirish ishonchliligiga bog'liq holda sinflar to'rtta guruhga ajratiladi.

Birinchi guruhda faqat yettinchi sinf bo'ladi (minimal himoyalanish).

Ikkinchi guruh tanlanadigan himoya bilan xarakterlanib oltinchi va beshinchi sinflarni o'z ichiga oladi. Tanlanuvchi himoya nomma-nom aytilgan subyektlarning tizimning nomma-nom aytilgan obyektlaridan foydalanishni ko'zda tutadi. Bunda har bir «subyekt-obyekt» juftligi uchun foydalanishning ruxsat etilgan turlari aniqlanishi shart. Foydalanish nazorati har bir obyektga va subyektga qo'llaniladi.

Uchinchi guruh muxtor huquqli himoya bilan xarakterlanib, to'rtinchi, uchinchi va ikkinchi sinflarni o'z ichiga oladi. Muxtor huquqli himoya tizimning har bir subyekt va obyektiga, uning mos ierarxiyadagi o'rnini ko'rsatuvchi turkumlash belgisini berish tizimdan foydalanuvchi yoki maxsus ajratilgan subyekt tomonidan amalga oshiriladi. Ushbu huquqqa kiruvchi sinflardan talab qilinadigan narsa-foydalanishning dispetcherini (reference monitor–havolalar monitori) amalga oshirilishi. Foydalanish nazorati barcha obyektlarga nisbatan har qanday subyekt tomonidan ochiq va yashirin foydalanishda amalga oshirilishi shart. Foydalanishga ruxsat berish faqat tanlanadigan va muxtor huquqli qoidalarning birgalikda ruxsati bo'lgandagina amalga oshirilishi mumkin.

To'rtinchi guruh tasdiqlangan himoya bilan xarakterlanib faqat birinchi sinfni o'z ichiga oladi.

Tizim himoyalanish sinfini olishi uchun quyidagilarga ega bo'lishi lozim:

- tizim bo'yicha ma'mur qo'llanmasi;
- foydalanuvchi qo'llanmasi;
- testlash va konstruktorlik hujjatlar.

Yuqorida ko'rib o'tilganidek, hozirda kompyuter jinoyatchiligi juda ham turli-tuman. Bu kompyuterdagi axborotdan ruxsatsiz foydalanish, dasturiy ta'minotga mantiqiy bombalarni kiritish, kompyuter viruslarini ishlab chiqish va tarqatish, kompyuter axborotini o'g'irlash, dasturiy-hisob komplekslarini ishlab chiqishda, qurishda va ekspluatatsiyasida pala-partishlik.

Axborot xavfsizligining bevosita ta'minlovchi, kompyuter jinoyatchiligining oldini oluvchi barcha choralarni quyidagilarga ajratish mumkin:

– huquqiy;
– tashkiliy-ma'muriy;
– muhandis-texnik.

Huquqiy choralarga kompyuter jinoyatchiligi uchun javobgarlikni belgilovchi me'yorlarni ishlab chiqish, dasturchilarning mualliflik huquqini himoyalash, jinoiy va fuqarolik qonunchiligini hamda sud jarayonini takomillashtirish kiradi. Ularga yana kompyuter tizimlarini yaratuvchi ustidan jamoatchilik nazorati masalalari hamda agar kompyuter tizimlarining bitimga kelgan mamlakatlarning harbiy, iqtisodiy va ijtimoiy jihatlariga ta'siri bo'lsa, cheklashlar bo'yicha mos xalqaro shartnomalarni qabul qilish kiradi. Faqat oxirgi yillarda kompyuter jinoyatchiliklariga qarshi huquqiy kurash muammolari bo'yicha ishlar paydo bo'ldi.

Tashkiliy-ma'muriy choralarga kompyuter tizimlarini qo'riqlash, xodimlarni tanlash, maxsus muhim ishlarni bir kishi tomonidan bajarilishi hollariga yo'l qo'ymaslik, markaz ishdan chiqqanida uning ishga layoqatligini tiklash rejasining mavjudligi, barcha foydalanuvchilardan (yuqori rahbarlar ham bunga kiradi) himoyalanish vositalarining universalligi, markaz xavfsizligini ta'minlashga mutasaddi shaxslarga javobgarlikni yuklash, markaz joylanadigan joyni tanlash va h. kiradi.

Muhandis-texnik choralarga kompyuter tizimini ruxsatsiz foydalanishdan himoyalash, muhim kompyuter tizimlarini rezervlash, o'g'irlash va diversiyadan himoyalanishni ta'minlash, rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish va hokazo kiradi.

III bob. AXBOROT XAVFSIZLIGINING HUQUQIY VA TASHKILIY TA'MINOTI

3.1. Axborot xavfsizligi sohasida huquqiy boshqarish

Axborot xavfsizligining huquqiy ta'minoti – axborotni himoyalash tizimida bajarilishi shart bo'lgan qonunlashtiruvchi dalolatnomalar, me'yoriy- huquqiy hujjatlar, qoidalar yo'riqnomalar, qo'llanmalar majmui. Hozirda axborot xavfsizligining huquqiy ta'minoti masalasi ham amaliy, ham qonunchilik jihatidan faol o'rganib chiqilmoqda.

Kompyuter jinoyatchiliklarini qilish instrumentlari sifatida telekommunikatsiya va hisoblash texnikasi vositalari, dasturiy ta'minot va intellektual bilim ishlatiladi. Kompyuter jinoyatchiliklarini qilish sohasi sifatida nafaqat kompyuterlar, global va korporativ tarmoqlar (Internet/Intranet), balki axborot texnologiyasining zamonaviy, yuqori unumli vositalari hamda axborotning katta hajmi ishlanadigan, masalan, statistik va moliya institutlari, tanlanadi.

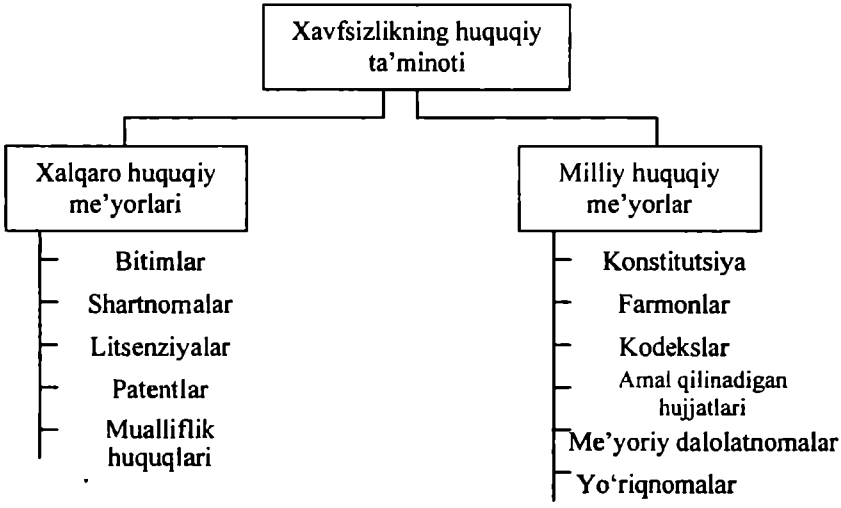
Shu sababli, har qanday tashkilot faoliyatini turli-tuman axborotni olish uchun qo'lda yoki hisoblash texnikasi vositalari yordamida ishlash, axborotni tahlillash natijasida qandaydir muayyan yechimlarni olish va ularni aloqa kanallari orqali uzatishsiz tasavvur etib bo'lmaydi. Kompyuterga ham tajovuz obyekti, ham tajovuz qiluvchi instrument sifatida qarash mumkin. Agar kompyuter faqat tajovuz obyekti bo'lsa, qonun buzilishini mavjud huquqiy me'yorlar orqali baholash mumkin. Agar kompyuter faqat instrument bo'lsa, «texnik vositalarni qo'llash» alomati yetarli bo'ladi. Yuqoridagi tushunchalarni birlashtirish mumkin - kompyuter bir vaqtning o'zida ham instrument va ham obyekt. Xususan bunday vaziyatga mashina axborotining o'g'irlanishi fakti taalluqli.

Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa, bu fakt jinoyat sifatida baholanadi. Shuningdek, agar ushbu fakt bilan milliy xavfsizlik, mualliflik manfaatlari bog'liq bo'lsa, jinoiy javobgarlik O'zbekiston Respublikasi qonunlarida bevosita ko'zda tutilgan.

Har qanday davlatda axborot xavfsizligining huquqiy ta'minoti xalqaro va milliy huquqiy me'yorlarni o'z ichiga oladi (3.1-rasm).

Huquqiy boshqarish predmetlari quyidagilar:

- axborot himoyasining huquqiy rejimi;
- axborotlashtirish jarayonlarida qonuniy munosabat qatnashchilarining huquqiy maqomi;
- subyektlarning, axborot tuzilmalari va ishlash jarayonining turli bosqich hamda sathlaridan huquqiy maqomini hisobga olgan holda, munosabatlari tartibi;



3.1-rasm. Axborot xavfsizligini ta'minlashning huquqiy me'yorlari

Axborot xavfsizligi bo'yicha qonunlarni O'zbekiston Respublikasi butun qonunlar tizimining ajralmas qismi sifatida tasavvur qilish mumkin, xususan:

– tarkibida axborotlashtirish masalalariga doir me'yorlar bo'lgan kons-titutsiya qonunlari;

– tarkibida axborotlashtirish masalalariga doir me'yorlar bo'lgan umumiy asosiy qonunlar (mulk, yer osti boyliklari, yer, fuqarolar huquqi, fuqorolik, soliq xususida);

– xo'jalikning alohida tuzilmalariga, iqtisodiyotga, davlat organlari tizimiga tegishli boshqarish va ularning maqomini aniqlash bo'yicha

qonunlar. Bu qonunlar axborot masalalari bo'yicha alohida me'yorlarni o'z ichiga oladi;

– munosabatlarning, xo'jalik sohalarining, jarayonlarning muayyan muhitiga butunlay tegishli maxsus qonunlar. Bularga axborotlashtirish bo'yicha qonunlar taalluqli;

– axborotlashtirish sohasidagi qonun talablarining bajarilishini reglamentlovchi me'yoriy hujjatlar;

– qonunlar bilan belgilangan axborotlashtirish sohasidagi me'yoriy hujjatlar;

– tarkibida axborotlashtirish sohasida qonun buzilishiga javobgarlik me'yorlari bo'lgan O'zbekiston Respublikasining huquqni muhofaza qilish qonunlari.

Kompyuter tarmoqlari xavfsizligini ta'minlovchi davlat huquqiy mexanizmining rivojlanmagan sharoitida korxonaning davlat va xodimlar jamoasi bilan munosabatlarni huquqiy asosda rostlovchi hujjatlari jiddiy ahamiyatga ega bo'ladi. Bunday muhim hujjatlar tarkibiga quyidagilarni kiritish mumkin:

– korxona (firma, bank) ustavi;

– jamoa shartnomasi;

– jamoa xodimlari bilan tuzilgan, tijorat siri bo'lgan ma'lumotlar himoyasini ta'minlash bo'yicha talablarga ega mehnat shartnomalari;

– ishchi va xizmatchilarning ichki mehnat tartib qoidalari;

– rahbarlar, mutaxassislar va xizmat ko'rsatuvchi xodimlarning mansab bilan bog'langan majburiyatlari.

3.2. Axborot xavfsizligining tashkiliy-ma'muriy ta'minoti

Axborotni ishonchli himoya mexanizmini yaratishda tashkiliy tadbirlar muhim rol o'ynaydi, chunki konfidensial axborotlardan ruxsatsiz foydalanish asosan, texnik jihatlar bilan emas, balki himoyaning elementar qoidalarini e'tiborga olmaydigan foydalanuvchilar va xodimlarning jinoyatkorona harakatlari, beparvoligi, sovuqqonligi va mas'uliyatsizligi bilan bog'liq.

Tashkiliy ta'minot konfidensial axborotdan foydalanishga imkon bermaydigan yoki jiddiy qiyinchilik tug'diruvchi ijrochilarning ishlab chiqarish va o'zaro munosabatlarini me'yoriy-huquqiy asosida reglamentlashdir.

Tashkiliy tadbirlarga quyidagilar kiradi:

– xizmatchi va ishlab chiqarish bino va xonalarni loyihalashda, qurishda va jihozlashda amalga oshiriladigan tadbirlar. Bu tadbirlarning asosiy maqsadi hududga va xonalarga yashirincha kirish imkonini yo'qotish; odamlarning va transportning yurishi nazoratining qulayligini ta'minlash; foydalanishning alohida tizimiga ega bo'lgan ishlab chiqarish zonalarini yaratish va h.;

– xodimlarni tanlashda amalga oshiriladigan tadbirlar. Bu tadbirlarga xodimlar bilan tanishish, konfidensial axborot bilan ishlash qoidalari bilan ishlashni o'rgatish, axborot himoyasi qoidasini buzganligi uchun javobgarlik darajasi va h. bilan tanishtirish kiradi;

– ishonchli propusk rejimini va tashrif buyuruvchilarning nazoratini tashkil qilish;

– xona va hududlarni ishonchli qo'riqlash;

– hujjatlar va konfidensial axborot eltuvchilarini saqlash va ishlatish, shu jumladan, qayd etish, berish, bajarish va qaytarish tartiblariga rioya qilish;

– axborot himoyasini tashkil etish, ya'ni muayyan ishlab chiqarish jamoalarida axborot xavfsizligiga javobgar shaxsni tayinlash, konfidensial axborot bilan ishlovchi xodimlar ishini muntazam tekshirib turish.

Bunday tadbirlar har bir muayyan tashkilot uchun o'ziga xos xususiyatga ega bo'ladi.

Tashkiliy tadbirlarning talaygina qismini xodimlar bilan ishlash egallaydi. Mulkchilikning turli shakllariga ega bo'lgan korxona xodimlari bilan ishlashda tashkiliy tadbirlar, umumiy holda quyidagilarni o'z ichiga oladi:

– ishga qabul qilishda suhbat. Suhbat natijasida nomzodning mos bo'sh joyga qabul qilinishi maqsadga muvofiqligi aniqlanadi;

– muayyan korxonada konfidensial axborot bilan ishlash qoidalari va muolajalari bilan tanishish; ishga qabul qilinuvchi korxona tijorat sirlarini saqlashi bo'yicha tilxat va firma sirlarini oshkor qilmaslikka va'da beradi;

– xodimlarni konfidensial axborot bilan ishlash qoidalari va muolajalariga o'qitish. Xodimlarni o'qitishda nafaqat ishlab chiqarish ko'nikmalariga ega bo'lish va ularni yuqori darajada saqlash, balki ularni sanoat (ishlab chiqarish) maxfiyligi axborot xavfsizligi, intellektual mulk va tijorat sirlari himoyasi talablarini bajarish zarurligiga qat'iy ishonch ruhida tarbiyalash ko'zda tutiladi. Muntazam o'qitish rahbariyat va xodimlarning korxona tijorat manfaatlarini himoya qilish masalalari bo'yicha bilimdonlik darajasini oshishiga imkon yaratadi;

– ishdan bo'shayotganlar bilan suhbat. Suhbat davomida ishdan bo'shayotgan xodimning firma sirlarini fosh qilmaslikka qat'iy va'da berishi lozimligi ta'kidlanadi va bu va'da, odatda, tilxat orqali rasmiylashtiradi.

Tadbirlarning muhim yo'nalishlaridan biri ish yuritish va hujjat yuritish tizimini puxta tashkil etish hisoblanadi. Bu esa, o'z navbatida, ish yuritish tartibini, hujjatlarni qaydlash, ishlash, saqlash, yo'qotish va mavjudligini hamda to'g'ri bajarilishini nazorat qilishni ta'minlaydi. Tizimni amalga oshirishda hujjatlar xavfsizligiga va axborot konfidensialligiga alohida e'tibor berish lozim.

Axborotni hujjatlashtirish qat'iy belgilangan qoidalar yordamida amalga oshiriladi. Bu qoidalarning asosiylari GOST 6.38-90 «Tashkiliy-boshqaruvchi hujjatlar tizimi. Hujjatlarni rasmiylashtirishga talablar», GOST 6.10.4-84 «Unifikatsiyalangan hujjatlar tizimi. Hisoblash texnika vositalari orqali yaratiluvchi mashina eltuvchilaridagi va mashinogrammalardagi hujjatlarga huquqiy kuch berish» kabilar bayon etilgan. Bu GOSTlarda axborotga hujjat huquqini beruvchi 31 ta rekvizitlar ko'zda tutilgan, ammo bu rekvizitlarning barchasining hujjatda mavjudligi shart emas. Asosiy rekvizit – matn. Shu sababli, har qanday ravon bayon etilgan matn hujjat hisoblanadi va unga huquqiy kuch berish uchun sana va imzo kabi muhim rekvizitlarning mavjudligi kifoya.

Avtomatlashtirilgan axborot tizimlaridan olingan hujjatlar uchun alohida tartib qo'llaniladi. Bunda, ma'lum hollarda, masofadan olingan axborot elektron imzo bilan tasdiqlanadi. Axborotni himoyalash uchun barcha tashkiliy tadbirlarni ta'minlovchi maxsus ma'muriy xizmatni yaratish talab qilinadi. Uning shtat tuzilmasi, soni va tarkibi firmaning real ehtiyojlari, axborotining konfidensiallik darajasi va xavfsizligining umumiy holati orqali aniqlanadi.

Ma'muriy tadbirlarga quyidagilar kiradi:

– operatsion tizimning to'g'ri konfiguratsiyasini madadlash;

– ish jurnallarining nazorati;

– parollar almashishining nazorati;

– himoya tizimida «rahna»larni aniqlash;

– axborotni himoyalovchi vositalarni testlash.

Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini madadlash masalasini, odatda, tizim ma'muri hal etadi. Ma'mur operatsion tizim (odamlar emas) rioya qilishi lozim bo'lgan ma'lum qoidalarni yaratadi. Tizimni ma'murlash – konfiguratsiya fayllarini to'g'ri tuzishdir. Bu

fayllarda (ular bir nechta bo'lishi mumkin, masalan, tizimning har bir qismiga bittadan fayl) tizim ishlashi qoidalarining tavsifi bo'ladi.

Xavfsizlik ma'muri kompyuter tarmog'i holatini tezkor tarzda (tarmoq kompyuterlari himoyalanishi holatini kuzatish orqali) va tezkor bo'lmagan tarzda (axborot himoyasi tizimidagi voqealarni qaydlovchi jurnallarni tahlillash orqali) nazoratlash lozim. Ishchi stansiyalar sonining oshishi va turli-tuman komponentlari bo'lgan dasturiy vositalarning ishlatilishi axborot himoyasi tizimidagi hodisalarni qaydlash jurnallar hajmini jiddiy oshishiga olib keladi. Jurnallardagi ma'lumotlar hajmi shunchalik oshib ketishi mumkinki, ma'mur ular tarkibini joiz vaqt mobaynida tahlillay olmaydi.

Tizim zaifligining sababi shundaki, birinchidan, foydalanuvchini autentifikatsiyalash tizimi foydalanuvchi ismiga va uning paroliga (ko'z to'ridan foydalanish kabi ekzotik holllar bundan mustasno), ikkinchidan, foydalanuvchi tizimida tizimni ma'murlash huquqi berilgan supervizorning (supervisor) mavjudligiga asoslanadi. Supervizor parolini saqlash rejimining buzilishi butun tizimdan ruxsatsiz foydalanish imkonini yaratadi.

Undan tashqari bunday qoidalarga asoslangan tizim-statik, qotib qolgan tizim. U faqat qat'iy ma'lum hujumlarga qarshi tura olishi mumkin. Oldindan ko'zda tutilmagan qandaydir yangi tahdidning paydo bo'lishida tarmoq hujumi nafaqat muvaffaqiyatli, balki tizim uchun ko'rinmaydigan bo'lishi mumkin. Shuning uchun muassasada ishlatiluvchi axborotning qaysisi himoyaga muhtoj ekanligini aniq tasavvur qilish muhim hisoblanadi. Mavjud axborotni tahlillashdan boshlash lozim. Bu muolajalar axborot himoyasini ta'minlash bo'yicha tadbirlarni differensiallash imkonini beradi va natijada, sarf-xarajatlarning qisqarishiga sabab bo'ladi.

Axborot himoyasi tizimini ekspluatatsiya qilish bosqichida xavfsizlik ma'murining faoliyati foydalanuvchilar vakolatlarini o'z vaqtida o'zgartirishdan hamda tarmoq kompyuterlaridagi himoya mexanizmlarini sozlashdan iborat bo'ladi. Foydalanuvchilar vakolatlarini va kompyuter tarmoqlarida axborotni himoyalash tizimini sozlashni boshqarish muammosi, masalan, tarmoqdan markazlashtirilgan foydalanish tizimidan foydalanish asosida hal etilishi mumkin. Bunday tizimni amalga oshirishda tarmoq asosiy serverida ishlovchi maxsus foydalanishni boshqaruvchi serverdan foydalaniladi. Bu server markaziy himoya ma'lumotlari bazasini lokal himoya ma'lumotlari bazasi bilan avtomatik tarzda sinxronlaydi. Foydalanishni boshqarishning bu tizimida

foydalanuvchi vakolati vaqti-vaqti bilan o'zgartiriladi va markaziy himoya ma'lumotlari bazasiga kiritiladi, ularning muayyan kompyuterlarda o'zgarishi navbatdagi sinxronlash seansi vaqtida amalga oshiriladi.

Undan tashqari, foydalanuvchi parolini ishchi stansiyalarining birida o'zgartirsa, uning yangi paroli markaziy himoya ma'lumotlari bazasida avtomatik tarzda akslanadi hamda bu foydalanuvchi ishlashiga ruxsat berilgan ishchi stansiyalarga uzatiladi.

3.3. Axborot xavfsizligi bo'yicha standartlar va spetsifikatsiyalar

Axborot xavfsizligi sohasida mutaxassislar o'z faoliyatlarida mos standartlar va spetsifikatsiyalarni chetlab o'taolmaydilar. Bunga sabab, birinchidan standartlar va spetsifikatsiyalar – avvalo axborot xavfsizligining muolajaviy va dasturiy-texnik darajalari bo'yicha bilimlarini to'plash shakllaridan biri. Ularda malakali mutaxassislar tomonidan ishlab chiqilgan, tasdiqlangan yuqori sifatli yechimlar va metodologiyalar qayd etilgan. Ikkinchidan, standartlar va spetsifikatsiyalar apparat-dasturiy tizimlar va ularning komponentlarining o'zaro qo'shila olishligini ta'minlovchi asosiy vosita hisoblanadi. (Internet–uyushmada bu vosita haqiqatan samarali ishlamoqda).

Standartlar va spetsifikatsiyalarning bir-biridan jiddiy farqlanuvchi ikkita guruhini ajratish mumkin:

- axborot tizimlarini va xavfsizlik talablari bo'yicha himoya vositalarini baholash va turkumlash uchun atalgan baholash standartlari;
- himoya vositalari va usullarini amalga oshirish va ulardan foydalanishning turli jihatlarini reglamentlovchi spetsifikatsiyalar.

Bu guruhlar ma'lumki, ixtilofga bormaydilar, balki bir-birini to'ldiradilar. Baholash standartlari tashkiliy va arxitekturaviy spetsifikatsiyalar vazifasini o'tagan holda axborot tizimlarining xavfsizligi nuqtai nazaridan muhim bo'lgan tushunchalari va jihatlarini tavsiflaydi. Spetsifikatsiyalar esa arxitektura belgilagan axborot tizimini qanday qurish lozimligini va tashkiliy talablarni qanday qondirilishini aniqlaydi.

Xalqaro e'tirofni qozongan va axborot xavfsizligi sohasida keyingi ishlanmalarda juda kuchli ta'sir ko'rsatgan birinchi baholash standarti AQSH mudofaa vazirligining «*To'q sariq kitob*» (muqovaning rangi bo'yicha) deb ataluvchi «Ishonchli kompyuter tizimlarini baholash mezonlari» (Department of Defeuse Trusted Computer System Evaliation Criteria, TCSEC) standarti bo'ldi. Mubolag'asiz tasdiqlash mumkinki, «To'q sariq kitob»i axborot xavfsizligining tushunchalar negizini

ifodalaydi. Undagi tushunchalarning sanab o'tishning o'zi yetarli: *xavfsiz va ishonchli tizimlar, xavfsizlik siyosati, kafolatlik darajasi, hisobkitobliligi, ishonchli hisoblash asosi, murojaatlar monitori, xavfsizlikning yadrosi va perimetri.*

«To'q sariq kitob»dan so'ng chiqarilgan hujjatlardan biri *«To'q sariq kitob»ning tarmoq konfiguratsiyalari uchun izohi»* (Trusted Network Interpretation) eng muhim hujjat hisoblanadi. Bu hujjat ikki qismdan iborat. Birinchi qism izohning o'ziga bag'ishlangan bo'lsa, ikkinchi qismida o'ziga xos yoki tarmoq konfiguratsiyalari uchun ayniqsa, muhim bo'lgan *xavfsizlik servislari* tavsiflanadi. Birinchi qismga kiritilgan eng muhim tushunchalardan biri – tarmoqdagi ishonchli hisoblash asosi. Muhim jihat–tarmoq konfiguratsiyalarining dinamikligi. Himoyalash mexanizmlari orasida *konfidensiallik* va *yaxlitlikni* ta'minlovchi *kriptografiya* ajratilgan. Foydalanuvchanlik masalalari, uni ta'minlashdagi arxitekturaviy prinsiplarning shakllantirilishi o'z vaqti uchun tartibli yondashishi bo'ldi.

Taqsimlangan axborot tizimlarini obyektga mo'ljallangan tarzda kommunikatsiyalarni kriptografik himoyalash bilan birgalikda dekompozitsiyalashning nazariy asosini – murojaatlar monitorini fragmentlashning korrektligi shartining yetarliligini aytib o'tish lozim.

Baholash standartlaridan yana biri *«Yevropa mamlakatlarining uyg'unlashtirilgan mezonlari»*da axborot tizimi ishlashi lozim bo'lgan sharoitlarga aprior shartlar yo'q. Faraz qilinadiki, avval baholash maqsadi ifodalanadi, so'ngra sertifikatsiyalash organi bu maqsadga qanchalik to'liq erishilishini, ya'ni muayyan vaziyatda xavfsizlikning arxitekturasi va amalga oshirilishi mexanizmlarining qanchalik korrektligini va samaraliligini aniqlaydi. Baholash maqsadini ifodalashni yengillashtirish niyatida standartda hukumat va tijorat tizimlariga xos funksionallikning o'nta taxminiy sinflari tavsiflangan.

Ushbu standartda axborot texnologiyalar tizimlari va mahsulotlari o'rtasidagi farq ta'kidlanadi, ammo talablarini unifikatsiyalash niyatida yagona - *baholash obyekti* tushunchasi kiritiladi. Standartda xavfsizlik funksiyalari (servislari) va ularni amalga oshiruvchi mexanizmlar orasida farqning ko'rsatilishi hamda kafolatlanishning ikki jihati – xavfsizlik vositalarining *samaradorligi* va *korrektligining* ajratilishi muhim hisoblanadi. Baholash standartlari guruhiga axborot xavfsizligining muayyan, ammo muhim va murakkab jihatini reglamentlovchi AQSHning *«Kriptografik modullar uchun xavfsizlik talablari»* Federal stan-

darti hamda *«Axborot texnologiyalar xavfsizligini baholovchi mezonlar»* xalqaro standarti taalluqli.

Texnik spetsifikatsiyalar orasida birinchi o'ringa, so'zsiz, X800 «Ochiq tizimlar o'zaro harakati uchun xavfsizlik arxitekturasi» hujjatini qo'yish lozim. Bu hujjatda xavfsizlikning eng muhim tarmoq servislari ajratilgan: *autentifikatsiya, foydalanishni boshqarish,* ma'lumotlarni konfidensialligi va yoki yaxlitligini ta'minlash hamda qilingan harakatdan *tonishning mumkin emasligi.* Servislarni amalga oshirish uchun xavfsizlikning quyidagi tarmoq mexanizmlari va ularning kombinatsiyalari ko'zda tutilgan: *shifrlash, elektron raqamli imzo,* foydalanishni boshqarish, ma'lumotlar yaxlitligining nazorati, autentifikatsiya, *trafikni to'ldirish, marshrutlashni boshqarish, notarizatsiya.* Xavfsizlikning servislari va mexanizmlari amalga oshiriluvchi yetti sathli etalon modelining sathlari tanlangan. Nihoyat, taqsimlangan konfiguratsiyalar uchun xavfsizlik vositalarining ma'murlash masalalari batafsil ko'rib chiqilgan.

Internet – uyushmaning RFS 1510 «Autentifikatsiyaning tarmoq serveri Kerberos (VS)» spetsifikatsiyasi xususiy, ammo muhim va dolzarb muammoga – turli taqsimlangan muhitda tarmoqqa yagona kirish konsepsiyasini madadlagan holda autentifikatsiyalashga tegishli.

Kerberos autentifikatsiyalash serveri ishonchli uchinchi taraf bo'lib, xizmat ko'rsatiluvchi subyektlarning mahfiy kalitlariga ega va ularga haqiqiylikning juftlashib tekshirishda yordam beradi. Kerberosning mijoz komponentlarining aksariyat zamonaviy operatsion tizimlarda mavjudligi uning qanchalik muhim ekanligidan dalolat beradi.

IPsec texnik spetsifikatsiyasi tarmoq sathida konfidensiallik va yaxlitlik vositalarining to'liq to'plamini tavsiflangan holda, mubolag'asiz fundamental ahamiyatga ega. IPsec asosida yuqoriroq sath (tatbiqiy sathga qadar) protokollarini himoyalash mexanizmi hamda xavfsizlikning tugallangan vositalari, xususan virtual xususiy tarmoqlar quriladi. Albatta, IPsec kriptografik mexanizmlariga va kalit infratuzilmalariga tayanadi.

Transport sathi xavfsizligi va signallari (Transport Layer Security, TLS) ham shunday xarakterlanadi. TLS spetsifikatsiyasi turli vazifalarni bajaruvchi ko'pgina dasturiy mahsulotlarda ishlatiluvchi ommaviy Secure Socket Layer (SSL) protokolini rivojlantiradi va oydinlashtiradi.

Yuqorida eslatib o'tilgan infratuzilma nuqtai nazaridan X.500 *«Direktoriya xizmati*: Konsepsiyalar, modellar va serverlar obzori» (The Directory: Overview of consepts, models and services) va X.509

«*Direktoriya xizmati: sertifikatlar, ochiq kalitlar va atributlar karkaslari*» (The Directory: Pubbic-key and attribute sertificate framworks) tavsiyalari juda muhim hisoblanadi. X.509 tavsiyalarida ochiq kalitlar va atributlar, ya'ni ochiq kalitlar infratuzilmasi va imtiyozlarni boshqarishning bazaviy elementlari sertifikatlarining formati tavsiflangan.

Ma'lumki, axborot xavfsizligini ta'minlash kompleks muammo bo'lib, qonuniy, ma'muriy, muolajaviy va dasturiy-texnik sathlarda choralarni kelishilgan holda ko'rishni talab etadi.

Ma'muriy sathning bazaviy hujjati tashkilot *xavfsizligi siyosatini* ishlab chiqishda va amalga oshirishda Internet - uyushmaning «Tashkilot axborot xavfsizligi bo'yicha qo'llanma»si (Site Security Handbook) na'munali ko'makchi vazifasini o'tashi mumkin. Unda xavfsizlik siyosati muolajalarini shakllantirilishining amaliy jihatlari yoritiladi, ma'muriy va muolajaviy sathlarning asosiy tushunchalari izohlanadi, tavsiya etuvchi harakatlarning sabablari ko'rsatilgan, xavf-xatarlar tahlili, axborot xavfsizligining buzilishiga munosabat va buzilish bartaraf etilganidan keyingi harakat mavzulariga to'xtab o'tilgan.

«Axborot himoyasi buzilishiga qanday munosabat bildirish lozim» (Expections for Computer Security Incident Response) tavsiyasida yuqorida keltirilgan masalalardan tashqari foydali axborot resurslariga havolalarni hamda muolajaviy darajadagi amaliy maslahatlarni topish mumkin.

Korporativ axborot tizimini rivojlantirishda va qayta tuzishda «*Internet-xizmat bilan ta'minlovchini* qanday tanlash lozim» (Site Security Handbook Addendum for ISPs) tavsiyasi so'zsiz foydalidir. Birinchi galda uning qoidalariga tashkiliy va arxitekturaviy himoyalashni shakllantirish jarayonida rioya qilish lozim.

Britaniya standarti BS 7799 «Axborot xavfsizligini boshqarish. Amaliy qoidalar» (Code of practice for information security managment) axborot xavfsizligiga javobgar tashkilot rahbarlari uchun foydali hisoblanadi. Bu standart jiddiy o'zgartirishsiz ISO/IES 17799 xalqaro standartga ko'chirilgan.

Bu borada mustaqil diyorimiz O'zbekiston Respublikasida ahamiyatga molik bo'lgan ulkan ishlar olib borilmoqda. Bunga misol tariqasida O'zbekiston aloqa va axborotlashtirish agentligining ilmiy-texnik va marketing tadqiqotlari markazi tomonidan ishlab chiqilgan O'z DSt 1092:2005 «Axborot texnologiyasi. Ma'lumotlarni kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish

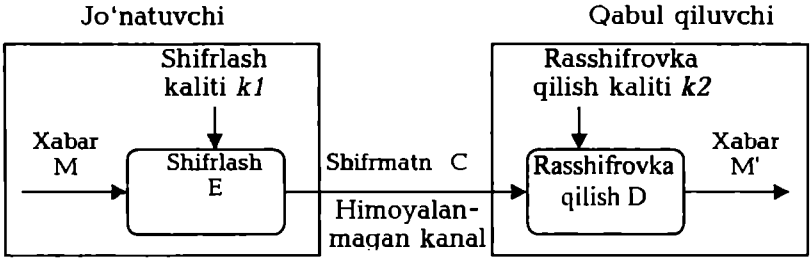
jarayonlari», O‘z DSt 1105:2006 «Axborot texnologiyasi. Ma’lumotlarni kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi», O‘z DSt 1106:2006 «Axborot texnologiyasi. Ma’lumotlarni kriptografik muhofazasi. Xeshlash funksiyasi» va O‘z DSt 1108:2006 «Axborot texnologiyasi. Ochiq tizimlar o‘zaro bog‘liqligi. Elektron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzilmasi» standartlarini va RH 45-187:2006 «Xavfsizlik talablari» boshqaruv hujjatini ko‘rsatib o‘tish mumkin. Ushbu markaz tomonidan ishlab chiqilgan standartlar №05-11 12.04.2006-yilda O‘zbekiston standartlashtirish, metrologiya va sertifikatsiyalash agentligi tomonidan tasdiqlangan.

Bundan tashqari, yurtimizda axborot xavfsizligi sohasida faoliyat yuritayotgan O‘zbekiston aloqa va axborotlashtirish agentligi qoshidagi «UZINFOCOM», «UZ-CERT» va boshqa tashkilotlarni aytib o‘tish lozim.

IV bob. AXBOROTNI HIMOYALASHNING KRIPTOGRAFIK USULLARI

4.1. Kriptografiyaning asosiy qoidalari va ta'riflari

Axborotning himoyalashning aksariyat mexanizmlari asosini shifrlash tashkil etadi. *Axborotni shifrlash* deganda ochiq axborotni (dastlabki matnni) shifrlangan axborotga o'zgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi. Shifrlash kriptotizimining umumlashtirilgan sxemasi 4.1-rasmda keltirilgan.



4.1-rasm. Shifrlash kriptotizimining umumlashtirilgan sxemasi.

Uzatiluvchi axborot matni M kriptografik o'zgartirish E_{k1} yordamida shifrlanadi, natijada shifrmatn C olinadi:

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

bu yerda, $k1$ – shifrlash kaliti deb ataluvchi E funksiyaning parametri.

Shifrlash kaliti yordamida shifrlash natijalarini o'zgartirish mumkin. Shifrlash kaliti muayyan foydalanuvchiga yoki foydalanuvchilar guruhiga tegishli va ular uchun yagona bo'lishi mumkin. Muayyan kalit yordamida shifrlangan axborot faqat ushbu kalit egasi (yoki egalari) tomonidan rasshifrovka qilinishi mumkin.

Axborotni teskari o'zgartirish quyidagi ko'rinishga ega:

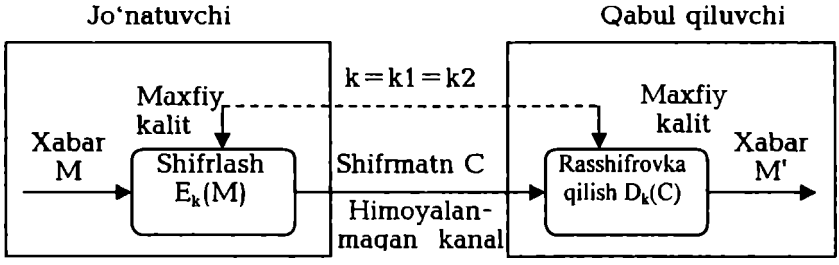
$M' = D_{k2}(C)$

D funksiyasi E funksiyaga nisbatan teskari funksiya bo'lib, shifr matnni rasshifrovka qiladi. Bu funksiya ham $k2$ kalit ko'rinishidagi qo'shimcha parametrga ega. $k1$ va $k2$ kalitlar bir ma'noli moslikka ega bo'lishlari shart. Bu holda rasshifrovka qilingan M' axborot M ga ekvivalent bo'ladi. $k2$ kaliti ishonchli bo'lmasa D funksiya yordamida $M' = M$ dastlabki matnni olib bo'lmaydi.

Kriptotizimlarning ikkita sinfi farqlanadi:

- simmetrik kriptotizim (bir kalitli);
- asimmetrik kriptotizim (ikkita kalitli).

Shifrlashning simmetrik kriptotizimida shifrlash va rasshifrovka qilish uchun bitta kalitning o'zi ishlatiladi. Demak, shifrlash kalitidan foydalanish huquqiga ega bo'lgan har qanday odam axborotni rasshifrovka qilishi mumkin. Shu sababli, simmetrik kriptotizimlar maxfiy kalitli kriptotizimlar deb yuritiladi. Ya'ni shifrlash kalitidan faqat axborot atalgan odamgina foydalana olishi mumkin. Shifrlashning simmetrik kriptotizimi sxemasi 4.2-rasmda keltirilgan.



4.2-rasm. Simmetrik shifrlash kriptotizimining sxemasi.

Elektron hujjatlarni uzatishning konfidensialligini simmetrik kriptotizim yordamida ta'minlash masalasi shifrlash kaliti konfidensialligini ta'minlashga keltiriladi. Odatda, shifrlash kaliti ma'lumotlar fayli va massividan iborat bo'ladi va shaxsiy kalit eltuvchisida, masalan, disketda yoki smartkartada saqlanadi. Shaxsiy kalit eltuvchisi egasidan boshqa odamlar-ning foydalanishiga qarshi choralar ko'rilishi shart.

Simmetrik shifrlash axborotni «o'zi uchun», masalan, egasi yo'qligida undan ruxsatsiz foydalanishni oldini olish maqsadida,

shifrlashda juda qulay hisoblanadi. Bu tanlangan fayllarni arxivli shifrlash va butun bir mantiqiy yoki fizik disklarni shaffof(avtomatik) shifrlash bo'lishi mumkin.

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

Simmetrik shifrlash algoritmining ma'lumotlarni abonentli shifrlashda, ya'ni shifrlangan axborotni abonentga, masalan, Internet orqali, uzatishda amalga oshirilgan variantlari mavjud. Bunday kriptografik tarmoqning barcha abonentlari uchun bitta kalitning ishlatilishi xavfsizlik nuqtai nazaridan nojoizdir. Haqiqatan, kalit obro'sizlantirilganda (yo'qotilganida, o'g'irla-tilganda) barcha abonentlarning hujjat almashishi xavf ostida qoladi. Bu holda kalitlarning matritsasi (4.3-rasm) ishlatilishi mumkin.

	1	2	3	...	n	
1	k_{11}	k_{12}	k_{13}	...	k_{1n}	1-abonent uchun kalitlar to'plami
2	k_{21}	k_{22}	k_{23}	...	k_{2n}	2-abonent uchun kalitlar to'plami
3	k_{31}	k_{32}	k_{33}	...	k_{3n}	3-abonent uchun kalitlar to'plami
...	...	...	...	...	...	...
n	k_{n1}	k_{n2}	k_{n3}	...	k_{nn}	n-abonent uchun kalitlar to'plami

4.3-rasm. Kalitlar matritsasi.

Kalitlar matritsasi abonentlarning juft-juft bog'lanishli jadvalidan iborat. Jadvalning har bir elementi i va j abonentlarni bog'lashga mo'ljallangan va undan faqat ushbu abonentlar foydalana oladilar. Mos holda, kalitlar matritsasi elementlari uchun quyidagi tenglik o'rinli.

$$K_{ij} = K_{ji}.$$

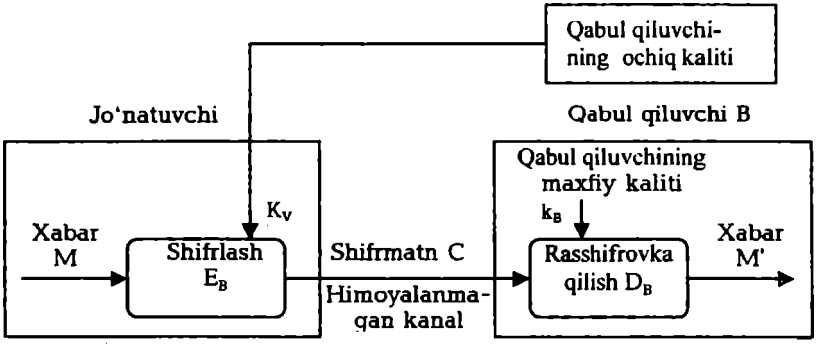
Matritsaning har bir *i*- qatori muayyan *i* abonentning qolgan *N*-1 abonentlar bilan bog'lanishini ta'minlovchi kalitlar to'plamidan iborat. Kalitlar to'plami (tarmoq to'plamlari) kriptografik tarmoqning barcha abonentlari o'rtasida taqsimlanadi. Taqsimlash aloqaning *himoyalangan kanallari* orqali yoki qo'ldan-qo'lga tarzda amalga oshiriladi.

Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilishda turli kalitlardan foydalaniladi:

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

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

Asimmetrik shifrlashning umumlashtirilgan sxemasi 4.4-rasmda keltirilgan.



4.4-rasm. Asimmetrik shifrlashning umumlashtirilgan sxemasi.

Asimmetrik kriptotizimda shifrlangan axborotni uzatish quyidagicha amalga oshiriladi:

1. Tayyorgarlik bosqichi:

– abonent V juft kalitni generatsiyalaydi: maxfiy kalit k_V va ochiq kalit K_V;

– ochiq kalit K_V abonent A ga va qolgan abonentlarga jo'natiladi.

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

– abonent A abonent Vning ochiq kaliti K_V yordamida axborotni shifrlaydi va shifrmatnni abonent Vga jo'natadi;

– abonent V o'zining maxfiy kaliti k_V yordamida axborotni rasshifrovka qiladi. Hech kim (shu jumladan, abonent A ham) ushbu axborotni rasshifrovka qilaolmaydi, chunki abonent Vning maxfiy kaliti unda yo'q.

Asimmetrik kriptotizimda axborotni himoyalash axborot qabul qiluvchi kaliti $k_V$ning maxfiyligiga asoslangan.

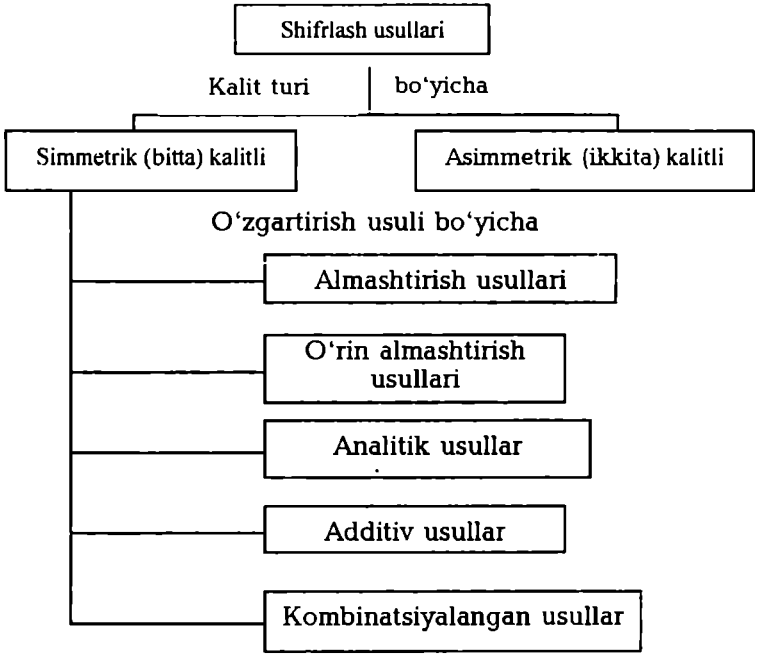
Asimmetrik kriptotizimlarning asosiy xususiyatlari quyidagilar:

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

2. Shifrlash $E_V: M \rightarrow C$ va rasshifrovka qilish $D_B: S \rightarrow M$ algoritmlari ochiq.

4.2. Simmetrik shifrlash tizimi

Shifrlash usullari turli alomatlari bo'yicha turkumlanishi mumkin. Turkumlanish variantlaridan biri 4.5- rasmda keltirilgan.



4.5-rasm. Shifrlash usullarining turkumlanishi.

Almashtirish usullari. Almashtirish (podstanovka) usullarining mohiyati bir alfavitda yozilgan axborot simvollarini boshqa alfavit simvollari bilan ma'lum qoida bo'yicha almashtirishdan iboratdir. Eng sodda usul sifatida ***to'g'ridan-to'g'ri almashtirishni*** ko'rsatish mumkin. Dastlabki axborot yoziluvchi A_0 alfavitning s_{0i} simvollariga shifrlovchi A_1 alfavitning s_{1i} simvollari mos quyiladi. Oddiy holda ikkala alfavit ham bir xil simvollar to'plamiga ega bo'lishi mumkin.

Ikkala alfavitdagi simvollar o'rtasidagi moslik ma'lum algoritm bo'yicha K simvollar uzunligiga ega bo'lgan dastlabki matn T_0 simvollari-ning raqamli ekvivalentlarini o'zgartirish orqali amalga oshiriladi.

Monoalfavitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko'rinishda ifodalanishi mumkin

1-qadam. [1xR] o'lchamli dastlabki A_0 alfavitdagi har bir simvol $s_0 \in T(i=\overline{1,K})$ ni A_0 alfavitdagi s_{0i} simvol tartib raqamiga mos keluvchi $h_{0i}(s_{0i})$ conga almashtirish yo'li bilan raqamlar ketma-ketligi L_{0h} ni shakllantirish.

2-qadam. L_{0h} ketma-ketligining har bir sonini $h_{1i}=(k_1 x h_{0i}(s_{0i})+k_2)(\mathrm{mod}R)$ formula orqali hisoblanuvchi L_{1h} ketma-ketlikning mos soni h_{1i} ga almashtirish yo'li bilan L_{1h} son ketma-ketligini shakllantirish, bu yerda k_1 –o'nlik koeffitsiyent; k_2–siljitish koeffitsiyenti. Tanlangan k_1, k_2 koeffitsiyentlar h_{0i}, h_{1i} sonlarning bir ma'noli mosligini ta'minlashi lozim, $h_{1i}=0$ olinganida esa $h_{1i}=R$ almashinuvi bajarilishi kerak.

3-qadam. L_{1h} ketma-ketlikning har bir soni $h_{1i}(s_{1i})$ni [1xR] o'lchamli shifrlash alfavitning mos $s_{1i} \in T_1(i=\overline{1,K})$ simvoli bilan almashtirish yo'li bilan T_1 shifrmatnni hosil qilish.

4-qadam. Olingan shifrmatn o'zgarmas b uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to'liq bo'lmasa, blok orqasiga maxsus simvol-to'ldiruvchilar joylashtiriladi(masalan, *).

Misol. Shifrlash uchun dastlabki ma'lumotlar quyidagilar:

T_0=<HIMOYA_XIZMATI>

A_0=<ABDEFGHIJKLMNOPRQSTUVXYZO'G'ShChNg_>

A_1=<ORYNTE_JMChXAVDFQKSZPIO'GHLShBUG'Ng>

R=30; k_1=3; k_2=15; b=4

Algoritmning qadamba-qadam bajarilishi quyidagi natijalarni olinishiga olib keladi.

1-qadam. L_{oh}=<7,8,12,14,23,1,30,22,8,24,12,1,19,8>

2-qadam. L_{1h}=<6,9,21,27,24,18,15,21,9,27,21,18,12,9>
3-qadam. T_1=<EMIBHSFIMBISAM>
4-qadam. T_1=< EMIB HSFI MBIS AM**>

Rasshifrovka qilishda bloklar birlashtirilib K simvolli shifrmatn T_1 hosil qilinadi. Rasshifrovka qilish uchun quyidagi butun sonli tenglamani yechish lozim:

$$k_1h_{01}+k_2=nR+h_{1i}$$

k_1, k_2, h_{11} va R butun sonlar ma'lum bo'lganda h_{0i} kattaligi n ni saralash orqali hisoblanadi. Bu muolajani shifrmatnning barcha simvollariga tatbiq qilish uning rasshifrovka qilinishiga olib keladi.

Almashtirish usulining kamchiligi sifatida dastlabki va berilgan matnlar statistik xarakteristkalarining bir xilligidir. Dastlabki matn qaysi tilda yozilganligini bilgan kriptoanalitik ushlab qolingan axborotlarni statistik ishlab, ikkala alfavitdagi simvollar o'rtasidagi muvofiqlikni aniqlashi mumkin.

Polialfavitli almashtirish usullari aytarlicha yuqori kriptobardoshlikka ega. Bu usullar dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan. Rasman polialfavitli almashtirishni quyidagicha tasavvur etish mumkin. N-alfavitli almashtirishda dastlabki A_0 alfavitdagi s_{01} simvoli A_1 alfavitdagi s_{11} simvoli bilan almashtiriladi va h. s_{0N} ni s_{NN} simvol bilan almashtirilganidan so'ng $S_{0(N+1)}$ simvolning o'rnini A_1 alfavitdagi $S_{1(N+1)}$ simvol oladi va h.

Polialfavitli almashtirish algoritmlari ichida ***Vijiner jadvali (matritsasi)*** T_B ni ishlatuvchi algoritm eng keng tarqalgan. Vijiner jadvali [RxR] o'lchamli kvadrat matritsadan iborat bo'lib, (R-ishlatilayotgan alfavitdagi simvollar soni) birinchi qatorida simvollar alfavit tartibida joylashtiriladi. Ikkinchi qatordan boshlab simvollar chapga bitta o'ringa siljitilgan holda yoziladi. Siqib chiqarilgan simvollar o'ng tarafdagi bo'shagan o'rinni to'ldiradi (siklik siljitish). Agar o'zbek alfaviti ishlatilsa, Vijiner matritsasi [36x36] o'lchamga ega bo'ladi (4.6-rasm).

ABDEFGHIJKLMNOPRQSTUVXYZO'G'ShChNg

BDEF..... ....ShChNg_A
DEFG..... .... ChNg_AB
....
_ABD..... ....G'ShChNg

4.6-rasm. Vijiner matritsasi.

Shifrlash takrorlanmaydigan M simvoldan iborat kalit yordamida amalga oshiriladi. Vijinerning to'liq matritsasidan $[(M+1),R]$ o'lchamli shifrlash matritsasi $T_{(SH)}$ ajratiladi. Bu matritsa birinchi qatordan va birinchi elementlari kalit simvollariga mos keluvchi qatorlardan iborat bo'ladi.

Agar kalit sifatida <G'O'ZA> so'zi tanlangan bo'lsa, shifrlash matritsasi beshta qatordan iborat bo'ladi (4.7-rasm).

$$T_{Sh}=\begin{vmatrix} \text{ABDEFGHIJKLMNOPRQSTUVXYZO'G'ShChNg\_} \\ \text{G'ShChNg\_ABDEFGHIJKLMNOPRQSTUVXYZO'} \\ \text{O'G'ShChNg\_ABDEFGHIJKLMNOPRQSTUVXYZ} \\ \text{ZO'G'ShChNg\_ ABDEFGHIJKLMNOPRQSTUVXY} \\ \text{ABDEFGHIJKLMNOPRQSTUVXYZO'G'ShChNg\_} \end{vmatrix}$$

4.7-rasm. «G'o'za» kaliti uchun shifrlash matritsasi.

Vijiner jadvali yordamida shifrlash algoritmi quyidagi qadamlar ketma-ketligidan iborat:

1-qadam. Uzunligi M simvolli kalit K ni tanlash.

2-qadam. Tanlangan kalit K uchun $[(M+1),R]$ o'lchamli shifrlash mat-ritsasi $T_{sh}=(b_{ij})$ ni qurish.

3- qadam. Dastlabki matnning har bir simvoli s_{0r} tagiga kalit simvoli k_m joylashtiriladi. Kalit keraklicha takrorlanadi.

4-qadam. Dastlabki matn simvollari shifrlash matritsasi T_{sh} dan quyidagi qoida bo'yicha tanlangan simvollar bilan ketma-ket almashtiriladi.

1) K kalitning almashtiriluvchi s_{0r} simvolga mos k_m simvoli aniqlanadi;

2) shifrlash matritsasi T_{sh} dagi $k_m = b_{j1}$ shart bajariluvchi i qator topiladi;

3) $s_{or} = b_{i1}$ shart bajariluvchi j ustun aniqlanadi;

4) s_{or} simvoli b_{ij} simvoli bilan almashtiriladi.

5-qadam. Shifrlangan ketma-ketlik ma'lum uzunlikdagi (masalan, 4 simvolli) bloklarga ajratiladi. Oxirgi blokning bo'sh joylari maxsus simvol-to'ldiruvchilar bilan to'ldiriladi.

Rasshifrovka qilish quyidagi ketma-ketlikda amalga oshiriladi:

1-qadam. Shifrlash algoritmining 3-qadamidagidek shifrmatn tagiga kalit simvollari ketma-ketligi yoziladi.

2-qadam. Shifrmatndan s_{1r} simvollari va mos kalit simvollari k_m ketma-ket tanlanadi. T_{sh} matritsada $k_m = b_{ij}$ shartni qanoatlantiruvchi i qator aniqlanadi. i-qatorda $b_{ij}=s_{1r}$ element aniqlanadi. Rasshifrovka qilingan ma-tnda r - o'rniga b_{ij} simvoli joylashtiriladi.

3-qadam. Rasshifrovka qilingan matn ajratilmasdan yoziladi. Xizmatchi simvollar olib tashlanadi.

Misol. K=<G'O'ZA> kaliti yordamida T=<PAXTA G'ARAMI> dastlabki matnni shifrlash va rasshifrovka qilish talab etilsin. Shifrlash va rasshifrovka qilish mexanizmi 4.8-rasmda keltirilgan.

Polialfavitli almashtirish usullarining kriptobardoshligi oddiy almashtirish usullariga qaraganda aytarlicha yuqori, chunki ularda dastlabki ketma-ketlikning bir xil simvollari turli simvollar bilan almashtirilishi mumkin. Ammo shifrning statistik usullariga bardoshliligi kalit uzunligiga bog'liq.

Dastlabki matn	PAXTA_G'ARAMI
Kalit	G'O'ZA G'O'ZA G'O'Z A
Almashtirilgan so'nggi matn	KO'NTG'ZTALO'FI
Shifrmatn	KO'NTG'ZTALO'FI
Kalit	G'O'ZA G'O'ZA G'O'ZA
Rasshifrovka qilingan matn	PAXT A G'A RAMI
Dastlabki matn	PAXTA G'ARAMI

4.8-rasm. Vijiner matritsasi yordamida shifrlash misoli.

O'rin almashtirish usullari. O'rin almashtirish usullariga binoan dastlabki matn belgilangan uzunlikdagi bloklarga ajratilib har bir blok ichidagi simvollar o'rni ma'lum algoritm bo'yicha almashtiriladi.

Eng oson o'rin almashtirishga misol tariqasida dastlabki axborot blokini matritsaga qator bo'yicha yozishni, o'qishni esa ustun bo'yicha amalga oshirishni ko'rsatish mumkin. Matritsa qatorlarini to'ldirish va shifrlangan axborotni ustun bo'yicha o'qish ketma-ketligi kalit yordamida berilishi mumkin. Usulning kriptobardoshligi blok uzunligiga (matritsa o'lchamiga) bog'liq. Masalan, uzunligi 64 simvolga teng bo'lgan blok (matritsa o'lchami 8x8) uchun kalitning $1,6 \cdot 10^9$ kombi-

natsiyasi bo'lishi mumkin. Uzunligi 256 simvolga teng bo'lgan blok (matritsa o'lchami 16x16) kalitning mumkin bo'lgan kombinatsiyasi $1{,}4 \cdot 10^{26}$ ga yetishi mumkin. Bu holda kalitni saralash masalasi zamonaviy EHMlar uchun ham murakkab hisoblanadi.

Gamilton marshrutlariga asoslangan usulda ham o'rin almashtirishlardan foydalaniladi. Ushbu usul quyidagi qadamlarni bajarish orqali amalga oshiriladi.

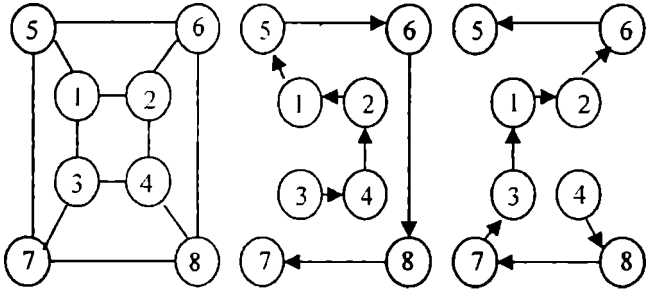
1-qadam. Dastlabki axborot bloklarga ajratiladi. Agar shifrlanuvchi axborot uzunligi blok uzunligiga karrali bo'lmasa, oxirgi blokdagi bo'sh o'rinlarga maxsus xizmatchi simvollar-to'ldiruvchilar joylashtiriladi (masalan, *).

2-qadam. Blok simvollari yordamida jadval to'ldiriladi va bu jadvalda simvolning tartib raqami uchun ma'lum joy ajratiladi (4.9-rasm).

3-qadam. Jadvaldagi simvollarni o'qish marshrutlarning biri bo'yicha amalga oshiriladi. Marshrutlar sonining oshishi shifr kriptobardoshligini oshiradi. Marshrutlar ketma-ket tanlanadi yoki ularning navbatlanishi kalit yordamida beriladi.

4-qadam. Simvollarning shifrlangan ketma-ketligi belgilangan L uzunlikdagi bloklarga ajratiladi. L kattalik 1-qadamda dastlabki axborot bo'linadigan bloklar uzunligidan farqlanishi mumkin.

Rasshifrovka qilish teskari tartibda amalga oshiriladi. Kalitga mos holda marshrut tanlanadi va bu marshrutga binoan jadval to'ldiriladi.



4.9-rasm. 8-elementli jadval va Gamilton marshrutlari variantlari.

Jadvaldan simvollar element nomerlari kelishi tartibida o'qiladi.

Misol. Dastlabki matn T_0 «O'RIN ALMASHTIRISH USULI»ni shifrlash talab etilsin. Kalit va shifrlangan bloklar uzunligi mos holda quyidagilarga teng: K=<2,1,1>, L=4. Shifrlash uchun 4.9-rasmda

keltirilgan jadval va ikkita marshrutdan foydalaniladi. Berilgan shartlar uchun matritsalari to'ldirilgan marshrutlar 4.10-rasmda keltirilgan ko'rinishga ega.

1-qadam. Dastlabki matn uchta blokka ajratiladi. *B1*=<O'RIN_ALM>, *B2*=<ASHTIRISH->, *B3*=<USULI**>;

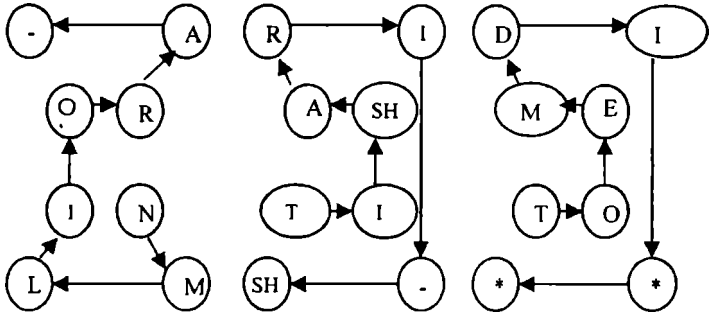
2-qadam. 2,1,1 marshrutli uchta matritsa to'ldiriladi;

3-qadam. Marshrutlarga binoan simvollarni joy-joyiga qo'yish orqali shifrmatnni hosil qilish.

T_1=<NMLIO'RA_TISHARI_SHTOEMDI**>

4-qadam. Shifrmatnni bloklarga ajratish.

T_1=<NMLI O'RA_ TISHA RI_SH TOEM DI**>



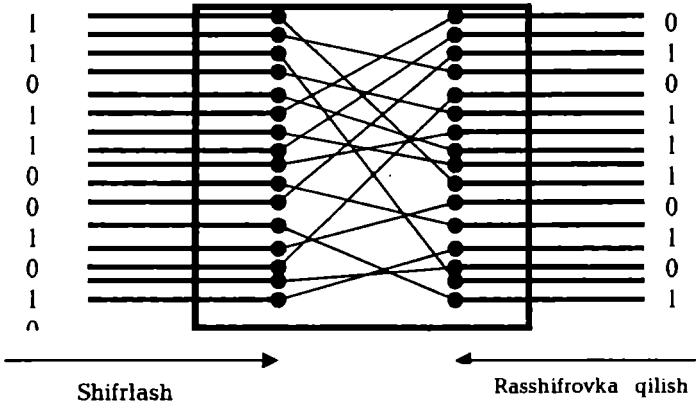
4.10-rasm. Gamilton marshruti yordamida shifrlash misoli.

Amaliyotda o'rin almashtirish usulini amalga oshiruvchi maxsus apparat vositalar katta ahamiyatga ega (4.11-rasm).

Dastlabki axborot blokining parallel ikkili kodi (masalan, ikki bayt) sxemaga beriladi. Ichki kommutatsiya hisobiga sxemada bitlarning bloklardagi o'rinlari almashtiriladi. Rasshifrovka qilish uchun esa shemaning kirish va chiqish yo'llari o'zaro almashtiriladi.

O'rin almashtirish usullarining amalga oshirilishi sodda bo'lsa-da, ular ikkita jiddiy kamchiliklarga ega. Birinchidan, bu usullarni statistik ishlash orqali fosh qilish mumkin. Ikkinchidan, agar dastlabki matn uzunligi K simvollardan tashkil topgan bloklarga ajratilsa, shifrni fosh

etish uchun shifrlash tizimiga bittasidan boshqa barcha simvollari bir xil bo'lgan test axborotining *K-1* blokini yuborish kifoya.



4.11-rasm. O'rin almashtirish sxemasi.

Shifrlashning analitik usullari. Matritsa algebrasiga asoslangan shifrlash usullari eng ko'p tarqalgan. Dastlabki axborotning $V_k=\|b_j\|$ vektor ko'rinishida berilgan *k*- blokini shifrlash $A=\|a_{ij}\|$ matritsa kalitni V_k vektorga ko'paytirish orqali amalga oshiriladi. Natijada, $S_k=\|c_i\|$ vektor ko'rinishidagi shifrmatn bloki hosil qilinadi. Bu vektorning elementlari $c_i = \sum_j a_{ij} b_j$ ifodasi orqali aniqlanadi.

Axborotni rasshifrovka qilish S_k vektorlarini A matritsaga teskari bo'lgan A^{-1} matritsaga ketma-ket ko'paytirish orqali aniqlanadi.

Misol. T_0=<AYLANA> so'zini matritsa-kalit

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

yordamida shifrlash va rasshifrovka qilish talab etilsin.

Dastlabki so'zni shifrlash uchun quyidagi qadamlarni bajarish lozim.

1-qadam. Dastlabki so'zning alfavitdagi harflar tartib raqami ketma-ketligiga mos son ekvivalentini aniqlash.

$$T_e = <1,10,12,1,14,1>$$

2-qadam. A matritsani $V_1=\{1,10,12\}$ va $V_2=\{1,14,1\}$ vektorlarga ko'paytirish.

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 23 \\ 11 \end{vmatrix} = \begin{vmatrix} 181 \\ 186 \\ 268 \end{vmatrix}$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 13 \\ 1 \end{vmatrix} = \begin{vmatrix} 61 \\ 96 \\ 128 \end{vmatrix}$$

3-qadam. Shifrlangan so'zni ketma-ket sonlar ko'rinishida yozish.

$$T_1 = <137,97,156,65,103,137>$$

Shifrlangan so'zni rasshifrovka qilish quyidagicha amalga oshiriladi:

1-qadam. A matritsaning aniqlovchisi hisoblanadi:

$$|A| = -115 .$$

2-qadam. Har bir elementi A matritsadagi a_{ij} elementning algebraik to'ldiruvchisi bo'lgan biriktirilgan matritsa A^* aniqlanadi.

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

3-qadam. Transponirlangan matritsa A^T aniqlanadi.

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

4-qadam. Quyidagi formula bo'yicha teskari matritsa A^{-1} hisoblanadi:

$$A^{-1} = \frac{A'}{|A|}$$

Hisoblash natijasida quyidagini olamiz.

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

5-qadam. B_1 va V_2 vektorlar aniqlanadi:

$$B_1 = A^{-1}S_1; \quad B_2 = A^{-1}S_2.$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 181 \\ 186 \\ 268 \end{vmatrix} = \begin{vmatrix} 1 \\ 23 \\ 11 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 61 \\ 96 \\ 128 \end{vmatrix} = \begin{vmatrix} 1 \\ 13 \\ 1 \end{vmatrix}$$

6-qadam. Rasshifrovka qilingan so'zning son ekvivalenti T_e=<1,23,11,1,13,1> simvollar bilan almashtiriladi. Natijada, dastlabki so'z T_0=<AYLANA> hosil bo'ladi.

Shifrlashning additiv usullari. Shifrlashning ***additiv usullariga*** binoan dastlabki axborot simvollariga mos keluvchi raqam kodlarini ketma-ketligi ***gamma*** deb ataluvchi qandaydir simvollar ketma-ketligiga mos keluvchi kodlar ketma-ketligi bilan ketma-ket jamlanadi. Shu sababli, shifrlashining additiv usullari ***gammalash*** deb ham ataladi.

Ushbu usullar uchun kalit sifatida gamma ishlatiladi. Additiv usulning kriptobardoshligi kalit uzunligiga va uning statistik xarakteristkalarining tekisligiga bog'liq. Agar kalit shifrlanuvchi simvollar ketma-ketligidan qisqa bo'lsa, shifrmatn kriptoanalitik tomonidan statistik usullar yordamida rasshifrovka qilinishi mumkin. Kalit va dastlabki axborot uzunliklari qanchalik farqlansa, shifr-matnga muvaffaqiyatli hujum ehtimolligi shunchalik ortadi. Agar kalit uzunligi shifrlanuvchi axborot uzunligidan katta bo'lgan tasodifiy sonlarning davriy bo'lmagan ketma-ketligidan iborat bo'lsa, kalitni bilmasdan turib shifrmatnni rasshifrovka qilish amaliy jihatdan mumkin emas. Almashtirish usul-

laridagidek gammalashda kalit sifatida raqamlarning takrorlanmaydigan ketma-ketligi ishlatilishi mumkin.

Amaliyotda asosini psevdotasodifiy sonlar generatorlari (datchiklari) tashkil etgan additiv usullar eng ko'p tarqalgan va samarali hisoblanadi. Generator psevdotasodifiy sonlarning cheksiz ketma-ketligini shakllantirishda nisbatan qisqa uzunlikdagi dastlabki axborotdan foydalanadi.

Psevdotasodifiy sonlar ketma-ketligini shakllantirishda kongruent generatorlardan ham foydalaniladi. Bu sinf generatorlari sonlarning shunday psevdotasodifiy ketma-ketliklarini shakllantiradiki, ular uchun generatorlarning davriyligi va chiqish yo'li ketma-ketliklarining tasodifiyligi kabi asosiy xarakteristkalarini qat'iy matematik tarzda ifodalash mumkin.

Kongruent generatorlar ichida o'zining soddaligi va samaraliligi bilan chiziqli generator ajralib turadi. Bu generator quyidagi munosabat bo'yicha sonlarning psevdotasodifiy ketma-ketliklarini shakllantiradi:

$$T(i+1) = (a \cdot T(i) + c) \bmod m;$$

bu yerda, a va c – o'zgarmaslar, T(0) – tug'diruvchi (sabab bo'luvchi) son sifatida tanlangan dastlabki kattalik.

Bunday datchikning takrorlanish davri a va c kattaliklariga bog'liq. m qiymati odatda 2^s ga teng qilib olinadi, bu yerda s–EHMdagi so'zning bitlardagi uzunligi. Shakllantiruvchi son ketma-ketliklarining takrorlanish davri s-toq son va $a \pmod 4 = 1$ bo'lgandagina maksimal bo'ladi. Bunday generatorlarni apparat yoki programm vositalari orqali osongina yaratish mumkin.

Shifrlashning kombinatsiyalangan usullari. Qudratli kompyuterlar, tarmoq texnologiyalari va neyronli hisoblashlarning paydo bo'lishi hozirgacha umuman fosh qilinmaydi deb hisoblangan kriptografik tizimlarni obro'sizlantirilishiga sabab bo'ldi. Bu esa, o'z navbatida, yuqori bardoshlikka ega kriptografik tizimlarni yaratish ustida ishlashni taqozo etdi. Bunday kriptografik tizimlarni yaratish usullaridan biri shifrlash usullarini kombinatsiyalashdir. Quyida eng kam vaqt sarfida kriptobardoshlikni jiddiy oshishini ta'minlovchi shifrlashning kombinatsiyalangan usuli ustida so'z boradi. Shifrlashning ushbu kombinatsiyalangan usuliga binoan ma'lumotlarni shifrlash ikki bosqichda amalga oshiriladi. Birinchi bosqichda ma'lumotlar standart usul (masalan, DES usul) yordamida shifrlansa, ikkinchi bosqichda shifrlangan ma'lumotlar maxsus usul bo'yicha qayta shifrlanadi. Maxsus usul sifatida ma'lumotlar vek-

torini elementlari noldan farqli bo'lgan son matritsasiga ko'paytirishdan foydalanish mumkin.

Gammalashni qo'llashda, agar shifr gammasi sifatida raqamlarning takrorlanmaydigan ketma-ketligi ishlatilsa, shifrlangan matnni fosh qilish juda qiyin. Odatda, shifr gammasi har bir shifrlanuvchi so'z uchun tasodifiy o'zgarishi lozim. Agar shifr gammasi shifrlangan so'z uzunligidan katta bo'lsa va dastlabki matnning hech qanday qismi ma'lum bo'lmasa, shifrni faqat to'g'ridan-to'g'ri saralash orqali fosh etish mumkin. Bunda kriptobardoshlik kalit o'lchami orqali aniqlanadi. Shifrlashning bu usulidan ko'pincha himoya tizimining dasturiy amalga oshirilishida foydalaniladi va shifrlashning bu usuliga asoslangan tizimlarda bir sekundda ma'lumot-larning bir necha yuz Kbaytini shifrlash imkoniyati mavjud. Rasshifrovka qilish jarayoni-kalit ma'lum bo'lganida shifr gammasini qayta generatsiyalash va uni shifrlangan ma'lumotlarga singdirishdan iborat.

Shifrlangan ma'lumotlar vektorini matritsaga ko'paytirishni qo'llashda shifrlangan matn bir bayt uzunlikdagi f_i vektorlarga ajratiladi va har bir vektor kvadrat matritsa $\|M_{ij}\|$ ga ko'paytiriladi va shifrlangan vektorlar shakllantiriladi:

$$f_i^* = f_i \cdot \|M_{ij}\|$$

Bu usulning asosiy afzalligi sifatida uning ma'lumotlar ishlanishining turli jabhalaridagi moslanuvchanligini ko'rsatish mumkin. Har bir vektor alohida shifrlanganligi sababli ma'lumotlar blokini uzatish va dasturlangan ma'lumotlardan ixtiyoriy foydalanish imkoniyati tug'iladi. Ushbu usulni apparat yoki dasturiy usulda amalga oshirish mumkin.

Rasshifrovka qilish jarayonida shifrlangan f^* vektorlarni teskari matritsa $\left(M_{ij}^{-1}\right)$ga ko'paytiriladi.

$$f_i = f_i^* \cdot \|M_{ij}^{-1}\|$$

Kombinatsiyalangan usullarning yuqori samaradorligiga uning ikkala bosqichini apparat usulda amalga oshirish orqali erishish mumkin. Ammo bu uskuna xarajatlarining jiddiy oshishiga olib keladi. Dasturiy usulda amalga oshirilishida esa ma'lumotlarni shifrlash va rasshifrovka qilish vaqti oshib ketadi. Shu sababli kombinatsiyalangan usularni apparat-dasturiy usulda, ya'ni usulning bir bosqichi apparat usulda, ikkinchi

bosqichi dasturiy usulda amalga oshirilishi maqsadga muvofiq hisoblanadi.

4.3. Asimmetrik shifrlash tizimlari

Asimmetrik shifrlash tizimlarida ikkita kalit ishlatiladi. Axborot ochiq kalit yordamida shifrlansa, maxfiy kalit yordamida rasshifrovka qilinadi. Asimmetrik shifrlash tizimlarini ochiq kalitli shifrlash tizimlar deb ham yuritiladi.

Ochiq kalitli tizimlarini qo'llash asosida qaytarilmas yoki bir tomonli funksiyalardan foydalanish yotadi. Bunday funksiyalar quyidagi xususiyatlarga ega. Ma'lumki x ma'lum bo'lsa $y=f(x)$ funksiyani aniqlash oson. Ammo uning ma'lum qiymati bo'yicha x ni aniqlash amaliy jihatdan mumkin emas. Kriptografiyada yashirin deb ataluvchi yo'lga ega bo'lgan bir tomonli funksiyalar ishlatiladi. Z parametrli bunday funksiyalar quyidagi xususiyatlarga ega. Ma'lum Z uchun E_z va D_z algoritmlarini aniqlash mumkin. E_z algoritmi yordamida aniqlik sohasidagi barcha x uchun $f_Z(x)$ funksiyani osongina olish mumkin. Xuddi shu tariqa D_z algoritmi yordamida joiz qiymatlar sohasidagi barcha y uchun teskari funksiya $x=f^{-1}(y)$ ham osongina aniqlanadi. Ayni vaqtda joiz qiymatlar sohasidagi barcha z va deyarli barcha, y uchun hatto E_z ma'lum bo'lganida ham $f^{-1}(y)$ni hisoblashlar yordamida topib bo'lmaydi. Ochiq kalit sifatida y ishlatilsa, maxfiy kalit sifatida x ishlatiladi.

Ochiq kalitni ishlatib shifrlash amalga oshirilganda o'zaro muloqotda bo'lgan subyektlar o'rtasida maxfiy kalitni almashish zaruriyati yo'qoladi. Bu esa, o'z navbatida, uzatiluvchi axborotning kriptohimoyasini soddalash-tiradi.

Ochiq kalitli kriptotizimlarni bir tomonli funksiyalar ko'rinishi bo'yicha farqlash mumkin. Bularning ichida RSA, El-Gamal va Mak-Elis tizimlarini alohida tilga olish o'rinli. Hozirda eng samarali va keng tarqalgan ochiq kalitli shifrlash algoritmi sifatida RSA algoritmini ko'rsatish mumkin. RSA nomi algoritmni yaratuvchilari familiyalarining birinchi harfidan olingan (Rivest, Shamir va Adleman).

Algoritm modul arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan. Algoritmni quyidagi qadamlar ketma-ketligi ko'rinishida ifodalash mumkin.

1-qadam. Ikkita 200 dan katta bo'lgan tub son p va q tanlanadi.

2-qadam. Kalitning ochiq tashkil etuvchisi n hosil qilinadi

$$n=p*q.$$

3-qadam. Quyidagi formula bo'yicha Eyler funksiyasi hisoblanadi:

$f(p,q)=(p-1)(q-1)$.

Eyler funksiyasi n bilan o'zaro tub, 1 dan n gacha bo'lgan butun musbat sonlar sonini ko'rsatadi. O'zaro tub sonlar deganda 1 dan boshqa birorta umumiy bo'luvchisiga ega bo'lmagan sonlar tushuniladi.

4-qadam. $f(p,q)$ qiymati bilan o'zaro tub bo'lgan katta tub son d tanlab olinadi.

5-qadam. Quyidagi shartni qanoatlantiruvchi e soni aniqlanadi

$$e \cdot d = 1 (mod f(p,q)).$$

Bu shartga binoan $e \cdot d$ ko'paytmaning $f(p,q)$ funksiyaga bo'lishdan qolgan qoldiq 1ga teng. e soni ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi. Maxfiy kalit sifatida d va n sonlari ishlatiladi.

6-qadam. Dastlabki axborot uning fizik tabiatidan qat'i nazar raqamli ikkili ko'rinishda ifodalanadi. Bitlar ketma-ketligi L bit uzunlikdagi bloklarga ajratiladi, bu yerda L–$L \geq \log_2(n+1)$ shartini qanoatlantiruvchi eng kichik butun son. Har bir blok $[0, n-1]$ oraliqqa taalluqli butun musbat son kabi ko'riladi. Shunday qilib, dastlabki axborot $X(i)$, $i=1, I$ sonlarning ketma-ketligi orqali ifodalanadi. i ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

7-qadam. Shifrlangan axborot quyidagi formula bo'yicha aniqlanuvchi $Y(i)$ sonlarning ketma-ketligi ko'rinishida olinadi:

$$Y(i) = (X(i))^e (\mathrm{mod}\, n).$$

Axborotni rasshifrovka qilishda quyidagi munosabatdan foydalaniladi:

$$X(i) = (Y(i))^d (\mathrm{mod}\, n).$$

Misol. <GAZ> so'zini shifrlash va rasshifrovka qilish talab etilsin. Dastlabki so'zni shifrlash uchun quyidagi qadamlarni bajarish lozim.

1-qadam. $p=3$ va $q=11$ tanlab olinadi.

2-qadam. $n = 3 \cdot 11 = 33$ hisoblanadi.

3-qadam. Eyler funksiyasi aniqlanadi.

$$f(p,q) = (3-1) \cdot (11-1) = 20$$

4-qadam. O'zaro tub son sifatida $d=3$ soni tanlab olinadi.

5-qadam. $(e \cdot 3) \cdot (\mathrm{mod}\, 20) = 1$ shartini qanoatlantiruvchi e soni tanlanadi. Aytaylik, $e=7$.

6-qadam. Dastlabki so'zning alfavitdagi harflar tartib raqami ketma-ketligiga mos son ekvivalenti aniqlanadi. A harfiga –1, G harfiga-4, Z harfiga –9. O'zbek alfavitida 36ta harf ishlatilishi sababli ikkili kodda ifodalash uchun 6 ta ikkili xona kerak bo'ladi. Dastlabki axborot ikkili kodda quyidagi ko'rinishga ega bo'ladi:

000100 000001 001001.

Blok uzunligi L butun sonlar ichidan $L \geq \log_2(33+1)$ shartini qanoatlantiruvchi minimal son sifatida aniqlanadi. n =33 bo'lganligi sababli L =6.

Demak, dastlabki matn $X(i) \leq< 4,1,9 >$ ketma-ketlik ko'rinishida ifodalanadi.

7-qadam. $X(i)$ ketma-ketligi ochiq kalit {7,33} yordamida shifrlanadi:

$$Y(1) = (4^7)(\text{mod}\,33) = 16384(\text{mod}\,33) = 16$$
$$Y(2) = (1^7)(\text{mod}\,33) = 1(\text{mod}\,33) = 1$$
$$Y(1) = (9^7)(\text{mod}\,33) = 4782969(\text{mod}\,33) = 15$$

Shifrlangan so'z $Y(i)$=<16,1,15>

Shifrlangan so'zni rasshifrovka qilish maxfiy kalit {3,33} yordamida bajariladi.:

$$Y(1) = (16^3)(\text{mod}\,33) = 4096(\text{mod}\,33) = 4$$
$$Y(1) = (1^3)(\text{mod}\,33) = 1(\text{mod}\,33) = 1$$
$$Y(1) = (15^3)(\text{mod}\,33) = 3375(\text{mod}\,33) = 9$$

Dastlabki son ketma-ketligi rasshifrovka qilingan $X(i)$=<4,1,9> ko'rinishida dastlabki matn <GAZ> bilan almashtiriladi.

Keltirilgan misolda hisoblashlarning soddaligini ta'minlash maqsadida mumkin bo'lgan kichik sonlardan foydalanildi.

El-Gamal tizimi chekli maydonlarda diskret logarifmlarning hisoblanish murakkabligiga asoslangan. RSA va El-Gamal tizimlarining asosiy kamchiligi sifatida modul arifmetikasidagi murakkab amallarning bajarilishi zaruriyatini ko'rsatish mumkin. Bu, o'z navbatida, aytarlicha hisoblash resurslarini talab qiladi.

Mak-Elis kriptotizimida xatoliklarni tuzatuvchi kodlar ishlatiladi. Bu tizim RSA tizimiga nisbatan tezroq amalga oshirilsa-da, jiddiy kamchilikka ega. Mak-Elis kriptotizimida katta uzunlikdagi kalit ishlatiladi va olingan shifrmatn uzunligi dastlabki matn uzunligidan ikki marta katta bo'ladi.

Barcha ochiq kalitli shifrlash usullari uchun *NP*-to'liq masalani (to'liq saralash masalasi) yechishga asoslangan kriptotahlil usulidan boshqa usullarining yo'qligi qat'iy isbotlanmagan. Agar bunday masalalarni yechuvchi samarali usullar paydo bo'lsa, bunday xildagi kriptotizim obro'sizlantiriladi.

Yuqorida ko'rilgan shifrlash usullarining kriptobardoshligi kalit uzunligiga bog'liq bo'lib, bu uzunlik zamonaviy tizimlar uchun, loaqal, 90 bitdan katta bo'lishi shart.

Ayrim muhim qo'llanishlarda nafaqat kalit, balki shifrlash algoritmi ham maxfiy bo'ladi. Shifrlarning kriptobardoshligini oshirish uchun bir necha kalit (odatda uchta) ishlatilishi mumkin. Birinchi kalit yordamida shifrlangan axborot ikkinchi kalit yordamida shifrlanadi va h.

4.4. Shifrlash standartlari

Rossiyaning' axborotni shifrlash standarti. Rossiya Federatsiyasida hisoblash mashinalari, komplekslari va tarmoqlarida axborotni kriptografik o'zgartirish algoritmlariga davlat standarti (GOST 2814–89) joriy etilgan. Bu algoritmlar maxfiylik darajasi ixtiyoriy bo'lgan axborotni hech qanday cheklovsiz shifrlash imkonini beradi. Algoritmlar apparat va dasturiy usullarida amalga oshirilishi mumkin.

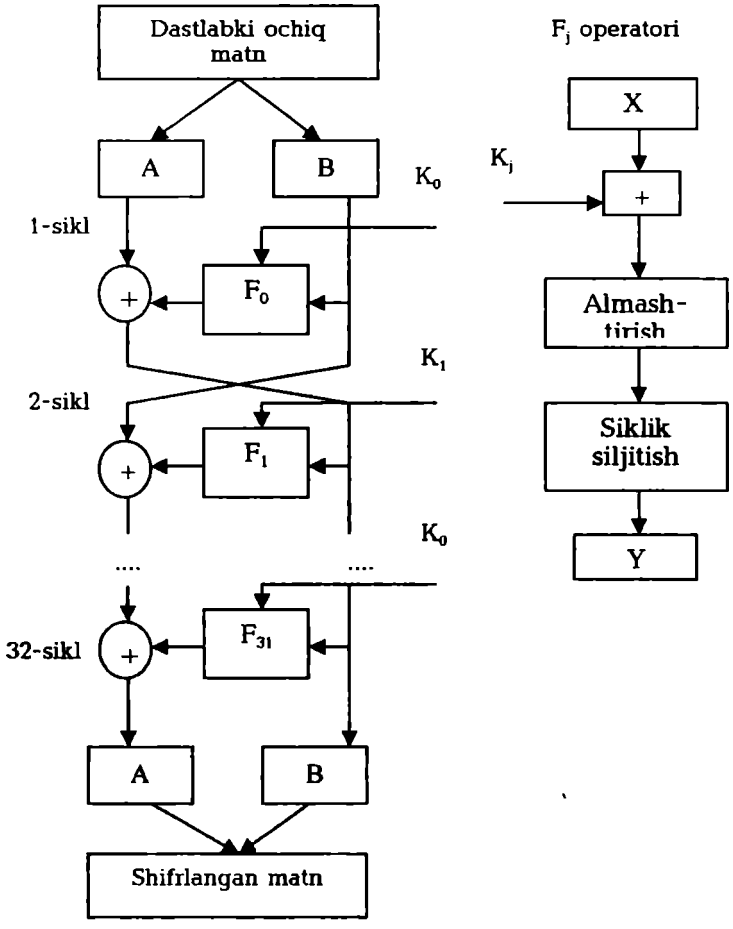
Standartda axborotni kriptografik o'zgartirishning quyidagi algoritmlari mavjud:

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

Bu algoritmlar uchun 8 ta 32 xonali ikkili so'zlarga ajratilgan 256 bit o'lchamli kalitning ishlatilishi hamda dastlabki shifrlanuvchi ikkili ketma-ketlikning 64 bitli bloklarga ajratilishi umumiy hisoblanadi.

Oddiy alamshtirish algoritmining mohiyati quyidagicha (4.12-rasm).

Dastlabki ketma-ketlikning 64 bitli bloki ikkita 32 xonali A va V ikkili so'zlarga ajratiladi. A so'zlar blokning kichik xonalarini V so'zlar esa katta xonalarini tashkil etadi. Bu so'zlarga soni i=32 bo'lgan siklik iteratsiya operatori F_i qo'llaniladi. Blokning kichik bitlaridagi so'z (birinchi iteratsiyadagi A so'zi) kalitining 32 xonali so'zi bilan mod 2^{32} bo'yicha jamlanadi; har biri 4 bitdan iborat qismlarga (4 xonali kirish yo'li vektorlari) ajratiladi; maxsus almashtirish uzellari yordamida har bir vektor boshqasi bilan almashtiriladi; olingan vektorlar 32 xonali so'zga birlashtirilib, chap tarafga siklik ravishda siljitiladi va 64 xonali blokdagi boshqa 32 xonali so'z (birinchi iteratsiyadagi V so'zi) bilan mod 2 bo'yicha jamlanadi.



4.12-rasm. Oddiy almashtirish algoritmida shifrlash jarayonining blok-sxemasi.

Birinchi iteratsiya tugaganidan so'ng kichik bitlar o'rnida V so'z joylanadi, chap tarafda esa *A* so'z joylanadi. Keyingi iteratsiyalarda so'zlar ustidagi amallar takrorlanadi.

Har bir *i*-iteratsiyada K_j kalitning (kalitlar 8 ta) 32 xonali so'zi quyidagi qoidaga binoan tanlanadi:

$$K_i = \begin{cases} (i-1) \bmod 8, & 1 \le i \le 24 \quad bo'lganda, \\ 32-i, & i \ge 25 \quad bo'lganda, \\ 0, & i = 32 \quad bo'lganda, \end{cases}$$

Demak, shifrlashda kalitning tanlanish tartibi quyidagi ko'rinishda bo'ladi:

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7,$
$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0,$.

Rasshifrovka qilishda kalitlar teskari tartibda ishlatiladi.

Almashtirish bloki ketma-ket tanlanuvchi 8 ta almashtirish uzellaridan iborat. Almashtirish uzeli har birida almashtirish vektori (4 bit) joylashgan 16 qatorli jadvaldan iborat. Kirish yo'li vektori jadvaldagi qator adresini aniqlasa, qatordagi son almashtirishning chiqish yo'li vektori hisoblanadi. Almashtirish jadvaliga axborot oldindan yoziladi va kamdan-kam o'zgartiriladi.

Gammalash algoritmida dastlabki bitlarning ketma-ketligi gammaning bitlari ketma-ketligi bilan mod2 bo'yicha jamlanadi. Gamma oddiy almashtirish algoritmiga binoan hosil qilinadi. Gammani shakllantirishda ikkita maxsus doimiylardan hamda 64-xonali ikkili ketma-ketlik sinxroposilkadan foydalaniladi. Axborotni faqat sinxroposilka borligida rasshifrovka qilish mumkin.

Sinxroposilka maxfiy bo'lmaydi va ochiq holda hisoblash mashinasi xotirasida saqlanishi yoki aloqa kanali orqali uzatilishi mumkin.

Teskari bog'lanishli gammalash algoritmi gammalash algoritmidan faqat shifrlash jarayonining birinchi qadamidagi harakatlar bilan farqlanadi.

Imitovstavka noto'g'ri axborotni zo'rlab kiritilishidan himoyalashda ishlatiladi. Imitovstavka dastlabki axborot va maxfiy kalitni o'zgartirish funksiyasi hisoblanadi. U k bit uzunlikdagi ikkili ketma-ketlikdan iborat bo'lib, k ning qiymati noto'g'ri axborotning zo'rlab kiritilishi ehtimolligi R_{zk} bilan quyidagi munosabat bilan bog'langan.

$$R_{zk} = \frac{1}{2^k}$$

Imitostavkani shakllantirish algoritmi quyidagi harakatlar ketma-ketligidan iborat. Ochiq axborot 64 bitli $T(i)$ (i=1,2,3,....,m) bloklarga ajratiladi, bu yerda m-shifrlanuvchi axborot hajmi orqali aniqlanadi. Birinchi blok $T(1)$ oddiy almashtirish algoritmining birinchi 16 iteratsi-

yalariga binoan o'zgartiriladi. Kalit sifatida dastlabki axborot shifrlanishda ishlatiladigan kalit olinadi. Olingan 64 bitli ikkili so'z ikkinchi blok $T(2)$ bilan mod2 bo'yicha jamlanadi. $T(1)$ blok ustida qanday iteratsiya o'zgartirishlari bajarilgan bo'lsa, jamlash natijasi ustida ham shunday o'zgartirishlar amalga oshiriladi va oxirida $T(3)$ blok bilan mod2 bo'yicha jamlanadi. Bunday harakatlar dastlabki axborotning m-1 bloki bo'yicha takrorlanadi. Agar oxirgi $T(m)$ blok to'liq bo'lmasa, u 64 xonagacha nollar bilan to'ldiradi. Bu $T(m-1)$ blok ishlanish natijasi bilan mod2 bo'yicha jamlanadi va oddiy almashtirish algoritmining birinchi 16 iteratsiyalari bo'yicha o'zgartiriladi. Hosil bo'lgan 64 xonali blokdan k bit uzunlikdagi so'z ajratib olinadi va bu so'z imitovstavka hisoblanadi.

Imitovstavka shifrlangan axborotning oxiriga joylashtiriladi. Bu axborot olingandan so'ng, u rasshifrovka qilinadi. Rasshifrovka qilingan axborot bo'yicha imitovstavka aniqlanadi va olingani bilan solishtiriladi. Agar imitovstavkalar mos kelmasa, rasshifrovka qilingan axborot noto'g'ri deb hisoblanadi.

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

DES standartida dastlabki axborot 64 bitli bloklarga ajratiladi va 56 yoki 64 bitli kalit yordamida kriptografik o'zgartiriladi.

Dastlabki axborot bloklari o'rin almashtirish va shifrlash funksiyalari yordamida iteratsion ishlanadi. Shifrlash funksiyasini hisoblash uchun 64 bitli kalitdan 48 bitligini olish, 32-bitli kodni 48 bitli kodga kengaytirish, 6-bitli kodni 4-bitli kodga o'zgartirish va 32-bitli ketmaketlikning o'rnini almashtirish ko'zda tutilgan.

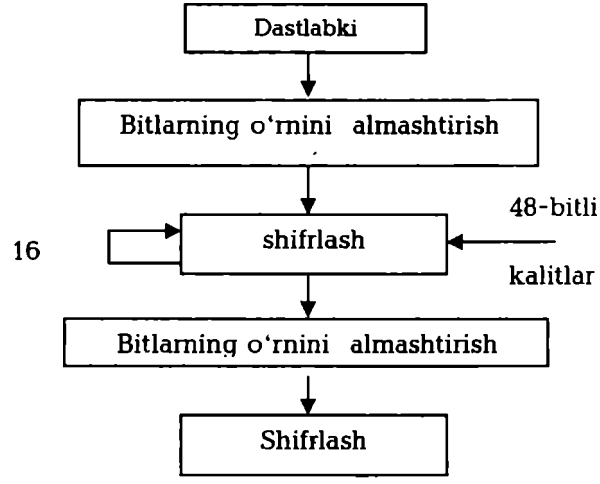
DES algoritmidagi shifrlash jarayonining blok-sxemasi 4.13-rasmda keltirilgan.

Rasshifrovka jarayoni shifrlash jarayoniga invers bo'lib, shifrlashda ishlatiladigan kalit yordamida amalga oshiriladi.

Hozirda bu standart quyidagi ikkita sababga ko'ra foydalanishga butunlay yaroqsiz hisoblanadi:

- kalitning uzunligi 56 bitni tashkil etadi, bu EHMlarning zamonaviy rivoji uchun juda kam;

• algoritm yaratilayotganida uning apparat usulda amalga oshirilishi ko'zda tutilgan edi, ya'ni algoritmda mikroprotsessorlarda bajarilishida ko'p vaqt talab qiluvchi amallar bor edi (masalan, mashina so'zida ma'lum sxema bo'yicha bitlarning o'rnini almashtirish kabi).



4.13- rasm. DES algoritmida shifrlash jarayonining blok-sxemasi.

Bu sabablar AQSH standartlash institutining 1997-yilda simmetrik algoritmning yangi standartiga tanlov e'lon qilishiga olib keldi. Tanlov shartlariga binoan algoritmga quyidagi talablar qo'yilgan edi:

• algoritm simmetrik bo'lishi kerak;

• algoritm blokli shifr bo'lishi kerak;

• blok uzunligi 128 bit bo'lib, 128, 192, va 256 bitli kalit uzunliklarini ta'minlashi lozim.

Undan tashqari tanlovda ishtirok etuvchilar uchun quyidagi tavsiyalar berilgan edi:

• ham apparat usulda ham programm usulda osongina amalga oshiri-luvchi amallardan foydalanish;

• 32 xonali protsessorlardan foydalanish;

• iloji boricha shifr tuzilmasini murakkablashtirmaslik. Bu o'z navbatida barcha qiziquvchilarning algoritmni mustaqil tarzda kriptotahlil qilib, unda qandaydir hujjatsiz imkoniyatlar yo'qligiga ishonch hosil qilishlari uchun zarur hisoblanadi.

2000-yil 2-oktabrda tanlov natijasi e'lon qilindi. Tanlov g'olibi deb Belgiya algoritmi RIJNDAEL topildi va shu ondan boshlab algoritm-g'olibdan barcha patent chegaralanishlari olib tashlandi.

Hozirda AES (Advanced Encryption Standard) deb ataluvchi ushbu algoritm Dj.Deymen (J. Daemen) va V. Raydjmen (V.Rijmen) tomonidan yaratilgan. Bu algoritm noan'anaviy blokli shifr bo'lib, kodlanuvchi ma'lumotlarning har bir bloki qabul qilingan blok uzunligiga qarab 4x4, 4x6 yoki 4x8 o'lchamdagi baytlarning ikki o'lchamli massivlari ko'rinishiga ega

Shifrdagi barcha o'zgartirishlar qat'iy matematik asosga ega. Amallarning tuzilmasi va ketma-ketligi algoritmning ham 8 bitli, ham 32 bitli mikroprotsessorlarda samarali bajarilishiga imkon beradi. Algoritm tuzilmasida ba'zi amallarning parallel ishlanishi ishchi stansiyalarida shifrlash tezligining 4 marta oshishiga olib keladi.

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

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

Standart EHM tarmoqlarida, telekommunikatsiyada, alohida hisoblash komplekslari va EHMda axborotni ishlash tizimlari uchun axborotni shifrlashning umumiy algoritmini va ma'lumotlarni shifrlash qoidasini belgilaydi.

Shifrlash algoritmi dasturiy va apparat usullarda amalga oshirilishi mumkin.

Simmetrik shifrlashning barcha tizimlari quyidagi kamchiliklarga ega:

- axborot almashuvchi ikkala subyekt uchun maxfiy kalitni uzatish kanalining ishonchliligi va xavfsizligiga qo'yiladigan talablarning qat'iyligi;
- kalitlarni yaratish va taqsimlash xizmatiga quyiladigan talablarning yuqoriligi. Sababi, o'zaro aloqaning «har kim – har kim bilan»

sxemasida «n» ta abonent uchun $n(n-1)/2$ ta kalit talab etiladi, ya'ni kalitlar sonining abonentlar soniga bog'liqligi kvadratli. Masalan, n=1000 abonent uchun talab qilinadigan kalitlar soni $n(n-1)/2$=499500. Shu sababli, foydala-nuvchilari yuz milliondan oshib ketgan «Internet» tarmog'ida simmetrik shifrlash tizimini qo'shimcha usul va vositalarsiz qo'llashning iloji yo'q.

Asimmetrik shifrlashning birinchi va keng tarqalgan kriptoalgoritmi RSA (4.3 ga qaralsin) 1993-yilda standart sifatida qabul qilindi. Ushbu kriptoalgoritm har taraflama tasdiqlangan va kalitning yetarli uzunligida bardoshligi e'tirof etilgan. Hozirda 512 bitli kalit bardoshlikni ta'minlashda yetarli hisoblanmaydi va 1024 bitli kalitdan foydalaniladi. Ba'zi mualliflarning fikricha protsessor quvvatining oshishi RSA kriptoalgoritmining to'liq saralash hujumlarga bardoshligining yo'qolishiga olib keladi. Ammo protsessor quvvatining oshishi yanada uzun kalitlardan foydalanishga va demak, RSA bardoshligini oshishiga imkon yaratadi.

Asimmetrik kriptoalgoritmlarda simmetrik kriptoalgoritmlardagi kamchiliklar bartaraf etilgan:

- kalitlarni maxfiy tarzda yetkazish zaruriyati yo'q; asimmetrik shifrlash ochiq kalitlarni dinamik tarzda yetkazishga imkon beradi, simmetrik shifrlashda esa himoyalangan aloqa seansi boshlanishidan avval maxfiy kalitlar almashinishi zarur edi;
- kalitlar sonining foydalanuvchilar soniga kvadratli bog'lanishligi yo'qoladi; RSA asimmetrik kriptotizimda kalitlar sonining foydalanuvchilar soniga bog'liqligi chiziqli ko'rinishga ega (N foydalanuvchisi bo'lgan tizimda $2N$ kalit ishlatiladi).

Ammo asimmetrik kriptotizimlar, xususan RSA kriptotizimi, kamchiliklardan xoli emas:

- hozirgacha asimmetrik algoritmlarda ishlatiluvchi funksiyalarning qaytarilmasligining matematik isboti yo'q;
- asimmetrik shifrlash simmetrik shifrlashga nisbatan sekin amalga oshiriladi, chunki shifrlashda va rasshifrovka qilishda katta resurs talab etiladigan amallar ishlatiladi (xususan, RSAda katta sonni katta sonli darajaga oshirish talab etiladi). Shu sababli asimmetrik algoritmlarni amalga oshirilishi, simmetrik algoritmlardagiga nisbatan anchagina murakkab;
- ochiq kalitlarni almashtirib quyilishidan himoyalash zarur. Faraz qilaylik «A» abonentning kompyuterida «V» abonentning ochiq kaliti «K_V» saqlanadi. «n» niyati buzuq odam «A» abonentda saqlana-

yotgan ochiq kalitlardan foydalana oladi. U o'zining juft (ochiq va maxfiy) «K_n» va «k_n» kalitlarini yaratadi va «A» abonentda saqlanayotgan «V» abonentning «K_V» kali-tini o'zining ochiq «K_n» kaliti bilan almashtiradi. «A» abonent qandaydir axborotni «V» abonentga jo'natish uchun uni «K_n» kalitda (bu «K_V» kalit deb o'ylagan holda) shifrlaydi. Natijada, bu xabarni «V» abonent o'qiy olmaydi, «n» abonent osongina rasshifrovka qiladi va o'qiydi. Ochiq kalitlarni almashtirishni oldini olishda kalitlarni sertifikatsiyalashdan foydalaniladi.

4.5. Xeshlash funksiyasi

Xeshlash funksiyasi (xesh-funksiyasi) shunday o'zgartirishki, kirish yo'liga uzunligi o'zgaruvchan xabar M berilganida chiqish yo'lida belgilangan uzunlikdagi qator $h(M)$ hosil bo'ladi. Boshqacha aytganda, xesh-funksiya $h(.)$ argument sifatida uzunligi ixtiyoriy xabar (hujjat) M ni qabul qiladi va belgilangan uzunlikdagi xesh-qiymat (xesh) $H=h(M)$ni qaytaradi (4.14-rasm).

4.14-rasm. Xeshni shakllantirish sxemasi.

Xesh-qiymat h(M) – xabar M ning daydjesti, ya'ni ixtiyoriy uzunlikdagi asosiy xabar Mning xichlantirilgan ikkilik ifodasi. Xeshlash funksiyasi o'lchami megabayt va undan katta bo'lgan imzo chekiluvchi hujjat Mni 128 va undan katta bitga (xususan, 128 yoki 256 bit) zichlashtirishga imkon beradi. Ta'kidlash lozimki, xesh-funksiya $h(M)$ qiymatining hujjat Mga bog'liqligi murakkab va hujjat Mning o'zini tiklashga imkon bermaydi.

Xeshlash funksiyasi quyidagi xususiyatlarga ega bo'lishi lozim:

1. Xesh-funksiya ixtiyoriy o'lchamli argumentga qo'llanishi mumkin.
2. Xesh-funksiya chiqish yo'lining qiymati belgilangan o'lchamga ega.
3. Xesh-funksiya $h(x)$ ni ixtiyoriy «x» uchun yetarlicha oson hisoblanadi. Xesh-funksiyani hisoblash tezligi shunday bo'lishi kerakki,

xesh-funksiya ishlatilganida elektron raqamli imzoni tuzish va tekshirish tezligi xabarning o'zidan foydalanilganiga qaraganda anchagina katta bo'lsin.

4. Xesh-funksiya matn M dagi orasiga qo'yishlar (vstavki), chiqarib tashlashlar (vibrosi), joyini o'zgartirishlar va h. kabi o'zgarishlarga sezgir bo'lishi lozim.

5. Xesh-funksiya qaytarilmaslik xususiyatiga ega bo'lishi lozim.

6. Ikkita turli hujjatlar (ularning uzunligiga bog'liq bo'lmagan holda) xesh-funksiyalari qiymatlarining mos kelishi ehtimolligi juda kichkina bo'lishi shart, ya'ni hisoblash nuqtai nazaridan $h(x')=h(x)$ bo'ladigan $x' \neq x$ ni topish mumkin emas.

Ikkita turli xabarni bitta tugunchaga (svertka) zichlashtirish nazariy jihatdan mumkin. Bu kolliziya yoki to'qnashish deb ataladi. Shuning uchun xeshlash funksiyasining bardoshligini ta'minlash maqsadida to'qnashishlarga yo'l qo'ymaslikni ko'zda tutish lozim. To'qnashishlarga butunlay yo'l qo'ymaslik mumkin emas, chunki umumiy holda mumkin bo'lgan xabarlar soni xeshlash funksiyalari chiqish yo'llari qiymatlarining mumkin bo'lgan sonidan ortiq. Ammo to'qnashishlar ehtimolligi past bo'lishi lozim.

5-xususiyat $h(.)$ bir tomonlama ekanligini bildirsa, 6-xususiyat bir xil tugunchani beruvchi ikkita axborotni topish mumkin emasligini kafolatlaydi. Bu soxtalashtirishni oldini oladi.

Shunday qilib, xeshlash funksiyasidan xabar o'zgarishini payqashda foydalanish mumkin, ya'ni u *kriptografik nazorat yig'indisini* (o'zgarishlarni payqash kodi yoki *xabarni autentifikatsiyalash kodi* deb ham yuritiladi) shakllantirishga xizmat qilishi mumkin. Bu sifatda xesh-funksiya xabarning yaxlitligini nazoratlashda, elektron raqamli imzoni shakllantirishda va tekshirishda ishlatiladi.

Xesh-funksiya foydalanuvchini autentifikatsiyalashda ham keng qo'llaniladi. Axborot xavfsizligining qator texnologiyalarida shifrlashning o'ziga xos usuli – *bir tomonlama xesh-funksiya yordamida shifrlash* ishlatiladi. Bu shifrlashning o'ziga xosligi shundan iboratki, u mohiyati bo'yicha, bir tomonlamadir, ya'ni teskari muolaja – qabul qiluvchi tomonda rasshifrovka qilish bilan birga olib borilmaydi. Ikkala taraf (jo'natuvchi va qabul qiluvchi) xesh-funksiya asosidagi bir tomonlama shifrlash muolajasidan foydalanadi.

Eng ommabop xesh-funksiyalar – MD2, MD4, MD5 va SHA.

MD2, MD4 va MD5 – R.Rivest tomonidan ishlab chiqilgan axborot daydjestini hisoblovchi algoritmlari. Ularning har biri 128 bitli xesh-kodni tuzadi. MD2 algoritmi eng sekin ishlasa, MD4 algoritmi tez ishlaydi. MD5 algoritmi MD4 algoritmining modifikatsiyasi bo'lib, natijada xavfsizlikning oshirilishi evaziga tezlikdan yutqazilgan. SHA(Secure Hash Algorithm) – 160 bitli *xesh-kod*ni tuzuvchi axborot daydjestini hisoblovchi algoritm. Bu algoritm MD4 va MD5 algoritmlariga nisbatan ishonchliroq.

4.6. Elektron raqamli imzo

Elektron hujjatlarni tarmoq orqali almashishda ularni ishlash va saqlash xarajatlari kamayadi, qidirish tezlashadi. Ammo elektron hujjat muallifini va hujjatning o'zini autentifikatsiyalash, ya'ni muallifning haqiqiyligini va olingan elektron hujjatda o'zgarishlarning yo'qligini aniqlash muammosi paydo bo'ladi.

Elektron hujjatlarni autentifikatsiyalashdan maqsad ularni mumkin bo'lgan jinoyatkorona harakatlardan himoyalashdir. Bunday harakatlarga quyidagilar kiradi:

– *faol ushlab qolish* - tarmoqqa ulangan buzg'unchi hujjatlarni (fayllarni) ushlab qoladi va o'zgartiradi.

– *maskarad* – abonent *S* hujjatlarni abonent *V* ga abonent *A* nomidan yuboradi;

– *renegatlik* – abonent *A* abonent *V* ga xabar yuborgan bo'lsa-da, yu-bormaganman deydi;

– *almashtirish* – abonent *V* hujjatni o'zgartiradi yoki yangisini shakillantiradi va uni abonent *A* dan olganman deydi;

– *takrorlash* – abonent *A* abonent *V* ga yuborgan hujjatni abonent *S* takrorlaydi.

Jinoyatkorona harakatlarning bu turlari o'z faoliyatida kompyuter axborot texnologiyalaridan foydalanuvchi bank va tijorat tuzilmalariga, davlat korxona va tashkilotlariga xususiy shaxslarga ancha-muncha zarar yetkazishi mumkin.

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

Elektron raqamli imzo telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. Raqamli imzo ish-

lashi bo'yicha oddiy qo'lyozma imzoga o'xshash bo'lib, quyidagi afzalliklarga ega:

– imzo chekilgan matn imzo qo'ygan shaxsga tegishli ekanligini tasdiqlaydi;

– bu shaxsga imzo chekilgan matnga bog'liq majburiyatlaridan tonish imkoniyatini bermaydi;

– imzo chekilgan matn yaxlitligini kafolatlaydi.

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

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

Elektron raqamli imzo tizimining qo'llanishida bir- biriga imzo chekilgan elektron hujjatlarni jo'natuvchi abonent tarmog'ining mavjudligi faraz qilinadi. Har bir abonent uchun juft – maxfiy va ochiq kalit generatsiyalanadi. Maxfiy kalit abonentda sir saqlanadi va undan abonent elektron raqamli imzoni shakllantirishda foydalanadi.

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

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

– raqamli imzoni shakllantirish muolajasi;

– raqamli imzoni tekshirish muolajasi.

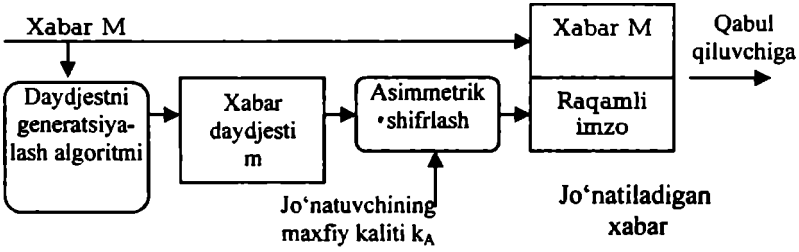
Imzoni shakllantirish muolajasida xabar jo'natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo'natuvchining ochiq kalitidan foydalaniladi.

Raqamli imzoni shakllantirish muolajasi:

Ushbu muolajani tayyorlash bosqichida xabar jo'natuvchi abonent A ikkita kalitni generatsiyalaydi: maxfiy kalit k_A va ochiq kalit K_A. Ochiq kalit K_A uning jufti bo'lgan maxfiy kalit k_A dan hisoblash orqali olinadi. Ochiq kalit K_A tarmoqning boshqa abonentlariga imzoni tekshirishda foydalanish uchun tarqatiladi.

Raqamli imzoni shakllantirish uchun jo'natuvchi A avvalo imzo chekiluvchi matn M ning xesh-funksiyasi $L(M)$ qiymatini hisoblaydi (4.15-rasm).

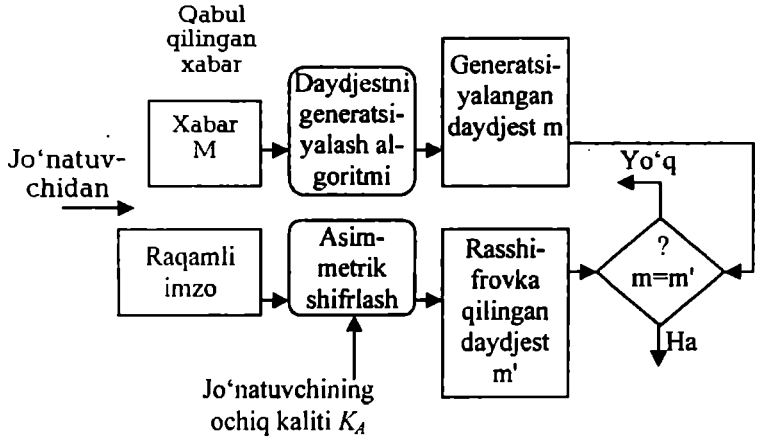
Xesh-funksiya imzo chekiluvchi dastlabki matn «*M*» ni daydjest «*m*» ga zichlashtirishga xizmat qiladi. Daydjest *m*–butun matn «*M*» ni xarakterlovchi bitlarning belgilangan katta bo'lmagan sonidan iborat nisbatan qisqa sondir. So'ngra jo'natuvchi *A* o'zining maxfiy kaliti k_A bilan daydjest «*m*»ni shifrlaydi. Natijada olingan sonlar jufti berilgan «*M*» matn uchun raqamli imzo hisoblanadi. Xabar «*M*» raqamli imzo bilan birgalikda qabul qiluvchining adresiga yuboriladi.



4.15-rasm. Elektron raqamli imzoni shakllantirish sxemasi.

Raqamli imzoni tekshirish muolajasi.

Tarmoq abonentlari olingan xabar «*M*» ning raqamli imzosini ushbu xabarni jo'natuvchining ochiq kaliti K_A yordamida tekshirishlari mumkin (4.16-rasm).



4.16-rasm. Elektron raqamli imzoni tekshirish sxemasi.

Elektron raqamli imzoni tekshirishda xabar «*M*»ni qabul qiluvchi «*B*» qabul qilingan daydjestni jo'natuvchining ochiq kaliti «K_A» yordamida rasshifrovka qiladi. Undan tashqari, qabul qiluvchini o'zi xesh-funksiya *h(M)* yordamida qabul qilingan xabar «*M'*» ning daydjesti «*m'*» ni hisoblaydi va uni rasshifrovka qilingani bilan taqqoslaydi. Agar ikkala daydjest «*m*» va «*m'*» mos kelsa, raqamli imzo haqiqiy hisoblanadi. Aks holda imzo qalbakilashtirilgan yoki axborot mazmuni o'zgartirilgan bo'ladi.

Elektron raqamli imzo tizimining prinsipial jihati– foydalanuvchining elektron raqamli imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirishning mumkin emasligidir. Shuning uchun imzo chekishdagi maxfiy kalitni ruxsatsiz foydalanishdan himoyalash zarur. Elektron raqamli imzoning maxfiy kalitini, simmetrik shifrlash kalitiga o'xshab, shaxsiy kalit elituvchisida, himoyalangan holda saqlash tavfsiya etiladi.

Elektron raqamli imzo chekiluvchi hujjat va maxfiy kalit orqali aniqlanuvchi noyob sondir. Imzo chekiluvchi hujjat sifatida har qanday fayl ishlatilishi mumkin. Imzo chekilgan fayl imzo chekilmaganiga bir yoki bir nechta elektron imzo qo'shilishi orqali yaratiladi.

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

– imzo chekilgan sana;

– ushbu imzo kaliti ta'sirining tugash muddati;

– faylga imzo chekuvchi shaxs xususidagi axborot (F.I.Sh., mansabi, ish joyi);

– imzo chekuvchining indentifikatori (ochiq kalit nomi);

– raqamli imzoning o'zi.

Asimmetrik shifrlashga o'xshash, elektron raqamli imzoni tekshirish uchun ishlatiladigan ochiq kalitning almashtirilishiga yo'l qo'ymaslik lozim. Faraz qilaylik, niyati buzuq odam «*n*» abonent «*B*» kompyuterida saqlanayotgan ochiq kalitlardan, xususan, abonent *A* ning ochiq kaliti K_A dan foydalana oladi. Unda u quyidagi harakatlarini amalga oshirishi mumkin:

– ochiq kalit K_A saqlanayotgan fayldan abonent *A* xususidagi indensifikatsiya axborotini o'qishi;

– ichiga abonent *A* xususidagi indentifikatsiya axborotini yozgan holda shaxsiy juft kalitlari k_n va K_n ni generatsiyalashi;

– abonent Vda saqlanayotgan ochiq kalit $K_A$ni o'zining ochiq kaliti K_n bilan almashtirishi.

So'ngra niyati buzuq odam «n» abonent V ga hujjatlarni o'zining maxfiy kaliti k_n yordamida imzo chekib jo'natishi mumkin. Bu hujjatlar imzosini tekshirishda abonent V abonent A imzo chekkan hujjatlarni va ularning elektron raqamli imzolarini to'g'ri va hech kim tomonidan modifikatsiyalanmagan deb hisoblaydi. Abonent A bilan munosabatlarini bevosita oydinlashtirilishigacha V abonentda olingan hujjatlarning haqiqiyligiga shubha tug'ilmaydi.

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

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

4.7. Kriptografik kalitlarni boshqarish

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

Simmetrik kriptotizimdan foydalanilganda axborot almashinuvida ishtirok etuvchi ikkala tomon avval maxfiy sessiya kaliti, ya'ni almashinuv jarayonida uzatiladigan barcha xabarlarni shifrlash kaliti

bo'yicha kelishishlari lozim. Bu kalitni boshqa barcha bilmasligi va uni vaqti-vaqti bilan jo'natuvchi va qabul qiluvchida bir vaqtda almashtirib turish lozim. Sessiya kaliti bo'yicha kelishish jarayonini kalitlarni almashtirish yoki taqsimlash deb ham yuritiladi.

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

Kalitlarni taqsimlashga quyidagi talablar qo'yiladi:

- taqsimlashning tezkorligi va aniqligi;
- taqsimlanuvchi kalitlarning konfidensialligi va yaxlitligi.

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

1. Kalitlarni taqsimlovchi bitta yoki bir nechta markazlardan foydalanish.
2. Tarmoq foydalanuvchilari o'rtasida kalitlarni to'g'ridan-to'g'ri almashish.

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

Ikkinchi usuldagi muammo – tarmoq subyektlarining haqiqiy ekanligiga ishonch hosil qilishdir.

Kalitlarni taqsimlash masalasi quyidagilarni ta'minlovchi kalitlarni taqsimlash protokolini qurishga keltiriladi:

- seans qatnashchilarining haqiqiyligiga ikkala tomonning tasdig'i;
- seans haqiqiyligining tasdig'i;
- kalitlar almashinuvida xabarlarning minimal sonidan foydalanish.

Birinchi usulga misol tariqasida Kerberos deb ataluvchi kalitlarni autentifikatsiyalash va taqsimlash tizimini ko'rsatish mumkin.

Ikkinchi usulga-tarmoq foydalanuvchilari o'rtasida kalitlarni to'g'ridan-to'g'ri almashishga batafsil to'xtalamiz.

Simmetrik kalitli kriptotizimdan foydalanilganda kriptografik himoyalangan axborot almashinuvini istagan ikkala foydalanuvchi umumiy maxfiy kalitga ega bo'lishlari lozim. Bu foydalanuvchilar umumiy kalitni aloqa kanali bo'yicha xavfsiz almashishlari lozim. Agar

foydalanuvchilar kalitni tez-tez o'zgartirib tursalar kalitni yetkazish jiddiy muammoga aylanadi.

Bu muammoni yechish uchun quyidagi ikkita asosiy usul qo'llaniladi:

1. Simmetrik kriptotizimning maxfiy kalitini himoyalash uchun ochiq kalitli asimmetrik kriptotizimdan foydalanish.

2. Diffi-Xellmanning kalitlarni ochiq taqsimlash tizimidan foydala-nish.

Birinchi usul simmetrik va asimmetrik kalitli kombinatsiyalangan kriptotizim doirasida amalga oshiriladi. Bunday yondashishda simmetrik kriptotizim dastlabki ochiq matnni shifrlash va uzatishda ishlatilsa, ochiq kalitli asimmetrik kriptotizim faqat simmetrik kriptotizimning maxfiy kalitini shifrlash, uzatish va keyingi rasshifrovka qilishda ishlatiladi. Shifrlashning bunday kombinatsiyalangan (gibrid) usuli ochiq kalitli asimmetrik kriptotizimning yuqori maxfiyligi bilan maxfiy kalitli simmetrik kriptotizimning yuqori tezkorligining uyg'unlashishga olib keladi. Bunday yondashish ba'zida *elektron raqamli konvert* sxemasi deb yuritiladi.

Faraz qilaylik, foydalanuvchi A xabar M ni foydalanuvchi V ga himoyalangan uzatish uchun shifrlashning kombinatsiyalangan usulidan foydalanmoqchi. Unda foydalanuvchilarning harakatlari quyidagicha bo'ladi.

Foydalanuvchi A ning harakatlari:

1. Simmetrik seans maxfiy kalit K_S ni yaratadi (masalan, tasodifiy tarzda generatsiyalaydi).

2. Xabar M ni simmetrik seans maxfiy kalit K_S da shifrlaydi.

3. Maxfiy seans kalit K_S ni foydalanuvchi (xabar qabul qiluvchi) Bning ochiq kaliti K_V da shifrlaydi.

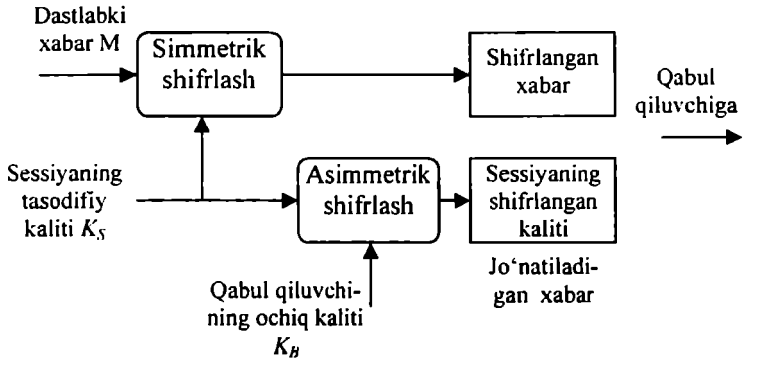
4. Foydalanuvchi V adresiga aloqaning ochiq kanali bo'yicha shifrlangan xabar M ni shifrlangan seans kaliti K_S bilan birgalikda uzatadi.

Foydalanuvchi A ning harakatalarini 4.17-rasmda keltirilgan xabarlarni kombinatsiyalangan usul bo'yicha shifrlash sxemasi orqali tushunish mumkin.

Foydalanuvchi V ning harakatlari (elektron raqamli konvertni shifrlangan xabar M ni va shifrlangan seans kaliti K_S ni olganidan so'nggi) quyidagicha:

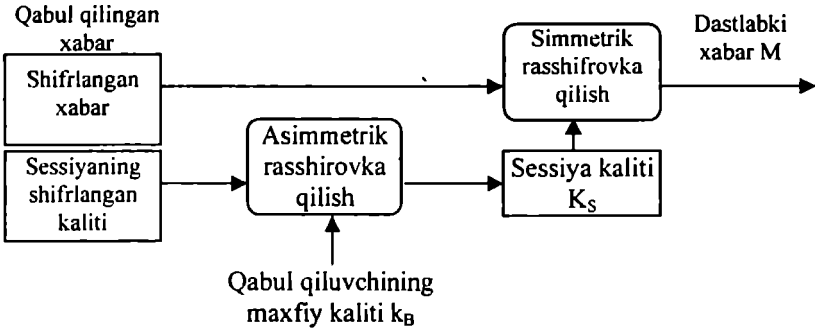
1. O'zining maxfiy kaliti k_V bo'yicha seans kaliti K_S ni rasshifrovka qiladi.

2. Olingan seans kaliti K_S bo'yicha olingan xabar M ni rasshifrovka qiladi.



4.17-rasm. Kombinatsiyalangan usul bo'yicha xabarni shifrlash sxemasi.

Foydalanuvchi V ning harakatlarini 4.18-rasmda keltirilgan xabarlarni kombinatsiyalangan usul bo'yicha rasshifrovka qilish sxemasi orqali tushunish mumkin.



4.18-rasm. Kombinatsiyalangan usul bo'yicha xabarni rasshifrovka qilish sxemasi.

Olingan elektron raqamli konvertni faqat qonuniy qabul qiluvchi-foydalanuvchi V ochishi mumkin. Faqat shaxsiy maxfiy kalit k_V egasi bo'lgan foydalanuvchi V maxfiy seans kaliti K_S ni to'g'ri rasshifrovka qilish va so'ngra bu kalit yordamida olingan xabar M ni rasshifrovka qilishi va o'qishi mumkin.

Raqamli konvert usulida simmetrik va asimmetrik kriptoalgoritmlarning kamchiliklari quyidagicha kompensatsiyalanadi:

- simmetrik kriptoalgoritm kalitlarini tarqatish muammosi bartaraf qilinadi, chunki xabarni shifrlovchi seans kaliti K_S ochiq kanal bo'yicha shifrlangan ko'rinishda uzatiladi, kalit $K_S$ni rasshifrovka qilish uchun asimmetrik kriptoalgoritmdan foydalaniladi;
- bu holda asimmetrik shifrlash tezkorligining sekinligi muammosi paydo bo'lmaydi, chunki asimmetrik algoritm bo'yicha faqat qisqa kalit K_S shifrlanadi, barcha ma'lumotlar esa tezkor simmetrik kriptoalgoritm bo'yicha shifrlanadi.

Natijada tezkor shifrlash bilan birgalikda kalitlarning qulay taqsimlanishi amalga oshiriladi.

Shifrlashning kombinatsiyalangan usulida simmetrik ham asimmetrik kriptotizimlarning kriptografik kalitlaridan foydalaniladi. Ravshanki, kriptotizimning har bir turi uchun kalitlar uzunligini shunday tanlash lozimki, niyati buzuq odamga kombinatsiyalangan kriptotizim himoyasining har qanday mexanizmiga hujum qilish bir xil qiyinchilik tug'dirsin.

4.1-jadvalda ko'p uchraydigan simmetrik va asimmetrik kriptotizimlar kalitlarining uzunligi keltirilgan.

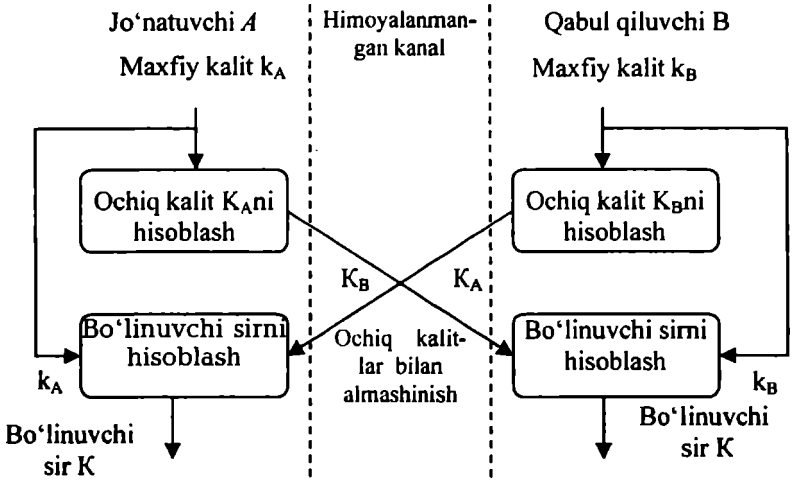
4.1-jadval

Simmetrik kriptotizim kalitlari uzunligi, bitlar	Asimmetrik kriptotizim kalitlari uzunligi, bitlar
56	384
64	512
80	768
112	1792
128	2304

U. Diffi va M.Xellman tomonidan kashf etilgan *kalitlarni ochiq taqsimlash usuli* foydalanuvchilarga kalitlarni himoyalanmagan aloqa kanallari orqali almashishga imkon beradi. Uning xavfsizligi chegara-

langan sohada diskret logarifmlarni hisoblashning mushkulligiga asoslanadi.

Diffi-Xellman usulining mohiyati quyidagicha (4.19-rasm).



4.19-rasm. Diffi-Xellmanning kalitlarni ochiq taqsimlash sxemasi.

Axborot almashinuvida ishtirok etuvchi foydalanuvchilar A va V mustaqil ravishda o'zlarining maxfiy kalitlarini k_A va k_B ni generatsiyalaydilar (k_A va k_B kalitlar – foydalanuvchilar A va V lar sir saqlovchi tasodifiy katta butun sonlar).

So'ngra foydalanuvchi A o'zining maxfiy kaliti k_A asosida ochiq kalitni hisoblaydi:

$$K_A = g^{k_A} (\mathrm{mod}\, N).$$

Bir vaqtning o'zida foydalanuvchi *V* o'zining maxfiy kaliti k_B asosida ochiq kalitni hisoblaydi:

$$K_B = g^{k_B} (\mathrm{mod}\, N).$$

Bu yerda, *N* va *g* – katta butun oddiy sonlar. Arifmetik amallar *N*ning moduliga keltirish orqali bajariladi. *N* va *g* sonlarni sir saqlash shart emas, chunki odatda, bu qiymatlar tarmoq va tizimdan foydalanuvchilarning barchasi uchun umumiy hisoblanadi.

So'ngra foydalanuvchilar A va V o'zlarining ochiq kalitlarini himoyalanmagan kanal orqali almashadilar va umumiy sessiya maxfiy kaliti *K*ni (bo'linuvchi sirni) hisoblashda ishlatadilar:

foydalanuvchi A: $K = (K_B)^{k_A} (\mathrm{mod}\, N) = (g^{k_B})^{k_A} (\mathrm{mod}\, N)$,

foydalanuvchi V: $K' = (K_A)^{k_B} (\mathrm{mod}\, N) = (g^{k_A})^{k_B} (\mathrm{mod}\, N)$,

bunda $K = K'$, chunki $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} (\mathrm{mod}\, N)$.

Shunday qilib, ushbu amallar natijasida ikkala maxfiy kalit k_A va $k_B$larning funksiyasi bo'lgan umumiy sessiya maxfiy kaliti hosil qilinadi.

Ochiq kalitlar K_A va K_V qiymatlarini ushlab qolgan niyati buzuq odam sessiya maxfiy kaliti *K* ni hisoblay olmaydi, chunki u maxfiy kalitlar k_A va k_V qiymatlarini bilmaydi. Bir tomonlama funksiyaning ishlatilishi sababli ochiq kalitni hisoblash amali qaytarilmaydigan amal, ya'ni abonentning ochiq kaliti qiymati bo'yicha uning maxfiy kalitini hisoblash mumkin emas.

Diffi-Xellman usulining noyobligi shundan iboratki, abonentlar jufti tarmoq orqali ochiq kalitlarni uzatganlarida faqat o'zlariga ma'lum maxfiy sonni olish imkoniyatiga ega. So'ngra abonentlar uzatilayotgan axborotni ma'lum tekshirilgan usulni – olingan umumiy sessiya maxfiy kalitidan foydalangan holda simmetrik shifrlashni ishlatib himoyalashga kirishishlari mumkin.

Diffi-Xellman sxemasi ma'lumotlarni har bir seansda yangi kalitlarda shifrlash imkonini beradi. Bu sirlarni disketlarda yoki boshqa eltuvchilarda saqlamaslikka imkon beradi, chunki bunday saqlash ularni raqiblar yoki niyati buzuq odamlar qo'liga tushib qolish ehtimolligini oshiradi.

Diffi-Xellman sxemasi *uzatilayotgan ma'lumotlarning konfidensialligini va autentligini (asliga to'g'riligini) kompleks himoyalash usuli*ni ham amalga oshirish imkonini beradi. Algoritm foydalanuvchiga raqamli imzoni va simmetrik shifrlashni bajarishda bir xil kalitlarni shakllantirish va ishlatish imkonini beradi.

Ma'lumotlar yaxlitligini va konfidensialligini bir vaqtda himoyalash uchun shifrlash va elektron raqamli imzodan kompleks foydalanish maqsadga muvofiq hisoblanadi. Diffi-Xellman sxemasi ishlashining oraliq natijalaridan uzatilayotgan ma'lumotlarning yaxlitligini va konfidensialligini kompleks himoyalash usulini amalga oshirishda foydalanish mumkin. Haqiqatan, ushbu algoritmga binoan foydalanuvchilar *A* va *V* avval o'zlarining maxfiy kalitlari k_A va k_B ni generatsiyalaydilar va

ochiq kalitlari K_A va K_B ni hisoblaydilar. So'ngra abonentlar A va V bu oraliq natijalardan ma'lumotlarni simmetrik shifrlashda foydalanilishi mumkin bo'lgan umumiy bo'linuvchi maxfiy kaliti K ni bir vaqtda hisoblash uchun ishlatadi.

Uzatilayotgan ma'lumotlarning konfidensialligini va autentiligini kompleks himoyalash usuli quyidagi sxema bo'yicha ishlaydi:

– abonent A raqamli imzoning standart algoritmidan foydalanib, o'zining maxfiy kaliti k_A yordamida xabar M ga imzo chekadi;

– abonent A o'zining maxfiy kaliti k_A va abonent V ning ochiq kaliti K_V dan Diffi-Xellman algoritmi bo'yicha umumiy bo'linuvchi maxfiy kaliti K ni hisoblaydi;

– abonent A olingan o'zaro bo'linuvchi maxfiy kalitda almashinuv bo'yicha sherigi bilan kelishilgan simmetrik shifrlash algoritmidan foydalangan holda xabar M ni shifrlaydi;

– abonent V shifrlangan xabar M ni olishi bilan o'zining maxfiy kaliti k_B va abonent A ning ochiq kaliti K_A dan Diffi-Xellman algoritmi bo'yicha o'zaro bo'linuvchi maxfiy kalit K ni hisoblaydi;

– abonent V olingan xabar M ni kaliti K da rasshifrovka qiladi;

– abonent V abonent A ning ochiq kalit K_A yordamida rasshifrovka qilingan xabar M imzosini tekshiradi.

Diffi-Xellman sxemasi asosida tarmoq sathida himoyalangan virtual tarmoqlar VPN qurilishida qo'llaniluvchi kriptokalitlarni boshqarish protokollari SKIP (Simple Key Management for Internet Protocols) va IKE (Internet Key Exchange) ishlaydi.

V bob. IDENTIFIKATSIYA VA AUTENTIFIKATSIYA

5.1. Asosiy tushunchalar va turkumlanishi

Kompyuter tizimida ro'yxatga olingan har bir subyekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma'noda indentifikatsiyalovchi axborot bog'liq.

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

Identifikatsiya (Identification) – foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan 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) haqiqatan aynan o'zi ekanligiga ishonch hosil qilishga imkon beradi. Autentifikatsiya o'tqazishda tekshiruvchi taraf tekshiriluvchi tarafning haqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi. Odatda, foydalanuvchi tizimga o'zi xususidagi noyob, boshqalarga ma'lum bo'lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya va autentifikatsiya subyektlarning (foydalanuvchilarning) 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 konfidensialligi 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 hodisalarini 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'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 memoriy 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 h.k.) asoslangan usullarni oladi. Bu kategoriyada kriptografik usullar va vositalar ishlatilmaydi. Buometrik xarak-

teristikalar binodan yoki qandaydir texnikadan foydalanishni nazorat-lashda 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) parol – bir marta ishlatilganidan so'ng boshqa umuman ishlatilmaydigan parol. Amalda, odatda, doimiy parolga yoki tayanch iboroga asoslanuvchi muntazam o'zgarib turuvchi qiymat ishlatiladi.

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

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 infratuzilmalari 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;

– nollik 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. Shu

bilan bir qatorda ta'kidlash lozimki, nollik 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.

Autentifikatsiya protokollariga bo'ladigan asosiy hujumlar quyidagilar:

– *maskarad* (impersonation). Foydalanuvchi o'zini boshqa shaxs deb ko'rsatishga urinib, u shaxs tarafidan harakatlarning 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 autentifikatsion 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, indentifikatorlar, raqamli imzolar kabi mexanizmlardan foydalanish;

– autentifikatsiya natijasini foydalanuvchilarning tizim doirasidagi keyingi harakatlariga bog'lash. Bunday yondashish misol tariqasida autentifikatsiya jarayonida foydalanuvchilarning keyingi o'zaro aloqalarida ishlatiluvchi maxfiy seans kalitlarini almashishni ko'rsatish mumkin;

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

«So'rov-javob» mexanizmi quyidagicha. Agar foydalanuvchi *A* foydalanuvchi *V* dan oladigan xabari yolg'on emasligiga ishonch hosil qilishni istasa, u foydalanuvchi *V* uchun yuboradigan xabarga oldindan bilib bo'lmaydigan element – *X* so'rovini (masalan, qandaydir tasodifiy sonni) qo'shadi. Foydalanuvchi V javob berishda bu amal ustida ma'lum amalni (masalan, qandaydir *f(X)* funksiyani hisoblash) bajarishi lozim. Buni oldindan bajarib bo'lmaydi, chunki so'rovda qanday tasodifiy son *X* kelishi foydalanuvchi *V* ga ma'lum emas. Foydalanuvchi *V* harakati natijasini olgan foydalanuvchi *A* foydalanuvchi *V* ning haqiqiy ekanligiga ishonch hosil qilishi mumkin. Ushbu usulning kamchiligi – so'rov va javob o'rtasidagi qonuniyatni aniqlash mumkinligi.

Vaqtni belgilash mexanizmi har bir xabar uchun vaqtni qaydlashni ko'zda tutadi. Bunda tarmoqning har bir foydalanuvchisi kelgan xabarning qanchalik eskirganini aniqlashi va uni qabul qilmaslik qaroriga kelishi mumkin, chunki u yolg'on bo'lishi mumkin. Vaqtni belgilashdan foydalanishda seansning haqiqiy ekanligini tasdiqlash uchun *kechikishning joiz vaqt oralig'i* muammosi paydo bo'ladi. Chunki, «vaqt tamg'asi»li xabar, umuman, bir lahzada uzatilishi mumkin emas. Undan tashqari, qabul qiluvchi va jo'natuvchining soatlari mutlaqo sinxronlangan bo'lishi mumkin emas.

Autentifikatsiya protokollarini taqqoslashda va tanlashda quyidagi xarakteristikalarni hisobga olish zarur:

– *o'zaro autentifikatsiyaning mavjudligi.* Ushbu xususiyat autentifikatsion almashinuv taraflari o'rtasida ikkiyoqlama autentifikatsiyaning zarurligini aks ettiradi;

– *hisoblash samaradorligi.* Protokolni bajarishda zarur bo'lgan amallar soni;

– *kommunikatsion samaradorlik.* Ushbu xususiyat autentifikatsiyani bajarish uchun zarur bo'lgan xabar soni va uzunligini aks ettiradi;

– *uchinchi tarafning mavjudligi.* Uchinchi tarafga misol tariqasida simmetrik kalitlarni taqsimlovchi ishonchli serverni yoki ochiq kalitlarni taqsimlash uchun sertifikatlar daraxtini amalga oshiruvchi serverni ko'rsatish mumkin;

– *xavfsizlik kafolati asosi.* Misol sifatida nollik bilim bilan isbotlash xususiyatiga ega bo'lgan protokollarni ko'rsatish mumkin;

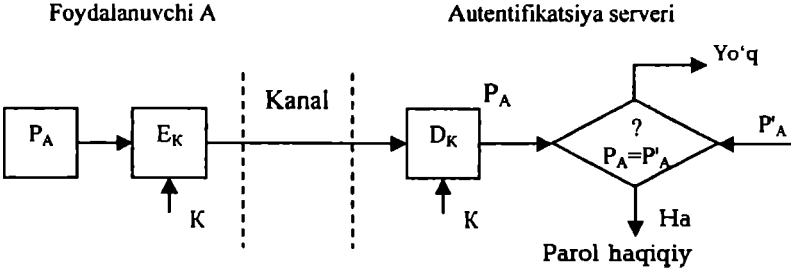
– *sirni saqlash.* Jiddiy kalitli axborotni saqlash usuli ko'zda tutiladi.

5.2. 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 huquqlarni va tarmoq resurslaridan foydalanishga ruxsatni oladi.

Paroldan foydalangan holda oddiy autentifikatsiyalash sxemasi 5.1-rasmda keltirilgan.

Ravshanki, foydalanuvchining parolini shifrlamasdan uzatish orqali autentifikatsiyalash varianti xavfsizlikning hatto minimal darajasini kafolatlamaydi. Parolni himoyalash uchun uni himoyalanmagan kanal orqali uzatishdan oldin shifrlash zarur. Buning uchun sxemaga shifrlash E_k va rasshifrovka qilish D_k vositalari kiritilgan. Bu vositalar bo'linuvchi maxfiy kalit K orqali boshqariladi. Foydalanuvchining haqiqiyligini tekshirish foydalanuvchi yuborgan parol P_A bilan autentifikatsiya serverida saqlanuvchi dastlabki qiymat P'_A ni taqqoslashga asoslangan. Agar P_A va P'_A qiymatlar mos kelsa, parol P_A haqiqiy, foydalanuvchi A esa qonuniy hisoblanadi.



5.1-rasm. Paroldan foydalangan holda oddiy autentifikatsiyalash.

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 funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi – niyati buzuq odamning tizimda ma'mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan, parol fayllaridan foydalanish imkoniyatidir.

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

Ko'p martali parollarga asoslangan oddiy autentifikatsiyalash 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 miniatur 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:

1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.

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

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

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

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

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

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

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo'lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar gen-

eratoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

• *o'zgartiriluvchi bir martali parollar ketma-ketligi.* Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;

• *bir tomonlama funksiyaga asoslangan parollar ketma-ketligi.* Ushbu usulning mohiyatini bir tomonlama funksiyaning ketma-ket ishlatilishi (Lamportning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o'zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

Keng tarqaigan bir martali paroldan foydalanishga asoslangan autentifikatsiyalash protokollaridan biri Internetda standartlashtirilgan S/Key (RFC1760) protokolidir. Ushbu protokol masofadagi foydalanuvchilarning haqiqiyligini tekshirishni talab etuvchi ko'pgina tizimlarda, xususan, Cisco kompaniyasining TACACS+tizimida amalga oshirilgan.

5.3. Sertifikatlar asosida autentifikatsiyalash

Tarmoqdan foydalanuvchilar soni millionlab o'lchanganida foydalanuvchilar parollarining tayinlanishi va saqlanishi bilan bog'liq foydalanuvchilarni dastlabki ro'yxatga olish muolajasi juda katta va amalga oshirilishi qiyin bo'ladi. Bunday sharoitda raqamli sertifikatlar asosidagi autentifikatsiyalash parollar qo'llanishiga ratsional alternativ hisoblanadi.

Raqamli sertifikatlar ishlatilganida kompyuter tarmog'i foydalanuvchilar xususidagi hech qanday axborotni saqlamaydi. Bunday axborotni foydalanuvchilarning o'zi so'rov-sertifikatlarida taqdim etadilar. Bunda maxfiy axborotni, xususan maxfiy kalitlarni saqlash vazifasi foydalanuvchilarning o'ziga yuklanadi.

Foydalanuvchi shaxsini tasdiqlovchi raqamli sertifikatlar foydalanuvchilar so'rovi bo'yicha maxsus vakolatli tashkilot-sertifikatsiya markazi CA (Certificate Authority) tomonidan, ma'lum shartlar bajarilganida beriladi. Ta'kidlash lozimki, sertifikat olish muolajasining o'zi ham foydalanuvchining haqiqiyligini tekshirish (ya'ni autentifikatsiyalash) bosqichini o'z ichiga oladi. Bunda tekshiruvchi taraf sertifikatsiyalovchi tashkilot (sertifikatsiya markazi SA) bo'ladi.

Sertifikat olish uchun mijoz sertifikatsiya markaziga shaxsini tasdiqlovchi ma'lumotni va ochiq kalitini taqdim etishi lozim. Zaruriy

ma'lumotlar ro'yxati olinadigan sertifikat turiga bog'liq. Sertifikatsiyalovchi tashkilot foydalanuvchining haqiqiyligi tasdig'ini tekshirganidan so'ng o'zining raqamli imzosini ochiq kalit va foydalanuvchi xususidagi ma'lumot bo'lgan faylga joylashtiradi hamda ushbu ochiq kalitning muayyan shaxsga tegishli ekanligini tasdiqlagan holda foydalanuvchiga sertifikat beradi.

Sertifikat elektron shakl bo'lib, tarkibida quyidagi axborot bo'ladi:

– ushbu sertifikat egasining ochiq kaliti;

– sertifikat egasi xususidagi ma'lumot, masalan, ismi, elektron pochta adresi, ishlaydigan tashkilot nomi va h.;

– ushbu sertifikatni bergan tashkilot nomi;

– sertifikatsiyalovchi tashkilotning elektron imzosi – ushbu tashkilotning maxfiy kaliti yordamida shifrlangan sertifikatsiyadagi ma'lumotlar.

Sertifikat foydalanuvchini tarmoq resurslariga murojaat etganida autentifikatsiyalovchi vosita hisoblanadi. Bunda tekshiruvchi taraf vazifasini korporativ tarmoqning autentifikatsiya serveri bajaradi. Sertifikatlar nafaqat autentifikatsiyalashda, balki foydalanishning ma'lum huquqlarini taqdim etishda ishlatilishi mumkin. Buning uchun sertifikatga qo'shimcha hoshiyalar kiritilib ularda sertifikatsiya egasining foydalanuvchilarning u yoki bu kategoriyasiga mansubligi ko'rsatiladi.

Ochiq kalitlarning sertifikatlar bilan uzviy bog'liqligini alohida ta'kidlash lozim. Sertifikat nafaqat shaxsni, balki ochiq kalit mansubligini tasdiqlovchi hujjatdir. Raqamli sertifikat ochiq kalit va uning egasi o'rtasidagi moslikni o'rnatadi va kafolatlaydi. Bu ochiq kalitni almashtirish xavfini bartaraf etadi.

Agar abonent axborot almashinuvi bo'yicha sherigidan sertifikat tarkibidagi ochiq kalitni olsa, u bu sertifikatdagi sertifikatsiya markazining raqamli imzosini ushbu sertifikatsiya markazining ochiq kaliti yordamida tekshirishi va ochiq kalit adresi va boshqa ma'lumotlari sertifikatda ko'rsatilgan foydalanuvchiga tegishli ekanligiga ishonch hosil qilishi mumkin. Sertifikatlardan foydalanilganda foydalanuvchilar ro'yxatini ularning parollari bilan korporatsiya serverlarida saqlash zaruriyati yo'qoladi. Serverda sertifikatsiyalovchi tashkilotlarning nomlari va ochiq kalitlarining bo'lishi yetarli.

Sertifikatlarning ishlatilishi sertifikatsiyalovchi tashkilotlarning nisbatan kamligiga va ularning ochiq kalitlaridan qiziqqan barcha shaxslar va tashkilotlar foydalana olishi (masalan, jurnallardagi nashrlar yordamida) taxminiga asoslangan.

Sertifikatlar asosida autentifikatsiyalash jarayonini amalga oshirishda sertifikatsiyalovchi tashkilot vazifasini kim bajarishi xususidagi masalani yechish muhim hisoblanadi. Xodimlarni sertifikat bilan ta'minlash masalasini korxonaning o'zi yechishi juda tabiiy hisoblanadi. Korxona o'zining xodimlarini yaxshi biladi va ular shaxsini tasdiqlash vazifasini o'ziga olishi mumkin. Bu sertifikat berilishidagi dastlabki autentifikatsiyalash muolajasini osonlashtiradi. Korxonalar sertifikatlarni generatsiyalash, berish va ularga xizmat ko'rsatish jarayonlarini avtomatlashtirishni ta'minlovchi mavjud dasturiy mahsulotlardan foydalanishlari mumkin. Masalan, Netscape Communi-cations kompaniyasi serverlarini korxonalarga shaxsiy sertifikatlarini chiqarish uchun taklif etadi.

Sertifikatsiyalovchi tashkilot vazifasini bajarishda tijorat asosida sertifikat berish bo'yicha mustaqil markazlar ham jalb etilishi mumkin. Bunday xizmatlarni, xususan, Verisign kompaniyasining sertifikatsiyalovchi markazi taklif etadi. Bu kompaniyaning sertifikatlari xalqaro standart X.509 talablariga javob beradi. Bu sertifikatlar ma'lumotlar himoyasining qator mahsulotlarida, jumladan, himoyalangan kanal SSL protokolida ishlatiladi.

5.4. Qat'iy autentifikatsiyalash

Kriptografik protokollarida amalga oshiriluvchi qat'iy autentifikatsiyalash g'oyasi quyidagicha. Tekshiriluvchi (isbotlovchi) taraf qandaydir sirni bilishini namoyish etgan holda tekshiruvchiga o'zining haqiqiy ekanligini isbotlaydi. Masalan, bu sir autentifikatsion almashish taraflari o'rtasida oldindan xavfsiz usul bilan taqsimlangan bo'lishi mumkin. Sirni bilishlik isboti kriptografik usul va vositalardan foydalanilgan holda so'rov va javob ketma-ketligi yordamida amalga oshiriladi.

Eng muhimi, isbotlovchi taraf faqat sirni bilishligini namoyish etadi, sirni o'zi esa autentifikatsion almashish mobaynida ochilmaydi. Bu tekshiruvchi tarafning turli so'rovlariga isbotlovchi tarafning javoblari yordami bilan ta'minlanadi. Bunda yakuniy so'rov faqat foydalanuvchi siriga va protokol boshlanishida ixtiyoriy tanlangan katta sondan iborat boshlang'ich so'rovga bog'liq bo'ladi.

Aksariyat hollarda qat'iy autentifikatsiyalashga binoan har bir foydalanuvchi o'zining maxfiy kalitiga egaligi alomati bo'yicha autentifikatsiyalanadi. Boshqacha aytganda foydalanuvchi aloqa bo'yicha

sherigining tegishli maxfiy kalitga egaligini va u bu kalitni axborot almashinuvi bo'yicha haqiqiy sherik ekanligini isbotlashga ishlata olishi mumkinligini aniqlash imkoniyatiga ega.

X.509 standarti tavsiyalariga binoan qat'iy autentifikatsiyalashning quyidagi muolajalari farqlanadi:

– bir tomonlama autentifikatsiya;

– ikki tomonlama autentifikatsiya;

– uch tomonlama autentifikatsiya.

Bir tomonlama autentifikatsiyalash bir tomonga yo'naltirilgan axborot almashinuvini ko'zda tutadi. Autentifikatsiyaning bu turi quyidagilarga imkon yaratadi:

– axborot almashinuvchining faqat bir tarafini haqiqiyligini tasdiqlash;

– uzatilayotgan axborot yaxlitligining buzilishini aniqlash;

– «uzatishning takrori» tipidagi hujumni aniqlash;

– uzatilayotgan autentifikatsion ma'lumotlardan faqat tekshiruvchi taraf foydalanishini kafolatlash.

Ikki tomonlama autentifikatsilashda bir tomonliligiga nisbatan isbotlovchi tarafga tekshiruvchi tarafning qo'shimcha javobi bo'ladi. Bu javob tekshiruvchi tomonni aloqaning aynan autentifikatsiya ma'lumotlari mo'ljallangan taraf bilan o'rnatilayotganiga ishontirishi lozim.

Uch tomonlama autentifikatsiyalash tarkibida isbotlovchi tarafdan tekshiruvchi tarafga qo'shimcha ma'lumotlar uzatish mavjud. Bunday yondashish autentifikatsiya o'tkazishda vaqt belgilaridan foydalanishdan voz kechishga imkon beradi.

Ta'kidlash lozimki, ushbu turkumlash shartlidir. Amalda ishlatiluvchi usul va vositalar to'plami autentifikatsiya jarayonini amalga oshirishdagi muayyan shart-sharoitlarga bog'liq. Qat'iy autentifikatsiyaning o'tkazilishi ishlatiladigan kriptografik algoritmlar va qator qo'shimcha parametrlarni taraflar tomonidan so'zsiz muvofiqlashtirishni talab etadi.

Qat'iy autentifikatsiyalashning muayyan variantlarini ko'rishdan oldin bir martali parametrlarning vazifalari va imkoniyatlariga to'xtash lozim. Bir martali parametrlar ba'zida «nonces» – bir maqsadga bir martadan ortiq ishlatilmaydigan kattalik deb ataladi.

Hozirda ishlatiladigan bir martali parametrlardan tasodifiy sonlar, vaqt belgilari va ketma-ketliklarning nomerlarini ko'rsatish mumkin.

Bir martali parametrlar uzatishning takrorlanishini, autentifikatsion almashinuv taraflarini almashtirib qo'yishni va ochiq matnni tanlash

bilan hujum qilishni oldini olishga imkon beradi. Bir martali parametrlar yordamida uzatiladigan xabarlarning noyobligini, bir ma'noliligini va vaqtiy kafolatlarini ta'minlash mumkin. Bir martali parametrlarning turli xillari alohida ishlatilishi yoki bir-birini to'ldirishi mumkin.

Bir martali parametrlarning quyidagi ishlatilish misollarini ko'rsatish mumkin:

– «so'rov-javob» prinsipida qurilgan protokollarda o'z vaqtidaligini tekshirish. Bunday tekshirishda tasodifiy sonlar, soatlarni sinxronlash bilan vaqt belgilari yoki muayyan juft (tekshiruvchi, isbotlovchi) uchun ketma-ketliklarning nomerlaridan foydalanish mumkin;

– o'z vaqtidaligini yoki noyoblik kafolatini ta'minlash. Protokolning bir martali parametrlarini bevosita (tasodifiy sonni tanlash yo'li bilan) yoki bilvosita (bo'linuvchi sirdagi axborotni tahlillash yordamida) nazoratlash orqali amalga oshiriladi;

– xabarni yoki xabarlar ketma-ketligini bir ma'noli identifikatsiyalash. Bir ohangda o'suvchi ketma-ketlikning bir martali qiymatini (masalan, seriya nomerlari yoki vaqt belgilari ketma-ketligi) yoki mos uzunlikdagi tasodifiy sonlarni tuzish orqali amalga oshiriladi.

Ta'kidlash lozimki, bir martali parametrlar kriptografik protokollarning boshqa variantlarida ham (masalan, kalit axborotini taqsimlash protokollarida) keng qo'llaniladi.

Qat'iy autentifikatsiyalash protokollarini qo'llaniladigan kriptografik algoritmlariga bog'liq holda quyidagi guruhlarga ajratish mumkin:

– shifrlashning simmetrik algoritmlari asosidagi qat'iy autentifikatsiyalash protokollari;

– bir tomonlama kalitli xesh-funksiyalar asosidagi qat'iy autentifikatsiyalash protokollari;

– shifrlashning asimmetrik algoritmlari asosidagi qat'iy autentifikatsiyalash protokollari;

– elektron raqamli imzo algoritmlari asosidagi qat'iy autentifikatsiyalash protokollari.

Simmetrik algoritmlarga asoslangan qat'iy autentifikatsiyalash Kerberos protokoli

Simmetrik algoritmlar asosida qurilgan autentifikatsiyalashning ishlashi uchun tekshiruvchi va isbotlovchi ayni boshidan bitta maxfiy kalitga ega bo'lishlari zarur. Foydalanuvchilari ko'p bo'lmagan yopiq tizimlar uchun foydalanuvchilarning har bir jufti maxfiy kalitni o'zaro bo'lib olishlari mumkin. Simmetrik shifrlash texnologiyasini qo'llovchi katta taqsimlangan tizimlarda ishonchli server qatnashuvidagi autentifi-

katsiyalash protokollaridan foydalaniladi. Bu server bilan har bir taraf kalitni bilishligini o'rtoqlashishadi.

Ushbu yondashish sodda bo'lib tuyulsada, aslida bunday autentifikatsiyalash protokolini ishlab chiqish murakkab va xavfsizlik nuqtai nazaridan shubhasiz emas.

Quyida shifrlashning simmetrik algoritmlariga asoslangan, ISO/IEC 9798-2da spetsifikatsiyalangan autentifikatsiyalash protocollarining uchta misoli keltirilgan. Bu protokollar bo'linuvchi maxfiy kalitlarni oldindan taqsimlanishini ko'zda tutadi. Autentifikatsiyalashning quyidagi variantlarini ko'rib chiqamiz.

– vaqt belgilaridan foydalanuvchi bir tomonlama autentifikatsiyalash;

– tasodifiy sonlardan foydalanuvchi bir tomonlama autentifikatsiyalash;

– ikki tomonlama autentifikatsiyalash.

Bu variantlarning har birida foydalanuvchi maxfiy kalitni bilishini namoyish qilgan holda, o'zining haqiqiyligini isbotlaydi, chunki ushbu maxfiy kalit yordamida so'rovlarni rasshifrovka qiladi. Autentifikatsiyalash jarayonida simmetrik shifrlashni qo'llashda uzatiladigan ma'lumotlarning yaxlitligini ta'minlash mexanizmini rasm bo'lib qolgan usullar asosida amalga oshirish ham zarur.

Quyidagi belgilashlarni kiritamiz:

r_A- qatnashuvchi A generatsiyalagan tasodifiy son;

r_V- qatnashuvchi V generatsiyalagan tasodifiy son;

t_A- qatnashuvchi A generatsiyalagan vaqt belgisi;

E_K- kalit Kda simmetrik shifrlash (kalit K oldindan A va V o'rtasida taqsimlanishi shart).

Vaqt belgilariga asoslangan bir tomonlama autentifikatsiyalash:

$A \rightarrow B: E_K(t_A, B)$ (1)

Ushbu xabarni olib rasshifrovka qilganidan so'ng qatnashuvchi V vaqt metkasi t_A haqiqiy ekanligiga va xabarda ko'rsatilgan identifikator o'ziniki bilan mos kelishiga ishonch hosil qiladi. Ushbu xabarni qaytadan uzatishni oldini olish kalitni bilmasdan turib vaqt metkasi t_A ni va indentifikator Vni o'zgartirish mumkin emasligiga asoslanadi.

Tasodifiy sonlardan foydalanishga asoslangan bir tomonlama autenti-fikatsiyalash:

$$A \leftarrow B: r_B \quad (1)$$

$$A \rightarrow B: E_K(r_B, B) \quad (2)$$

Qatnashuvchi V qatnashuvchi A ga tasodifiy son r_B ni jo'natadi. Qatnashuvchi A olingan son r_B va identifikator V dan iborat xabarni shifrlaydi va shifrlangan xabarni qatnashuvchi V ga jo'natadi. Qatnashuvchi V olingan xabarni rasshifrovka qiladi va xabardagi tasodifiy sonni qatnashuvchi Aga yuborgani bilan taqqoslaydi. Qo'shimcha u xabardagi ismni tekshiradi.

Tasodifiy qiymatlardan foydalanuvchi ikki tomonlama autentifikatsiyalash:

$$A \leftarrow B : r_B \tag{1}$$

$$A \rightarrow B : E_K(r_A, r_B, B) \tag{2}$$

$$A \leftarrow B : E_K(r_A, r_B) \tag{3}$$

Ikkinchi axborotni olishi bilan qatnashuvchi V oldingi protokoldagi tekshirishni amalga oshiradi va qatnashuvchi A ga atalgan uchinchi xabarga kiritish uchun qo'shimcha tasodifiy son r_A ni rasshifrovka qiladi. Qatnashuvchi A uchinchi xabarni olganidan so'ng r_A va r_B larning qiymatlarini tekshirish asosida aynan qatnashuvchi V bilan ishlayotganiga ishonch hosil qiladi.

Autentifikatsiya jarayonida uchinchi tarafni jalb etish bilan foydalanuvchilarni autentifikatsiyalashni ta'minlovchi protokollarning mashhur namunalari sifatida Nidxem va Shrederning maxfiy kalitlarni taqsimlash protokolini va Kerberos protokolini ko'rsatish mumkin.

Kerberos protokoli «mijoz-server» lokal va global tarmoqlarda ishlovchi abonentlar orasida aloqaning himoyalangan kanalini o'rnatishga atalgan kalit axborotini almashish tizimlarida autentifikatsiyalash uchun ishlatiladi. Bu protokolning **Microsoft Windows** 2000 va **UNIX BSD** operatsion tizimlariga autentifikat-siyalashning asosiy protokoli sifatida o'rnatilganligi alohida qiziqish uyg'otadi.

Kerberos ishonch qozonmagan tarmoqlarda autentifikatsiyalashni ta'minlaydi, ya'ni Kerberos ishlashida niyati buzuq odamlar quyidagi harakatlarni bajarishlari mumkin:

– o'zini tarmoq ulanishining e'tirof etilgan taraflaridan biri deb ko'rsatish;

– ulanishda ishtirok etayotgan kompyuterlarning biridan foydalana olish;

– har qanday paketni ushlab qolish, ularni modifikatsiyalash va/yoki ikkinchi marta uzatish.

Kerberos protokolida xavfsizlik ta'minoti yuqorida keltirilgan niyati buzuq odamlarning harakatlari natijasida paydo bo'ladigan har qanday muammolarning betaraflanishini ta'minlaydi.

Kerberos protokoli oldingi asrning 80-yillarida yaratilgan va shu paytgacha beshta versiyada o'z aksini topgan qator jiddiy o'zgarishlarga duchor bo'ldi.

Kerberos **TCP/IP** tarmoqlari uchun yaratilgan bo'lib, protokol qatnashchilarining uchinchi(ishonilgan) tarafga ishonishlari asosiga qurilgan. Tarmoqda ishlovchi Kerberos xizmati ishonilgan vositachi sifatida harakat qilib, tarmoq resurslaridan mijozning (mijoz ilovasining) foydalinishini avtorizatsiyalash bilan tarmoqda ishonchli autentifikatsiyalashni ta'minlaydi. Kerberos xizmati alohida maxfiy kalitni tarmoqning har bir subyekti bilan bo'lishadi va bunday maxfiy kalitni bilish tarmoq subyekti haqiqiyligining isbotiga teng kuchlidir.

Kerberos asosini Nidxem-Shrederning uchinchi ishonilgan taraf bilan autentifikatsiyalash va kalitlarni taqsimlash protokoli tashkil etadi. Nidxem-Shreder protokolining ushbu versiyasini Kerberosga tatbiqan ko'raylik. Kerberos protokolida (5-versiya) aloqa qiluvchi ikkita taraf va kalitlarni taqsimlash markazi KDC (Key Distribution Center) vazifasini bajaruvchi ishonilgan server KS ishtirok etadi.

Chaqiruvchi obyekt A orqali, chaqiriluvchi obyekt V orqali belgilanadi. Seans qatnashchilari, mos holda Id_A va Id_B noyob identifikatorlarga ega. A va V taraflar, har biri alohida, o'zining maxfiy kalitini server KS bilan bo'lishadi.

Aytaylik, A taraf V taraf bilan axborot almashish maqsadida seans kalitini olmoqchi. A taraf tarmoq orqali server KSga Id_A va Id_B identifikatorlarni yuborish bilan kalitlar taqsimlanishi davrini boshlab beradi:

$$A \rightarrow KS : Id_A, Id_B$$

Server KS vaqtiy belgi T, ta'sir muddati L, tasodifiy kalit K va identfikator Id_A bo'lgan xabarni generatsiyalab, bu xabarni V taraf bilan bo'lingan maxfiy kalit yordamida shifrlaydi.

So'ngra server KS V tarafga tegishli vaqtiy belgi T, ta'sir muddati L, tasodifiy kalit K, identifikator Id_V ni olib uni A taraf bilan bo'lingan maxfiy kalit yordamida shifrlaydi. Bu ikkala shifrlangan xabarlarni A tarafga jo'natadi.

$$KS \rightarrow A : E_A(T, L, K, Id_B), E_B(T, L, K, Id_A)$$

A taraf birinchi xabarni o'zining maxfiy kaliti bilan rasshifrovka qiladi va ushbu xabar kalitlar taqsimotining oldingi muolajasining qaytarilishi emasligiga ishonch hosil qilish maqsadida vaqt belgisi T ni

tekshiradi. So'ngra A taraf o'zining identifikatori Id_A va vaqt belgisi bilan xabarni generatsiyalab, uni seans kaliti K yordamida shifrlaydi va V tarafga uzatadi. Undan tashqari, A taraf V taraf uchun KS dan V taraf kaliti yordamida shifrlangan xabarni jo'natadi:

$$A \rightarrow B : E_K(Id_A, T), E_B(T, L, K, Id_A)$$

Bu xabarni faqat V taraf rasshifrovaka qilishi mumkin. V taraf vaqt belgisi T, ta'sir muddati L, seans kaliti K va identifikator Id_A ni oladi. So'ngra V taraf seans kalit K yordamida xabarning ikkinchi qismini rasshifrovka qiladi. Xabarning ikkala qismidagi T va Id_A qiymatlarining mos kelishi A ning V ga nisbatan haqiqiyligini tasdiqlaydi.

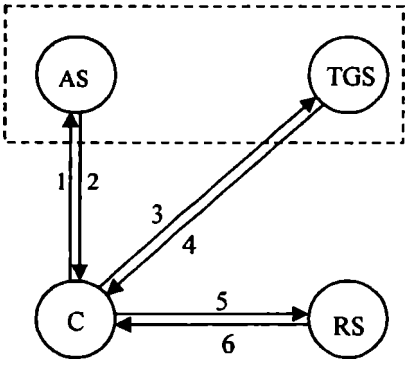
Haqiqiylikni o'zaro tasdiqlash maqsadida V taraf vaqt belgisi T plus 1 dan iborat xabar yaratadi, uni K kalit yordamida shifrlaydi va A tarafga jo'natadi.

$$B \rightarrow A : E_K(T+1)$$

Agar bu xabar rasshifrovka qilinganidan keyin A taraf kutilgan natijani olsa, u aloqa liniyasining boshqa tarafida haqiqatan V turganligiga ishonch hosil qiladi.

Bu protokol barcha qatnashuvchilarning soatlari server KS soatlari bilan sinxronlanganida muvaffaqiyatli ishlaydi. Ta'kidlash lozimki, bu protokolda A tarafning V taraf bilan aloqa o'rnatishga har bir xohishida seans kalitini olish uchun KS bilan almashinuv zarur bo'ladi. Protokolning A va V obyektlarni ishonchli ulashi uchun, hech bir kalit obro'sizlanmasligi va server KS ning himoyalanishi talab etiladi.

Umuman *Kerberos* tizimida (5 versiya) foydalanuvchini identifikatsiyalash va autentifikatsiyalash jarayonini quyidagicha tavsiflash mumkin (5.2-rasm).



Belgilashlar:
KS – Kerberos tizimi serveri
AS – autentifikatsiya serveri
TGS – mandatlarni ajratish xizmati serveri
RS – axborot resurslari serveri
C – Kerberos tizimining mijozi

5.2-rasm. Kerberos protokolining ishlash sxemasi.

Mijoz *S*, tarmoq resursidan foydalanish maqsadida autentifikatsiya serveri *AS* ga so'rov yo'llaydi. Server *AS* foydalanuvchini uning ismi va paroli yordamida identifikatsiyalaydi va mijozga mandat ajratish xizmati serveri *TGS*dan (*Ticket Grating Service*) foydalanishga mandat yuboradi.

Axborot resurslarining muayyan maqsadli serveri *RS* dan foydalanish uchun mijoz *S TGS* dan maqsadli server *RS* ga murojaat qilishga mandat so'raydi. Hamma narsa tartibda bo'lsa *TGS* kerakli tarmoq resurslaridan foydalanishga ruxsat berib, klient *S* ga mos mandatni yuboradi.

Kerberos tizimi ishlashining asosiy qadamlari (5.2 -rasmga qaralsin):

1. $C \rightarrow AS$ – mijoz *S* ning *TGS* xizmatiga murojaat qilishga ruxsat so'rab server *AS*dan so'rovi.

2. $AS \rightarrow C$ – server *AS* ning mijoz *S* ga *TGS* xizmatidan foydalanishga ruxsati (mandati).

3. $C \rightarrow TGS$ – mijoz *S* ning resurslar serveri *RS* dan foydalanishga ruxsat (mandat) so'rab, *TGS* xizmatidan so'rovi.

4. $TGS \rightarrow C$ – *TGS* xizmatining mijoz *S* ga resurslar serveri *RS* dan foydalanishiga ruxsati (mandati).

5. $C \rightarrow RS$ – server *RS* dan axborot resursining (xizmatning) so'rovi.

6. $RS \rightarrow C$ – server *RS* ning haqiqiyligini tasdiqlash va mijoz *S* ga axborot resursini (xizmatni) taqdim etish.

Mijoz bilan server aloqasining ushbu modeli faqat uzatiladigan boshqaruvchi axborotning konfidensialligi va yaxlitligi ta'minlanganida ishlashi mumkin. Axborot xavfsizligini qat'iy ta'minlamasdan *AS, TGS* va *RS* serverlarga mijoz *S* so'rov yuboraolmaydi va tarmoq xizmatidan foydala-nishga ruxsat ololmaydi.

Axborotning ushlab qolinishi va ruxsatsiz foydalanishi imkoniyat-larini bartaraf etish maqsadida Kerberos tarmoqda har qanday boshqar-ish axboroti uzatilganida maxfiy kalitlar kompleksi (mijozning maxfiy kaliti, server-ning maxfiy kaliti, mijoz-server juftining maxfiy seans kalitlari) yordamida ko'p marta shifrlashni ishlatadi. Kerberos shifrlash-ning simmetrik algoritmlaridan va xesh-funksiyalardan foydalanishi mumkin, ammo madadlash uchun Triple DES va MD5 algoritmlari o'rnatilgan.

Kerberos tizimida ishonch hujjatlarining ikki turidan foydalaniladi: mandat (ticket) va autentifikator (authentifacator).

Mandat serverga mandat berilgan mijozning identifikatsion ma'lumotlarini xavfsiz uzatish uchun ishlatiladi. Uning tarkibida ax-borot ham bo'lib, undan server mandatdan foydalanayotgan mijozning haqiqiy ekanligini tekshirishda foydalanishi mumkin.

Autentifikator – mandat bilan birga ko'rsatiluvchi qo'shimcha atribut(alomat). Quyida Kerberos hujjatlarida ishlatiluvchi belgilashlar tizimi keltirilgan:

S – mijoz;

S – server;

a – mijozning tarmoq adresi;

v – mandat ta'siri vaqtining boshlanishi va oxiri;

t – vaqt belgisi;

K_x – maxfiy kalit x;

K_{xy} – x va y uchun seans kaliti;

$\{m\}K_x$ – subyekt x ning maxfiy kaliti K_x bilan shifrlangan xabar m;

$T_{x,y}$ – y dan foydalanishga mandat x;

$A_{x,y}$ – x va y uchun autentifikator.

Kerberos mandati

Kerberos mandati quyidagi shaklga ega: $T_{c,s} = S, \{C, a, v, K_{C,S}\}K_S$.

Mandat bitta mijozga qat'iy belgilangan serverdan foydalanish uchun qat'iy belgilangan vaqtga beriladi. Uning tarkibida mijoz ismi, uning tarmoq adresi, mijoz harakatining boshlanish va tugash vaqti va

serverning maxfiy kaliti K_S shifrlangan seans kaliti $K_{C,S}$ bo'ladi. Mijoz mandatni rasshifrovka qilaolmaydi (u serverning maxfiy kalitini bilmaydi), ammo u mandatni shifrlangan shaklda serverga ko'rsatishi mumkin. Mandat tarmoq orqali uzatilayotganda tarmoqdagi yashirincha eshitib turuvchilarning birortasi ham uni o'qiy olmaydi va o'zgartira olmaydi.

Kerberos autentifikatori

Kerberos autentifikatori quyidagi shaklga ega: $A_{C,S} = \{C, t, kalit\}K_{C,S}$

Mijoz maqsadli serverdan foydalanishni xohlaganida autentifikatorni yaratadi. Uning tarkibida mijoz va server uchun umumiy bo'lgan seans kaliti $K_{C,S}$ shifrlangan mijoz ismi, vaqt belgisi, seans kaliti bo'ladi. Mandatdan farqli holda autentifikator bir marta ishlatiladi.

Autentifikatorning ishlatilishi ikkita maqsadni ko'zlaydi. Birinchidan, autentifikatorda seans kalitida shifrlangan qandaydir matn bo'ladi. Bu kalitning mijozga ma'lumligidan dalolat beradi. Ikkinchidan, shifrlangan ochiq matnda vaqt belgisi mavjud. Bu vaqt belgisi autentifikator va mandatni ushlab qolgan niyati buzuq odamga ulardan biror vaqt o'tganidan so'ng autentifikatsiyalash muolajasini o'tishda ishlatishiga imkon bermaydi.

Kerberos xabarlari

Kerberosning 5-versiyasida xabarlarning quyidagi turlari ishlatiladi (5.2-rasmga qaralsin).

1. Mijoz – Kerberos: *C, tgs.*
2. Kerberos – mijoz : $\{K_{c,tgs}\}K_c\{T_{cftgs}\}K_{tgs}$.
3. Mijoz – *TGS* : $\{A_{C,S}\}K_{C,tgs}(T_{C,tgs})K_{tgs,S}$.
4. TGS – mijoz: $\{K_{C,S}\}K_{C,tgs}\{T_{C,S}\}K_S$,.
5. Mijoz – server: $\{A_{C,S}\}K_{C,S}\{T_{C,S}\}K_S$.

Ushbu xabarlardan foydalanishni batafsil ko'raylik.

Dastlabki mandatni olish

Mijozdan shaxsini isbotlovchi axborotning qismi – uning paroli mavjud. Mijozni parolini tarmoq orqali jo'natishiga majbur qilib bo'lmaydi. Kerberos protokoli parolni obro'sizlantirish ehtimolini minimallashtiradi, agar foydalanuvchi parolni bilmasa, unga o'zini to'g'ri identifikatsiyalashga imkon bermaydi.

Mijoz Kerberosning autentifikatsiya serveriga o'zining ismi, serveri *TGS* ning (bir nechta server *TGS* bo'lishi mumkin) bo'lgan xabarni

jo'natadi. Amalda foydalanuvchi ko'pincha ismini o'zini kiritadi, tizimga kirish dasturi esa so'rov yuboradi.

Kerberosning autentifikatsiyalash serveri o'zining ma'lumotlar bazasida mijoz xususidagi ma'lumotlarni qidiradi. Agar mijoz xususidagi axborot ma'lumotlar bazasida bo'lsa, Kerberos mijoz va *TGS* orasida ma'lumot almashish uchun ishlatiladigan seans kalitini generatsiyalaydi. Kerberos bu seans kalitini mijozning maxfiy kaliti bilan shifrlaydi. So'ngra u *TGS* xizmatiga mijozning haqiqiyligini isbotlovchi *TGT* (*Ticket Granting Ticket*) mandatining ajratilishi uchun mijozga mandat yaratadi. *TGS* ning maxfiy kalitida *TGT* shifrlanadi va uning tarkibida mijoz va server identifikatori, *TGS* – mijoz juftining seans kaliti hamda *TGT* ta'sirining boshlanish va oxirgi vaqtlari bo'ladi. Autentifikatsiyalash serveri bu ikkita shifrlangan xabarni mijozga yuboradi.

Endi mijoz bu xabarlarni qabul qiladi, birinchi xabarni o'zining maxfiy kaliti K_S bilan rasshifrovka qilib, seans kaliti $K_{S,tgs}$ ni hosil qiladi. Maxfiy kalit mijoz parolining bir tomonlama xesh-funksiyasi bo'lganligi sababli qonuniy foydalanuvchida hech qanday muammo tug'ilmaydi. Niyati buzuq odam to'g'ri parolni bilmaydi va demak, autentifikatsiyalash serverining javobini rasshifrovka qila olmaydi. Shu sababli niyati buzuq odam mandatni yoki seans kalitini ola olmaydi. Mijoz *TGT* mandatini va seans kalitini saqlab, parol va xesh-qiymatni, ularning obro'sizlanish ehtimolliklarini pasaytirish maqsadida, o'chiradi. Agar niyati buzuq odam mijoz xotirasi tarkibining nusxasini olishga urinsa, u faqat *TGT* va seans kalitini oladi. Bu ma'lumotlar faqat *TGT* ta'siri vaqtidagina muhim hisoblanadi. *TGT* ta'sir muddati tugaganidan so'ng bu ma'lumotlar ma'noga ega bo'lmaydi. Endi mijoz *TGT* dan olingan mandat yordamida unda ko'rsatilgan *TGT* ta'sirining butun muddati mobaynida server *TGS* da autentifikatsiyalashdan o'tish imkoniyatiga ega.

Server mandatlarini olish

Mijoz o'ziga kerak bo'lgan har bir xizmat uchun alohida mandat olishi mumkin. Shu maqsadda mijoz *TGS* xizmatiga *TGT* mandati va autentifikatordan iborat so'rov yuborishi lozim. (Amalda so'rovni dasturiy ta'minot avtomatik tarzda, ya'ni foydalanuvchiga bildirmasdan yuboradi.) Mijoz va *TGS* serveri juftining kalitida shifrlangan autentifikator tarkibida mijoz va unga kerakli serverning identifikatori, tasodifiy seans kaliti va vaqt belgisi bo'ladi.

TGS so'rovni olib, o'zining maxfiy kalitida *TGT* ni rasshifrovka qiladi. So'ngra *TGS TGT* dagi seans kalitidan autentifikatorni rasshi-

frovka qilishda foydalanadi. Nihoyasida autentifikatordagi axborot mandat axboroti bilan taqqoslanadi. Aniqrog'i, chiptadagi mijozning tarmoq adresi so'rovda ko'rsatilgan tarmoq adresi bilan hamda vaqt belgisi joriy vaqt bilan solishtiriladi. Agar barchasi mos kelsa, *TGS* so'rovni bajarishga ruxsat beradi.

Vaqt belgilarini tekshirishda barcha kompyuterlarning soatlari, bo'lmaganda, bir necha minut aniqligida sinxronlanganligi ko'zda tutiladi. Agar so'rovda ko'rsatilgan vaqt joriy ondan anchagina farq qilsa, TGS bunday so'rovni oldingi so'rovni qaytarishga urinish deb hisoblaydi.

TGS xizmati autentifikator ta'siri muddatining to'g'riligini kuzatishi lozim, chunki server xizmati bitta mandat, ammo turli autentifikatorlar yordamida ketma-ket bir necha marta so'ralishi mumkin. O'sha mandat va autentifikatorning ishlatilgan vaqt belgisi bilan qilingan boshqa so'rov qaytariladi.

To'g'ri so'rovga javob tariqasida *TGS* mijozga maqsad serverdan foydalanish uchun mandat taqdim etadi. *TGS* mijoz va maqsad serveri uchun mijoz va *TGS* ga umumiy bo'lgan seans kalitida shifrlangan seans kalitini ham yaratadi. Bu ikkala xabar mijozga yuboriladi. Mijoz xabarni rasshifrovka qiladi va seans kalitini chiqarib oladi.

Xizmat so'rovi

Endi mijoz o'zining haqiqiyligini maqsad serveriga isbotlashi mumkin. Maqsad serverida autentifikatsiyadan muvaffaqiyatli o'tish uchun mijoz tarkibida o'zining ismi, tarmoq adresi, vaqt belgisi bo'lgan va seans kaliti «mijoz-server»da shifrlangan autentifikatorni yaratadi va uni TGS xizmatidan olib berilgan maqsad serverining maxfiy kalitida shifrlangan mandat bilan birga jo'natadi.

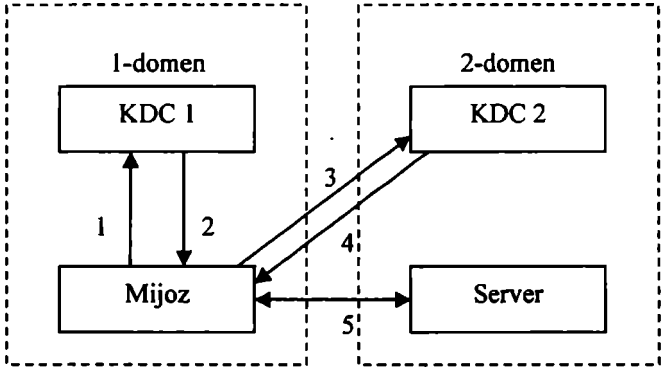
Maqsad serveri mijozdan ma'lumotlarni olib, autentifikatorni o'zining maxfiy kalitida rasshifrovka qiladi va undan «mijoz-server» seans kalitini chiqarib oladi. Mandat ham tekshiriladi. Tekshirish muolajasi «mijoz-TGS» sessiyasida o'tkaziladigan muolajaga o'xshash, ya'ni tarmoq adreslari va vaqt belgisining mosligi tekshiriladi. Agar barchasi mos kelsa, server mijozning haqiqiyligiga ishonch hosil qiladi.

Agar ilova haqiqiylikning o'zaro tekshirilishini talab etsa, server mijozga tarkibida seans kalitida shifrlangan vaqt belgisi bo'lgan xabarni yuboradi. Bu serverga to'g'ri maxfiy kalitning ma'lum ekanligini va u mandat hamda guvohnomani rasshifrovka qila olishini isbotlaydi. Zaruriyat tug'ilganida mijoz va server keyingi xabarlarni umumiy kalitda shifrlashlari mumkin. Chunki bu kalit faqat ularga ma'lum, bu kalit bi-

lan shifrlangan oxirgi xabar ikkinchi tarafdan yuborilganiga ikkala taraf ishonch hosil qilishlari mumkin. Amalda bu barcha murakkab muolajalar avtomatik tarzda bajariladi va mijozga qandaydir noqulayliklar yetkazilmaydi.

Domenlararo autentifikatsiyalash xususiyatlari

Kerberosdan domenlararo autentifikatsiyalashda ham foydalanish mumkin. Mijoz boshqa domendagi serverdan foydalanish maqsadida kalitlarni taqsimlash markazi *KDC* ga murojaat qilsa, *KDC* mijozga so'ralayotgan server joylashgan domenning *KDC* iga murojaat etishga *qayta adreslash mandatini* (referal ticket) taqdim etadi (5.3-rasm).



5.3-rasm. Kerberos protokolida domenlararo autentifikatsiyalash sxemasi.

Rasmda quyidagi belgilashlar qabul qilingan:

1. Autentifikatsiyalashga so'rov.
2. *KDC*1 uchun *TGT*
3. *KDC*2 uchun *TGT*.
4. Serverdan foydalanish mandati.
5. Ma'lumotlarni autentifikatsiyalash va almashish.

Qayta adreslash mandati ikkita domen KDCsining juftli aloqa kalitida shifrlangan TGTdir. Bunda mijozga serverdan foydalanishga mandatni so'ralayotgan server joylashgan KDC taqdim etadi.

Juda ko'p domenli tarmoqda autentifikatsiyalash uchun Kerberosdan foydalanish nazariy jihatdan mumkin bo'lsa-da, murojaatlar soni-

ning domenlar soniga mutanosib ravishda oshishi sababli, so'rovlarni muayyan KDClarga bir ma'noda qayta adreslovchi qandaydir markaziy domen qu-rishga to'g'ri keladi.

Kerberos xavfsizligi

Kerberos, kriptografik himoyalashning boshqa har qanday dasturiy vositasi kabi ishonchsiz dasturiy muhitda ishlaydi. Ushbu muhitning hujjatlashtirilmagan imkoniyatlari yoki noto'g'ri konfiguratsiyasi jiddiy axborotning chiqib ketishiga olib kelishi mumkin. Hatto kalitlar foydalanuvchi ishlash seansida faqat tezkor xotirada saqlansa ham, operatsion tizimdagi buzilish kalitlarning qattiq diskda nusxalanishiga olib kelishi mumkin.

Kerberos dasturiy ta'minoti o'rnatilgan ishchi stansiyasidan ko'pchilik foydalanuvchi rejimning ishlatilishi yoki ishchi stansiyalardan foydalanishning nazorati bo'lmasligi dastur-zakladkani kiritish yoki kriptografik dasturiy ta'minotni modifikatsiyalash imkoniyatini tug'diradi.

Shu sababli, Kerberos xavfsizligi ko'p jihatdan ushbu protokol o'rnatilgan ishchi stansiyasi himoyasining ishonchligiga bog'liq.

Kerberos protokolining o'ziga quyidagi qator talablar qo'yiladi:

– Kerberos xizmati xizmat qilishdan voz kechishga yo'naltirilgan hujumlardan himoyalanishi shart;

– vaqt belgisi autentifikatsiya jarayonida qatnashishi sababli, tizimdan foydalanuvchilarining barchasi uchun tizimli vaqtni sinxronlash zarur;

– Kerberos parolni saralash orqali hujum qilishdan himoyalamaydi. Muammo shundaki, *KDC* da saqlanuvchi foydalanuvchi kaliti uning parolini xesh-funksiya yordamida qayta ishlash natijasidir. Parolning bo'shligida uni saralab topish mumkin.

– Kerberos xizmati ruxsatsiz foydalanishining barcha turlaridan ishonchli himoyalanishi shart;

– mijoz olgan mandatlar hamda maxfiy kalitlar ruxsatsiz foydalanishdan himoyalanishi shart.

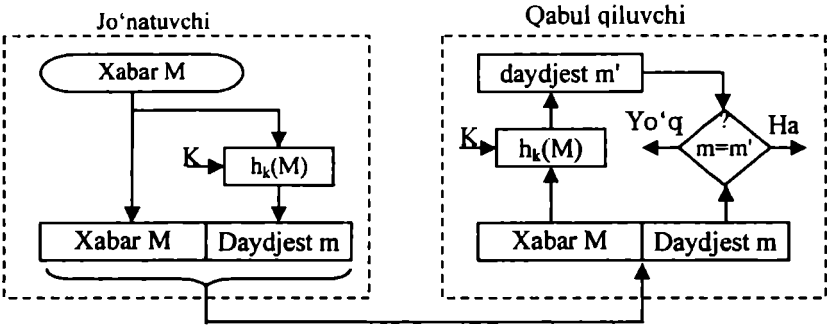
Yuqorida keltirilgan talablarning bajarilmasligi muvaffaqiyatli hujumga sabab bo'lishi mumkin.

Hozirda Kerberos protokoli autentifikatsiyalashning keng tarqalgan vositasi hisoblanadi. Kerberos turli kriptografik sxemalar, xususan, ochiq kalitli shifrlash bilan birgalikda ishlatilishi mumkin.

Bir tomonlama kalitli xesh-funksiyalardan foydalanishga asoslangan protokollar

Bir tomonlama xesh-funksiya yordamida shifrlashning o'ziga xos xususiyati shundaki, u mohiyati bo'yicha bir tomonlamadir, ya'ni teskari o'zgartirish-qabul qiluvchi tarafda rasshifrovka qilish bilan birga olib borilmaydi. Ikkala taraf (jo'natuvchi va qabul qiluvchi) bir tomonlama shifrlash muolajasidan foydalanadi.

Shifrlanayotgan ma'lumot M ga qo'llanilgan K parametr-kalitli bir tomonlama xesh-funksiya $h_k(.)$ natijada baytlarning belgilangan katta bo'lmagani sonidan iborat xesh-qiymat (daydjest) m ni beradi (5.4-rasm).



5.4-rasm. Ma'lumotlar yaxlitligini tekshirishda bir tomonlama xesh-funksiyaning ishlatilishi (I-variant).

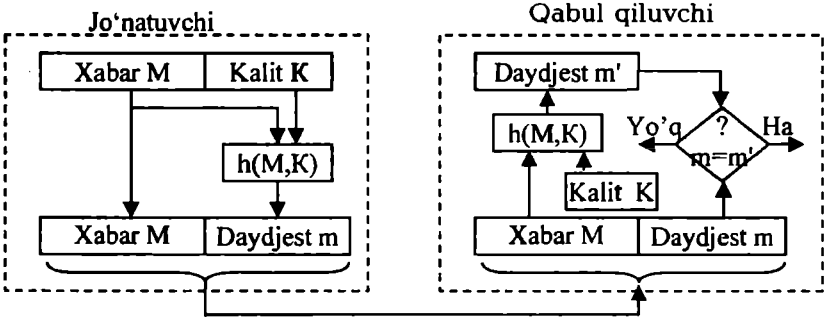
Daydjest m qabul qiluvchiga dastlabki xabar M bilan birga uzatiladi. Xabarni qabul qiluvchi, daydjest olinishida qanday bir tomonlama xesh-funksiya ishlatilganligini bilgan holda, rasshifrovka qilingan xabar M dan foydalanib, daydjestni boshqatdan hisoblaydi. Agar olingan daydjest bilan hisoblangan daydjest mos kelsa, xabar M ning tarkibi hech qanday o'zgarishga duchor bo'lmaganini bildiradi.

Daydjestni bilish dastlabki xabarni tiklashga imkon bermaydi, ammo ma'lumotlar yaxlitligini tekshirishga imkon beradi. Daydjestga dastlabki xabar uchun o'ziga xos nazorat yig'indisi sifatida qarash mumkin. Ammo daydjest va oddiy nazorat yig'indisi orasida jiddiy farq ham mavjud. Nazorat yig'indisidan aloqaning ishonchsiz liniyasi bo'yicha uzatiladigan xabarlarning yaxlitligini tekshirish vositasi sifatida foydalaniladi. Tekshirishning bu vositasi niyati buzuq odamlar bilan

kurashishga mo'ljallanmagan. Chunki, bu holda nazorat yig'indisining yangi qiymatini qo'shib xabarni almashtirib qo'yishga ularga hech kim xalaqit bermaydi. Qabul qiluvchi bunda hech narsani sezmaydi.

Daydjestni hisoblashda, oddiy nazorat yig'indisidan farqli ravishda, maxfiy kalitlar ishlatiladi. Agar daydjest olinishida faqat jo'natuvchi va qabul qiluvchiga ma'lum bo'lgan parametr-kalitli bir tomonlama xesh-funksiya ishlatilsa, dastlabki xabarning har qanday modifikatsiyasi darhol ma'lum bo'ladi.

5.5-rasmda ma'lumotlar yaxlitligini tekshirishda bir tomonlama xesh-funksiya ishlatilishining boshqa varianti keltirilgan.



5.5-rasm. Ma'lumotlar yaxlitligini tekshirishda bir tomonlama xesh-funksiyaning ishlatilishi (II-variant).

Bu holda bir tomonlama xesh-funksiya *h(.)* parametr–kalitga ega emas, ammo u maxfiy kalit bilan to'ldirilgan xabarga qo'llaniladi, ya'ni jo'natuvchi daydjest m=h(M, K)ni hisoblaydi. Qabul qiluvchi dastlabki xabarni chiqarib olib, uni o'sha ma'lum maxfiy kalit bilan to'ldiradi. So'ngra olingan ma'lumotlarga bir tomonlama xesh-funksiya h(.)ni qo'llaydi. Hisoblash natijasi – daydjest «m» tarmoq orqali olingan daydjest «m» bilan taqqoslanadi.

Asimmetrik algoritmlarga asoslangan qat'iy autentifikatsiyalash

Qat'iy autentifikatsiyalash protokollarida ochiq kalitli asimmetrik algoritmlardan foydalanish mumkin. Bu holda isbotlovchi maxfiy kalitni bilishligini quyidagi usullarning biri yordamida namoyish etishi mumkin:

– ochiq kalitda shifrlangan so'rovni rasshifrovka qilish;

– so'rov so'ziga raqamli imzosini qo'yish.

Autentifikatsiyaga zarur bo'lgan kalitlarning jufti, xavfsizlik mulohazasiga ko'ra, boshqa maqsadlarga (masalan, shifrlashda) ishlatilmasligi shart. Ochiq kalitli tanlangan tizim shifrlangan matnni tanlash bilan hujumlarga, hatto buzg'unchi o'zini tekshiruvchi deb ko'rsatib va uning nomidan harakat qilganda ham, bardosh berishi lozimligiga foydalanuvchilarni ogohlantirish kerak.

Shifrlashning asimmetrik algoritmlaridan foydalanib autentifikatsiyalash

Shifrlashning asimmetrik algoritmlaridan foydalanishga asoslangan protokolga misol tariqasida autentifikatsiyalashning quyidagi protokolini keltirish mumkin:

$$A \leftarrow B : h(r), B, P_A(r, B),$$

$$A \rightarrow B : r.$$

Qatnashuvchi V tasodifiy holda r ni tanlaydi va $x=h(r)$ qiymatini hisoblaydi (x qiymati r ning qiymatini ochmasdan turib r ni bilishligini namoyish etadi), so'ngra u $e = P_A(r, B)$ qiymatni hisoblaydi. P_A orqali asimmetrik shifrlash algoritmi faraz qilinsa, $h(.)$ orqali xesh-funksiya faraz qilinadi. Qatnashuvchi V axborot xabarni qatnashuvchi A ga jo'natadi. Qatnashuvchi A $e = P_A(r, B)$ ni rasshifrovka qiladi va r' va B' qiymatlarni oladi hamda $x' = h(r')$ ni hisoblaydi. Undan keyin $x=x'$ ekanligini va B' identifikator haqiqatan qatnashuvchi Vga ko'rsatayotganini tasdiqlovchi qator taqqoslashlar bajariladi. Taqqoslash muvaffaqiyatli o'tsa qatnashuvchi A qatnashuvchi V ga uzatadi. Qatnashuvchi B r ni olganidan so'ng uni birinchi xabarda jo'natgan qiymat ekanligini tekshiradi.

Keyingi misol sifatida asimmetrik shifrlashga asoslangan Nidxem va Shrederning modifikatsiyalangan protokolini keltiramiz. Faqat autentifikatsiyalashda ishlatiluvchi Nidxem va Shreder protokoli variantini ko'rishda P_B orqali qatnashuvchi B uning ochiq kaliti yordamida shifrlash algoritmi faraz qilinadi. Protokol quyidagi tuzilmaga ega:

$$A \rightarrow B : P_B(r_1, A)$$

$$A \leftarrow B : P_A(r_2, r_i)$$

$$A \leftarrow B : r_2$$

Raqamli imzodan foydalanish asosidagi autentifikatsiyalash

X.509 standartining tavsiyalarida raqamli imzo, vaqt belgisi va tasodifiy sonlardan foydalanish asosidagi autentifikatsiyalash sxemasi spetsifikatsiyalangan. Ushbu sxemani tavsiflash uchun quyidagi belgilashlarni kiritamiz:

– t_A, r_A va r_V – mos holda vaqt belgisi va tasodifiy sonlar;

– S_A – qatnashuvchi A generatsiyalagan imzo;

– S_B – qatnashuvchi B generatsiyalagan imzo;

– $cert_A$ – qatnashuvchi A ochiq kalitining sertifikati;

– $cert_V$ – qatnashuvchi V ochiq kalitining sertifikati;

Misol tariqasida autentifikatsiyalashning quyidagi protokollarini keltiramiz:

1. Vaqt belgisidan foydalanib bir tomonlama autentifikatsiyalash:

$$A \rightarrow B : cert_A, t_A, B, S_A(t_A, B)$$

Qatnashuvchi B ushbu xabarni olganidan so'ng vaqt belgisi t_A ning, olingan identifikator V ning to'g'riligini va sertifikat $cert_A$ dagi ochiq kalitdan foydalanib, raqamli imzo $S_A(t_A, B)$ ning korrektligini tekshiradi.

2. Tasodifiy sonlardan foydalanib bir tomonlama autentifikatsiyalash:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B)$$

Qatnashuvchi V qatnashuvchi A dan xabarni olib aynan u xabarning adresati ekanligiga ishonch hosil qiladi; sertifikat $cert_A$ dan olingan qatnashuvchi A ochiq kalitidan foydalanib ochiq ko'rinishda olingan r_A soni, birinchi xabarda jo'natilgan r_V soni va o'zining identifikatori V ostidagi imzo $S_A(r_A, r_B, B)$ ning korrektligini tekshiradi. Imzo chekilgan tasodifiy son r_A ochiq matnni tanlash bilan hujumni oldini olish uchun ishlatiladi.

3. Tasodifiy sonlardan foydalanib ikki tomonlama autentifikatsiyalash:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B)$$

$$A \leftarrow B : cert_B, A, S_B(r_A, r_B, A)$$

Ushbu protokoldagi xabarlarni ishlash oldingi protokoldagidek bajariladi.

5.5. Foydalanuvchilarni biometrik identifikatsiyalash va autentifikatsiyalash

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 alomatlarni ishga layoqatli shaxsdan ajratib bo'lmasligi;

– biometrik alomatlarni soxtalashtirishning qiyinligi.

Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik alomatlari quyidagilar:

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

Autentifikatsiyaning biometrik qism tizimi ishlashining namunaviy sxemasi quyidagicha. Tizimda ro'yxatga olinishida foydalanuvchidan o'zining xarakterli alomatlarini bir yoki bir necha marta namoyish qilinishi talab etiladi. Bu alomatlar (haqiqiy sifatida ma'lum) tizim tomonidan qonuniy foydalanuvchining qiyofasi sifatida ro'yxatga olinadi. Foydalanuvchining bu qiyofasi tizimda elektron shaklda saqlanadi va o'zini qonuniy foydalanuvchi deb da'vo qilgan har bir odamni tekshirishda ishlatiladi. Taqdim etilgan alomatlar majmuasi bilan ro'yxatga olinganlarining mosligi yoki mos kelmasligiga qarab qaror qabul qilinadi. Iste'molchi nuqtai nazaridan biometrik autentifikatsiyalash tizimi quyidagi ikkita parametr orqali xarakterlanadi:

- xatolik inkorlar koeffitsiyenti FRR (false-reject rate);
- xatolik tasdiqlar koeffitsiyenti FAR (false-alarm 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 tas-

diqlaganida paydo bo'ladi (odatda FAP qiymati taxminan 10000 dan bimi 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 nolga teng bo'lishi shart. Afsuski, biometrik tizim ideal emas, shu sababli nimanidir 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.

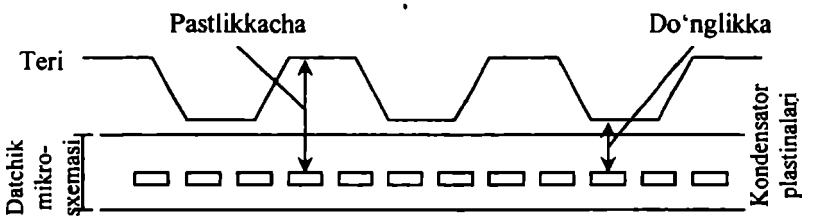
Autentifikatsiyaning daktiloskopik tizimi quyidagicha ishlaydi. Avval foydalanuvchi ro'yxatga olinadi. Odatda, skanerda barmoqning turli holatlarida skanerlashning bir necha varianti amalga oshiriladi. Tabiiyki, namunalar bir-biridan biroz farqlanadi va qandaydir umumlashtirilgan namuna, «pasport» shakllantirilishi 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 tendensiya 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 yarimo'tkazgichli datchik yor-

damida sig'im qarshiligini aniqlash orqali axborotni yig'adi. Sensor ishlashining prinsipi quyidagicha: ushbu asbobga quyilgan barmoq kondensator plastinalarining biri vazifasini o'taydi (5.6-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.



5.6-rasm. Sensor ishlashining prinsipiga.

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 mukammal 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 ishlatilsa-da, 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 xususiy matematik algoritmlardan foydalanadilar.

Ma'lum bo'lishicha, ko'pgina tashkilotlarning xodimlari 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 hisoblanadi.

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 45^0 ga o'zgarishi aniqlashni samarasiz bo'lishiga olib keladi.

Ovoz bo'yicha autentifikatsiyalash tizimlari. Bu tizimlar arzonligi tufayli foydalanuvchan hisoblanadilar. Xususan, 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, modulatsiyasi 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'lanishlarning sifati so'zlovchi shaxsini aniqlashni qiyinlashtiradi. Shu sababli ovoz bo'yicha aniqlashni yuz tuzilishini yoki barmoq izlarini aniqlash kabi boshqa usullar 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.

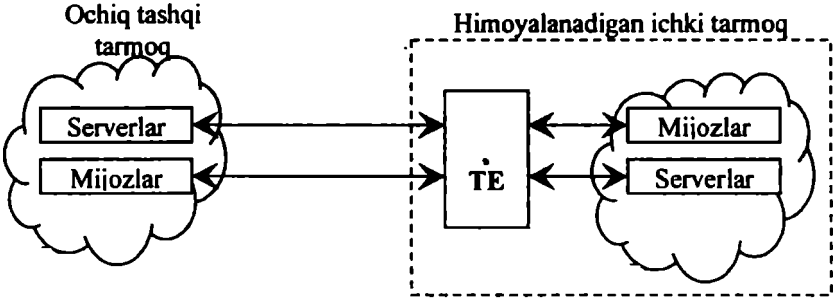
Foydalanuvchini biometrik autentifikatsiyalash maxfiy kalitdan foydalanishni modul. ko'rinishida shifrlashda jiddiy ahamiyatga ega bo'lishi mumkin. Bu modul axborotdan faqat haqiqiy xususiy kalit egasining foydalanishiga imkon beradi. So'ngra kalit egasi o'zining maxfiy kalitini ishlatib xususiy tarmoqlar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

VI bob. TARMOQLARARO EKRAN TEXNOLOGIYASI

6.1. Tarmoqlararo ekranlarning ishlash xususiyatlari

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 ekranlar garchi korxona lokal tarmog'i ulangan korporativ intratarmog'idan qilinuvchi hujumlardan himoyalashda ishlatilishlari mumkin bo'lsa-da, 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.

Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta'sir ko'rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning himoyalanuvchi tarmog'i va tashqi g'anim tarmoq orasida joylanishi lozim (6.1-rasm). Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtai nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi.



6.1-rasm. Tarmoqlararo ekranni ulash sxemasi.

Ichki tarmoqning ko'pgina uzellarini birdaniga himoyalovchi tarmoqlararo ekran quyidagi ikkita vazifani bajarishi kerak:

– tashqi (himoyalanuvchi tarmoqqa nisbatan) foydalanuvchilarning korporativ tarmoqning ichki resurslaridan foydalanishini chegaralash. Bunday foydalanuvchilar qatoriga tarmoqlararo ekran himoyalovchi ma'lumotlar bazasining serveridan foydalanishga urinuvchi sheriklar, masofadagi foydalanuvchilar, xakerlar, hatto kompaniyaning xodimlari kiritilishi mumkin;

– himoyalanuvchi tarmoqdan foydalanuvchilarning tashqi resurslardan foydalanishlarini chegaralash. Bu masalaning yechilishi, masalan, serverdan xizmat vazifalari talab etmaydigan foydalanishni tartibga solishga imkon beradi.

Hozirda ishlab chiqarilayotgan tarmoqlararo ekranlarning tavsiflariga asoslangan holda, ularni quyidagi asosiy alomatlari bo'yicha turkumlash mumkin:

OSI modeli sathlarida ishlashi bo'yicha:

– paketli filtr (ekranlovchi marshrutizator – screening router);

– seans sathi shlyuzi (ekranlovchi transport);

– tatbiqiy shlyuz (application gateway);

– ekspert sathi shlyuzi (stateful inspection firewall).

Ishlatiladigan texnologiya bo'yicha:

– protokol holatini nazoratlash (stateful inspection);

– vositachilar modullari asosida (proxy);

Bajarilishi bo'yicha:

– apparat-dasturiy;

– dasturiy;

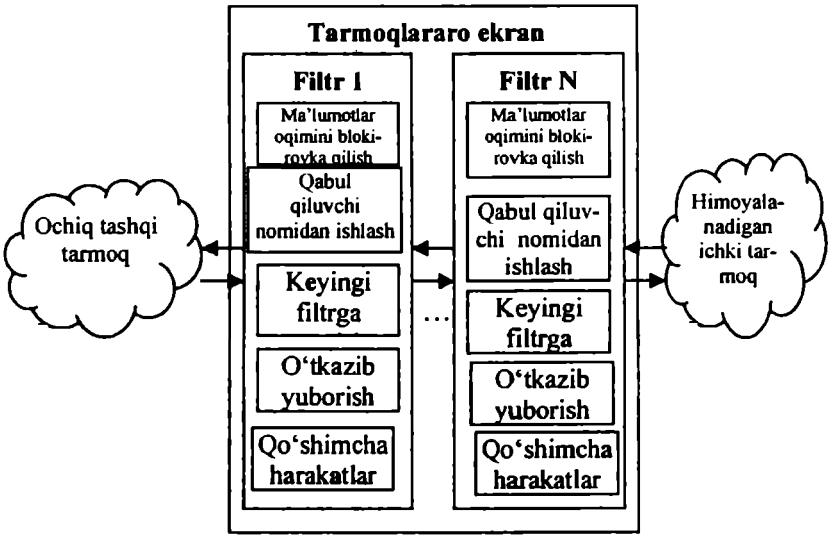
Ulanish sxemasi bo'yicha:

– tarmoqni umumiy himoyalash sxemasi;

– tarmoq segmentlari himoyalanuvchi berk va tarmoq segmentlari himoyalanmaydigan ochiq sxema;

– tarmoqning berk va ochiq segmentlarini alohida himoyalovchi sxema.

Trafiklarni filtrlash. Axborot oqimlarini filtrlash ularni ekran orqali, ba'zida qandaydir o'zgartirishlar bilan, o'tkazishdan iborat. Filtrlash qabul qilingan xavfsizlik siyosatiga mos keluvchi, ekranga oldindan yuklangan qoidalar asosida amalga oshiriladi. Shu sababli tarmoqlararo ekranni axborot oqimlarini ishlovchi filtrlar ketma-ketligi sifatida tasavvur etish qulay (6.2-rasm).



6.2-rasm. Tarmoqlararo ekran tuzilmasi.

Filtrlarning har biri quyidagi harakatlarni bajarish orqali filtrlashning alohida qoidalarini izohlashga atalgan:

1. Axborotni izohlanuvchi qoidalardagi berilgan mezonlar bo'yicha tahlillash, masalan, qabul qiluvchi va jo'natuvchi adreslari yoki ushbu axborot atalgan ilova xili bo'yicha.

2. Izohlanuvchi qoidalar asosida quyidagi yechimlardan birini qabul qi-lish:

– ma'lumotlarni o'tkazmaslik;

– ma'lumotlarni qabul qiluvchi nomidan ishlash va natijani jo'natuvchiga qaytarish;

– tahlillashni davom ettirish uchun ma'lumotlarni keyingi filtrga uzatish;

– keyingi filtrlarga e'tibor qilmay ma'lumotlarni uzatish.

Filtrlash qoidalari vositachilik funksiyalariga oid qo'shimcha, masalan, ma'lumotlarni o'zgartirish, hodisalarni qaydlash va h. kabi harakatlarni ham berishi mumkin. Mos holda, filtrlash qoidalari quyidagilarning amalga oshirilishini ta'minlovchi shartlar ro'yxatini aniqlaydi:

– ma'lumotlarni keyingi uzatishga ruxsat berish yoki ruxsat bermaslik;

– himoyalashning qo'shimcha funksiyalarini bajarish.

Axborot oqimini tahlillash mezoni sifatida quyidagi parametrlardan foydalanish mumkin:

– tarkibida tarmoq adreslari, identifikatorlar, interfeyslar adresi, portlar nomeri va boshqa muhim ma'lumotlar bo'lgan xabar paketlarining xizmatchi hoshiyalari;

– masalan, kompyuter viruslari borligiga tekshiriluvchi xabar paketlarining bevosita tarkibi;

– axborot oqimining tashqi xarakteristikalari, masalan, vaqt va chastota xarakteristikalari, ma'lumotlar hajmi va h.

Ishlatiluvchi tahlillash mezonlari filtrlashni amalga oshiruvchi OSI modelining sathlariga bog'liq. Umumiy holda, paketni filtrlashni amalga oshiruvchi OSI modelining sathi qanchalik yuqori bo'lsa, ta'minlanuvchi himoyalash darajasi ham shunchalik yuqori bo'ladi.

Vositachilik funksiyalarining bajarilishi. Tarmoqlararo ekran vositachilik funksiyalarini *ekranlovchi agentlar* yoki *vositachi dasturlar* deb ataluvchi maxsus dasturlar yordamida bajaradi. Bu dasturlar rezident dasturlar hisoblanadi, tashqi va ichki tarmoq orasida xabarlar paketini bevosita uzatishni taqiqlaydi.

Tashqi tarmoqdan ichki tarmoqning va aksincha foydalanish zaruriyati tug'ilganda avval tarmoqlararo ekran kompyuterida ishlovchi vositachi-dastur bilan mantiqiy ulanish o'rnatilishi lozim. Vositachi-dastur so'ralgan tarmoqlararo aloqaning joizligini tekshiradi va ijobiy natijada o'zi so'ralgan kompyuter bilan alohida ulanish o'rnatadi. So'ngra tashqi va ichki tarmoq kompyuterlari orasida axborot almashish, xabarlar oqimini filtrlashni hamda boshqa himoyalash funksiyalarini bajaruvchi dasturiy vositachi orqali amalga oshiriladi.

Ta'kidlash lozimki, tarmoqlararo ekran filtrlash funksiyasini vositachi-dastur ishtirokisiz amalga oshirib, tashqi va ichki tarmoq orasida o'zaro aloqaning shaffofligini ta'minlashi mumkin. Shu bilan birga vositachi dasturlar xabarlar oqimini filtrlashni amalga oshirmasligi ham mumkin.

Umuman, vositachi-dasturlar, xabarlar oqimini shaffof uzatilishini blokirovka qilgan holda, quyidagi funksiyalarni bajarishi mumkin:

– uzatiluvchi va qabul qilinuvchi ma'lumotlarning haqiqiyligini tekshirish;

– ichki tarmoq resurslaridan foydalanishni chegaralash;

– tashqi tarmoq resurslaridan foydalanishni chegaralash;

– tashqi tarmoqdan so'raluvchi ma'lumotlarni keshlash;

– xabarlar oqimini filtrlash va o'zgartirish, masalan, viruslarni dinamik tarzda qidirish va axborotni shaffof shifrlash;

– foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;

– ichki tarmoq adreslarini translatsiyalash;

– hodisalarni qaydlash, hodisalarga reaksiya ko'rsatish hamda qaydlangan axborotni tahlillash va hisobotlarni generatsiyalash.

Uzatiluvchi va qabul qilinuvchi ma'lumotlarning haqiqiyligini tekshirish nafaqat elektron xabarlarni, balki soxtalashtirilishi mumkin bo'lgan migratsiyalanuvchi dasturlarni (Java, Active X Controls) autentifikatsiyalash uchun dolzarb hisoblanadi. Xabar va dasturlarning haqiqiyligini tekshirish ularning raqamli imzosini tekshirishdan iboratdir.

Ichki tarmoq resurslaridan foydalanishni chegaralash usullari operatsion tizim sathida madadlanuvchi chegaralash usullaridan farq qilmaydi.

*Tashqi tarmoq resurslaridan foydalanishni chegarlash*da ko'pincha quyidagi yondashishlardan biri ishlatiladi:

– faqat tashqi tarmoqdagi berilgan adres bo'yicha foydalanishga ruxsat berish;

– yangilanuvchi nojoiz adreslar ro'yxati bo'yicha so'rovlarni filtrlash va o'rinsiz kalit so'zlari bo'yicha axborot resurslarini qidirishni blokirovka qilish;

– ma'mur tomonidan tashqi tarmoqning qonuniy resurslarini brandmauerning diskli xotirasida to'plash va yangilash va tashqi tarmoqdan foydalanishni to'la taqiqlash.

Tashqi tarmoqdan so'raluvchi *ma'lumotlarni keshlash* maxsus vositachilar yordamida madadlanadi. Ichki tarmoq foydalanuvchilari tashqi tarmoq resurslaridan foydalanganlarida barcha axborot, proxy-server deb ataluvchi brandmauer qattiq diski makonida to'planadi. Shu sababli, agar navbatdagi so'rovda kerakli axborot proxy-serverda bo'lsa, vositachi uni tashqi tarmoqqa murojaatsiz taqdim etadi. Bu foydalanishni

jiddiy tezlashtiradi. Ma'murga faqat proxy-server tarkibini vaqti-vaqti bilan yangilab turish vazifasi qoladi.

Keshlash funksiyasi tashqi tarmoq resurslaridan foydalanishni chegaralashda muvaffaqiyatli ishlatilishi mumkin. Bu holda tashqi tarmoqning barcha qonuniy resurslari ma'mur tomonidan proxy-serverda to'planadi va yangilanadi. Ichki tarmoq foydalanuvchilariga faqat proxy-serverning axborot resurslaridan foydalanishga ruxsat beriladi, tashqi tarmoq resurslaridan bevosita foydalanish esa man qilinadi.

Xabarlar oqimini filtrlash va o'zgartirish vositachi tomonidan qoidalarning berilgan to'plami yordamida bajariladi. Bunda vositachidasturlarning ikki xili farqlanadi:

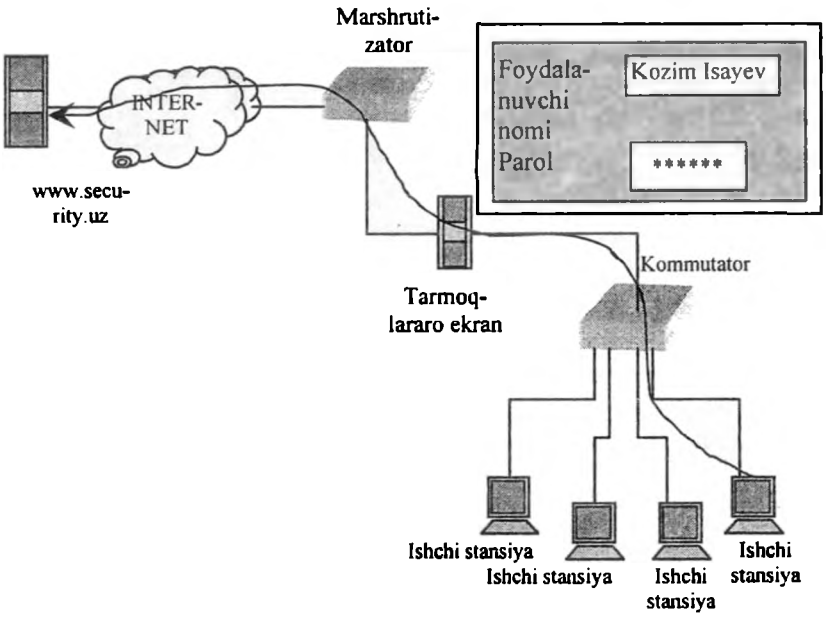
– servis turini aniqlash uchun xabarlar oqimini tahlillashga mo'ljallangan ekranlovchi agentlar, masalan, FTP, HTTP, Telnet;

– barcha xabarlar oqimini ishlovchi universal ekranlovchi agentlar, masalan, kompyuter viruslarini qidirib zararsizlantirishga yoki ma'lumotlarni shaffof shifrlashga mo'ljallangan agentlar.

Dasturiy vositachi unga keluvchi ma'lumotlar paketini tahlillaydi va agar qandaydir obyekt berilgan mezonlarga mos kelmasa, vositachi uning keyingi siljishini blokirovka qiladi yoki mos o'zgarishini, masalan, oshkor qilingan kompyuter viruslarni zararsizlantirishni bajaradi. Paketlar tarkibini tahlillashda ekranlovchi agentning o'tuvchi faylli arxivlarni avtomatik tarzda ocha olishi muhim hisoblanadi.

Foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash ba'zida oddiy identifikatorni (ism) va parolni taqdim etish bilan amalga oshiriladi (6.3-rasm). Ammo bu sxema xavfsizlik nuqtai nazaridan zaif hisoblanadi, chunki parolni begona shaxs ushlab qolib ishlatishi mumkin. Internet tarmog'idagi ko'pgina mojarolar qisman an'anaviy ko'p marta ishlatiluvchi parollarning zaifligidan kelib chiqqan.

Autentifikatsiyalashning ishonchliroq usuli – bir marta ishlatiluvchi parollardan foydalanishdir. Bir martali parollarni generatsiyalashda apparat va dasturiy vositalardan foydalaniladi. Apparat vositalari kompyuterning slotiga o'rnatiluvchi qurilma bo'lib, uni ishga tushirish uchun foydalanuvchi qandaydir maxfiy axborotni bilishi zarur. Masalan, smart-karta yoki foydalanuvchi tokeni axborotni generatsiyalaydi va bu axborotni xost an'anaviy parol o'rnida ishlatadi. Smart-karta yoki token xostning apparat va dasturiy ta'minoti bilan birga ishlashi sababli, generatsiyalanuvchi parol har bir seans uchun noyob bo'ladi.



6.3-rasm. Parol bo'yicha foydalanuvchini autentifikatsiyalash sxemasi.

Ishonchli organ, masalan, kalitlarni taqsimlash markazi tomonidan beriluvchi raqamli sertifikatlarni ishlatish ham qulay va ishonchli. Ko'pgina vositachi dasturlar shunday ishlab chiqiladiki, foydalanuvchi faqat tarmoqlararo ekran bilan ishlash seansining boshida autentifikatsiyalansin. Bundan keyin ma'mur belgilangan vaqt mobaynida undan qo'shimcha autentifikatsiyalanish talab etilmaydi.

Tarmoqlararo ekranlar tarmoqdan foydalanishni boshqarishni markazlashtirishlari mumkin. Demak, ular kuchaytirilgan autentifikatsiyalash dasturlari va qurilmalarini o'rnatishga munosib joy hisoblanadi. Garchi kuchaytirilgan autentifikatsiya vositalari har bir xostda ishlatilishi mumkin bo'lsa-da, ularning tarmoqlararo ekranlarda joylashtirish qulay. Kuchaytirilgan autentifikatsiyalash choralaridan foydalanuvchi tarmoqlararo ekranlar bo'lmasa, Telnet yoki FTP kabi ilovalarning au-

tentifikatsiyalanmagan trafigi tarmoqning ichki tizimlariga to'g'ridan-to'g'ri o'tishi mumkin.

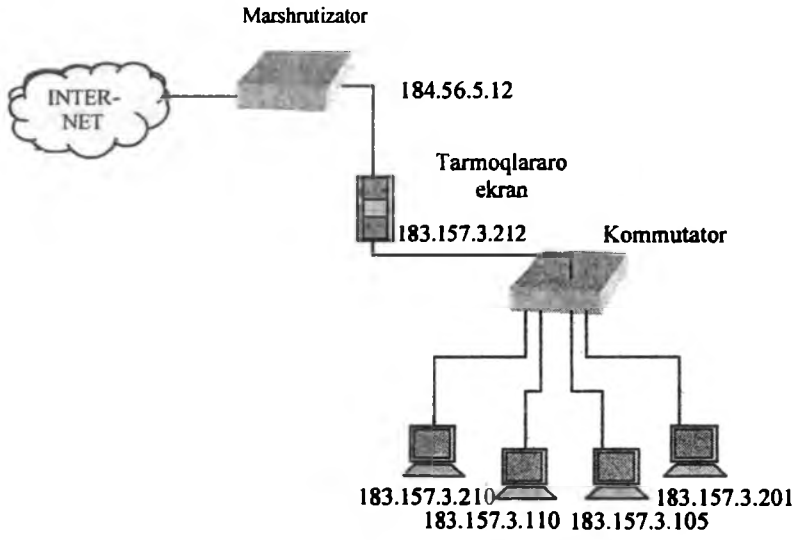
Qator tarmoqlararo ekranlar autentifikatsiyalashning keng tarqalgan usullaridan biri – Kerberosni madadlaydi. Odatda, aksariyat tijorat tarmoqlararo ekranlar autentifikatsiyalashning turli sxemalarini madadlaydi. Bu esa tarmoq xavfsizligi ma'muriga o'zining sharoitiga qarab eng maqbul sxemani tanlash imkonini beradi.

Ichki tarmoq adreslarini translatsiyalash. Ko'pgina hujumlarni amalga oshirishda niyati buzuq odamga qurbonining adresini bilish kerak bo'ladi. Bu adreslarni hamda butun tarmoq topologiyasini berkitish uchun tarmoqlararo ekranlar eng muhim vazifani – ichki tarmoq adreslarini translatsiyalashni bajaradi (6.4-rasm).

Bu funksiya ichki tarmoqdan tashqi tarmoqqa uzatiluvchi barcha paketlarga nisbatan bajariladi. Bunday paketlar uchun jo'natuvchi kompyuterlarning IP-adreslari bitta «ishonchli» IP adresga avtomatik tarzda o'zgartiriladi.

Ichki tarmoq adreslarini translatsiyalash ikkita usul-dinamik va statik usullarda amalga oshirilishi mumkin. Dinamik usulda adres uzelga tarmoqlararo ekranga murojaat onida ajratiladi. Ulanish tugallanganidan so'ng adres bo'shaydi va uni korporativ tarmoqning boshqa uzeli ishlatishi mumkin. Statik usulda uzel adresi barcha chiquvchi paketlar uzatiladigan tarmoqlararo ekranning bitta adresiga doimo bog'lanadi. Tarmoqlararo ekranning IP-adresi tashqi tarmoqqa tushuvchi yagona faol IP-adresga aylanadi. Natijada, ichki tarmoqdan chiquvchi barcha paketlar tarmoqlararo ekrandan jo'natilgan bo'ladi. Bu avtorizatsiyalangan ichki tarmoq va xavfli bo'lishi mumkin bo'lgan tashqi tarmoq orasida to'g'ridan-to'g'ri aloqani istisno qiladi.

Bunday yondashishda ichki tarmoq topologiyasi tashqi foydalanuvchilardan yashiringan, demak, ruxsatsiz foydalanish masalasi qiyinlashadi. Adreslarni translatsiyalash tarmoq ichida tashqi tarmoq, masalan, Internetdagi adreslash bilan kelishilmagan adreslashning xususiy tizimiga ega bo'lishiga imkon beradi. Bu ichki tarmoqning adres makonini kengaytirish va tashqi adres tanqisligi muammosini samarali yechadi.



6.4-rasm. Tarmoq adreslarini translatsiyalash.

Hodisalarni qaydlash, hodisalarga reaksiya ko'rsatish hamda qaydlangan axborotni tahlillash va hisobotlarni generatsiyalash tarmoqlararo ekranlarning muhim vazifalari hisoblanadi. Korporativ tarmoqni himoyalash tizimining jiddiy elementi sifatida tarmoqlararo ekran barcha harakatlarni ro'yxatga olish imkoniyatiga ega. Bunday harakatlarga nafaqat tarmoq paketlarini o'tkazib yuborish yoki blokirovka qilish, balki xavfsizlik ma'muri tomonidan foydalanishni chegaralash qoidasini o'zgartirish va h. ham taalluqli. Bunday ro'yxatga olish zaruriyat tug'ilganda (xavfsizlik mojarosi paydo bo'lganida yoki sud instansiyalariga yoki ichki tergov uchun dalillarni yig'ishda) yaratiluvchi jurnallarga murojaat etishga imkon beradi.

Shubhali hodisalar (alarm) xususidagi signallarni qaydlash tizimi to'g'ri sozlanganida tarmoqlararo ekran o'zi yoki tarmoq hujumga duchor bo'lganligi yoki zondlanganligi to'g'risidagi batafsil axborotni berishi mumkin. Tarmoqdan foydalanish va uning zondlanganligining isboti statistikasini yig'ish qator sabablarga ko'ra muhimdir. Avvalo, tarmoqlararo ekranning zondlanishga va hujumlarga bardoshligini aniq bilish zarur va tarmoqlararo ekranni himoyalash tadbirlarining adekvat-

ligini aniqlash lozim. Undan tashqari, tarmoqdan foydalanish statistikasi tarmoq asbob-uskunalariga va dasturlariga talablarni ifodalash maqsadida xavf-xatarni taqiqlash va tahlillashda dastlabki ma'lumotlar sifatida muhim hisoblanadi.

Ko'pgina tarmoqlararo ekranlar statistikani qaydlovchi, yig'uvchi va tahlillovchi quvvatli tizimga ega. Mijoz va server adresi, foydalanuvchilar identifikatori, seans vaqtlari, ulanish vaqtlari, uzatilgan va qabul qilingan ma'lumotlar soni, ma'mur va foydalanuvchilar harakatlari bo'yicha hisob olib borilishi mumkin. Hisob tizimlari statistikani tahlillashga imkon beradi va ma'murlarga batafsil hisobotlarni taqdim etadi. Tarmoqlararo ekranlar maxsus protokollardan foydalanib, ma'lum hodisalar to'g'risida real vaqt rejimida masofadan xabar berishni bajarishi mumkin.

Ruxsatsiz harakatlarni qilishga urinishlarni aniqlanishiga bo'ladigan majburiy reaksiya sifatida ma'murning xabari, ya'ni ogohlantiruvchi signallarni berish belgilanishi lozim. Hujum qilinganligi aniqlanganda ogohlantiruvchi signallarni yuborishga qodir bo'lmagan tarmoqlararo ekranni tarmoqlararo himoyaning samarali vositasi deb bo'lmaydi.

6.2. Tarmoqlararo ekranlarning asosiy komponentlari

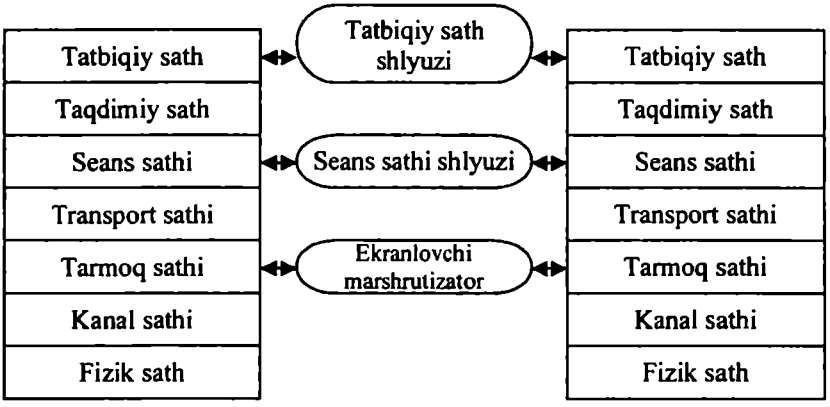
Tarmoqlararo ekranlar tarmoqlararo aloqa xavfsizligini OSI modelining turli sathlarida madadlaydi. Bunda etalon modelning turli sathlarida bajariladigan himoya funksiyalari bir-biridan jiddiy farqlanadi. Shu sababli, tarmoqlararo ekranlar kompleksini, har biri OSI modelining alohida sathiga mo'ljallangan, bo'linmaydigan ekranlar majmui ko'rinishida tasavvur etish mumkin.

Ekranlar kompleksi ko'pincha etalon modelning tarmoq, seans, tatbiqiy sathlarida ishlaydi. Mos holda, quyidagi bo'linmaydigan brandmauerlar farqlanadi (6.5-rasm):

– ekranlovchi marshrutizator;
– seans sathi shlyuzi (ekranlovchi transport);
– tatbiqiy sath shlyuzi (ekranlovchi shlyuz).

Tarmoqlarda ishlatiladigan protokollar (TCP/IP, SPX/IPX) OSI etalon modeliga batamom mos kelmaydi, shu sababli sanab o'tilgan ekranlar xili funksiyalarini amalga oshirishda etalon modelining qo'shni sathlarini ham qamrab olishlari mumkin. Masalan, tatbiqiy ekran xabarlarning tashqi tarmoqqa uzatilishida ularni avtomatik tarzda shifrlashni

hamda qabul qilinuvchi kriptografik berkitilgan ma'lumotlarni avtomatik tarzda rasshifrovka qilishni amalga oshirishi mumkin. Bu holda bunday ekran OSI modelining nafaqat tatbiqiy sathida, balki taqdimiy sathida ham ishlaydi.



6.5-rasm. OSI modelining alohida sathlarida ishlaydigan tarmoqlararo ekranlar turi.

Seans sathi shlyuzi ishlashida OSI modelining transport va tarmoq sathlarini qamrab oladi. Ekranlovchi marshrutizator xabarlar paketini tahlillashda ularning nafaqat tarmoq, balki transport sathi sarlavhalarini ham tekshiradi.

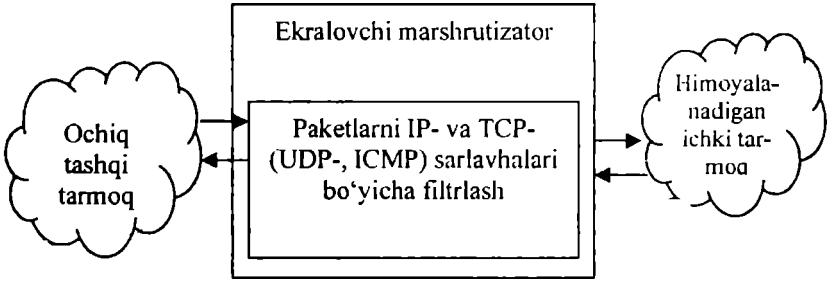
Yuqorida keltirilgan tarmoqlararo ekranlaming xillari o'zining afzalliklari va kamchiliklariga ega. Ishlatiladigan brandmauerlarning ko'pchiligi yoki tatbiqiy shlyuzlar, yoki ekranlovchi marshrutizatorlar bo'lib, tarmoqlararo aloqaning to'liq xavfsizligini ta'minlamaydi. Ishonchli himoyani esa faqat har biri ekranlovchi marshrutizator, seans sathi shlyuzi hamda tatbiqiy shlyuzni birlashtiruvchi tarmoqlararo ekranlarning kompleksi ta'minlaydi.

Ekranlovchi marshrutizator (screening router) (paketli filtr – packet filter deb ham ataladi) xabarlar paketini filtrlashga atalgan ichki va tashqi tarmoqlar orasida shaffof aloqani ta'minlaydi. U OSI modelining tarmoq sathida ishlaydi, ammo o'zining ayrim funksiyalarini bajarishida etalon modelining transport sathini ham qamrab olishi mumkin.

Ma'lumotlarni o'tkazish yoki yaroqsiz holda chiqarish xususidagi qaror filtrlashning berilgan qoidalariga binoan har bir paket uchun mustaqil qabul qilinadi. Qaror qabul qilishda tarmoq va transport sathlari paketlarining sarlavhalari tahlil etiladi (6.6-rasm).

Har bir paketning IP- va TCP/UDP – sarlavhalarining tahlillanuvchi hoshiyalari sifatida quyidagilar ishlatilishi mumkin:

– jo'natuvchi adresi;
– qabul qiluvchi adresi;
– paket xili;
– paketni fragmentlash bayrog'i;
– manba porti nomeri;
– qabul qiluvchi port nomeri.



6.6-rasm. Paketli filtrni ishlash sxemasi.

Birinchi to'rtta parametr paketning IP-sarlavhasiga, keyingilari esa TCP-yoki UDP sarlavhasiga taalluqli. Jo'natuvchi va qabul qiluvchi adreslari IP-adreslar hisoblanadi. Bu adreslar paketlarni shakllantirishda to'ldiriladi va uni tarmoq bo'yicha uzatganda o'zgarmaydi.

Paket xili hoshiyasida tarmoq sathiga mos keluvchi ICMP protokol kodi yoki tahlillanuvchi IP-paket taalluqli bo'lgan transport sathi protokolining (TCP yoki UDP) kodi bo'ladi.

Paketni fragmentlash bayrog'i IP-paketlar fragmentlashining borligi yoki yo'qligini aniqlaydi. Agar tahlillanuvchi paket uchun fragmentlash bayrog'i o'rnatilgan bo'lsa, mazkur paket fragmentlangan IP-paketning qism paketi hisoblanadi.

Manba va qabul qiluvchi portlari nomerlari TCP yoki UDP drayver tomonidan har bir jo'natiluvchi xabar paketlariga qo'shiladi va jo'natuvchi ilovasini hamda ushbu paket atalgan ilovani bir ma'noda identifikatsiyalaydi. Port nomerlari bo'yicha filtrlash imkoniyati uchun yuqori sath protokollariga port nomerlarini ajratish bo'yicha tarmoqda qabul qilingan kelishuvni bilish lozim.

Har bir paket ishlanishida ekranlovchi marshrutizator berilgan qoidalar jadvalini, paketning to'liq assotsiatsiyasiga mos keluvchi qoidani topgunicha, ketma-ket ko'rib chiqadi. Bu yerda assotsiatsiya deganda berilgan paket sarlavhalarida ko'rsatilgan parametrlar majmui tushuniladi. Agar ekranlovchi marshrutizator jadvaldagi qoidalarning birortasiga ham mos kelmaydigan paketni olsa, u xavfsizlik nuqtai nazaridan, uni yaroqsiz holga keltiradi.

Paketli filtrlar apparat va dasturiy amalga oshirilishi mumkin. Paketli filtr sifatida oddiy marshrutizator hamda kiruvchi va chiquvchi paketlarni filtrlashga moslashtirilgan, serverda ishlovchi dasturdan foydalanish mumkin. Zamonaviy marshrutizatorlar har bir port bilan bir necha o'nlab qoidalarni bog'lashi va kirishda, ham chiqishda paketlarni filtrlashi mumkin.

Paketli filtrlarning kamchiligi sifatida quyidagilarni ko'rsatish mumkin. Ular xavfsizlikning yuqori darajasini ta'minlamaydi, chunki faqat paket sarlavhalarini tekshiradilar va ko'pgina kerakli funksiyalarni madadlamaydi. Bu funksiyalarga, masalan, oxirgi uzellarni autentifikatsiyalash, xabarlar paketlarini kriptografik berkitish hamda ularning yaxlitligini va haqiqiyligini tekshirish kiradi. Paketli filtrlar dastlabki adreslarni almashtirib qo'yish va xabarlar paketi tarkibini ruxsatsiz o'zgartirish kabi keng tarqalgan tarmoq hujumlariga zaif hisoblanadilar. Bu xil brandmauerlarni «aldash» qiyin emas - filtrlashga ruxsat beruvchi qoidalarni qondiruvchi paket sarlavhaiarini shakllantirish kifoya.

Ammo paketli filtrlarning amalga oshirilishining soddaligi, yuqori unumdorligi, dasturiy ilovalar uchun shaffofligi va narxining pastligi, ularning hamma yerda tarqalishiga va tarmoq xavfsizligi tizimining majburiy elementi kabi ishlatilishiga imkon yaratdi.

Seans sathi shlyuzi, (*ekranlovchi transport* deb ham yuritiladi) virtual ulanishlarni nazoratlashga va tashqi tarmoq bilan o'zaro aloqa qilishda IP-adreslarni translatsiyalashga atalgan. U OSI modelining seans sathida ishlaydi va ishlash jarayonida etalon modelning transport va

tarmoq sathlarini ham qamrab oladi. Seans sathi shlyuzining himoyalash funksiyalari vositachilik funksiyalariga taalluqli.

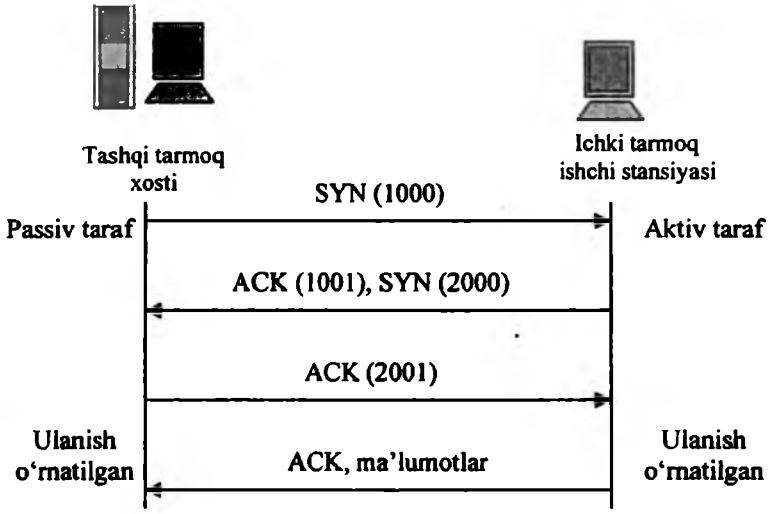
Virtual ulanishlarning nazorati aloqani kvitirlashni kuzatishdan hamda o'rnatilgan virtual kanallar bo'yicha axborot uzatilishining nazoratlashdan iborat. Aloqani kvitirlashning nazoratida seans sathida shlyuz ichki tarmoq ishchi stansiyasi va tashqi tarmoq kompyuteri orasida virtual ulanishni kuzatib, so'ralayotgan aloqa seansining joizligini aniqlaydi.

Bunday nazorat TCP protokolining seans sathi paketlarining sarlavhasidagi axborotga asoslanadi. Ammo TCP-sarlavhalarni tahlillashda paketli filtr faqat manba va qabul qiluvchi portlarining nomerini tekshirsa, ekranlovchi transport aloqani kvitirlash jarayoniga taalluqli boshqa hoshiyalarni tahlillaydi.

Aloqa seansiga so'rovning joizligini aniqlash uchun seans sathi shlyuzi quyidagi harakatlarni bajaradi. Ishchi stansiya (mijoz) tashqi tarmoq bilan bog'lanishni so'raganida, shlyuz bu so'rovni qabul qilib uning filtrlashning bazaviy mezonlarini qanoatlantirishini, masalan, server mijoz va u bilan assotsiatsiyalangan ismning IP-adresini aniqlay olishini tekshiradi. So'ngra shlyuz, mijoz ismidan harakat qilib, tashqi tarmoq kompyuteri bilan ulanishni o'rnatadi va TCP protokoli bo'yicha kvitirlash jarayonining bajarilishini kuzatadi.

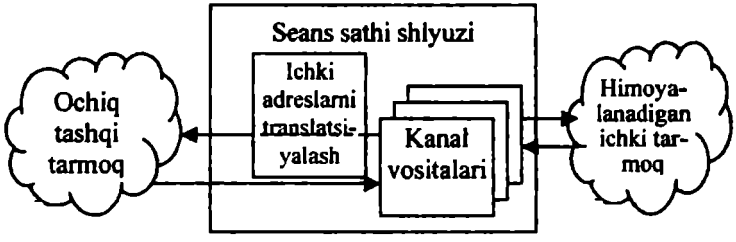
Bu muolaja SYN (sinxronlash) va ACK (tasdiqlash) bayroqlari orqali belgilanuvchi TCP-paketlarni almashishdan iborat (6.7-rasm).

SYN bayroq bilan belgilangan va tarkibida ixtiyoriy son, masalan, 1000, bo'lgan TCP seansining birinchi paketi mijozning seans ochishga so'rovi hisoblanadi. Bu paketni olgan tashqi tarmoq kompyuteri javob tariqasida ACK bayroq bilan belgilangan va tarkibida olingan paketdagidan bittaga katta (bizning holda 1001) son bo'lgan paketni jo'natadi. Shu tariqa, mijozdan SYN paketi olinganligi tasdiqlanadi. So'ngra, teskari muolaja amalga oshiriladi: tashqi tarmoq kompyuteri ham mijozga uzatiluvchi ma'lumotlar birinchi baytining tartib raqami bilan (masalan, 2000) SYN paketini jo'natadi, mijoz esa uni olganligini, tarkibida 2001 soni bo'lgan paketni uzatish orqali tasdiqlaydi. Shu bilan aloqani kvitirlash jarayoni tugallanadi.



6.7- rasm. TSR protokoli bo'yicha aloqani kvitirlash sxemasi.

Seans sathi shlyuzi (6.8-rasm) uchun so'ralgan seans joiz hisoblanadi, qachonki aloqani kvitirlash jarayoni bajarilishida SYN va ACK bayroqlar hamda TCP-paketlari sarlavhalaridagi sonlar o'zaro mantiqiy bog'langan bo'lsa.



6.8-rasm. Seans sathi shlyuzi ishlash sxemasi.

Ichki tarmoqning ichki stansiyasi va tashqi tarmoqning kompyuteri TCP seansining avtorizatsiyalangan qatnashchilari ekanligi hamda ushbu seansning joizligi tasdiqlanganidan so'ng shlyuz ulanishni

o'rnatadi. Bunda shlyuz ulanishlarning maxsus jadvaliga mos axborotni (jo'natuvchi va qabul qiluvchi adreslari, ulanish holati, ketma-ketlik nomeri xususidagi axborot va h.) kiritadi.

Shu ondan boshlab shlyuz paketlarni nusxalaydi va ikkala tomonga yo'naltirib, o'rnatilgan virtual kanal bo'yicha axborot uzatilishini nazorat qiladi. Ushbu nazorat jarayonida seans sathi shlyuzi paketlarni filtrlamaydi. Ammo u uzatiluvchi axborot sonini nazorat qilishi va qandaydir chegaradan oshganida ulanishni uzishi mumkin. Bu esa, o'z navbatida, axborotning ruxsatsiz eksport qilinishiga to'siq bo'ladi. Virtual ulanishlar xususidagi qaydlash axborotining to'planishi ham mumkin.

Seans sathi shlyuzlarida virtual ulanishlarni nazoratlashda *kanal vositachilari* (pipe proxy) deb yuritiluvchi maxsus dasturlardan foydalaniladi. Bu vositachilar ichki va tashqi tarmoqlar orasida virtual kanallarni o'rnatadi, so'ngra TCP/IP ilovalari generatsiyalangan paketlarning ushbu kanal orqali uzatilishini nazoratlaydi.

Kanal vositachilari TCP/IPning muayyan xizmatlariga mo'ljallangan. Shu sababli, ishlashi muayyan ilovalarning vositachi-dasturlariga asoslangan tatbiqiy sath shlyuzlari imkoniyatlarini kengaytirishda seans sath shlyuzlaridan foydalanish mumkin.

Seans sathi shlyuzi tashqi tarmoq bilan o'zaro aloqada tarmoq sathi ichki adreslarini (IP-adreslarini) translatsiyalashni ham ta'minlaydi. Ichki adreslarni translatsiyalash ichki tarmoqdan tashqi tarmoqqa jo'natiluvchi barcha paketlarga nisbatan bajariladi.

Amalga oshirilishi nuqtai nazaridan seans sathi shlyuzi yetarlicha oddiy va nisbatan ishonchli dastur hisoblanadi. U ekranlovchi marshrutizatorni virtual ulanishlarni nazoratlash va ichki IP-adreslarni translatsiyalash funksiyalari bilan to'ldiradi.

Seans sathi shlyuzining kamchiliklari – ekranlovchi marshrutizatorlarning kamchiliklariga o'xshash. Ushbu texnologiyaning yana bir jiddiy kamchiligi ma'lumotlar hoshiyalari tarkibini nazoratlash mumkin emasligi. Natijada, niyati buzuq odamlarga zarar keltiruvchi dasturlarni himoyalanuvchi tarmoqqa uzatish imkoniyati tug'iladi. Undan tashqari, TCP-sessiyasining (TCP hijacking) ushlab qolinishida niyati buzuq odam hujumlarini hatto ruxsat berilgan sessiya doirasida amalga oshirishi mumkin.

Amalda aksariyat seans sath shlyuzlari mustaqil mahsulot bo'lmay, tatbiqiy sath shlyuzlari bilan komplektda taqdim etiladi.

Tatbiqiy sath shlyuzi (*ekranlovchi shlyuz* deb ham yuritiladi) OSI modelining tatbiqiy sathida ishlab, taqdimiy sathni ham qamrab oladi va tarmoqlararo aloqaning eng ishonchli himoyasini ta'minlaydi. Tatbiqiy sath shlyuzining himoyalash funksiyalari, seans sathi shlyuziga o'xshab, vositachilik funksiyalariga taalluqli. Ammo tatbiqiy sath shlyuzi seans sathi shlyuziga qaraganda himoyalashning ancha ko'p funksiyalarini bajarishi mumkin:

– brandmauer orqali ulanishni o'rnatishga urinishda foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;

– shlyuz orqali uzatiluvchi axborotning haqiqiyligini tekshirish;

– ichki va tashqi tarmoq resurslaridan foydalanishni chegaralash;

– axborotlar oqimini filtrlash va o'zgartirish, masalan, viruslarni dinamik tarzda qidirish va axborotni shaffof shifrlash;

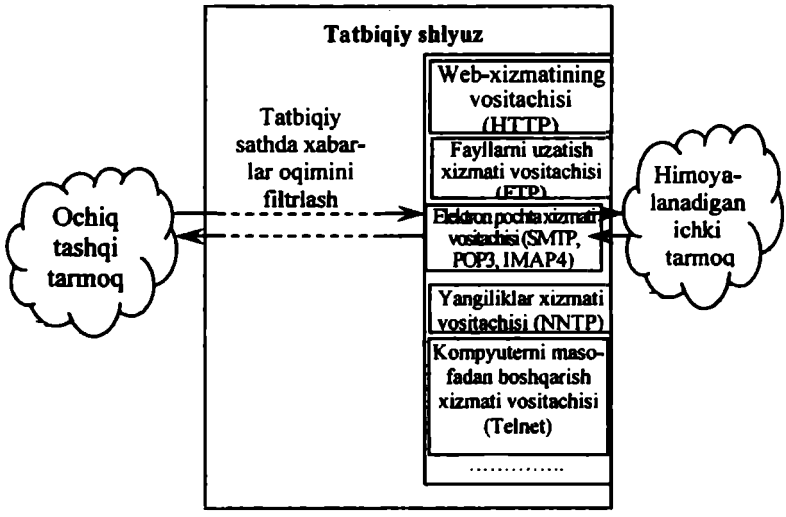
– hodisalarni qaydlash, hodisalarga reaksiya ko'rsatish hamda qaydlangan axborotni tahlillash va hisobotlarni generatsiyalash;

– tashqi tarmoqdan so'raluvchi ma'lumotlarni keshlash.

Tatbiqiy sath shlyuzi funksiyalari vositachilik funksiyalariga taalluqli bo'lganligi sababli, bu shlyuz universal kompyuter hisoblanadi va bu kompyuterda har bir xizmat ko'rsatiluvchi tatbiqiy protokol (HTTP, FTP, SMTP, NNTP va h.) uchun bittadan vositachi dastur (ekranlovchi agent) ishlatiladi. TCP/IPning har bir xizmatining vositachi dasturi (application proxy) aynan shu xizmatga taalluqli xabarlarni ishlashga va himoyalash funksiyalarini bajarishga mo'ljallangan.

Tatbiqiy sath shlyuzi mos ekranlovchi agentlar yordamida kiruvchi va chiquvchi paketlarni ushlab qoladi, axborotni nusxalaydi va qayta jo'natadi, ya'ni ichki va tashqi tarmoqlar orasidagi to'g'ridan-to'g'ri ulanishni istisno qilgan holda, server-vositachi funksiyasini bajaradi (6.9-rasm).

Tatbiqiy sath shlyuzi ishlatadigan vositachilar seans sathi shlyuzlarining kanal vositachilaridan jiddiy farqlanadi. Birinchidan, tatbiqiy sath shlyuzlari muayyan ilovalar (dasturiy serverlar) bilan bog'langan, ikkinchidan ular OSI modelining tatbiqiy sathida xabarlar oqimini filtrlashlari mumkin.



6.9-rasm. Tatbiqiy shlyuz ishlash sxemasi.

Tatbiqiy sath shlyuzlari vositachi sifatida mana shu maqsadlar uchun maxsus ishlab chiqilgan TCP/IPning muayyan xizmatlarining dasturiy serverlari – HTTP, FTP, SMTP, NNTP va h. – serverlaridan foydalanadi. Bu dasturiy serverlar brandmauerlarda rezident rejimida ishlaydi va TCP/IPning mos xizmatlariga taalluqli himoyalash funksiyalarini amalga oshiradi. UDP trafigiga UDP-paketlar tarkibining maxsus translatori xizmat ko'rsatadi.

Ichki tarmoq ishchi serveri va tashqi tarmoq kompyuteri orasida ikkita ulanish amalga oshiriladi: ishchi stansiyadan brandmauergacha va brandmauerdan belgilangan joygacha. Kanal vositachilaridan farqli holda, tatbiqiy sath shlyuzining vositachilari faqat o'zlari xizmat qiluvchi ilovalar generatsiyalagan paketlarni o'tkazadi. Masalan, HTTP xizmatining vositachi-dasturi faqat shu xizmat generatsiyalagan trafikni ishlaydi.

Agar qandaydir ilovada o'zining vositachisi bo'lmasa, tatbiqiy sathdagi shlyuz bunday ilovani ishlay olmaydi va u blokirovka qilinadi. Masalan, agar tatbiqiy sathdagi shlyuz faqat HTTP, FTP va Telnet vositachi dasturlaridan foydalansa, u faqat shu xizmatlarga tegishli paketlarni ishlaydi va qolgan xizmatlarning paketlarini blokirovka qiladi.

Tatbiqiy sath shlyuzi vositachilari, kanal vositachilaridan farqli holda, ishlanuvchi ma'lumotlar tarkibini tekshirishni ta'minlaydi. Ular o'zlari xizmat ko'rsatadigan tatbiqiy sath protokollaridagi komandalarning alohida xillarini va xabarlardagi axborotlarni filtrlashlari mumkin.

Tatbiqiy sath shlyuzini sozlashda va xabarlarni filtrlash qoidalarini tavsiflashda quyidagi parametrlardan foydalaniladi: servis nomi, undan foydalanishning joiz vaqt oralig'i, ushbu servisga bog'liq xabar tarkibiga chegaralashlar, servis ishlatadigan kompyuterlar, foydalanuvchi identifikatori, autentifikatsiyalash sxemalari va h.

Tatbiqiy sath shlyuzi quyidagi afzalliklarga ega:

– aksariyat vositachilik funksiyalarini bajara olishi tufayli lokal tarmoq himoyasining yuqori darajasini ta'minlaydi;

– ilovalar sathida himoyalash ko'pgina qo'shimcha tekshirishlarni amalga oshirishga imkon beradi, natijada dasturiy ta'minot kamchiliklariga asoslangan muvaffaqiyatli hujumlar o'tkazish ehtimolligi kamayadi;

– tatbiqiy sath shlyuzining ishga layoqatligi buzilsa, bo'linuvchi tarmoqlar orasida paketlarning to'ppa-to'g'ri o'tishi blokirovka qilinadi, natijada, rad qilinishi tufayli himoyalanuvchi tarmoqning xavfsizligi pasaymaydi.

Tatbiqiy sath shlyuzining kamchiliklariga quyidagilar kiradi:

– narxining nisbatan yuqoriligi;

– brandmauerning o'zi hamda uni o'rnatish va konfiguratsiyalash muolajasi yetarlicha murakkab;

– kompyuter platformasi unumdorligiga va resurslari hajmiga quyiladigan talablarning yuqoriligi;

– foydalanuvchilar uchun shaffoflikning yo'qligi va tarmoqlararo aloqa o'rnatilishida o'tkazish qobiliyatining susayishi.

Oxirgi kamchilikka batafsil to'xtalamiz. Vositachilar server va mijoz orasida paketlar uzatilishida oraliq rolini bajaradi. Avval vositachi bilan ulanish o'rnatiladi, so'ngra vositachi adresat bilan ulanishni yaratish yoki yaratmaslik xususida qaror qabul qiladi. Mos holda tatbiqiy sath shlyuzi ishlashi jarayonida har qanday ruxsat etilgan ulanishni qaytalaydi. Natijada, foydalanuvchilar uchun shaffoflik yo'qoladi va ulanishga xizmat qilishga qo'shimcha xarajat sarflanadi.

Ekspert sathi shlyuzi. Tatbiqiy sath shlyuzining foydalanuvchilar uchun shaffofligining yo'qligi va tarmoqlararo aloqa o'rnatilishida o'tkazish qobiliyatining susayishi kabi jiddiy kamchiliklarini bartaraf etish maqsadida paketlarni filtrlashning yangi texnologiyasi ishlab

chiqilgan. Bu texnologiyani ba'zida *ulanish holatini nazoratlashli filtrlash* (stateful inspection) yoki ekspert sathidagi filtrlash deb yuritishadi. Bunday filtrlash paketlar holatini ko'p sathli tahlillashning maxsus usullari (SMLT) asosida amalga oshiriladi.

Ushbu gibrid texnologiya tarmoq sathida paketlarni ushlab qolish va undan ulanishni nazorat qilishda ishlatiluvchi tatbiqiy sath axborotini chiqarib olish orqali ulanish holatini kuzatishga imkon beradi.

Ishlashi asosini ushbu texnologiya tashkil etuvchi tarmoqlararo ekran *ekspert sath brandmaueri* deb yuritiladi. Bunday brandmauerlar o'zida ekranlovchi marshrutizatorlar va tatbiqiy sath shlyuzlari elementlarini uyg'unlashtiradi. Ular har bir paket tarkibini berilgan xavfsizlik siyosatiga muvofiq baholaydilar.

Shunday qilib, ekspert sathidagi brandmauerlar quyidagilarni nazoratlashga imkon beradi:

– mavjud qoidalar jadvali asosida har bir uzatiluvchi paketni;

– holatlar jadvali asosida har bir sessiyani;

– ishlab chiqilgan vositachilar asosida har bir ilovani.

Ekspert sath tarmoqlararo ekranlarining afzalliklari sifatida ularning foydalanuvchilar uchun shaffofligini, axborot oqimini ishlashining yuqori tezkorligini hamda ular orqali o'tuvchi paketlarning IP-adreslarini o'zgartirmasligini ko'rsatish mumkin. Oxirgi afazallik IP-adresdan foydalanuvchi tatbiqiy sathning har qanday protokolining bunday brandmauerlardan hech qanday o'zgarishsiz yoki maxsus dasturlashsiz birga ishlay olishini anglatadi.

Bunday brandmauerlarning avtorizatsiyalangan mijoz va tashqi tarmoq kompyuteri orasida to'g'ridan-to'g'ri ulanishga yo'l qo'yishi, himoyaning unchalik yuqori bo'lmagan darajasini ta'minlaydi. Shu sababli, amalda ekspert sathini filtrlash texnologiyasidan kompleks brandmauerlar ishlashi samaradorligini oshirishda foydalaniladi. Ekspert sathning filtrlash texnologiyasini ishlatuvchi kompleks brandmauerlarga misol tariqasida Fire Wall-1 va ON Guard larni ko'rsatish mumkin.

6.3. Tarmoqlararo ekranlar asosidagi tarmoq himoyasining sxemalari

Tarmoqlararo aloqani samarali himoyalash uchun brandmauer tizimi to'g'ri o'rnatilishi va konfiguratsiyalanishi lozim. Ushbu jarayon quyidagilarni o'z ichiga oladi:

– tarmoqlararo aloqa siyosatini shakllantirish;

– brandmauerni ulash sxemasini tanlash va parametrlarini sozlash.

Tarmoqlararo aloqa siyosatini shakllantirish

Tarmoqlararo aloqa siyosatini shakllantirishda quyidagilarni aniqlash lozim:

– tarmoq servislaridan foydalanish siyosati;

– tarmoqlararo ekran ishlashi siyosati.

Tarmoq servislaridan foydalanish siyosati himoyalanuvchi kompyuter tarmoqning barcha servislarini taqdim etish hamda ulardan foydalanish qoidalarini belgilaydi. Ushbu siyosat doirasida tarmoq ekrani orqali taqdim etiluvchi barcha servislar va har bir servis uchun mijozlarning joiz adreslari berilishi lozim. Undan tashqari, foydalanuvchilar uchun qachon va qaysi foydalanuvchilar qaysi servisdan va qaysi kompyuterda foydalanishlarini tavsiflovchi qoidalar ko'rsatilishi lozim. Foydalanish usullariga chegaralashlar ham beriladi. Bu chegaralashlar foydalanuvchilarning Internet ning man etilgan servislaridan aylanma yo'l orqali foydalanishlariga yo'l qo'ymaslik uchun zarur. Foydalanuvchilar va kompyuterlarni autentifikatsiyalash qoidalari hamda tashkilot lokal tarmog'i tashqarisidagi foydalanuvchilarning ishlash sharoitlari alohida belgilanishi lozim.

Tarmoqlararo ekran ishlashi siyosatida tarmoqlararo aloqani boshqarishning brandmauer ishlashi asosidagi bazaviy prinsipi beriladi. Bunday prinsiplarning quyidagi ikkitasidan biri tanlanishi mumkin:

– oshkora ruxsat etilmagani man qilingan;

– oshkora man etilmaganiga ruxsat berilgan.

«Oshkora ruxsat etilmagani man qilingan» prinsipi tanlanganida tarmoqlararo ekran shunday sozlanadiki, harqanday ruxsat etilmagan tarmoqlararo aloqalar blokirovka qilinadi. Ushbu prinsip axborot xavfsizligining barcha sohalarida ishlatiluvchi foydalanishning mumtoz modeliga mos keladi. Bunday yondashish, imtiyozlarni minimallashtirish prinsipini adekvat amalga oshirishga imkon berishi sababli, xavfsizlik nuqtai nazaridan yaxshiroq hisoblanadi. Mohiyati bo'yicha «oshkora ruxsat etilmagani man qilingan» prinsipi bilmaslik zarar keltirishi faktini e'tirof etishdir. Ta'kidlash lozimki, ushbu prinsipga asosan ta'riflangan foydalanish qoidalari foydalanuvchilarga ma'lum noqulayliklar tug'dirishi mumkin.

«Oshkora man etilmaganiga ruxsat berilgan» prinsipi tanlanganida tarmoqlararo ekran shunday sozlanadiki, faqat oshkora man etilgan tarmoqlararo aloqalar blokirovka qilinadi. Bu holda, foydalanuvchilar tomonidan tarmoq servislaridan foydalanish qulayligi oshadi, ammo tar-

moqlararo aloqa xavfsizligi pasayadi. Foydalanuvchilarning tarmoqlararo ekranni chetlab o'tishlariga imkon tug'iladi, masalan, ular siyosat man qilmagan (hatto siyosatda ko'rsatilmagan) yangi servislaridan foydalanishlari mumkin. Ushbu prinsip amalga oshirilishida ichki tarmoq xakerlarning hujumlaridan kamroq himoyalangan bo'ladi. Shu sababli, tarmoqlararo ekranlarni ishlab chiqaruvchilari odatda ushbu prinsipdan foydalanmaydilar.

Tarmoqlararo ekran simmetrik emas. Unga ichki tarmoqning tashqi tarmoqdan va aksincha foydalanishni chegaralovchi qoidalar alohida beriladi. Umumiy holda, tarmoqlararo ekranning ishi quyidagi ikkita guruh funksiyalarni dinamik tarzda bajarishga asoslangan:

– u orqali o'tayotgan axborot oqimini filtrlash;

– tarmoqlararo aloqa amalga oshirilishida vositachilik.

Oddiy tarmoqlararo ekranlar bu funksiyalarning birini bajarishga mo'ljallangan. Kompleks tarmoqlararo ekranlar himoyalashning ko'rsatilgan funksiyalarining birgalikda bajarilishini ta'minlaydi.

Tarmoqlararo ekranlarni ulashning asosiy sxemalari. Korporativ tarmoqni global tarmoqlarga ulaganda himoyalanuvchi tarmoqning global tarmoqdan va global tarmoqning himoyalanuvchi tarmoqdan foydalanishini chegaralash hamda ulanuvchi tarmoqdan global tarmoqning masofadan ruxsatsiz foydalanishidan himoyalashni ta'minlash lozim. Bunda tashkilot o'zining tarmog'i va uning komponentlari xususidagi axborotni global tarmoq foydalanuvchilaridan berkitishga manfaatdor. Masofadagi foydalanuvchilar bilan ishlash himoyalanuvchi tarmoq resurslaridan foydalanishning qat'iy chegaralanishini talab etadi.

Tashkilotdagi korporativ tarmoq tarkibida ko'pincha himoyalanishning turli sathli bir necha segmentlarga ega bo'lishi ehtiyoji tug'iladi:

– bemalol foydalaniluvchi segmentlar (masalan, reklama WWW-serverlari);

– foydalanish chegaralangan segmentlar (masalan, tashkilotning masofadagi uzellari xodimlarining foydalanishi uchun);

– yopiq segmentlar (masalan, tashkilotning moliya lokal qism tarmog'i).

Tarmoqlararo ekranlarni ulashda turli sxemalardan foydalanish mumkin. Bu sxemalar himoyalanuvchi tarmoq ishlashi sharoitiga hamda ishlatiladigan brandmauerlarning tarmoq interfeyslari soniga va boshqa xarakteristikalariga bog'liq. Tarmoqlararo ekranni ulashning quyidagi sxemalari keng tarqalgan:

– ekranlovchi marshrutizatordan foydalanilgan himoya sxemalari;

– lokal tarmoqni umumiy himoyalash sxemalari;

– himoyalanuvchi yopiq va himoyalanmaydigan ochiq qism tarmoqli sxemalar;

– yopiq va ochiq qism tarmoqlarni alohida himoyalovchi sxemalar.

Ekranlovchi marshrutizatordan foydalanilgan himoya sxemasi.

Paketlarni filtrlashga asoslangan tarmoqlararo ekran keng tarqalgan va amalga oshirilishi oson. U himoyalanuvchi tarmoq va bo'lishi mumkin bo'lgan g'anim ochiq tarmoq orasida joylashgan ekranlovchi marshrutizatordan iborat (6.10-rasm).

Ekranlovchi marshrutizator (paketli filtr) kiruvchi va chiquvchi paketlarni ularning adreslari va portlari asosida blokirovka qilish va filtrlash uchun konfiguratsiyalangan.

6.10-rasm. Tarmoqlararo ekran – ekranlovchi marshrutizator.

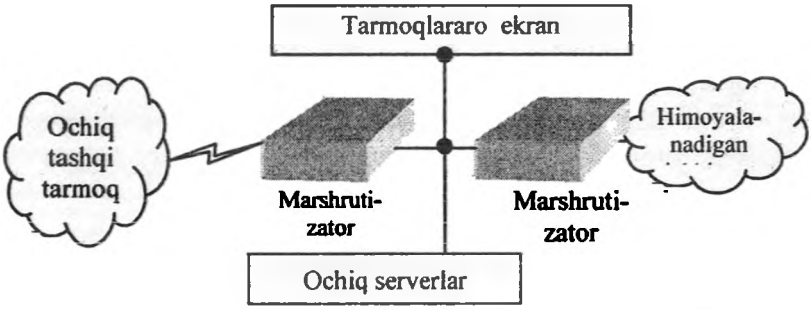
Himoyalanuvchi tarmoqdagi kompyuterlar Internetdan to'g'ridan-to'g'ri foydalanaoladi, Internetning ulardan foydalanishining ko'p qismi esa blokirovka qilinadi. Umuman, ekranlovchi marshrutizator yuqorida tavsiflangan himoyalash siyosatidan istalganini amalga oshirishi mumkin. Ammo, agar marshrutizator paketlarni manba porti va kirish yo'li hamda chiqish yo'li portlari nomeri bo'yicha filtrlamasa, «oshkora ruxsat etilmagani man qilingan» siyosatini amalga oshirish qiyinlashadi.

Paketlarni filtrlashga asoslangan tarmoqlararo ekranning kamchiliklari quyidagilar:

– filtrlash qoidalarining murakkabligi; ba'zi hollarda bu qoidalar majmui bajarilmasligi mumkin;

– filtrlash qoidalarini to'liq testlash mumkin emasligi; bu tarmoqni testlanmagan hujumlardan himoyalanmasligiga olib keladi;

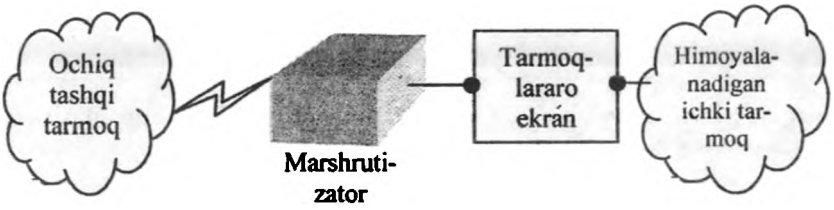
– hodisalarni ro'yxatga olish imkoniyatining yo'qligi; natijada ma'murga mashrutizatorning hujumga duch kelganligini va obro'-sizlantirilganligini aniqlash qiyinlashadi.



6.11-rasm. Bitta tarmoq interfeysli firewall yordamida lokal tarmoqni himoyalash.

Lokal tarmoqni umumiy himoyalash sxemalari. Bitta tarmoq interfeysli brandmauerlardan foydalanilgan himoyalash sxemalari (6.11-rasm) xavfsizlik va konfiguratsiyalashning qulayligi nuqtai nazaridan samarasiz hisoblanadi. Ular ichki va tashqi tarmoqlarni fizik ajratmaydilar, demak, tarmoqlararo aloqaning ishonchli himoyasini ta'minlay olmaydilar.

Lokal tarmoqni umumiy himoyalash sxemasi eng oddiy yechim bo'lib, unda brandmauer lokal tarmoqni tashqi g'anim tarmoqdan butunlay ekranlaydi (6.12-rasm). Marshrutizator va brandmauer orasida faqat bitta yo'l bo'lib, bu yo'l orqali butun trafik o'tadi. Brandmauerning ushbu varianti «oshkora ruxsat etilmagani man qilingan» prinsipiga asoslangan himoyalash siyosatini amalga oshiradi. Odatda, marshrutizator shunday sozlanadiki, brandmauer tashqaridan ko'rinadigan yagona mashina bo'ladi.



6.12-rasm. Lokal tarmoqni umumiy himoyalash sxemasi.

Lokal tarmoq tarkibidagi ochiq serverlar ham tarmoqlararo ekranlar tomonidan himoyalanadi. Ammo tashqi tarmoq foydalanaoladigan serverlarni himoyalanuvchi lokal tarmoqlarning boshqa resurslari bilan birlashtirish tarmoqlararo aloqa xavfsizligini jiddiy pasaytiradi.

Tarmoqlararo ekran foydalanadigan xostga foydalanuvchilarni kuchaytirilgan autentifikatsiyalash uchun dastur o'ranatilishi mumkin.

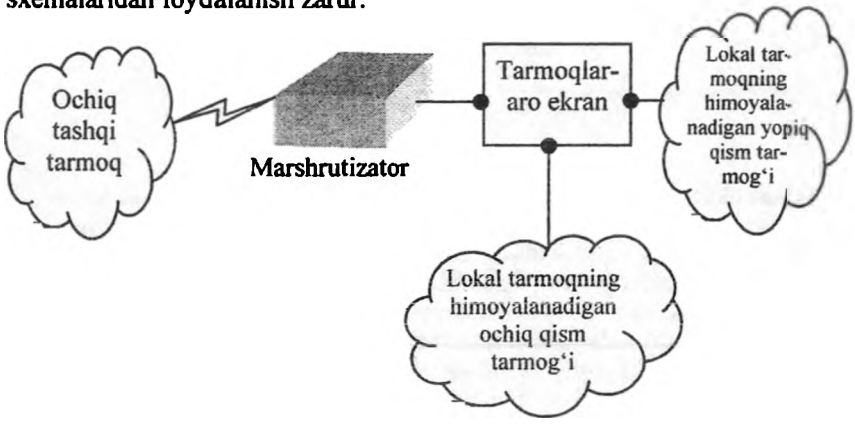
Himoyalanuvchi yopiq va himoyalanmaydigan ochiq qism tarmoqli sxemalar. Agar lokal tarmoq tarkibida umumfoydalanuvchi ochiq serverlar bo'lsa, ularni tarmoqlararo ekrandan oldin ochiq qism tarmoq sifatida chiqarish maqsadga muvofiq hisoblanadi (6.13-rasm).

Ushbu usul lokal tarmoq yopiq qismining kuchli himoyalanishini, ammo tarmoqlararo ekrangacha joylashgan ochiq serverlarning pasaygan himoyalanishini ta'minlaydi.

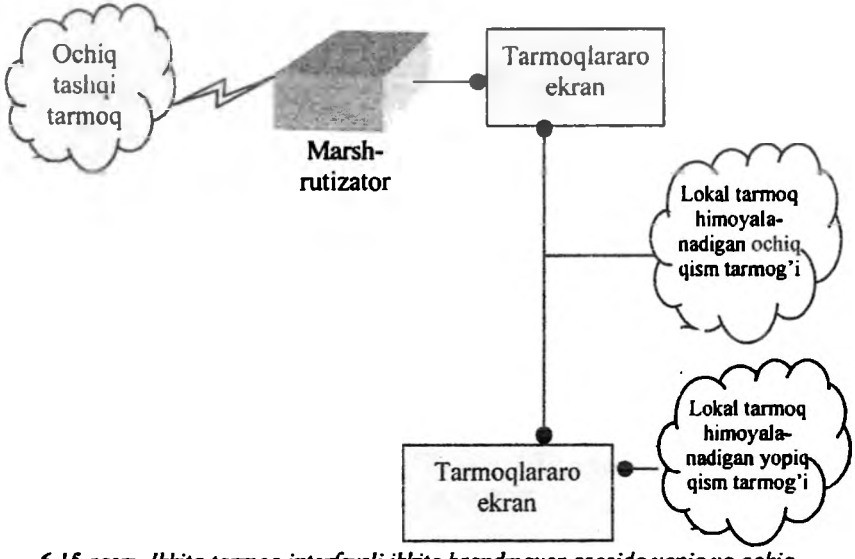
6.13-rasm. Himoyalanadigan yopiq va himoyalanmaydigan ochiq qism tarmoqli sxema.

Ba'zi brandmauerlar bu serverlarni o'zida joylashtiradi. Ammo bu brandmauerning xavfsizligi va kompyuterning yuklanishi nuqtai nazari-

dan yaxshi yechim hisoblanmaydi. Himoyalanuvchi yopiq va himoyalanmaydigan ochiq qism tarmoqli sxemani ochiq qism tarmoq xavfsizligiga qo'yiladigan talablarning yuqori bo'lmagan hollarida ishlatilishi maqsadga muvofiq hisoblanadi. Agar ochiq server xavfsizligiga yuqori talablar qo'yilsa, yopiq va ochiq qism tarmoqlarni alohida himoyalash sxemalaridan foydalanish zarur.



6.14-rasm. Uchta tarmoq interfeysli bir brandmauer asosida yopiq va ochiq qism tarmoqlarni alohida himoyalash sxemasi.



6.15-rasm. Ikkita tarmoq interfeysli ikkita brandmauer asosida yopiq va ochiq qism tarmoqlarni alohida himoyalash sxemasi ikkita.

Yopiq va ochiq qism tarmoqlarni alohida himoyalovchi sxemalar. Bunday sxemalar uchta tarmoq interfeysli bitta brandmauer (6.14-rasm) yoki ikkita tarmoq interfeysli ikkita brandmauer (6.15-rasm) asosida qurilishi mumkin. Ikkala holda ham ochiq va yopiq qism tarmoqlardan faqat tarmoqlararo ekran orqali foydalanish mumkin. Bunda ochiq qism tarmoq-dan foydalanish yopiq qism tarmoqdan foydalanishga imkon bermaydi.

Ikkita brandmauerli sxema tarmoqlararo aloqa xavfsizligining yuqori darajasini ta'minlaydi. Bunda har bir brandmauer yopiq tarmoqni himoyalashning alohida eshelonini hosil qiladi, himoyalanuvchi ochiq qism tarmoq esa ekranlovchi qism tarmoq sifatida ishtirok etadi.

Odatda ekranlovchi qism tarmoq shunday konfiguratsiyalanadiki, qism tarmoq kompyuteridan g'anim tashqi tarmoq va lokal tarmoqning yopiq qism tarmog'i foydalana olsin. Ammo tashqi tarmoq va yopiq qism tarmoq orasida to'g'ridan-to'g'ri axborot paketlarini almashish mumkin emas. Ekranlovchi qism tarmoqli tizimni hujum qilishda, bo'lmaganida himoyaning ikkita mustaqil chizig'ini bosib o'tishga to'g'ri keladi. Bu esa juda murakkab masala hisoblanadi. Tarmoqlararo ekran holatlarini monitoringlash vositalari bunday urinishni doimo aniqlashi va tizim ma'muri o'z vaqtida ruxsatsiz foydalanishga qarshi zaruriy choralar ko'rishi mumkin.

Ta'kidlash lozimki, aloqaning kommutatsiyalanuvchi liniyasi orqali ulanuvchi masofadagi foydalanuvchilarning ishi ham tashkilotda o'tkaziluvchi xavfsizlik siyosatiga muvofiq nazorat qilinishi shart. Bunday masalaning namunaviy hal etilishi – zaruriy funksional imkoniyatlarga ega bo'lgan masofadan foydalanish serverini (terminal serverni) o'rnatish. Terminal server bir necha asinxron portlarga va lokal tarmoqning bitta interfeysiga ega bo'lgan tizim hisoblanadi. Asinxron portlar va lokal tarmoq orasida axborot almashish faqat tashqi foydalanuvchini autentifikatsiyalashdan keyin amalga oshiriladi.

Terminal serverni ulash shunday amalga oshirish lozimki, uning ishi faqat tarmoqlararo ekran orqali bajarilsin. Bu masofalagi foydalanuvchilarning tashkilot axborot resurslari bilan ishlash xavfsizligining kerakli darajasini ta'minlashga imkon beradi.

Terminal serverni ochiq qism tarmoq tarkibiga kiritilganida bunday ulanish joiz hisoblanadi. Terminal serverning dasturiy ta'minoti kommutatsiyalanuvchi kanallar orqali aloqa seanslarini ma'murlash va nazoratlash imkoniyatini ta'minlashi lozim. Zamonaviy terminal serverlarni boshqarish modullari serverni o'zini xavfsizligini ta'minlash va mi-

jozlarning foydalanishini chegaralash bo'yicha yetarlicha rivojlangan imkoniyatlarga ega va quyidagi funksiyalarni bajaradi:

– ketma-ket portlardan, PPP protokoli bo'yicha masofadan hamda ma'mur konsolidan foydalanishda lokal parolni ishlatish;

– lokal tarmoqning qandaydir mashinasining autentifikatsiyalashga so'rovidan foydalanish;

– autentifikatsiyalashning tashqi vositalaridan foydalanish;

– terminal serveri portlaridan foydalanishni nazoratlovchi ro'yxatni o'rnatish;

– terminal server orqali aloqa seanslarini protokollash.

Shaxsiy va taqsimlangan tarmoq ekranlari. Oxirgi bir necha yil mobaynida korporativ tarmoq tuzilmasida ma'lum o'zgarishlar sodir bo'ldi. Agar ilgari bunday tarmoq chegaralarini aniq belgilash mumkin bo'lgan bo'lsa, hozirda bu mumkin emas. Yaqindayoq bunday chegara barcha marshrutizatorlar yoki boshqa qurilmalar (masalan, modemlar) orqali o'tar va ular yordamida tashqi tarmoqlarga chiqilar edi. Ammo hozirda tarmoqlararo ekran orqali himoyalanuvchi tarmoqning to'la huquqli egasi – himoyalanuvchi perimetr tashqarisidagi xodim hisoblanadi. Bunday xodimlar sirasiga uydagi yoki mehnat safaridagi xodimlar kiradi. Shubhasiz, ularga ham himoya zarur. Ammo barcha an'anaviy tarmoqlararo ekranlar shunday qurilganki, himoyalanuvchi foydalanuvchilar va resurslar ularning himoyasida korporativ yoki lokal tarmoqning ichki tomonida bo'lishlari shart. Bu esa mobil foydalanuvchilar uchun mumkin emas.

Bu muammoni yechish uchun quyidagi yondashishlar taklif etilgan:

– taqsimlangan tarmoqlararo ekranlardan (distributed firewall) foydalanish;

– virtual xususiy tarmoq VPNlar imkoniyatidan foydalanish.

Taqsimlangan tarmoqlararo ekran tarmoqning alohida kompyuterini himoyalovchi markazdan boshqariluvchi tarmoq miniekranlar majmuidir.

Taqsimlangan brandmauerlarning qator funksiyalari (masalan, markazdan boshqarish, xavfsizlik siyosatini tarqatish) shaxsiy foydalanuvchilar uchun ortiqcha bo'lganligi sababli, taqsimlangan brandmauerlar modifikatsiyalandi. Yangi yondashish *shaxsiy tarmoqli ekranlash texnologiyasi* nomini oldi. Bunda tarmoqli ekran himoyalanuvchi shaxsiy kompyuterda o'rnatiladi. Kompyuterning shaxsiy ekrani (personal firewall) yoki tarmoqli ekranlash tizimi deb ataluvchi bunday ekran, boshqa barcha tizimli himoyalash vositalariga bog'liq bo'lmagan

holda butun chiquvchi va kiruvchi trafikni nazoratlaydi. Alohida kompyuterni ekranlashda tarmoq servisdan foydalanuvchanlik madadlanadi, ammo tashqi faollikning yuklanishi pasayadi. Natijada, shu tariqa himoyalanuvchi kompyuter ichki servislarining zaifligi pasayadi, chunki chetki niyati buzuq odam oldin, himoyalash vositalari sinchiklab va qat'iy konfiguratsiyalangan, ekranni bosib o'tishi lozim.

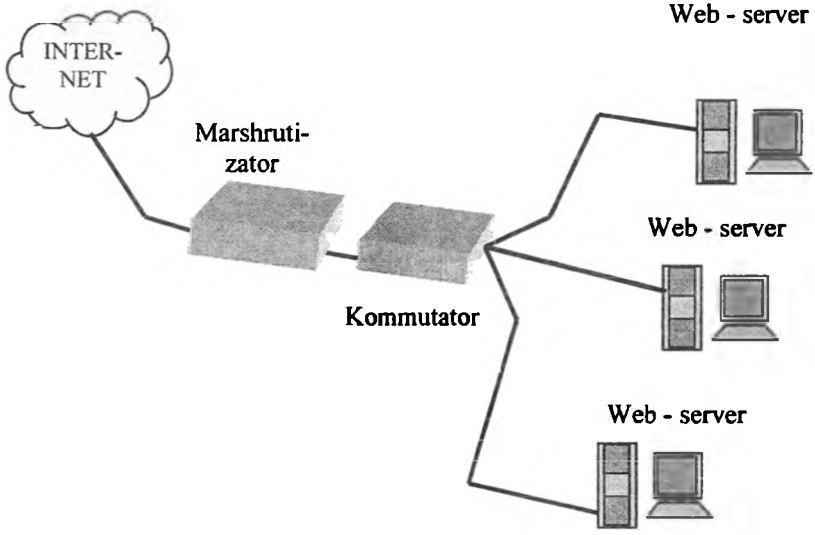
Taqsimlangan tarmoqlararo ekranning shaxsiy ekrandan asosiy farqi–taqsimlangan tarmoqlararo ekranda markazdan boshqarish funksiyasining borligi. Agar shaxsiy tarmoqli ekranlar ular o'rnatilgan kompyuter orqali boshqarilsa (uy sharoitida qo'llanishga juda mos), taqsimlangan tarmoqlararo ekranlar tashkilotning bosh ofisida o'rnatilgan boshqarishning umumiy konsoli tomonidan boshqarilishi mumkin.

Korporativ tarmoq ruxsatsiz foydalanishdan haqiqatan ham himoyalangan hisoblanadi, qachonki uning Internetdan kirish nuqtasida himoya vositalari hamda tashkilot lokal tarmog'i fragmentlarini, korporativ serverlarini va alohida kompyuterlar xavfsizligini ta'minlovchi yechimlar mavjud bo'lsa. Taqsimlangan yoki shaxsiy tarmoqlararo ekran asosidagi yechimlar alohida kompyuterlar, korporativ serverlar va tashkilot lokal tarmoq fragmentlari xavfsizligini ta'minlashni a'lo darajada bajaradi.

Taqsimlangan tarmoqlararo ekranlar, an'anaviy tarmoqlararo ekranlardan farqli ravishda, qo'shimcha dasturiy ta'minot bo'lib, xususan korporativ serverlarni, masalan, Internet-serverlarni ishonchli himoyalashi mumkin. Korporativ tarmoqni himoyalashning oqilona yechimi – himoyalash vositasini u himoya qiluvchi serveri bilan bir platformada joylashtirishdir. 6.16-rasmda korporativ serverlarni taqsimlangan tarmoqlararo ekranlar yordamida himoyalash sxemasi keltirilgan.

An'anaviy va taqsimlangan tarmoqlararo ekranlarni quyidagi ko'rsatkichlari bo'yicha taqqoslaylik.

Samaradorlik. An'anaviy brandmauer ko'pincha tarmoq perimetri bo'yicha joylashtiriladi, ya'ni u himoyaning bir qatlamini ta'minlaydi xolos. Agar bu yagona qatlam buzilsa, tizim harqanday hujumga bardosh beraolmaydi. Shaxsiy brandmauer operatsion tizimning yadro sathida ishlaydi va barcha kiruvchi va chiquvchi paketlarni tekshirib korporativ serverlarni ishonchli himoyalaydi.



6.16-rasm. Taqsimlangan tarmoqlararo ekranlar yordamida korporativ serverlarni himoyalsh.

O'rnatilishining osonligi. An'anaviy brandmauer korporativ tarmoq konfiguratsiyasining bo'limi sifatida o'rnatilishi lozim. Taqsimlangan brandmauer dasturiy ta'minot bo'lib, sanoqli daqiqalarda o'rnatiladi va olib tashlanadi.

Boshqarish. An'anaviy brandmauer tarmoq ma'muri tomonidan boshqariladi. Taqsimlangan brandmauer tarmoq ma'muri yoki lokal tarmoq foydalanuvchisi tomonidan boshqarilishi mumkin.

Unumdorlik. An'anaviy brandmauer tarmoqlararo almashishni ta'minlovchi qurilma bo'lib, unumdoroigi (paket/daqiqa bo'yicha) belgilangan chegaralanishga ega. U bir-biri bilan kommutatsiyalanuvchi mahalliy tarmoq orqali bog'langan o'suvchi server parklari uchun to'g'ri kelmaydi. Taqsimlangan brandmauer qabul qilingan xavfsizlik siyosatiga ziyon yetkazmasdan server parklarini o'sishiga imkon beradi.

Narxi. An'anaviy brandmauer, odatda, funksiyalari belgilangan narxi yetarlicha yuqori tizim hisoblanadi. Brandmauerning taqsimlangan mahsulotlari dasturiy ta'minot bo'lib, an'anaviy tarmoqlararo ekranlar narxining 1/5 yoki 1/10 ga teng.

VII bob. HIMOYALANGAN VIRTUAL XUSUSIY TARMOQLAR

7.1. Himoyalangan virtual xususiy tarmoqlarni qurish konsepsiyasi

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

Internetning hamma yerda tarqalishidan manfaat ko'rish maqsadida tarmoq 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 konsepsiyasi yaratildi. «Virtual» iborasi VPN atamasiga ikkita uzel o'rtasidagi ulanishni vaqtincha, deb ko'rilishini ta'kidlash maqsadida kiritilgan. Haqiqatan, bu ulanish doimiy, qat'iy bo'lmay, faqat ochiq tarmoq bo'yicha trafik o'tganida mavjud bo'ladi.

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

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

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

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

VPN-mijoz, odatda shaxsiy kompyuter asosidagi dasturiy yoki dasturiy-apparat kompleksi bo'lib, uning tarmoq dasturiy ta'minoti u boshqa VPN-mijoz, VPN-server yoki VPN xavfsizligi shlyuzlari bilan almashinadigan trafikni shifrlash va autentifikatsiyalash uchun modifikatsiyalanadi. Odatda, VPN-mijozning amalga oshirilishi standart operatsion tizim – Windows NT/2000 yoki Unixni to'ldiruvchi dasturiy yechimdan iborat bo'ladi.

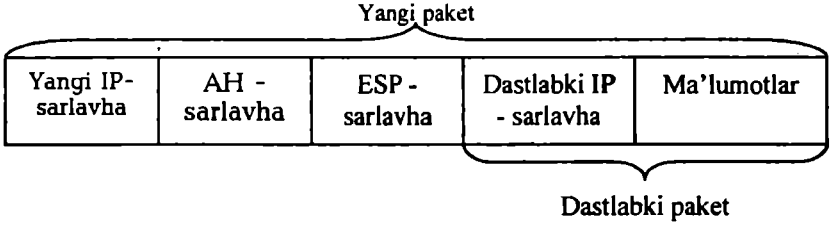
VPN-server server vazifasini o'tovchi, kompyuterga o'rnatiluvchi dasturiy yoki dasturiy-apparat kompleksidan iborat. VPN-server tashqi tarmoqlarning ruxsatsiz foydalanishidan serverlarni himoyalashni hamda alohida kompyuterlar va mos VPN-mahsulotlari orqali himoyalangan lokal tarmoq segmentlaridagi kompyuterlar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

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

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

Tunnellashga binoan, uzatiluvchi ma'lumotlar porsiyasi xizmatchi hoshiyalar bilan birga yangi «convert»ga «joylash» amalga oshiriladi. Bunda pastroq sath protokoli paketi yuqoriroq yoki xuddi shunday sath protokoli paketi ma'lumotlari maydoniga joylashtiriladi. Ta'kidlash lozimki, tunnelashning o'zi ma'lumotlarni ruxsatsiz foydalanishdan yoki buzishdan himoyalamaydi, ammo tunnellash tufayli inkapsulatsiyalanuvchi dastlabki paketlarni to'la kriptografik himoyalash imkoniyati paydo bo'ladi. Uzatiluvchi ma'lumotlar konfidensialligini ta'minlash maqsadida jo'natuvchi dastlabki paketlarni shifrlaydi, ularni, yangi IP-sarlavha bilan tashqi paketga joylaydi va tranzit tarmoq bo'yicha jo'natadi (7.1-rasm).

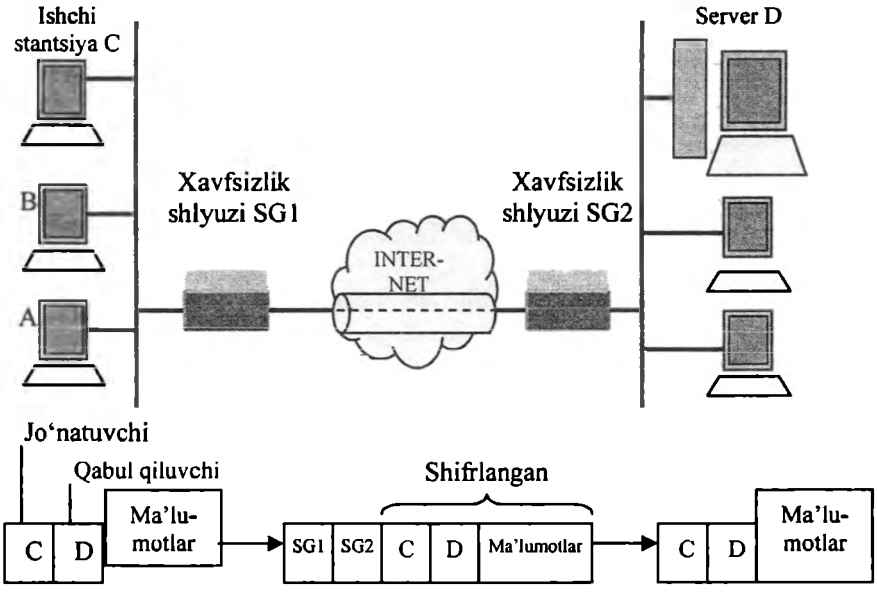
Ochiq tarmoq bo'yicha ma'lumotlarni tashishda tashqi paket sarlavhasining ochiq kanallaridan foydalaniladi.



7.1-rasm. Tunnellashga tayyorlangan paket misoli.

Tashqi paket himoyalangan kanalning oxirgi nuqtasiga kelishi bilan undan ichki dastlabki paket chiqarib olinib, rasshifrovka qilinadi va

uning tiklangan sarlavhasi ichki tarmoq bo'yicha keyingi uzatish uchun ishlatiladi (7.2-rasm).



7.2-rasm. Virtual himoyalangan tunnel sxemasi.

Tunnellashdan paket tarkibini nafaqat konfidensialligini, balki uning yaxlitligini va autentligini ta'minlashda foydalaniladi. Bunda elektron raqamli imzoni paketning barcha hoshiyalariga tarqatish mumkin.

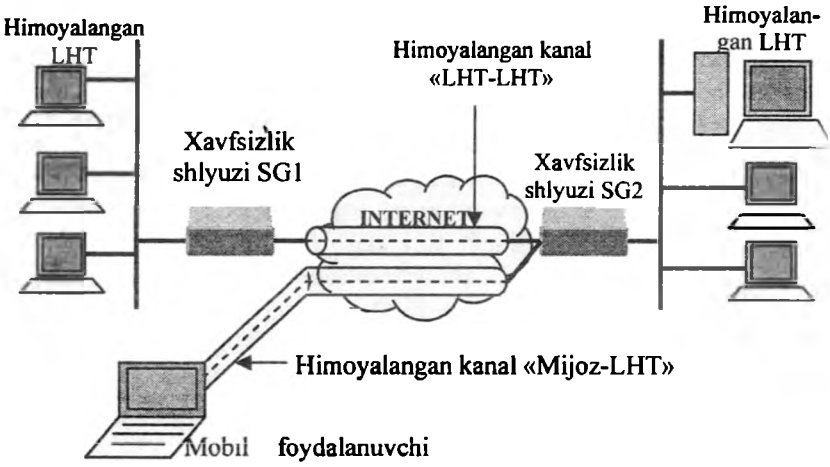
Internet bilan bog'lanmagan lokal tarmoq yaratilganda kompaniya o'zining tarmoq qurilmalari va kompyuterlari uchun xohlagan IP-adresdan foydalanishi mumkin. Oldin yakkalangan tarmoqlarni birlashtirishda bu adreslar bir-birlari va Internetda ishlatilayotgan adreslar bilan to'qnashishlari mumkin. Paketlarni inkapsulatsiyalash bu muammoni yechadi, chunki u dastlabki adreslarni berkitishga va Internet IP adreslari makonidagi noyob adreslarni qo'shishga imkon beradi. Bu adreslar keyin ma'lumotlarni ajratiluvchi tarmoqlar bo'yicha uzatishda ishlatiladi. Bunga lokal tarmoqqa ulanuvchi mobil foydalanuvchilarning IP-adreslarini va boshqa parametrlarini sozlash masalasi ham kiradi.

Tunellash mexanizmi himoyalanuvchi kanalni shakllantiruvchi turli protokollarda keng qo'llaniladi. Odatda tunnel faqat ma'lumotlarning konfidensialligi va yaxlitligining buzilishi xavfi mavjud bo'lgan ochiq tarmoq qismida, masalan, ochiq Internet va korporativ tarmoq kirish nuqtalari orasida yaratiladi. Bunda tashqi paketlar uchun ushbu ikki nuqtada o'rnatilgan chegara marshrutizatorlarining adreslaridan foydalanilsa, oxirgi uzellarning ichki adreslari ichki dastlabki paketlarda himoyalangan holda saqlanadi. Ta'kidlash lozimki, tunellash mexanizmining o'zi qanday maqsadlarda tunnellash qo'llanilayotganiga bog'liq emas. Tunnellash nafaqat uzatilayotgan barcha ma'lumotlarning konfidensialligi va yaxlitligini ta'minlashda, balki turli protokolli (masalan, IPv4 va IPv6) tarmoqlar orasida o'tishni tashkil etishda ham qo'llaniladi. Tunnellash bir protokol paketini boshqa protokoldan foydalanuvchi mantiqiy muhitda uzatishni tashkil etishga imkon beradi. Natijada bir necha turli xil tarmoqlarning o'zaro aloqalari muammosini hal etish imkoniyati paydo bo'ladi.

Tunnellash mexanizmini amalga oshirilishiga uch xil protokollar: protokol– «yo'lovchi», protokol eltuvchi va tunnellash protokoli ishlashi natijasi deb qarash mumkin. Masalan, protokol – «yo'lovchi» sifatida bitta korxona filiallarining lokal tarmoqlarida ma'lumotlarni tashuvchi transport protokoli IPX ishlatilishi mumkin. Eltuvchi protokolning eng ko'p tarqalgan varianti Internet tarmog'ining IP protokoli hisoblanadi. Tunnellash protokoli sifatida kanal sathi protokolari PPTP va L2TP hamda tarmoq sathi protokoli IPSec ishlatilishi mumkin. Tunnellash tufayli Internet infratuzilmasini VPN-ilovalardan berkitish mumkin bo'ladi.

VPN tunnellari turli foydalanuvchilar uchun yaratilishi mumkin. Bular xavfsizlik shlyuzi bo'lgan *lokal tarmoq* LAN yoki masofadagi va mobil foydalanuvchilarning alohida kompyuterlari bo'lishi mumkin. Yirik korxonaning virtual xususiy tarmog'ini yaratish uchun VPN-shlyuzlar, VPN-serverlar va VPN-mijozlar kerak bo'ladi. VPN-shlyuzlarni korxona lokal tarmoqlarini himoyalash uchun ishlatish maqsadga muvofiq bo'lsa, VPN-serverlar va VPN-mijozlardan masofadagi va mobil foydalanuv-chilarni Internet orqali korporativ tarmoq bilan himoyalangan ulanishini tashkil etishda foydalaniladi.

Virtual himoyalangan kanallarni qurish variantlari. VPN ni loyihalashda, odatda, ikkita asosiy sxema ko'riladi (7.3-rasm):



7.3-rasm. «LHT-LHT» va «Mijoz-LHT» xilidagi virtual himoyalangan kanallar.

– lokal tarmoqlar orasidagi virtual himoyalangan kanal («LXT-LHT» kanal);

– uzel va lokal tarmoq orasidagi virtual himoyalangan kanal («mijoz-LHT» kanali).

Ulanishning birinchi sxemasi alohida ofislar orasidagi qimmatli ajratilgan liniyalar o'rniga o'tadi va ular orasida doimo foydalanuvchan, himoyalangan kanallarni yaratadi. Bu holda xavfsizlik shlyuzi tunnel va lokal tarmoq orasida interfeys vazifasini o'taydi va lokal tarmoq foydalanuvchilari bir-birlari bilan muloqot qilishda tunneldan foydalanadilar. Aksariyat kompaniyalar VPNning bu xilidan global tarmoqning mavjud Frame Relay kabi ulanishlarni almashtirish uchun yoki ularga qo'shimcha sifatida foydalanadilar.

VPN himoyalangan kanalning ikkinchi sxemasi masofadagi yoki mobil foydalanuvchilar bilan ulanishni o'rnatishga atalgan. Tunnelni yaratishni mijoz (masofadan foydalanuvchi) boshlab beradi. Masofadagi tarmoqni himoyalovchi shlyuz bilan bog'lanish uchun u o'zining kompyuterida maxsus mijoz dasturiy ta'minotini ishga tushiradi. VPNning bu turi kommutatsiyalanuvchi ulanishlarni o'rniga o'tadi va masofadan foydalanishning an'anaviy usullari bilan bir qatorda ishlatilishi mumkin.

Virtual himoyalangan kanallarning qator variantlari mavjud. Umuman, orasida virtual himoyalangan kanal shakllantiriluvchi korporativ tarmoqning har qanday ikkita uzeli himoyalanuvchi axborot oqimining oxirgi va oraliq nuqtasiga taalluqli bo'lishi mumkin. Axborot xavfsizligi nuqtai nazaridan himoyalangan tunnel oxirgi nuqtalarining himoyalanuvchi axborot oqimining oxirgi nuqtalariga mos kelishi varianti ma'qul hisoblanadi. Bu holda kanalning axborot paketlari o'tishining barcha yo'llari bo'ylab himoyalanishi ta'minlanadi. Ammo bu variant boshqarishning detsentralizatsiyalanishiga va resurs sarfining oshishiga olib keladi. Agar virtual tarmoqdagi lokal tarmoq ichida trafikni himoyalash talab etilmasa, himoyalangan tunnelning oxirgi nuqtasi sifatida ushbu lokal tarmoqning tarmoqlararo ekrani yoki chegara marshrutizatori tanlanishi mumkin. Agar lokal tarmoq ichidagi axborot oqimi himoyalanishi shart bo'lsa, bu tarmoq oxirgi nuqtasi vazifasini himoyalangan aloqada ishtirok etuvchi kompyuter bajaradi. Lokal tarmoqdan masofadan foydalanilganida foydalanuvchi kompyuteri virtual himoyalangan kanalning oxirgi nuqtasi bo'lishi shart.

Faqat paketlarni kommutatsiyalashli ochiq tarmoq, masalan, Internet ichida o'tkaziluvchi himoyalangan tunnel varianti yetarlicha keng tarqalgan. Ushbu variant ishlatilishi qulayligi bilan ajralib tursada, nisbatan past xavfsizlikka ega. Bunday tunnelning oxirgi nuqtalari vazifasini, odatda Internet provayderlari yoki lokal tarmoq chegara marshrutizatorlari (tarmoqlararo ekranlar) bajaradi.

Lokal tarmoqlar birlashtirilganida tunnel faqat Internetning chegara provayderlari yoki lokal tarmoqning marshrutizatorlari (tarmoqlararo ekranlari) orasida shakllantiriladi. Lokal tarmoqdan masofadan foydalanilganida tunnel Internet provayderining masofadan foydalanish serveri hamda Internetning chegara provayderi yoki lokal tarmoq marshrutizatori (tarmoqlararo ekran) orasida yaratiladi. Ushbu variant bo'yicha qurilgan korporativ tarmoqlar yaxshi masshtablanuvchanlik va boshqariluvchanlikka ega bo'ladi. Shakllantirilgan himoyalangan tunnellar ushbu virtual tarmoqdagi mijoz kompyuterlari va serverlari uchun to'la shaffof hisoblanadi. Ushbu uzellarning dasturiy ta'minoti o'zgarmaydi. Ammo bu variant axborot aloqasining nisbatan past xavfsizligi bilan xarakterlanadi, chunki trafik qisman ochiq aloqa kanali bo'yicha himoyalanmagan holda o'tadi. Agar shunday VPNni yaratish va ekspluatatsiya qilishni provayder ISP o'z zimmasiga olsa, barcha virtual xususiy tarmoq uning shlyuzlarida, lokal tarmoqlar va korxonalarning masofadagi foydalanuvchilari uchun shaffof holda quril-

ishi mumkin. Ammo bu holda provayderga ishonch va uning xizmatiga doimo to'lash muammosi paydo bo'ldi.

Himoyalangan tunnel, orasida tunnel shakllantiriluvchi uzellardagi virtual tarmoq komponentlari yordamida yaratiladi. Bu komponentlarni tunnel initsiatorlari va tunnel terminatorlari, deb yuritish qabul qilingan.

Tunnel initsiatori dastlabki paketni yangi paketga, jo'natuvchi va qabul qiluvchi xususidagi axboroti bo'lgan yangi sarlavhali paketga inkapsulatsiyalaydi. Inkapsulatsiyalangan paketlar har qanday protokol turiga, jumladan, marshrutlanmaydigan protokollarga (masalan, Net BEUI) mansub bo'lishlari mumkin. Tunnel bo'yicha uzatiladigan barcha paketlar IP paketlari hisoblanadi. Tunnelning initsiatori va terminatori orasidagi marshrutni odatda Internetdan farqlanishi mumkin bo'lgan, oddiy marshrutlanuvchi tarmoq IP aniqlaydi.

Tunnelni initsiallash va uzish turli tarmoq qurilmalari va dasturiy ta'minot yordamida amalga oshirilishi mumkin. Masalan, tunnel masofadan foydalanish uchun ulashni ta'minlovchi modem va mos dasturiy ta'minot bilan jihozlangan mobil foydalanuvchining noutbuki tomonidan initsiallanishi mumkin. Initsiator vazifasini mos funksional imkoniyatlarga ega bo'lgan lokal tarmoq marshrutizatori ham bajarishi mumkin. Tunnel, odatda tarmoq kommutatori yoki xizmatlar provayderi shlyuzi bilan tugallanadi.

Tunnel terminatori inkapsulatsiyalash jarayoniga teskari jarayonni bajaradi. Terminator yangi sarlavhalarni olib tashlab, har bir dastlabki paketni lokal tarmoqdagi adresatga yo'llaydi.

Inkapsulatsiyalanuvchi paketlarning konfidensialligi ularni shifrlash, yaxlitligi va haqiqiyligi esa elektron raqamli imzoni shakllantirish yo'li bilan ta'minlanadi. Ma'lumotlarni kriptografik himoyalashning juda ko'p usullari va algoritmlari mavjud bo'lganligi sababli, tunnel initsiatori va terminatori himoyaning bir xil usullaridan foydalanishga o'z vaqtida kelishib olishlari maqsadga muvofiq hisoblanadi. Ma'lumotlarni rasshifrovka qilish va raqamli imzoni tekshirish imkoniyatini ta'minlash uchun tunnel initsiatori va terminatori kalitlarni xavfsiz almashish vazifasini ham madadlashlari zarur. Undan tashqari, VPN tunnelarini vakolatli foydalanuvchilar tomonidan yaratilishini kafolatlash maqsadida axborot aloqasining asosiy taraflari autentifikatsiyalashdan o'tishlari lozim. Korporatsiyaning mavjud tarmoq infratuzilmalari VPNdan foydalanishga ham dasturiy, ham apparat ta'minot yordamida tayyorlanishlari mumkin.

7.2. Himoyalangan virtual xususiy tarmoqlarning turkumlanishi

Himoyalangan virtual xususiy tarmoqlar VPNni turkumlashni turli variantlari mavjud. Ko'pincha turkumlashning quyidagi uchta alomati ishlatiladi:

– OSI modelining ish sathi;
– VPN texnik yechimining arxitekturasi;
– VPNni texnik amalga oshirish usuli.

OSI modelining ish sathi bo'yicha VPNning turkumlanishi. Ushbu turkumlash anchagina qiziqish tug'diradi, chunki amalga oshiriluvchi VPNning funksionalligi va uning korporativ axborot tizimlari ilovalari hamda himoyaning boshqa vositalari bilan birgalikda ishlatilishi ko'p hollarda tanlangan OSI sathiga bog'liq bo'ladi.

OSI modelining ish sath alomati bo'yicha kanal sathidagi VPN, tarmoq sathidagi VPN va seans sathidagi VPN farqlanadi. Demak, VPNlar, odatda OSI modelining pastki sathlarida quriladi. Buning sababi shuki, himoyalangan kanal vositalari qanchalik pastki sathda amalga oshirilsa, ularni ilovalarga va tatbiqiy protokollarga shunchalik shaffof qilish soddalashadi. Tarmoq va kanal sathlarida ilovalarning himoya protokollariga bog'liqligi umuman yo'qoladi. Shu sababli, foydalanuvchilar uchun universal va shaffof himoyani faqat OSI modelining pastki sathlarida qurish mumkin. Ammo bunda biz boshqa muammoga-himoya protokolining muayyan tarmoq texnologiyasiga bog'liqligi muammosiga duch kelamiz.

Kanal sathidagi VPN. OSI modelining kanal sathida ishlatiluvchi VPN vositalari uchinchi (va yuqoriroq) sathning turli xil trafigini inkapsulatsiyalashni ta'minlashga va «nuqta-nuqta» xilidagi virtual tunnellarni (marshrutizatordan marshrutizatorga yoki shaxsiy kompterdan lokal hisoblash tarmog'ining shlyuzigacha) qurishga imkon beradi. Bu guruhga L2F (Layer 2 Forwarding) va PPTP (Point-to-Point Tunneling Protocol) protokollari hamda Cisco Systemsi MicroSoft firmalarining birga ishlab chiqqan L2TP(Layer 2 Tunneling Protocol) standartidan foydalanuvchi VPN-mahsulotlar taalluqli.

Himoyalangan kanalning protokoli PPTP «nuqta-nuqta» ulanishlarida, masalan, ajratilgan liniyalarda ishlaganda keng qo'llaniluvchi PPP protokoliga asoslangan. PPTP protokoli ilovalari va tatbiqiy sath xizmatlari uchun himoya vositalarining shaffofligini ta'minlaydi va tarmoq sathida ishlatiluvchi protokolga bog'liq emas. Xususan, PPTP protokoli ham IP tarmoqlarida, ham IPX, DECnet yoki NetBEUL protokol-

lari asosida ishlovchi tarmoqlarda paketlarni tashishi mumkin. Ammo PPP protokoli hamma tarmoqlarda ham ishlatilmasligi sababli (aksariyat lokal tarmoqlarida kanal sathida Ethernet protokoli ishlasa, global tarmoqlarda ATM, Frame Relay protokollari ishlaydi), uni universal vosita deb bo'lmaydi. Yirik birikma tarmoqning turli qismlarida, umuman aytganda, turli kanal protokollari ishlatiladi. Shu sababli, bu geterogen muhit orqali kanal sathining yagona protokoli yordamida himoyalangan kanalni o'tkazish mumkin emas.

L2TP protokoli, ehtimol, lokal hisoblash tarmoqlaridan foydalanishni tashkil etishda ustunlik qiluvchi yechim bo'lib qolishi mumkin (chunki u, asosan, Windows operatsion tizimiga tayanadi.)

Tarmoq sathidagi VPN. Tarmoq sathidagi VPN-mahsulotlar IPni IPga inkapsulatsiyalashni 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.

Tarmoq sathida ishlovchi IPSec protokoli murosaga asoslangan variant hisoblanadi. Bir tomondan u ilovalar uchun shaffof, ikkinchi tomondan keng tarqalgan IP protokoliga asoslanganligi sababli barcha tarmoqlarda ishlashi mumkin. Shu orada esdan chiqarmaslik lozimki, IPSecning spetsifikatsiyasi IPga mo'ljallanganligi sababli u tarmoq sathining boshqa protokollari trafigi uchun to'g'ri kelmaydi. IPSec protokoli L2TP protokoli bilan birgalikda ishlashi mumkin. Natijada, bu ikki protokol ishonchli identifikatsiyalashni, standartlangan shifrlashni va ma'lumotlar yaxlitligini ta'minlaydi. Ikkita lokal tarmoq orasidagi IPSec tunneli ma'lumotlar uzatuvchi yakka tarmoqlar to'plamini madadlashi mumkin. Natijada, bu xildagi ilovalar masshtablanish nuqtai nazaridan ikkinchi sath texnologiyalariga nisbatan ustunlikka ega bo'ladi.

IPSec protokoli bilan masofadagi qurilmalar orasida kriptografik kalitlarni xavfsiz boshqarish va almashish masalalarini yechuvchi IKE (Internet Key Exchange) protokoli bog'langan. IKE protokoli kalitlarni almashishni avtomatlashtiradi va himoyalangan ulanishni o'ranatadi, IPSec esa paketlarni kodlaydi va «imzo chekadi». Undan tashqari, IKE o'rnatilgan ulanish uchun kalitni o'zgartirish imkoniyatiga ega. Bu uzatiluvchi axborotning konfidensialligini oshiradi.

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 retranslatsiyalaydi. (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.)

Tunnelning initsiatori va terminatori orasida uzatiluvchi axborotni shifrlash transport sathi TLS(Transport Layer Security) yordamida amalga oshiriladi. Tarmoqlararo ekran orqali autentifikatsiyalangan o'tishni standartlash uchun SOCKS deb ataluvchi protokol aniqlangan va hozirda SOCKS protokolining 5-versiyasi kanal vositachilarini standart amalga oshirilishida ishlatiladi.

SOCKS protokolining 5-versiyasida mijoz kompyuteri vositachi (proxy) vazifalarini bajaruvchi server bilan autentifikatsiyalangan soket (yoki seans) o'rnatadi. Bu vositachi-tarmoqlararo ekran orqali bog'lanishning yagona usuli. Vositachi, o'z navbatida, mijoz tomonidan so'ralgan har qanday amalni bajaradi. Vositachiga soket sathidagi trafik ma'lumligi sababli, u sinchiklab nazorat qilishi, masalan, muayyan ilovalarni, agar ular zaruriy vakolatlarga ega bo'lmasa, blokirovka qilishi mumkin.

Agar IPSec protokoli mohiyati bo'yicha, IP tarmoqni himoyalangan tunnelga tarqatsa, SOCKS protokoli asosidagi mahsulotlar uni alohida har bir ilova va har bir soketga kengaytiradi. Ikkinchi va uchinchi sathning yaratilgan tunnellari ikkala yo'nalishda birday ishlasa, 5 sathning VPN tarmog'i har bir yo'nalishda uzatishni mustaqil boshqarishga ruxsat beradi. IPSec protokolga va ikkinchi sath protokollariga o'xshab 5 sathning VPN tarmoqlari virtual xususiy tarmoqlarning boshqa turlari bilan birga ishlatilishi mumkin, chunki bu texnologiyalar bir-birini inkor qilmaydi.

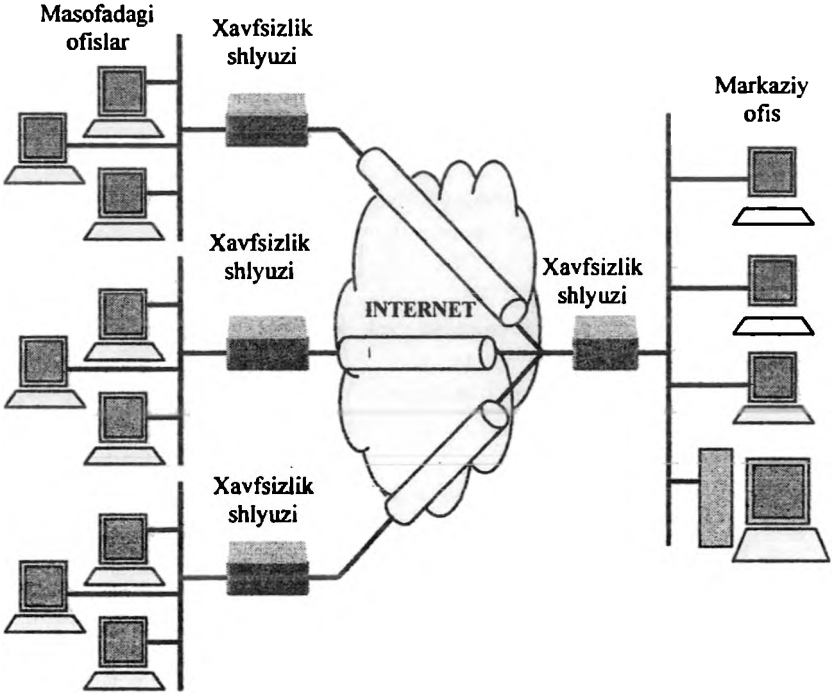
Texnik yechimining arxitekturasi bo'yicha VPNning turkumlanishi. Ushbu turkumlash bo'yicha virtual xususiy tarmoqlar quyidagi uch turga bo'linadi:

– korporatsiya ichidagi VPN tarmoq;
– masofadan foydalaniluvchi VPN tarmoq;
– korporatsiyalararo VPN tarmoq.

Korporatsiya ichidagi VPN tarmoq. Korporatsiya ichidagi VPN tarmoqlar (Intranet VPN) korxona ichidagi bo'linmalar yoki aloqaning korporatsiya tarmoqlari (shu jumladan, ajratilgan liniyalar) yordamida birlashtirilgan korxonalar guruhi orasida himoyalangan aloqani tashkil etish uchun ishlatiladi. O'zining filiallari va bo'limlari uchun axborot-

ning markazlashtirilgan omboridan foydalanishga ehtiyoj sezgan kompaniyalar masofadagi uzellarni ajratilgan liniyalar yoki frame relay texnologiyasi yordamida ulaydilar. Ammo ajratilgan liniyalarning ishlatilishi egallanadigan o'tkazish polosasining va obyektlar orasidagi masofaning kattalashgani sari joriy sarf-xarajatlarning oshishiga sabab bo'ladi. Bularni kamaytirish uchun kompaniya uzellarini virtual xususiy tarmoq yordamida ulashi mumkin (7.4-rasm).

Intranet VPN tarmoqlar Internetdan yoki servis-provayderlar tomonidan taqdim etiluvchi bo'linuvchi tarmoq infratuzilmalaridan foydalangan holda quriladi. Kompaniya narxi qimmat ajratilgan liniyalardan voz kechib, ularni arzonroq Internet orqali aloqa bilan almashtiradi. Bu o'tkazish polosasidan foydalanishdagi sarf-xarajatni jiddiy kamaytiradi, chunki Internetda masofa ulanish narxiga hech ta'sir etmaydi.



7.4-rasm. VPN intranet texnologiyasi yordamida tarmoq uzellarini ulash.

Intranet VPN uchun quyidagi afzalliklar xarakterli:

– konfidensial axborotni himoyalash uchun shifrlashning kuchli kriptografik protokollaridan foydalanish;

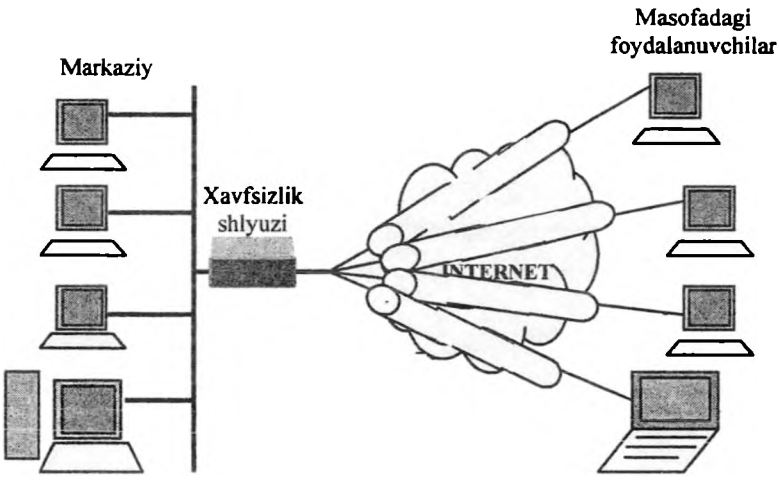
– avtomatlashtirilgan savdo tizimi va ma'lumotlar bazasini boshqarish tizimi kabi jiddiy ilovalarni bajarishda ishlashining ishonchliligi;

– soni tez o'sayotgan foydalanuvchilar, yangi ofislar va yangi dasturiy ilovalarni samaraliroq joylashtirish uchun boshqarishning moslashuvchanligi.

Internetdan foydalanib Intranet VPNni qurish VPN-texnologiyani amalga oshiruvchi eng rentabel usuli hisoblanadi. Ammo Internetda servis darajasi umuman kafolatlanmaydi. Kafolatlangan servis darajasini xohlovchi kompaniyalar o'zlarining VPNlarini server-provayderlari tomonidan taqdim etiluvchi bo'linuvchi tarmoq infatuzilmalaridan foydalanib saflash imkoniyatlarini ko'rishlari shart.

Masofadan foydalaniluvchi VPN tarmoq. Masofadan foydalaniluvchi virtual xususiy tarmoqlar VPN (Remote Access VPN) korporatsiyaning mobil yoki masofadagi xodimlariga (kompaniya rahbariyati, mehnat safaridagi xodimlar, kasanachilar va h.) korxona axborot resurslaridan himoyalangan masofadan foydalanishni ta'minlaydi.

Masofadan foydalanuvchi virtual xususiy tarmoqlarning (7.5-rasm) kommutatsiyalanuvchi va ajratilgan liniyalardan foydalanishning har oydagi sarf-xarajatlarini anchagina kamaytirishga imkon berishi, ularning umumiy e'tirof etilishiga sabab bo'ldi. Ularning ishlash prinsipi oddiy: foydalanuvchilar global tarmoqdan foydalanishning mahalliy nuqtasi bilan ulanishlarni o'rnatadi. So'ngra ularning so'rovlari Internet orqali tunnellanadi. Bu shaharlararo va xalqaro aloqa uchun to'lovdan qutilishga imkon beradi. Undan keyin barcha so'rovlar mos uzellarda to'planadi va korporatsiya tarmoqlariga uzatiladi.



7.5-rasm. Masofadan foydalanishli virtual xususiy tarmoq.

Xususiy boshqariluvchi tarmoqlardan (dial networks) masofadan foydalaniluvchi VPN tarmoqlarga (Remote Access VPN) o'tish quyidagi afzalliklarni beradi:

– shaharlararo nomerlar o'rniga mahalliy nomerlardan foydalanish imkoniyati shaharlararo telekommunikatsiyaga sarf-xarajatlarni anchagina kamaytiradi;

– autentifikatsiyalash jarayonini ishonchli o'tkazishni ta'minlovchi masofadagi va mobil foydalanuvchilar haqiqiyligini aniqlash tizimining samaradorligi;

– masshtablanishning yanada yuqoriligi va tarmoqqa qo'shiluvchi yangi foydalanuvchilar sarflanishining oddiyligi;

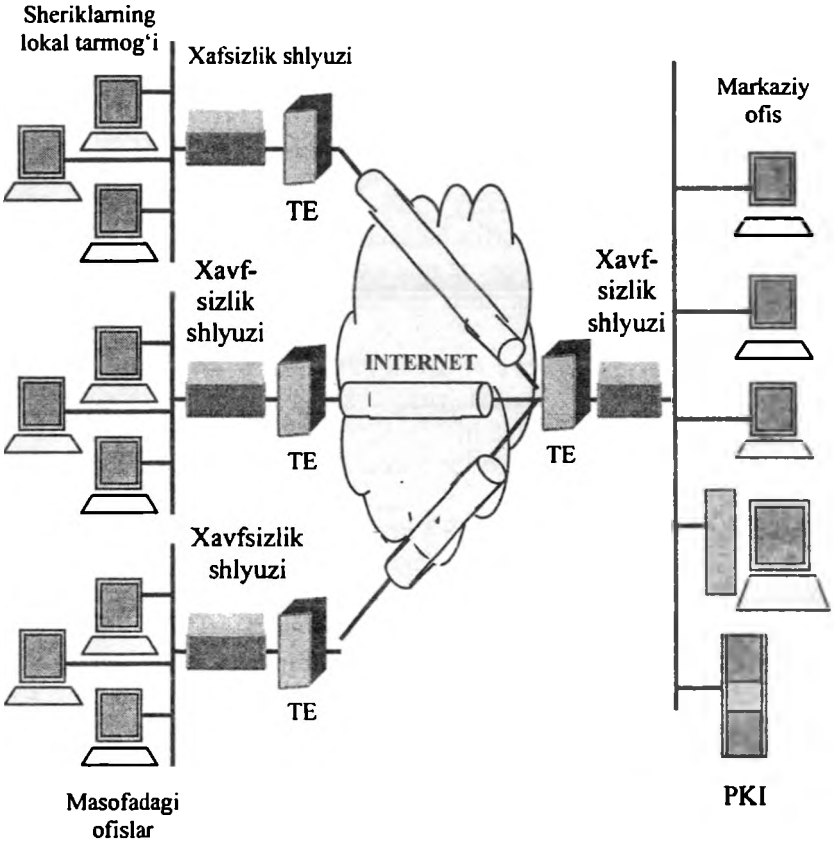
– kompaniya e'tiborini tarmoq ishlashi muammolari o'rniga korporatsiya asosiy biznes-maqsadlariga qaratish.

Ta'kidlash lozimki, sezuvchan korporatsiya trafigini tashishda ochiq tarmoq Internet ning birlashtiruvchi magistral sifatida ishlatilishining ko'lami oshib bormoqda. Bu axborot himoyasi mexanizmini ushbu texnologiyaning eng muhim elementiga aylantiradi.

Korporatsiyalararo VPN tarmoq. Korporatsiyalararo VPN tarmoqlardan (Extranet VPN) biznes bo'yicha strategik sheriklar, ta'minotchilar, yirik buyurtmachilar, mijozlar va h. bilan samarali aloqani va axborotni himoyalangan almashinuvini tashkil etishda foydalaniladi

(7.6-rasm). Extranet – bir kompaniya tarmog'idan ikkinchi kompaniya tarmog'ining to'g'ridan-to'g'ri foydalanishini ta'minlash orqali ish yuzasidan hamkorlik jarayonida aloqa ishonchliligini oshirishga imkon beruvchi texnologiyadir.

Extranet VPN tarmoqlari umuman korporatsiya ichidagi virtual xususiy tarmoqlarga o'xshash, farqi shundaki, korporatsiyalararo virtual xususiy tarmoqlar uchun axborot himoyasi muammosi keskinroqdir. Extranet VPN uchun ishbilarmon sheriklar o'zlarining tarmoqlarida qo'llashlari mumkin bo'lgan turli VPN-yechimlar bilan aloqa qilish imkoniyatlarini kafolatlovchi standartlashtirilgan VPN-mahsulotlardan foydalanish xarakterlidir.



7.6-rasm. Korporatsiyalararo extranet VPN tarmog'i.

Bir necha kompaniyalar birga ishlashga kelishib, bir-birlariga tarmoqlarini ochishganida, ular yangi sheriklarining faqat ma'lum axborotdan foydalanishlariga yo'l qo'yishlari lozim. Bunda konfidensial axborot ruxsatsiz foydalanishdan ishonchli himoyalanishi zarur. Aynan, shu sababli, korporatsiyalararo tarmoqlarda ochiq tarmoq tomonidan tarmoqlararo ekran (brandmauer) yordamida nazoratga katta ahamiyat beriladi. Axborotdan haqiqiy foydalanuvchining foydalanishini kafolatlovchi autentifikatsiyalash ham muhim hisoblanadi. Shu bilan bir qatorda ruxsatsiz foydalanishdan himoyalashning saflangan tizimi o'ziga e'tiborni jalb qilmasligi shart.

Extranet VPN ulanishlari intranet VPN va remote access VPN lar amalga oshirilishidagi ishlatilgan arxitektura va protokollardan foydalanib saflanadi. Asosiy farq shundan iboratki, extranet VPN foydalanuvchilariga beriladigan foydalanishga ruxsat ular sherigining tarmog'i bilan bog'liq.

Ba'zida VPN tarmog'ining lokal varianti (Localnet VPN) alohida guruhga ajratiladi. Localnet VPN lokal tarmog'i kompaniya lokal tarmog'i ichida (odatda, markaziy ofis) aylanuvchi axborotlar oqimidan kompaniyadan ishlovchi «ortiqcha qiziquvchi» xodimlarning ruxsatsiz foydalanishidan himoyalashni ta'minlaydi. Ta'kidlash lozimki, hozirda VPNni amalga oshiruvchi turli usullarning konvergensiyasi g'oyasi ko'zga tashlanmoqda.

Texnik amalga oshirish bo'yicha VPNning turkumlanishi. Virtual xususiy tarmoqning konfiguratsiyasi va xarakteristikalari ko'p jihatdan ishlatiladigan VPN-qurilmalarining turiga bog'liq.

Texnik amalga oshirish bo'yicha VPNning quyidagi guruhlari farqlanadi:

– marshrutizatorlar asosidagi VPN;
– tarmoqlararo ekranlar asosidagi VPN;
– dasturiy ta'minot asosidagi VPN;
– ixtisoslashtirilgan apparat vositalari asosidagi VPN.

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 narxining 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 apparat vositalari asosida VPN tizimlarda shifrlashning mikrosxemalarda amalga oshirilishi tezkorlikning ta'minlanishiga sabab bo'ladi. Ixtisoslashtirilgan VPN-qurilmalar xavfsizlikning yuqori darajasini ta'minlaydi, ammo ularning narxi anchagina yuqori.

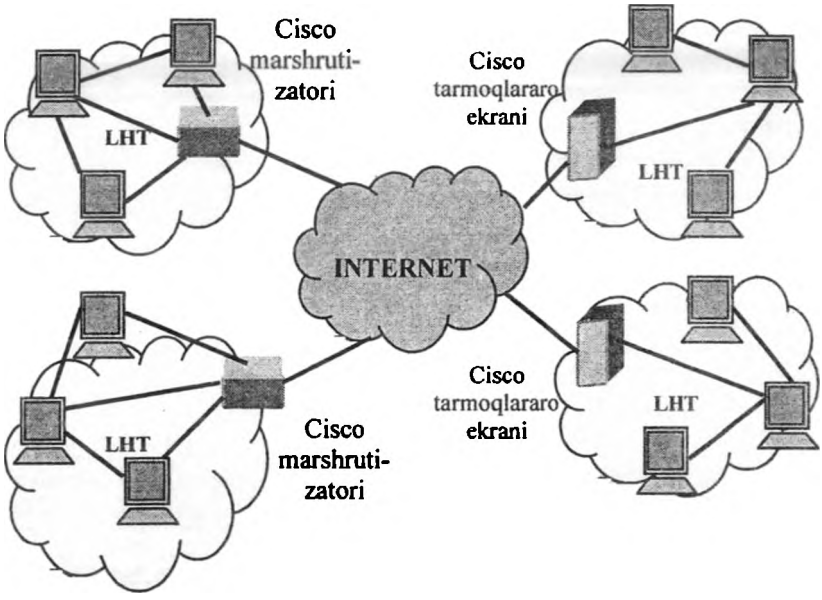
7.3. Himoyalangan korporativ tarmoqlarni qurish uchun VPN yechimlar

Marshrutizatorlar asosidagi VPN. Tashqi dunyo bilan lokal tarmoq almashadigan barcha axborot mashrutizator orqali o'tadi. Bu marshrutizatorlarni chiquvchi paketlarni shifrlovchi va kiruvchi paketlarni rasshifrovka qiluvchi tabiiy platformaga aylantiradi. Boshqacha aytganda, marshrutizator, umuman, marshrutlash vazifasini VPNni madadlash bilan birga olib borishi mumkin. Bunday yechim o'zining afzalliklari va kamchiliklariga ega. Afzalligi – marshrutlash va VPN vazifalarini birgalikda ma'murlash qulayligidir. Korxona tarmoqlararo ekranni ishlatmasdan korporativ tarmoq himoyasini faqat ham tarmoqdan foydalanish bo'yicha, ham uzatiladigan trafikni shifrlash bo'yicha himoyalash vazifalarini birgalikda hal etuvchi marshrutizator yordamida tashkil etgan hollarda mashrutizatorlarni VPNni madadlashda ishlatilishi,

ayniqsa, foydalidur. Ushbu yechimning kamchiligi marshrutlash bo'yicha asosiy amallarning ko'p mehnat sarfini talab etuvchi trafikni shifrlash va autentifikatsiyalash amallari bilan birga olib borilishi natijasida, marshrutizator unumdorligiga quyiladigan talablarning oshishi bilan bog'liq. Marshrutizatorlarning unumdorligini oshirishga shifrlash vazifalarini apparat madadlash orqali erishiladi. Hozirda barcha marshrutizator va boshqa tarmoq qurilmalarini yetakchi ishlab chiqaruvchilari o'zlarining mahsulotlarida turli VPN-protokollarini madadlaydilar. Bu sohada Cisco Systems va 3 Com kompaniyalari lider hisoblanadilar. Cisco Systems kompaniyasi o'zlari ishlab chiqqan marshrutizatorlarga eng keng tarqalgan standartlar asosida VPNlarni qurishga imkon beruvchi kanal sathi protokolini madadlovchi IOS 11.3 (Internetwork Operation System 11.3) va tarmoq sathi protokoli IPSec ni kiritdi. L2F protokoli avvalroq IOS operatsion tizimning komponentiga aylandi va Cisco ishlab chiqaradigan barcha tarmoqlararo aloqa va masofadan foydalanish qurilmalarida madadlanadi.

Cisco marshrutizitorlarida VPN vazifalari butunlay dasturiy yo'l bilan yoki shifrlash soprotsessori bo'lgan maxsus kengaytirish platasidan foydalanilgan holda amalga oshirilishi mumkin. Oxirgi variant VPN amallarida marshrutizator unumdorligini anchagina oshiradi. Cisco Systems kompaniyasi tomonidan ishlab chiqilgan VPN qurish texnologiyasi yuqori unumdorligi va moslanuvchanligi bilan ajralib turadi. Unda «toza» yoki inkapsulatsiya qilingan ko'rinishda uzatiluvchi har qanday IP-oqim uchun shifrlash bilan tunnellash ta'minlanadi. Cisco kompaniyasining marshrutizatorlari asosida VPN-kanallarini qurish operatsionizimining vositalari yordamida Cisco IOS 12.x. versiyasidan boshlab amalga oshiriladi. Agar mazkur operatsion tizim kompaniyaning boshqa bo'limlaridagi Cisco chegara marshrutizatorlarida o'rnatilgan bo'lsa, bir marshrutizatordan ikkinchisiga «nuqta-nuqta» turidagi virtual himoyalangan tunnellar majmuasidan iborat bo'lgan korporativ VPN tarmoqni shakllantirish imkoniyati bo'ladi (7.7-rasm).

Marshrutizatorlar asosida VPNlarni qurishda esda tutish lozimki, bunday yondashishning o'zi kompaniyaning umumiy axborot xavfsizligini ta'minlash muammosini hal etmaydi, chunki barcha ichki axborot resurslar baribir tashqaridan hujum qilish uchun ochiq qoladi. Bu resurslarni himoyalash uchun, odatda, chegara marshrutizatorlaridan keyin joylashgan tarmoqlararo ekranlardan foydalaniladi.



7.7-rasm. Cisco marshrutizatorlari asosida korporativ VPN tarmog'ini qurishning namunaviy sxemasi.

Marshrutizatorlar asosida VPNlarni qurishda esda tutish lozimki, bunday yondashishning o'zi kompaniyaning umumiy axborot xavfsizligini ta'minlash muammosini hal etmaydi, chunki barcha ichki axborot resurslar baribir tashqaridan hujum qilish uchun ochiq qoladi. Bu resurslarni himoyalash uchun, odatda, chegara marshrutizatorlaridan keyin joylashgan tarmoqlararo ekranlardan foydalaniladi.

Cisco 1720 VPN Access Router marshrutizatori katta bo'lmagan va o'rtacha korxonalarda himoyalangan foydalanishini tashkil etishga atalgan. Bu marshrutizator Internet va intratarmoqlardan foydalanishni tashkil etishga zarur bo'lgan imkoniyatlarni ta'minlaydi va Cisco IOS dasturiy ta'minot asosidagi virtual xususiy tarmoqlarni tashkil etish vazifalarini madadlaydi. Cisco IOS operatsion tizimi ma'lumotlarni himoyalash, xizmat sifatini boshqarish va yuqori ishonchililikni ta'minlash bo'yicha VPN vazifalarining juda keng to'plamini ta'minlaydi.

Cisco 1720 marshrutizatori ma'lumotlar himoyasining quyidagi vazifalarini bajaradi:

– *tarmoqlararo ekranlash.* Cisco IOS Firewall komponenta lokal tarmoqlarni hujumlardan himoyalaydi. *Foydalanishning kontekstli nazorati* CBAC (Context-based access control) funksiyasi ma'lumotlarni dinamik yoki holatlarga asoslangan, ilovalar bo'yicha differensiallangan filtrlashni bajaradi. Bu funksiya samarali tarmoqlararo ekranlash uchun juda muhim hisoblanadi. Cisco IOS Firewall komponenta qator boshqa foydali vazifalarni ham, xususan, «xizmat qilishdan voz kechish» kabi hujumlarni aniqlash va oldini olish, Javani blokirovka etish, audit va vaqtning real masshtabida ogohlantirishlarni tarqatish vazifalarini bajaradi.

– *shifrlash.* IPSec protokolidagi DES va Triple DES shifrlash algoritmlarini madadlash ma'lumotlarni konfidensialligi va yaxlitligini va ma'lumotlar manbaini autentifikatsiyalashni (ma'lumotlar global tarmoqdan o'tganidan so'ng) ta'minlash maqsadida ishonchli va standart shifrlaydi.

– *tunnellash.* Tunnellashning IPSec, GRE (Generic Routing Encapsulation), L2F va L2TP standartlari ishlatiladi. L2F va L2TP standartlari masofadagi foydalanuvchilarning korxona lokal tarmog'ida o'rnatilgan Cisco 1720 marshrutizatorigacha virtual tunnel o'tkazganlarida ishlatiladi. Bunday qo'llanishda korxonada masofadan foydalanish serveriga ehtiyoj qolmaydi va shaharlararo yoki xalqaro qo'ng'iroqlar uchun to'lovi tejaladi.

– *qurilmalarni autentifikatsiyalash va kalitlarni boshqarish.* IPSec katta tarmoqlarda ma'lumotlar va qurilmalarni masshtablanuvchi autentifikatsiyalashni ta'minlovchi kalitlarni boshqarish protokoli IKE, raqamli sertifikatlar X.509 versiya 3, sertifikatlarni boshqaruvchi protokol CEP hamda Verisign va Entrust kompaniya sertifikat serverlari madadlanadi.

– *VPNning mijoz dasturiy ta'minoti.* IPSec va L2TP protokollarining standart versiyalari bilan ishlovchi harqanday mijoz Cisco IOS bilan o'zaro aloqa qilishi mumkin.

– *foydalanuvchilarni autentifikatsiyalash.* Buning uchun PAP, CHAP protokollari, TACACS$^+$ va RADIUS tizimlari, foydalanish tokenlari kabi vositalardan foydalaniladi.

Virtual himoyalangan tarmoqlar nafaqat ma'lumotlarni himoyalash, balki himoyalashning yuqori saviyasi QoSni (Quality of Service)

ta'minlashi lozim. Cisco 1720 marshrutizatori QoSni quyidagi boshqarish mexanizmlarini madadlaydi:

– *foydalanishning kelishilgan tezligi CAR* (Committed Access Rate) ilovalar yoki foydalanuvchilar bazisida quiydagi uchta muhim vazifani bajaradi:

- trafik turini turkumlaydi;
- berilgan ilovaga ruxsat etilgan o'tkazish qobiliyatining maksimal darajasini o'rnatadi;
- trafikning har bir turi ustuvorligini belgilaydi;

– *siyosat asosida marshrutlash* (Policy Routing) ham trafikni turkumlaydi va ustuvorlaydi hamda trafikning qaysi turini marshrutizatorning mos chiqish yo'li portiga jo'natish lozimligini hal etadi;

– *mulohazali odilona navbat* WFQ (Weighted Fair Queneing) trafikni hisobga olgan holda maqbul javob vaqtini ta'minlaydi;

– *protokol RSVP* ilovalarga yo'lning boshidan oxirigacha kafolatlangan o'tkazish qobiliyatini rezervlashga imkon beradi.

Marshrutizatorning moslashuvchanligi modulli konstruksiya va ikkita slotda o'rnatiluvchi interfeys WAN-kartalari to'plami orqali ta'minlanadi. Cisco 1720 modelida Cisco 1600, 2800, va 3600 modellarda ishlatiladigan WAN-kartalardan foydalaniladi.

Kompaniya 3Com VPN texnologiyani amalga oshirishda boshidan standartlarni ko'zga tutgan edi. VPN ni madadlash uning NetBuilder II, Super Stack II NetBuilder marshrutizatorlariga Office Connect Net Builder Platform pladformalariga o'rnatilgan.

3Com kompaniyasi PPTP va L2TP protokollarni madadlovchi masofadan foydalaniluvchi konsentratorlarni yirik ishlab chiqaruvchilaridan biridir. 3Com kompaniyasining VPN tarmoqlari IPSec bilan birga ishlatiladi va tashqi kataloglar, jumladan Novell NDS va Windows NT Directory Serviceslar bilan o'zaro aloqa qilish uchun ishlab chiqilgan.

Kompaniya Web-texnologiyaga asoslangan va VPN yuklanganligini nazoratlashga hamda yuz beruvchi hodisalar asosida statistika va axborotni yig'ishga atalgan dasturiy ilova Transcend Ware Secure VPN Manager ni ham ishlab chiqdi. Undan tashqari, 3Com kriptohimoyalangan tunnellarni osongina yaratishga imkon beruvchi Web asosidagi instrumentariyni ishlab chiqaradi.

Internet Devices kompaniyasining Fort Knox marshrutizatorlarida tezlik va quvvat uyg'unlashgan. Undagi tarmoqni himoyalashni ta'minlashga yo'naltirilgan IP-trafikni ishlash vazifalari ro'yxatining

kengligi uning afzalligidir. Fort Knox marshrutizatori tarmoqlararo ekran rejimida ishlashi, NAT standarti bo'yicha adreslarni translatsiyalashi, xavfsizlik siyosatini boshqarishi, Web-sahifalar va DNS jadval yozuvlarini xeshlashi, auditni bajarishi mumkin. Odatda, Fort Knox korporativ tarmoq chegarasida, korporativ tarmoqni global tarmoq bilan ulovchi marshrutizatordan keyin o'rnatiladi. Demak, u boshqa lokal tarmoqlar bilan VPN-aloqani o'rnatish va tarmoqlararo ekranlar kabi foydalanishni nazoratlashning turli qoidalarini shakllantirishi mumkin. Fort Knoxda NAT adreslarini translatsiyalash funksiyasining mavjudligi, unga ichki IP-adreslarni berkitish va marshrutizatorlar trafigini qayta yo'naltirish imkonini beradi. Bu korporativ tarmoq ma'murlarini VPNni qurishda marshrutizatorlarni yangidan konfiguratsiyalashdan ozod etadi. Fort Knox funksiyalari to'plamining kengligiga qaramay uning narxi oddiy marshrutizator narxiga teng.

Tarmoqlararo ekranlar asosidagi VPN. Lokal tarmoqning tarmoqlararo ekrani orqali, xuddi marshrutizatordagidek, butun trafik o'tadi. Shu sababli, tarmoqlararo ekran ham chiquvchi trafikni shifrlash, kiruvchi trafikni rasshifrovka qilish vazifasini bajarishi mumkin. Hozirgi qator VPN-yechimlar tarmoqlararo ekranlarni VPNning qo'shimcha madad funksiyalari bilan to'ldirilishiga tayanadi. Bu Internet orqali boshqa tarmoqlararo ekranlar bilan shifrlangan ulanishni o'rnatishga imkon beradi. Axborot xavfsizligi bo'yicha qator mutaxassislarning fikricha, VPNni tarmoqlararo ekranlar asosida qurish, korporativ tarmoqlarni ochiq tarmoqlar hujumlaridan kompleks himoyalash nuqtai nazaridan, to'la asoslangan yechimdir. Haqiqatan, tarmoqlararo ekran va VPN-shlyuz funksiyalari bir nuqtada, yagona boshqarish va audit tizimi nazoratida birlashtirilsa, korporativ tarmoqni himoyalash funksiyalari bitta qurilmada to'planadi. Natijada, himoya vositalarini ma'murlash sifati oshadi.

Ammo himoyalash vositalarining bunday universallashtirilishi, hisoblash vositalarining mavjud imkoniyatlari darajasida nafaqat ijobiy, balki salbiy tomoniga ham ega. Shifrlash va autentifikatsiyalash amallarini hisoblash murakkabligi tarmoqlararo ekran uchun an'anaviy bo'lgan paketlarni filtrlash amallariga nisbatan ancha yuqori. Shu sababli, VPNning qo'shimcha vazifalarini amalga oshirishda murakkabligi katta bo'lmagan amallarni bajarishga mo'ljallangan tarmoqlararo ekran ko'pincha kerakli unumdorlikni ta'minlamaydi. Korporativ tarmoq tezkor kanal orqali ochiq tarmoqqa ulanganida sifatli himoyani ta'minlash

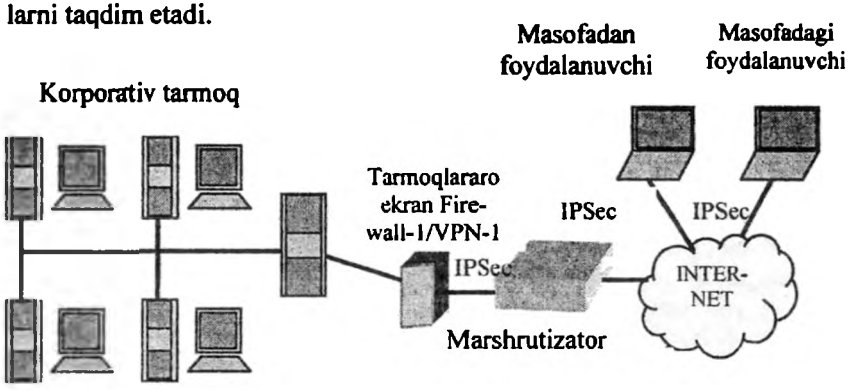
uchun alohida apparat, dasturiy yoki kombinatsiyalangan qurilma ko'rinishidagi VPN-shlyuzdan foydalanish lozim.

Aksariyat tarmoqlararo ekranlar server dasturiy ta'minotidan iborat, shu sababli, unumdorlikni oshirish muammosi yuqori unumdorlikka ega bo'lgan kompyuter platformasidan foydalanish evaziga yechilishi mumkin.

Check Point Software Technologies kompaniyasi Internet bilan ishlaganda axborot xavfsizligini kompleks ta'minlash mahsulotlarini ishlab chiqarish sohasidagi yetakchilardan biri hisoblanadi. Check Point Fire Wall-1 tarmoqlararo ekran korporativ axborot resurslari uchun yagona kompleks doirasida himoyaning chuqur eshelonlangan chegarasini qurishga imkon beradi. Bunday kompleks tarkibiga Check Point FW-1 ning o'zi va korporativ VPN tarmoq (himoyalangan tunnellarni shakllantiruvchi qism tizim) qurish uchun mahsulotlar to'plami Check Point VPN-1 hamda suqilib kirishni payqash vositalari Flood Gate va hokazolar kiradi.

Dasturiy ta'minotlar Check Point Fire Wall-1/VPN-1 asosida korporativ tarmoq qurish misoli 7.8-rasmda keltirilgan.

Check Point VPN-1 qism tizim tarkibidagi barcha mahsulotlar ham o'zaro, ham ommaviy brandmauer Fire Wall-1 bilan uzviy integratsiyalangan. Check Point kompaniyasi «tarmoq-tarmoq» (VPN-1 Gateway) va «tarmoq-masofadagi foydalanuvchi» (VPN-1 Gateway+VPN-1 Secu Remote) tipidagi himoyalangan tarmoqlarni tashkil etish uchun vositalarni taqdim etadi.



7.8-rasm. Check Point FW-1/VPN-1 asosida korporativ VPN tarmog'ini qurish sxemasi.

Check Point VPN-1 mahsulotlari ochiq standartlar (IPSec) asosida amalga oshirilgan, foydalanuvchilarni autentifikatsiyalashning rivojlangan tizimiga ega, ochiq kalitlarni (PKI) taqsimlashning tashqi tizimlari bilan o'zaro aloqani madadlaydi, boshqarish va auditning markazlashtirilgan tizimini qurishga imkon beradi va hokazo.

Check Point Fire Wall-1/VPN-1 nafaqat ochiq, balki kriptohimoyalangan trafikni ham nazoratlaydi. Tarmoqlararo ekran FW-1ga kelgan ma'lumotlar VP-1 vositalari yordamida rasshifrovka qilinadi, so'ngra axborotlar paketi yana shifrlanadi va o'tkazib yuboriladi.

VPN-1 qism tizimi trafikni nafaqat kriptografik berkitadi, balki axborotlar paketini autentifikatsiyalaydi ham. Check Point Fire Wall-1/VPN-1 kanallarida trafikni shifrlashda mashhur DES, 3-Des, CAST, IDEA, FWZ1 va h. kriptoalgoritmlardan foydalaniladi. FWZ1 kriptotizimi Check Point kompaniyasining ishlanmasidir. Axborot paketlarini autentifikatsiyalashda MD5, SHA-1, CBC DES va MAC algoritmlari ishlatiladi.

VPN Gateway shlyuzi – shifrlashning dasturiy moduli tarmoqlararo ekran Fire Wall – 1 bilan uzviy integratsiyalangan. Bu mahsulot korxonaga uzatiluvchi ma'lumotlarning to'la konfidensialligini, autentifikatsiyalanganligi va yaxlitligini kafolatlagan holda Internet orqali aloqa kanallarini qurishga imkon beradi. VPN funksiyalari korxonaning umumiy xavfsizlik siyosatiga to'la integratsiyalanganligi sababli, brandmauer va VPN-mahsulotlarni alohida boshqarishga ehtiyoj qolmaydi.

VPN Gateway shlyuzi himoyalangan VPN-tunnelni o'rnatgan holda tarmoqlar orasida Intrenet orqali uzatilayotgan konfidensial ma'lumotlarni shifrlaydi. Bu shlyuz uni javobgarlik doirasiga, ya'ni uning domeniga kiruvchi kompyuterlardan keladigan ma'lumotlar oqimini shifrlaydi. Bu lokal tarmoq yoki ushbu shlyuz orqasidagi oddiy xostlar guruhi bo'lishi mumkin. Bu ma'lumotlar tarmoqning ommaviy qismi bo'yicha shifrlangan ko'rinishda uzatiladi, ichki tarmoq bo'yicha uzatilganda shifrlanmaydi. VPN-amallarining barchasi oxirgi foydalanuvchi va barcha ilovalar uchun shaffofdir.

VPN-1 Gateway shlyuzi shifrlashning bir necha algoritmini va bir necha kalitlarni boshqarish protokolini madadlaydi. Bu shlyuz IKE (Internet Key Exchange) kabi industrial standart VPN-protokollarni madadlashi sababli, ekstratarmoqlarni tashkil etishda qo'llash qulay hisoblanadi. Ekstratarmoqlarda VPN biznes-sheriklar orasida xavfsiz aloqani ta'minlaydi. Sheck Point kompaniyasining VPN-mahsulotlari

IKE standartiga amal qiladi. Shu sababli, ular qarshi tomon bilan muzokaralar jarayonida avtomatik tarzda shifrlashning eng kriptobardosh algoritmini (DES va Triple DES) va autentifikatsiyalashning eng qat'iy algoritmini (SHA-1 va MD5) tanlaydi. Undan tashqari, shifrlashning maxfiy kalitlari, maksimal himoyalanishni kafolatlagan holda, tez-tez yangilanadi.

VPN-1 Gateway shlyuzi virtual xususiy tarmoqdagi ikkita oxirgi uzellarga ham shifrlangan, ham shifrlanmagan ma'lumotlarni almashishga imkon beruvchi shifrlashning tanlov rejimini madadlaydi. Buning uchun tarmoq ma'muri trafigi uchun himoyalashning alohida shartlari ta'minlanadigan ilovalarni beradi. So'ngra VPN-1 Gateway ushbu ilovalar ma'lumotlarini shifrlangan, qolgan konfidensial bo'lmagan ma'lumotlarni ochiq ko'rinishda uzatishni boshlaydi. Bunday moslanuvchanlik VPN-1 Gateway shlyuzining unumdorligini oshiradi.

VPN-1 Gateway shlyuzi kalitlarni boshqarishning quyidagi mexanizmlarini madadlaydi: IPSec uchun standart bo'lgan IKE, kalitlarni boshqarishning sanoat standarti FWZ, ommaviy protokol SKIP va kalitlarni qo'l bilan tarqatiladigan usuli. U X.509 sertifikatlari va Entrus Technologies kompaniyasining sertifikatlar serverlari texnologiyasi asosida ochiq PKI kalitlarni boshqarish infratuzilmasini madadlaydi.

VPN-1 Secu Remote mijoz dasturiy ta'minoti VPN-1 Gateway Shlyuzi yordamida «tarmoq-masofadagi foydalanuvchi» xilidagi himoyalangan ulanishlarni tashkil etishda ishlatiladi. Windows 98/XP/NT/2000 boshqaruvida ishlovchi masofadagi kompyuterlarga VPN-1Secu Remotening o'rnatilishi mobil xodimlarning yoki telekompyuterlarning korxona bosh tarmog'i bilan Internet orqali himoyalangan bog'lanishini ta'minlaydi. VPN-1 Secu Remotening ma'lumotlarni OSI modelining tarmoq sathida shifrlashi va rasshifrovka qilishi ushbu amallarning barcha ilovalar uchun shaffofligini, mavjud ilovalarga o'zgartirish kiritishni talab qilmagan holda, ta'minlaydi. SecuRemote foydalanuvchilarga VPN-vositalar o'rnatilgan bir necha turli tarmoqlar bilan bog'lanishiga imkon beradi.

VPN-1 Accelator Card qurilmasi Chrysalis-ITS kompaniyasi tomonidan ishlab chiqilgan apparat kriptografik tezlatgichdir. VPNning himoyalangan kanallarida trafikni shifrlash va kalitlarni generatsiyalovchi amallar anchagina hisoblash murakkabligiga ega va VPN orqali uzatiluvchi trafikning hajmi oshgan sari kompyuterning prosessori va xotirasining haddan ortiq yuklanishi ro'y berishi mumkin. VPN-1 Accelator mahsuloti bu muammoni hal etishi mumkin.

VPN-1 Accelator Card tezlatgichi VPN-1 Gateway shlyuzi bilan birgalikda ishlashga atalgan va IKE va IPSeclar talab etadigan barcha kriptografik amallarni bajaradi. VPN-1 Accelator Card bevosita shlyuz orqali ma'murlanadi.

VPN funksiyalari o'rnatilgan SecureZone tarmoqlararo ekrani Secure Computing kompaniyasi tomonidan ishlab chiqilgan va asosiy xarakteristikalari quyidagicha:

– VPNni madadlash funksiyalari – IPSec standarti, DES va Triple DES, PKI boshqarish va Netscape, Entrust va Verisign kompaniyalardan X.509 sertifikatlari;

– ixtisoslashtirilgan operatsion tizimi Secure OS (Unixning himoyalangan varianti) boshqaruvida ishlaydi;

– quyidagilarni qanoatlantiruvchi apparat platformalar: prosessor Intel Pentium, Pentium Pro, yoki Pentium II; RAM-kamida 64Mbayt; tashqi qurilmalar qattiq disk 4 Gbayt SCSI-2, qayishqoq disklar 3,5, CD ROM, strimmer DAT; SVGA video, PS/2- bilan birga ishlay oluvchi sichqon.

– standart tarmoq interfeyslari: 2-4 Ethernet, FAST Ethernet, Token Ring yoki FDDI;

– buzilishga bardoshlik xossasiga ega.

Secure Computing kompaniyasi MicroSoft Windows muhitida ishlovchi, alohida foydalanuvchilarga TCP/IP protokollari bo'yicha telefon tarmog'i yoki paketlarni kommutatsiyalovchi, ommaviy tarmoqdan himoyalangan masofaviy foydalanishni ta'minlovchi, IPSec bilan birga ishlayoluvchi mijoz dasturiy ta'minotini (SecureClient) ham tavsiya etadi.

VPN funksiyalari o'rnatilgan Raptor Firewall 5.0 tarmoqlararo ekrani Axent Technologies kompaniyasi tomonidan ishlab chiqilgan va Eagle Firewallning modifikatsiyalangan mahsuloti hisoblanadi. Bu tarmoqlararo ekranning xarakteristikalari quyidagicha:

– VPN madadi tarmoqlararo ekranga o'rnatilgan;

– IPSec standarti madadlanadi, dasturiy shifrlash IP (tekin tarqatiluvchi shifrlash usuli swIPe);

– xavfsizlikning umumiy siyosati tarmoqlararo ekran funksiyalariga va VPN funksiyasi yordamida tunnellanuvchi trafikka taalluqli;

– Windows NT/2000 va Solaris operatsion tizimlar boshqaruvida ishlaydi.

Axent kompaniyasi masofadagi foydalanuvchilar uchun VPNning mijoz dasturiy ta'minotini ham taqdim etadi. Raptor Firewall 5.0 versi-

yasi IPSec protokoli bo'yicha himoyalangan virtual tarmoq qurilishini ta'minlaydi.

Gauntlet Global VPN mahsuloti Network Associates kompaniyasi tarkibiga kiruvchi Trusted Information Systems kompaniyasining Gauntlet Firewall tarmoqlararo ekrani uchun, ushbu tarmoqlararo ekran muhitida uzviy integratsiyalanuvchi, qo'shimcha dasturiy mahsulot hisoblanadi.

IPSec protokoliga asoslangan Gauntlet Global VPN qism tizimi trafik-ni kriptografik himoyalashning quyidagi ikkita rejimini madadlaydi:

– Smart Gate shlyuzlari yordamida amalga oshiriluvchi tarmoqlararo ekrandan tarmoqlararo ekrangacha;

– masofadagi mijoz dasturiy ta'minoti Gauntlet.PC Extender yordamida amalga oshiriluvchi tarmoqlararo ekrandan masofadagi foydalanuvchi kompyuterigacha.

Gauntlet Global VPNda shifrlashning DES algoritmi ishlatiladi. Gauntlet Global VPN sertifikatsiya markazining dasturiy ta'minoti bilan ham taqdim etiladi. Ushbu dasturiy ta'minot yordamida tashkilotlar X.509 standartiga mos keluvchi raqamli sertifikatlarni generatsiyalashi va tekshirishi mumkin.

VPN qurish funksiyasini madadlovchi Border Manager tarmoqlararo ekrani Novell kompaniyasining mahsuloti bo'lib, nafaqat VPN qurish imkoniyatini, balki foydalanishni chegaralashni, paketlarni filtrlash va tarmoq adreslarini translatsiyalashni ta'minlaydi, vositachi HTTPning xizmatlarini tavsiya etadi, Web sahifalarini xeshlaydi, kanal sathida shlyuzlarga ega, ko'p protokolli marshrutlashni bajaradi va masofadan foydalanishni madadlaydi.

Border Manager tarmoqlararo ekranning NDS (Novell Directory Service) kataloglari xizmati bilan uzviy integratsiyasi himoyalangan virtual tarmoqlarni samarali boshqarishga imkon beradi. Shifrlash kalitining taqsimoti RSA kriptotizimi va Diffi-Xellman algoritmi bo'yicha amalga oshiriladi. Axborot paketlarini kriptografik berkitish va autentifikatsiyalashda RC2 va RSA kriptotizimlardan foydalaniladi. Border Managerning bir versiyasida IPSec protokoli madadlanadi. Border Manager tarmoqlararo ekran asosida qurilgan himoyalangan virtual tarmoqlarda brandmauerlardan birining asosiy bo'lishi, boshqarish markazi rolini bajarishi lozim.

Ixtisoslashtirilgan dasturiy ta'minot asosidagi VPN. VPN qurishda ixtisoslashtirilgan dasturiy vositalar keng qo'llaniladi. VPN qu-

rishning dasturiy vositalari himoyalangan tunnellarni faqat dasturiy shakllantirishga imkon beradi va ular ishlaydigan kompyuterni TCP/IP marshrutizatoriga aylantiradi. Bu marshrutizator shifrlangan paketlarni qabul qiladi, rasshifrovka qiladi va lokal tarmoq orqali tayinlangan nuqtaga uzatadi. Oxirgi vaqtda bunday mahsulotlarning yetarlicha soni paydo bo'ldi. Ixtisoslashtirilgan dasturiy ta'minot ko'rinishida VPN-shlyuzlar, VPN-serverlar va VPN-mijozlar bajarilishi mumkin.

Dasturiy usul bo'yicha amalga oshirilgan VPN-mahsulotlar unumdorlik nuqtai nazaridan ixtisoslashtirilgan apparat qurilmalardan qolishsada, dasturiy mahsulotlar masofadagi foydalanuvchilarga yetarli unumdorlikni osongina ta'minlaydi. Dasturiy mahsulotlarning shubhasiz afzalligi ishlatilishida moslanuvchanligi va qulayligi hamda nisbatan yuqori bo'lmagan narxidir. Apparat shlyuzlarni ishlab chiqaruvchi ko'pgina kompaniyalar (masalan, Time Step, VPNet, Shiva) o'zlarining mahsulotlariga standart operatsion tizimda ishlashga mo'ljallangan VPN-mijozning dasturiy amalga oshirilishini qo'shadilar.

MicroSoft kompaniyasining RAS va RRAS dasturiy mahsulotlari. MicroSoft kompaniyasining masofadan foydalanuvchi dasturiy serveri RAS (Remote Access Service) mashhur PPP (Point to Point Protocol) protokolning kengaytirilgan varianti-himoyalangan kanal protokoli PPTPni (Point-to-Point Tunneling Protocol) o'rnatilishi evaziga VPN texnologiyani madadlaydi. Trafikni tunnellash ochiq IP-tarmoq bo'yicha uzatiladigan standart PPP- freymlarni IP-datagrammalarga inkapsulatsiyalash va keyin shifrlash orqali amalga oshiriladi.

RASning asosiy afzalligi – tejamliligi, kamchiligi – unumdorligining pastligi. Hozirda bu mahsulotning takomillashtirilgan versiyasi – RRAS (Routing and Remote Acces Service) paydo bo'ldi. RRAS tarkibidagi takomillashtirilgan dasturiy ko'p protokolli marshrutizator marshrutlashning RIP (Routing Information Protocol) va OSFP (Open Shortest Path First) protokollarini madadlaydi. RRASning bu xususiyatlari undan VPN shlyuzi kabi «tarmoq-tarmoq» aloqasida foydalanishga imkon yaratadi. RAS xizmati masofadan foydalanuvchilarning ko'pchiligiga (256 tagacha) bitta Windows NT serveriga ulanish va lokal tarmoq resurslaridan IPX va TCP/IP protokollari bo'yicha foydalanish imkoniyatini beradi.

Alta Vista Tunnel 98 mahsulotlari oilasi uchta mahsulotni o'z ichiga oladi: Telecommuter Server, Extranet Server, AltaVista Tunnel Client. Telecommuter Server serveri Internet korporativ foydalanuvchilar orasida himoyalangan tunnellarni Internet orqali tashkil etishga

atalgan. Extranet Server serveri yordamida tarmoqlar orasida himoyalangan kanal hosil qilinadi. Bu ikkala server umumiy Alta Vista Tunnel Server nomiga ega. Alta Vista Tunnel Client VPN klientning dasturiy ta'minotidir.

Alta Vista Tunnel 98 oilasining barcha mahsulotlari foydalanuvchilarni autentifikatsiyalashda va RSA kriptografik tizimning sessiya kalitlarini almashishda ishlatiladi. Foydalanuvchilarni autentifikatsiyalashda Security Dynamics kompaniyasining apparat kaliti SecurID ham ishlatilishi mumkin. Mijoz va server yangi sessiya kalitlari bilan har 30 minutda almashishadi.

Ma'lumotlarni shifrlashda RC4 algoritmidan foydalaniladi. Mahsulotlarning xalqaro versiyasi RC4 algoritmi bo'yicha shifrlashda 56 yoki 40 bitli kalitlardan foydalanadi. Ma'lumotlarni autentifikatsiyalash va yaxlitligini ta'minlash uchun MD5 xesh-funksiyasi ishlatiladi. Alta Vista Tunnel 98 oilasining mahsulotlari LZO algoritmi bo'yicha ma'lumotlarni zichlashtirishi mumkin.

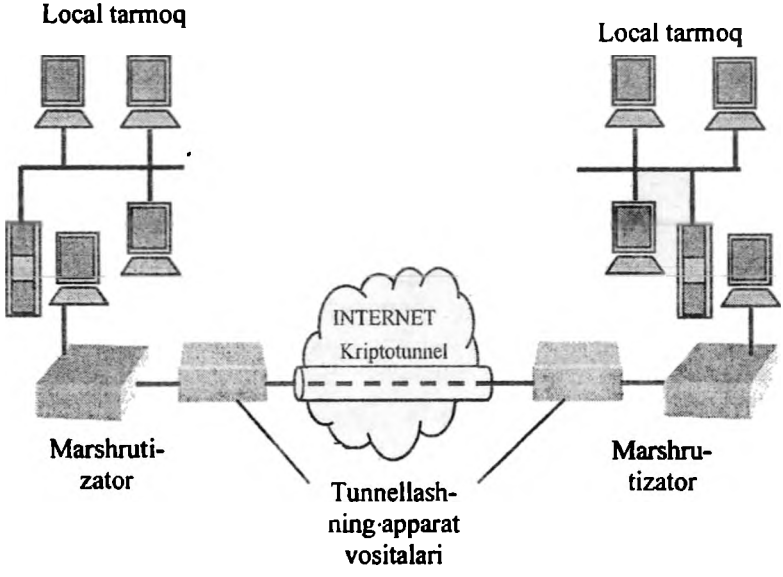
Ushbu oila mahsulotlari aksariyat zamonaviy operatsion tizimlar – Windows NT/2000, Unix BSD/OS, Unix Free BSD va Digital UNIX boshqaruvida ishlashi mumkin. Windows NT/2000 operatsion muhitda Alta Vista Tunnel Server mahsuloti bir vaqtning o'zida 200 tunnel ulanishlarini, UNIX operatsion muhitda esa 2000 gacha tunnel ulanishlarni madadlaydi.

Ixtisoslashtirilgan apparat vositalari asosidagi VPN. Ixtisoslashtirilgan apparat qurilmalari asosidagi VPN-vositalarning asosiy afzalligi-yuqori unumdorligi. VPN-paketlarni ishlashda kerakli hisoblashlar hajmi oddiy paketlarni ishlashdagiga nisbatan 50–100 marta oshadi. Apparat vositalari asosidagi VPNlarda yuqori tezlikka ularda shifrlashning ixtisoslashtirilgan mikrosxemalarda amalga oshirilishi evaziga erishiladi. Bunday VPN-vositalar ko'pincha IPSec protokoli bilan birga ishlay oladi va lokal tarmoqlar orasida kriptohimoyalangan tunnellarni shakllantirishda ishlatiladi. Ba'zi ishlab chiqaruvchilarning VPNni shakllantiruvchi asbob-uskunalari bir vaqtning o'zida «masofadagi kompyuter-lokal tarmoq» rejimida himoyalangan bog'lanishni ham madadlaydi.

Apparat VPN-shlyuzlar alohida apparat qurilmasi ko'rinishida bo'ladi. Ularning asosiy vazifasi – trafikni yuqori unumdorlik bilan shifrlash. Bu VPN-shlyuzlar X.509 raqamli sertifikatlari PKI ochiq kalitlarni boshqarish infratuzilmalari bilan ishlaydi, LDAP bo'yicha ma'lumot beradigan xizmatlar bilan ishlashni madadlaydi.

Apparat himoyalangan tunnel ishlashining eng oddiy varianti – apparat shifrlashdan foydalanib ulanishlarni yaratish. Tunnellashning apparat vositalari, odatda, lokal va global tarmoqlarning tutashgan joyida, marshrutizatordan keyin o'rnatiladi (7.9-rasm) va avtomatik tarzda berilgan trafikni shifrlaydi. Bunday yondashishning asosiy afzalligi shundaki, ishchi stansiyalar va marshrutizatorlarning shakllantiriluvchi kriptotunnellar bilan hech qanday bog'liqligi yo'q, VPN o'rnatilganida ularni konfiguratsiyasini o'zgartirish talab etilmaydi.

Apparat shlyuzlarni installyatsiyalash dasturiy shlyuzlar va marshrutizatorlar va brandmauerlar asosidagi shlyuzlarga nisbatan juda oson amalga oshiriladi. Bunday qurilmalarni boshqarish ikkita asosiy masalani yechishni talab etadi: sertifikatsiya markazi orqali kalitlarni boshqarish va himoyalangan tunnellashni boshqarish. Aksariyat apparat tunnellash vositalarida sertifikatsiya markazlari Windowsga moslashgan dasturiy ilovalardir. Apparat tunnellarini markazlashgan holda bitta ish joyida turib boshqarish mumkin. Boshqaruvchi dasturlar tunnelning asosiy himoyalash funksiyalarining bajarilishini va xatoliklarni ishlashni ta'minlaydi.



7.9-rasm. Ixtisoslashtirilgan apparat vositalar asosida tunnellash sxemasi.

Ixtisoslashtirilgan apparat VPN-vositalar narxidan tashqari barcha bo'lishi mumkin bo'lgan ko'rsatkichlari bo'yicha yetakchi hisoblanadi.

TimeStep kompaniyasi korxonalarda keng masshtabli axborot almashinuvi uchun IPSec bilan birga ishlay oluvchi PERMIT Enterprise Snite deb ataluvchi VPN-mahsulotni ishlab chiqdi. Ushbu mahsulot Internet orqali masofadan foydalanishni tashkil etish, korporativ intratarmoq va ekstratarmoqlarni qurish uchun to'liq yechim hisoblanadi. PERMIT Enterprise mavjud tarmoqlarda tarmoq va oxirgi foydalanuvchi unumdorligiga jiddiy ta'sir qilmagan holda, osongina saflanadi, uning masshtablanuvchi arxitekturasi bir necha VPNlarni yaratish va ularni boshqarish imkoniyatini beradi.

Kompaniya tomonidan shlyuzning quyidagi to'rtta modifikatsiyasi taqdim etiladi:

– PERMIT/Gate 1520 narxi qimmat bo'lmagan avtonom qurilma bo'lib, quvvatli telekompyuterlar yoki SOHO sinfidagi katta bo'lmagan masofadagi ofislar uchun ishlatiladi;

– PERMIT/Gate 2520 va PERMIT/Gate 4520 o'tkazish qobiliyati, mos holda 4 va 1- Mbit/s, bo'linmalar ofislari va kichik lokal hisoblash tarmoqlariga mo'ljallangan, masofadagi yuzlab foydalanuvchilarni madadlaydi;

– PERMIT/Gate 7520 (70 Mbit/s) ichki lokal hisoblash tarmoqlarida ishlatiladi va masofadagi minglab foydalanuvchilarni madadlaydi.

PERMIT/Gate shlyuzlarining muhim afzalligi – trafik ishlanishining yuqori unumdorligini ta'minlsh maqsadida DES va 3-DES shifrlash algoritmining apparat amalga oshirilishi.

PERMIT/Gate7520 shlyuzi IPSecning amalga oshirilishining apparat vositasi bilan ham jihozlanganligi, unumdorlikka ta'sir qilmagan holda minglab VPN ulanishlarni madadlashga imkon beradi. Bu zaruriyat tug'ilganda, korporativ tarmoqni osongina kengaytirish imkonini yaratadi.

Mijoz dasturiy ta'minoti PERMIT/Client IPSec protokolini madadlaydi va masofadagi foydalanuvchilarga o'zining tarmog'i bilan xavfsiz bog'lanish imkonini beradi. Ushbu dasturiy ta'minot Windows95/98/XP/NT yoki MAC OS 7.1. boshqaruvida ishlovchi alohida ishchi stansiya tomonidan adreslangan tarmoq trafigini himoyalaydi.

PERMIT/Gate shlyuzlarining har biri dasturli utilita PERMIT/Config bilan birga taqdim etiladi. Bu dasturli utilita virtual xususiy tarmoqning har qanday nuqtasidan bir necha shlyuzlaming das-

turiy ta'minotini masofadan konfiguratsiyalash, boshqarish va modifikatsiyalashga imkon yaratadi.

VPNet kompaniyasi VPN qurish uchun dastlabki integratsiyalangan yechimlardan biri – VPNwareni taklif etdi. Bu yechim o'z ichiga quyidagi mahsulotlarni oladi:

– uchta VPN-shlyuz: shtab qarorgohi va yirik lokal tarmoqlar uchun VSU.1100, bo'linmalar uchun VSU-1010 va katta bo'lmagan ofislar uchun VSU-10;

– iPass kompaniyasidan dasturiy server RoamServer;

– mijoz dasturiy ta'minoti VPN remote;

– boshqarishning dasturiy tizimi VPN manager.

VPNet asbob-uskunalari, «tarmoq-tarmoq» va «tarmoq – masofadagi foydalanuvchi» xilidagi ulanishlarga mo'ljallangan VPNni madadlaydi. Ishlatiladigan mahsulotlarga bog'liq holda VPNware tizimi IPSecning standart amalga oshirilishi yordamida ommaviy IP tarmoq orqali uzatilayotgan ma'lumotlarni himoyalash bilan 25dan 5000tacha foydalanuvchilarni madadlashi mumkin. Bu tizim turli masshtabli tarmoqlarda yirik korxonaning markaziy lokal tarmog'ida, bo'linma va katta bo'lmagan ofis lokal tarmog'ida va masofadagi foydalanuvchilarni himoyalashda ishlatilishi mumkin.

VSU-1010 va VSU-10 shlyuzlar IPSec bilan birga ishlay oladi va DES va 3-DES algoritmlari bo'yicha ma'lumotlarni shifrlashni apparat madadlashga ega. VPNning boshqaruvchi ilovasi statistikani yig'ishga va VPNdagi hodisalarni qaydlashga imkon beradi. Har xil VPNlarni boshqarishni markazlashtirish evaziga himoyani boshqarishning boshqa funksiyalarini soddalashtirish va markazlashtirish, masalan, korporativ brandmauer yaxlitligini buzilishini nazoratini ta'minlash mumkin. VPNet mahsulotlarining afzalligi-mavjud tarmoq bilan integratsiyalanishining soddaligi, unumdorligining nisbatan yuqoriligi va IPSecning to'la amalga oshirilishi.

Mijoz dasturiy ta'minoti VPNremote IPSec protokolini madadlaydi va Windows NT muhitida hamda telefon tarmoqlari orqali foydalanilganda masofadagi va mobil foydalanuvchilar, telekompyuterlar va biznes-sheriklarning ma'lumotlarini himoyalashda Windows95/98/XP muhitida ishlaydi.

Boshqaruv tizimi VPNmanager virtual xususiy tarmoqlarni yaratish, konfiguratsiyalash va boshqarish uchun maxsus ishlab chiqilgan. Tarmoq ma'muri ushbu tizim yordamida, grafik interfeysni ishlatib masofadagi foydalanuvchilarni va biznes-sheriklarni VPNga osongina

qo'shishi mumkin. VPN mijozlarini masofadan ma'murlashga Dyna-Policy funksiyasi atalgan.

LanRover VPN Gateway shlyuzi Shiva kompaniyasi tomonidan taqdim etilgan bo'lib, ICSA tomonidan sertifikatsiyalangan. Bu shlyuz ochiq tarmoq orqali uzatiladigan ma'lumotlarni himoyalash texnologiyalarining keng to'plamini madadlaydi. Yaxlitlikni va konfidensiallikni ta'minlash, foydalanishning nazorati, X.509ning raqamli sertifikatlariga, Security Dynamics apparat kalitlariga, RADIUS protokoli yoki domenli sxemaga asoslangan autentifikatsiyalashning turli sxemalari bu to'plamga kiradi.

Ma'lumotlarni apparat shifrlash DES yoki 3-DES algoritmlari asosida amalga oshiriladi. LanRover VPN Gateway shlyuzlari Pentium-texnologiyaning tezligi, shifrlovchi ixtisoslashtirilgan integral sxemalarning tezkorligi va real vaqtning ko'p vazifali operatsion tizimning reaktivligining noyob birikmasidan foydalanadi. Bu shlyuzlar ishlatishda qulay va ularning ishlashi oxirgi foydalanuvchilar uchun shaffof. Bu shlyuzlar bilan ishlash qulayligini ta'minlash maqsadida grafik foydalanuvchi interfeysli utilita VPN manager taqdim etiladi. Bu utilita ma'murga har qanday Windows 95/NT tizimidan birdaniga bir necha shlyuzlarni boshqarishni ta'minlaydi.

7.4. Kanal va seans sathlarda himoyalangan virtual kanallarni qurish

Kanal sathida himoyalangan virtual kanallarni shakllantirish protokollari

PPTP, L2F va L2TP protokollar OSI modeli kanal sathining tunnellash protokollari hisoblanadi. Ushbu protokollarning umumiy xususiyati shundan iboratki, ular ochiq tarmoq, masalan, Internet orqali korporativ tarmoq resurslaridan himoyalangan ko'p protokolli masofadan foydalanishni tashkil etishda ishlatiladi. Uchala protokolni, odatda, himoyalangan kanalni shakllantirish protokollariga mansub deb hisoblaydilar. Ammo bu ta'rifga uzatiladigan ma'lumotlarni tunnellashni va shifrlashni ta'minlovchi faqat PPTP protokoli aniq mos keladi, chunki L2F va L2TP protokollar faqat tunnellash funksiyalarini madadlaydi. Tunnellangan ma'lumotlarni himoyalash (shifrlash, yaxlitlik, autentifikatsiya) uchun bu protokollarda qo'shimcha, protokol, xususan, IPSec protokoli ishlatiladi.

PPTP protokoli ma'lumotlarni IP, IPX va NetBEUI protokollari bo'yicha almashish uchun himoyalangan kanallarni yaratishga imkon beradi. Ushbu protokollar ma'lumotlari PPP kadrlariga joylanadi va so'ngra PPTP protokoli vositasida IP protokolining paketlariga inkapsulat-siyalanadi va shu protokol yordamida shifrlangan ko'rinishda har qanday TCP/IP tarmog'i orqali tashiladi.

PPP sessiyasi doirasida uzatiluvchi paketlar quyidagi tuzilmaga ega (7.10-rasm):

– Internet ichida ishlatiluvchi kanal sathining sarlavhasi, masalan, Ethernet kadrining sarlavxasi;

– tarkibida paketni jo'natuvchi va qabul qiluvchi adreslari bo'lgan IP sarlavhasi;

– marshrutlash uchun inkapsulatsiyalashning umumiy usulining sarlavhasi GRE(Generic Routing Encapsulation);

– tarkibida IP, IPX yoki NetBEUI paketlari bo'lgan dastlabki paket PPP.

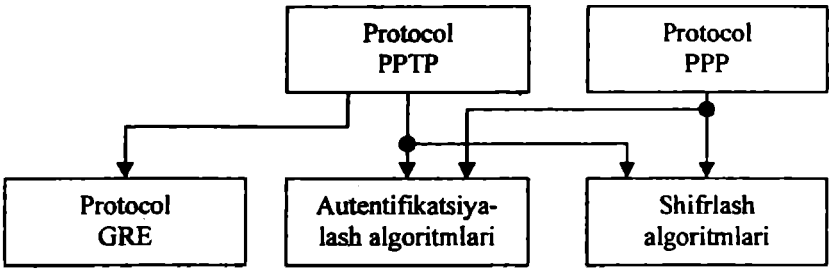
Uzati-ladigan kadr sar-lavhasi	IP - sarlav-ha	GRE - sarlav-ha	PPP – sarlav-ha	Shifrlangan ma'lumotlar PPP	Uzati-ladigan kadr oxiri

7.10-rasm. PPTP tunneli bo'yicha jo'natiladigan paket tuzilmasi.

Tarmoqning qabul qiluvchi uzeli IP paketlardan PPP kadrlarni chiqarib oladi, so'ngra PPP kadrdan dastlabki paket IP, IPX yoki NetBEUI paketini chiqarib olib uni lokal tarmoq bo'yicha muayyan adresatga jo'natadi. Kanal sathining inkapsulatsiyalovchi protokollarining ko'p protokolliligi (unga PPTP protokol ham taalluqli), ularning yanada yuqoriroq sathning himoyalangan kanal protokollaridan afzalligidir. Masalan, agar korporativ tarmoqda IPX yoki NetBEUI ishlatilsa, IPSec yoki SSLprotokollarini ishlatib bo'lmaydi, chunki ular IP tarmoq sathining faqat bitta protokoliga mo'ljallangan.

Inkapsulatsiyalashning mazkur usuli OSI modelining tarmoq sathi protokollariga bog'liq bo'lmaslikni ta'minlaydi va ochiq IP-tarmoqlar orqali har qanday lokal tarmoqlardan (IP, IPX yoki NetBEUI) himoyalangan masofadan foydalanishni amalga oshirishga imkon beradi. PPTP protokoliga muvofiq, himoyalangan virtual kanal yaratishda masofadagi

foydalanuvchini autentifikatsiyalash va uzatiluvchi ma'lumotlarni shifrlash amalga oshiriladi (7.11-rasm).



7.11-rasm. PPTP protocoli arxitekturasi.

Masofadagi foydalanuvchini autentifikatsiyalashda PPP uchun qo'llaniladigan turli protokollardan foydalanish mumkin. Microsoft kompaniyasi tomonidan Windows 98/XP/NT/2000 ga kiritilgan PPTPning amalga oshirilishida autentifikatsiyalashning quyidagi protokollari madadlanadi: parol bo'yicha aniqlash protokoli PAP(Pasword Athentication Protocol), qo'l berishishda aniqlash protokoli MSCHAP (Microsoft Challenge – Handshaking Authentication Protocols) va aniqlash protokoli EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAP protokolidan foydalanilganda identifikatorlar va parollar aloqa liniyalari orqali shifrlanmagan ko'rinishda uzatiladi, bunda autentifikatsiyalashni faqat server o'tkazadi. MSCHAP va EAP-TLS protokollaridan foydalanilganda niyati buzuq odamning ushlab qolingan shifrlangan parolli paketdan qayta foydalanishidan himoyalash va mijoz va VPN-serverni autentifikatsiyalash ta`minlanadi.

PPTP yordamida shifrlash Internet orqali jo'natishda ma'lumotlardan hech kim foydalana olmasligini kafolatlaydi. Shifrlash protokoli MPPE (Microsoft Point-to-Point Encryption) faqat MSCHAP(1 va 2 versiyalari) va EAP-TLS bilan birga ishlay oladi, mijoz va server orasida parametrlar muvofiqlashtirilishida shifrlash kalitining uzunligini avtomatik tarzda tanlay oladi. MPPE protokoli uzunligi 40, 56 yoki 128 bit bo'lgan kalitlar bilan ishlashni madadlaydi.

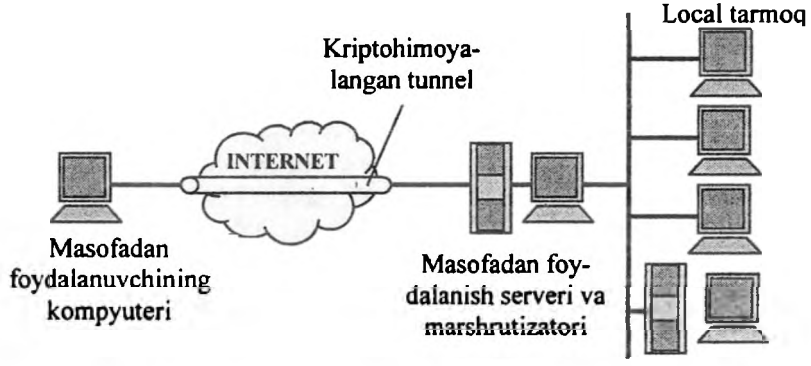
PPTP protokoli har bir olingan paketdan so'ng shifrlash kaliti qiymatini o'zgartiradi. MMPE protokoli «nuqta-nuqta» xilidagi aloqa kanallari uchun ishlab chiqilgan bo'lib, bu aloqa kanallarida paketlar

ketma-ket uzatiladi va ma'lumotlar yo'qotilishi juda kam. Bu vaziyatda navbatdagi paket uchun kalit qiymati oldingi paketning rasshifrovkasi natijasiga bog'liq. Umumfoydalanuvchi tarmoq orqali virtual tarmoq qurishda bu shartlarga rioya qilish mumkin emas, chunki ma'lumotlar paketi ko'pincha qabul qiluvchiga jo'natilgan ketma-ketlikda kelmaydi. Shuning uchun PPTP shifrlash kalitini o'zgartirishda paketlarning tartib raqamidan foydalanadi. Bu rasshifrovka qilishni oldingi qabul qilingan paketlarga bog'liq bo'lmagan holda amalga oshirishga imkon beradi.

PPTP protokoli uchun qo'llashning quyidagi ikkita asosiy sxemasi aniqlangan:

– masofadan foydalanuvchining Internet bilan to'g'ridan-to'g'ri ula-nishidagi tunnellash sxemasi;

– masofadan foydalanuvchining Internet bilan provayder orqali telefon liniyasi bo'yicha ulanishidagi tunnellash sxemasi.



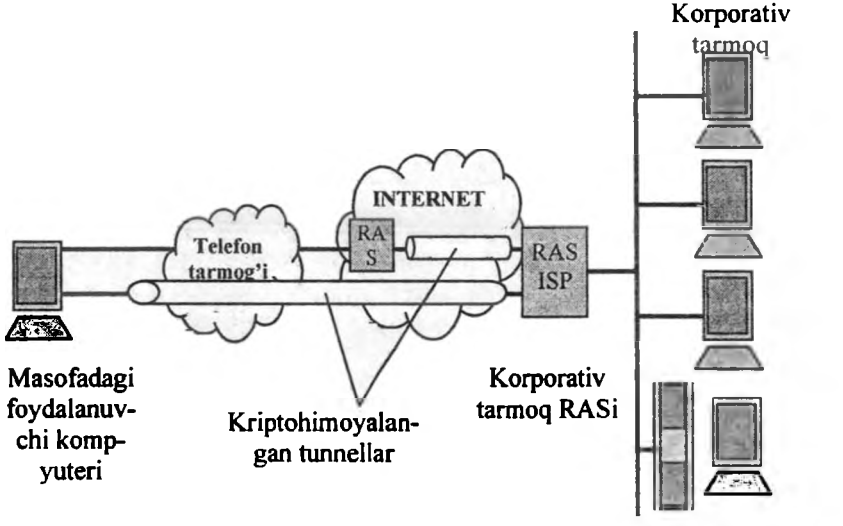
7.12 -rasm. Masofadan foydalanuvchi kompyuterini Internetga to'g'ridan-to'g'ri ulanishidagi tunnellash sxemasi.

Tunnellashning birinchi sxemasi amalga oshirilganida (7.12-rasm) masofadan foydalanuvchi Windows 98/XP/NT tarkibidagi masofadan foydalanish servisi RAS (Remote Access Service)ning mijoz qismi yordamida lokal tarmoq bilan masofaviy bog'lanishni o'rnatadi. So'ngra foydalanuvchi lokal tarmoqdan masofadan foydalanish serveriga, uning IP adresini ko'rsatib murojaat etadi va u bilan PPTP protokoli bo'yicha aloqa o'rnatadi.

Masofadan foydalanish serveri vazifasini lokal tarmoqning chegara marshrutizatori bajarishi mumkin. Masofadan foydalanuvchining kompyuterida Windows 98/XP/NT tarkibidagi RAS serverning mijoz qismi

va PPTPning drayveri, masofadan foydalanuvchi lokal tarmog'ining serverida esa Windows NT Server tarkibidagi RAS serveri va PPTP drayveri o'rnatilishi shart. PPTP protokoli o'zaro aloqadagi tomonlar almashadigan bir nechta xizmatchi xabarni aniqlaydi. Xizmatchi xabarlar TCP protokoli bo'yicha uzatiladi. Muvaffaqiyatli autentifikatsiyalashdan so'ng himoyalangan almashish jarayoni boshlanadi. Lokal tarmoqning ichki serverlari PPTP protokolini madadlamasligi mumkin, chunki chegara marshrutizator IP paketlardan PPP kadrlarini chiqarib olib ularni lokal tarmoq orqali kerakli IP, IPX yoki NetBIOS formatida jo'natadi.

Masofadagi kompyuterni Internetga telefon liniyasi bo'yicha provayder ISP (Internet Service Provider) orqali ulashda tunnellash sxemasining ikkita varianti bo'lishi mumkin (7.13-rasm).



7.13-rasm. Masofadan foydalanuvchi kompyuterini ISP provayderi orqali telefon liniyasidan foydalanib Internetga ulanishini tunnellash sxemasining ikkita varianti.

Sxemaning birinchi variantining qurilishi protokol PPTPning provayder ISPning masofadan foydalanish serveri va chegara korporativ marshrutizator orqali madadlanish taxminiga asoslangan. Server, odatda, foydalanuvchilarning ulanishini ta'minlovchi ko'p sonli tezkorligi past portlarga ega. Provayder ISPning serveri RAS va marshrutizator orasida

himoyalangan kanal hosil bo'ladi. Mohiyati bo'yicha bu – «shlyuz-shlyuz» xilidagi himoyalangan kanal varianti.

Bu variantda masofadan foydalanuvchining kompyuteri protokol PPTPni madadlamasligi mumkin. Masofadagi foydalanuvchi standart protokol PPP yordamida provayder ISPda o'rnatilgan masofadan foydalanish serveri RAS bilan bog'lanadi va autentifikatsiyalashni provayderda o'taydi.

Provayderning serveri RAS foydalanuvchining ismi bo'yicha foydalanuvchilarning hisob ma'lumotlari bazasidan marshrutizatorning IP-adresini topadi. Bu marshrutizator chegara marshrutizatori va ushbu foydalanuvchining lokal tarmoqdan masofadan foydalanish serveri hisoblanadi. Bu marshrutizator bilan provayder serveri RAS Intrenet orqali PPTP protokoli bo'yicha sessiya o'tkazadi. Provayderning serveri RAS lokal tarmoqdan masofadan foydalanish serveriga foydalanuvchining identifikatorini va boshqa ma'lumotlarni uzatadi. Ular asosida bu server CHAP protokoli bo'yicha foydalanuvchini yana autentifikatsiyalaydi. Agar foydalanuvchi ikkinchi autentifikatsiyalashdan (bu uning uchun shaffof bo'ladi) muvaffaqiyatli o'tsa, provayderning RASi bu to'g'rida foydalanuvchini PPP protokol bo'yicha ogohlantiradi va so'ngra, provayderning masofadan foydalanuvchi serveri va lokal tarmoq orasida himoyalangan virtual kanal shakllanadi.

Masofadan foydalanuvchining kompyuteri lokal tarmoq IP, IPX yoki NetBIOS bilan o'zaro aloqa paketlarini PPP kadrlariga joylab provayderning masofadan foydalanuvchi serveri RASga uzatadi. Provayderning RASi atalgan adres sifatida chegara marshrutizatori adresini, manba adresi sifatida o'zining shaxsiy IP-adresini ko'rsatgan holda PPP kadrlarining IP paketlarga inkapsulatsiyasini amalga oshiradi. Provayderning masofadan foydalanuvchi serveri va lokal tarmoq orasida uzatishga atalgan PPP paketlari simmetrik shifrda shifrlanadi. Bunda simmetrik maxfiy kalit sifatida CHAP protokoli bo'yicha autentifikatsiyalash uchun provayder RASining hisob ma'lumotlari bazasida saqlanuvchi foydalanuvchi parolining daydjesti ishlatiladi. Simmetrik shifrlash algoritmlari sifatida DES yoki RC-4 algoritm ishlatiladi.

Tavsif etilgan variant keng tarqalmadi, chunki protokol PPTP, asosan, Microsoft kompaniyasining mahsulotlarida – RAS Windows NT 4.0 ning mijoz va server qismlarida hamda RAS Windows 98/XPning mijoz qismida amalga oshirilgan. Provayderlar masofadan foydalanish serveri sifatida odatda RAS Windows NTga nisbatan quvvatliroq vositalardan foydalanadi. Bunda protokol PPTP Internet provayderlarining masofadan foydalanish serverlari RAS orqali doimo madadlanmaydi. Undan tashqari, bu sxemada ma'lumotlar foydalanuvchi kompyuteri va Intrenet provayderi orasida himoyalanmagan holda uzatiladi, natijada, uning xavfsizligi jiddiy yomonlashadi.

Microsoft kompaniyasi tomonidan PPTP protokolini qo'llashning yana bir boshqa sxemasi tavsiya etilgan. Bu sxemaga binoan PPTP protokolining provayderning masofadan foydalanish serveri tomonidan madadlanishi talab etilmaydi. Tunnellashning bu varianti (7.13-rasm) keng tarqaldi.

Ta'kidlash lozimki, bu sxemada korporativ tarmoqning chegara marshrutizatori, oldingi sxemadagidek PPTP protokolni madadlashi shart. Bunday marshrutizator sifatida, xususan, RAS xizmati o'rnatilgan dasturiy marshrutizator Windows NT 4.0 ishlatilishi mumkin. Umuman, RAS xizmati va PPTP protokoli ishlaydigan, masofadagi mijoz kompyuteri va korporativ tarmoq ichidagi kompyuter orasida himoyalangan kanalni yaratish mumkin.

Ushbu sxemaga binoan foydalanuvchi ikki marta masofadan ulanishni o'rnatishi lozim. Birinchi marta foydalanuvchi provayderning masofadan foydalanish serveriga modem bo'yicha qo'ng'iroq qilib, PPP protokoli bo'yicha u bilan aloqa o'rnatadi va provayder ISP tomonidan madadlanuvchi protokollarning biriga (PAP yoki CHAP) yoki terminal dialogiga muvofiq autentifikatsiyadan o'tadi. ISP provayderida autentifikatsiyadan muvaffaqiyatli o'tganidan so'ng foydalanuvchi lokal tarmoqdan masofadan foydalanish serveri bilan, uning IP-adresini ko'rsatib ulanishni o'rnatadi. Natijada, masofadagi kompyuter va lokal tarmoq RAS orasida PPTP protokoli bo'yicha sessiya o'rnatiladi. Mijoz yana, endi o'zining korporativ tarmog'i serverida autentifikatsiyalanadi. Masofadan foydalanish serveri foydalanuvchining haqiqiyligini o'zining hisob ma'lumotlari bazasi asosida tekshiradi. Muvaffaqiyatli autentifikatsiyalashdan so'ng axborotni himoyalangan almashish jarayoni boshlanadi.

Kriptohimoyalangan tunnelning chegara qurilmalarining o'zaro aloqasi uchun PPTP protokolida boshqaruvchi xabarlar ko'zda tutilgan bo'lib, bu boshqaruvchi xabarlar tunnelni o'rnatish, madadlash va uzish uchun atalgan. Boshqaruvchi xabarlarni almashish mijoz va PPTPning serveri orasida o'rnatiluvchi TCP-ulanish bo'yicha amalga oshiriladi. Bu ulanish bo'yicha uzatiladigan paketlarda kanal sathi sarlavhasi bilan bir qatorda IP protokolining sarlavhasi, TCP protokolining sarlavhasi va paket ma'lumotlari sohasidagi PPTPning boshqaruvchi xabari bo'ladi.

L2F protokoli Cisco System kompaniyasi tomonidan OSI modelining kanal sathida himoyalangan virtual tarmoq qurish uchun, PPTP protokoliga alternativ sifatida ishlab chiqilgan. L2F protokoli turli tarmoq protokollari tomonidan madadlanishi bilan ajralib turadi va Internet provayderlari uchun foydalanishda ancha qulay. L2F protokoli masofadagi foydalanuvchi kompyuteri bilan provayder serveri aloqasini tashkil etishda masofadan foydalanishninig turli protokollarini (PPP, SLIP va h.) ishlatishga yo'l quyadi. Tunnel orqali paketlarni tashishda ishlati-

luvchi ochiq tarmoq IP protokoli asosida va boshqa, xususan, X.25 protokoli asosida ishlashi mumkin.

L2F protokoli quyidagi xususiyatlarga ega:

– haqiqiylikni tekshiruvchi muayyan protokolga qat'iy bog'lanmaganlikni taxminlovchi autentifikatsiyalash muolajalarining moslanuvchanligi;

– oxirgi tizimlar uchun shaffofligi, ya'ni lokal tarmoqning ishchi stansiyalari va masofadagi tizimga himoyalash serveridan foydalanish uchun maxsus dasturiy ta'minot talab etilmaydi;

– vositalar uchun shaffofligi, ya'ni masofadagi foydalanuvchilarni avtorizatsiyalash lokal tarmoqning masofadan foydalanish serveriga foydalanuvchilarni bevosita ulanishiga o'xshab amalga oshiriladi;

– auditning to'liqligi, ya'ni lokal tarmoq serveridan foydalanish hodisa-sini qaydlash nafaqat masofadan foydalanish serveri tomonidan, balki provayder serveri tomonidan ham amalga oshiriladi.

L2F protokolining spetsifikatsiyasiga muvofiq himoyalangan tunnelni hosil qilishda quyidagi protokollar ishlatiladi:

– dastlabki inkapsulatsiyalanuvchi protokol – bu protokol (IP, IPX, yoki NetBEUI) asosida lokal tarmoq ishlaydi;

– protokol - yo'lovchi – bu protokolga dastlabki protokol inkapsulatsiyalanadi va bu protokolning o'zi ham ochiq tarmoq orqali masofadan foydalanganda inkapsulatsiyalanishi mumkin; PPP protokoli tavsiya etiladi;

– boshqaruvchi (inkapsulatsiyalovchi) protokol, tunnelni yaratishda, madadlashda va uzishda ishlatiladi (bunday protokol sifatida L2F ishlatiladi);

– provayder protokoli, inkapsulatsiyalanuvchi protokollarni (dastlabki protokol va protokol – yo'lovchi) tashishda ishlatiladi; eng ko'p tarqalgan provayder protokoli IP protokolidir.

Ta'kidlash lozimki, L2F texnologiyasidan foydalanilganda provayderning masofadan foydalanish serveri foydalanuvchini autentifikatsiyalashni faqat virtual kanal yaratilishi zarurligini aniqlash va istalgan lokal tarmoqning masofadan foydalanish serveri adresini topishda ishlatadi. Haqiqiylikni yakuniy tekshirish lokal tarmoqning masofadan foydalanish serveri tomonidan, u bilan provayder serveri ulanganidan so'ng, bajariladi.

L2F protokolining quyidagi kamchiliklarini ko'rsatish mumkin:

– unda IP protokolining joriy versiyasi uchun axborot almashinuvining oxirgi nuqtalari orasida kriptohimoyalangan tunnel yaratish ko'zda tutilmagan;

– virtual himoyalangan kanal faqat provayderning masofadan foydalanish serveri va lokal tarmoqning chegara marshrutizatori orasida yaratilishi mumkin, bunda masofadagi foydalanuvchi kompyuteri bilan provayder serveri orasidagi joy ochiq qoladi.

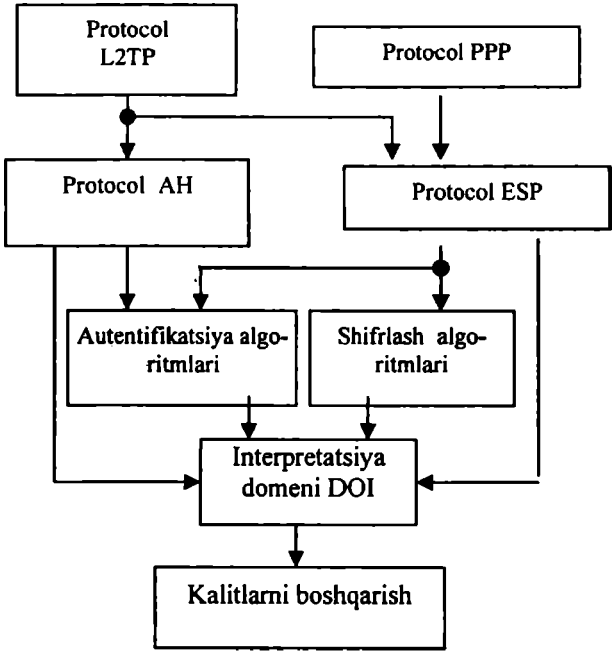
Hozirda L2F protokoli Internet standarti loyihasi maqomiga ega bo'lgan L2TP protokoliga singdirilgan.

L2TP protokoli IETF tashkilotida Microsoft va Cisco Systems kompaniyalari madadida ishlab chiqilgan. L2TP protokoli ixtiyoriy muhitli umummaqsad tarmoq orqali PPP-trafikni himoyalangan tunnellash protokoli sifatida ishlab chiqilgan.

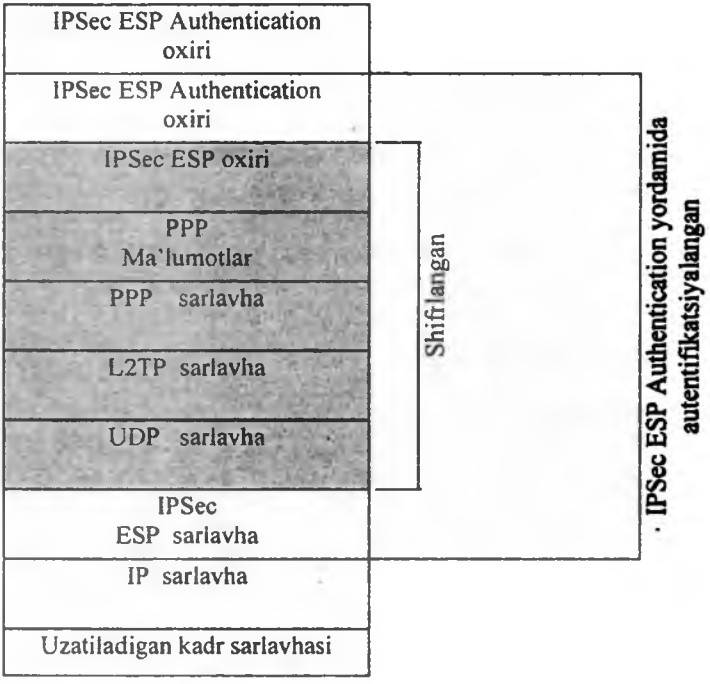
PPTPdan farqli holda L2TP protokoli IP protokoliga bog'langan emas, shu sababali undan paketlarni kommutatsiyalovchi tarmoqlarda, masalan, ATM (Asynchronous Transfer Mode) yoki kadrlarni retranslatsiyalovchi (frame relay) tarmoqlarda foydalanish mumkin.

L2TP protokolida PPTP va L2F protokollarining nafaqat yaxshi xususiyatlari birlashtirilgan, balki yangi funksiyalar, jumladan IPSec protokollari stekining AH va ESP protokollari bilan ishlash imkoniyati qo'shilgan.

L2TP protokolining arxitekturasi 7.14-rasmda keltirilgan.



7.14-rasm. L2TP protokolining arxitekturasi.



7.15-rasm. L2TP tunneli bo'ylab jo'natiladigan paket tuzilmasi.

AH va ESP protokollari foydalanuvchilarning, kelishilgan holda, shifrlash va autentifikatsiyalashning turli kriptografik algoritmlarini ishlatishlariga yo'l qo'yadi. Interpretatsiya domeni DOT (Domain of Interpretation) ishlatiluvchi protokollar va algoritmlarning birga ishlashini ta'minlaydi.

Mohiyati bo'yicha, gibrid protokol L2TP masofadagi foydalanuvchilarni autentifikatsiyalash, himoyalangan virtual ulanishni yaratish va ma'lumotlar oqimlarini boshqarish funksiyalari bilan kengaytirilgan PPP protokolidir.

L2TP protokoli transport sifatida UDP protokolini ishlatadi va tunnelni boshqarishda va ma'lumotlarni tashishda xabarlarning bir xil formatidan foydalanadi.

PPTP protokolidagidek, L2TP protokoli tunnelga uzatish uchun paketni yig'ishda avval PPP axborot ma'lumotlari maydoniga PPP sarlavhasini, so'ngra L2TP sarlavhasini qo'shadi. Shu tariqa olingan paket UDP protokol tomonidan inkapsulatsiyalanadi. L2TP protokol jo'natuvchi va qabul qiluvchi porti sifatida UDP-portdan foydalanadi. 7.15-rasmda L2TP tunneli bo'yicha jo'natiluvchi paket tuzilmasi keltirilgan.

IPSec protokollar steki xavfsizligi siyosatining tanlangan xiliga bog'liq holda L2TP protokoli UDP-xabarni shifrlashi va unga ESP (Encapsulation Security Payload)ning sarlavhasini va oxirini hamda IPSec ESP Authenticationning oxirini qo'shishi mumkin. So'ngra IPga inkapsulyatsiyalash bajariladi. Tarkibida jo'natuvchi va qabul qiluvchi adreslari bo'lgan IP-sarlavha qo'shiladi. Oxirida L2TP ma'lumotlarni uzatishga tayyorlash uchun ikkinchi PPP-inkapsulatsiyalashni bajaradi.

Kompyuter – qabul qiluvchi ma'lumotlarni qabul qiladi, PPPning sarlavhasi va oxirini ishlaydi. IP sarlavhani olib tashlaydi, IPSec ESP Authentication yordamida IP ning axborot maydoni autentifikatsiyalanadi, IPSec ESP protokoli esa paketning rasshifrovkasida yordam beradi. Keyin kompter UDP sarlavhasini ishlaydi va tunnelni identifikatsiyalash uchun L2TP sarlavhasidan foydalanadi. Endi PPP paketning tarkibida faqat foydali ma'lumotlar bo'ladi, ular ishlanadi va ko'rsatilgan qabul qiluvchiga yuboriladi.

L2TP protokoli «foydalanuvchi» va «kompyuter» sathlarda autentifikatsiyalashni ta'minlaydi hamda ma'lumotlarni autentifikatsiyalaydi va shifrlaydi. Mijozlarni va VPN serverlarini autentifikatsiyalashning birinchi bosqichida L2TP sertifikatsiya xizmatidan olingan lokal sertifikatlardan foydalanadi. Mijoz va server sertifikatlar bilan almashishadi va himoyalangan ulanish ESP SA (Security Association)ni yaratishadi.

L2TP kompyuterni autentifikatsiyalashni tugatganidan so'ng, foydalanuvchi sathda autentifikatsiyalashda foydalanuvchi ismini va parolni ochiq ko'rinishda uzatuvchi har qanday protokol, hatto PAP, ishlatilishi mumkin. Bu tamomila xavfsiz, chunki L2TP butun sessiyani shifrlaydi. Ammo foydalanuvchini autentifikatsiyalashni, kompyuter va foydalanuvchini autentifikatsiyalashda turli kalitlardan foydalanuvchi MSCHAP yordamida o'tkazish xavfsizlikni oshirishi mumkin.

L2TP protokolining taxmini bo'yicha, provayderning masofadan foydalanish serveri va korporativ tarmoq marshrutizatori orasida tunnel hosil qiluvchi sxemalardan foydalaniladi. Bu protokol oldingilaridan (PPTP va L2F protokollaridan) farqli holda oxirgi abonentlar orasida, har biri alohida ilovaga ajratilishi mumkin bo'lgan, bir necha tunnelni birdaniga ochish imkoniyatini taqdim etadi. Bu xususiyat tunnellashning moslanuvchanligini va xavfsizligini ta'minlaydi.

L2TP protokolining spetsifikatsiyasiga binoan, provayderning masofadan foydalanish serveri rolini, L2TP protokolining mijoz qismini amalga oshiruvchi va masofadagi foydalanuvchiga uning lokal tarmog'idan Internet orqali tarmoqli foydalanishni ta'minlovchi, foydalanishning konsentratori LAC (L2TP Access Concentrator) bajarishi lozim. Lokal tarmoqning masofadan foydalanish serveri sifatida PPP protokoli bilan birga ishlay oluvchi platformalarda ishlovchi tarmoq serveri LNS (L2TP Network Server)dan foydalaniladi (7.16-rasm).

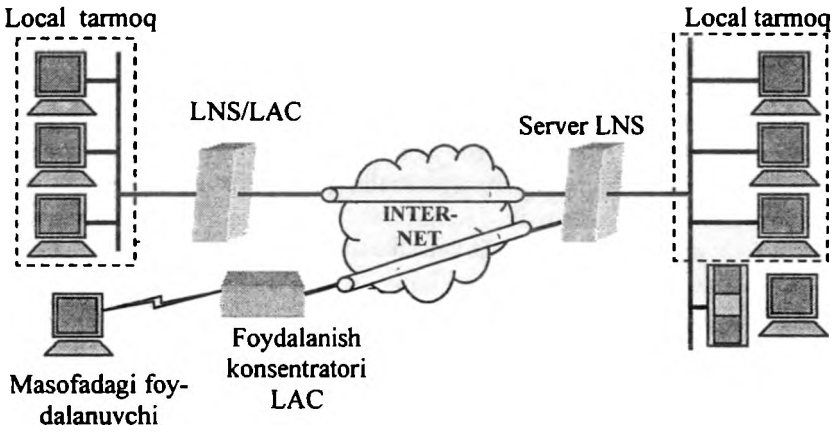
PPTP va L2F protokollaridek L2TP protokolida himoyalangan virtual kanalni shakllantirish uch bosqichda amalga oshiriladi:

– lokal tarmoqning masofadan foydalanish serveri bilan ulanishni o'rnatish;

– foydalanuvchini autentifikatsiyalash;

– himoyalangan tunnelni konfiguratsiyalash.

Birinchi bosqichda lokal tarmoqning masofadan foydalanish serveri bilan ulanishni o'rnatish uchun masofadagi foydalanuvchi provayder ISP bilan PPP – ulashni boshlab beradi. Provayder serveri ISPda ishlovchi foydalanish konsentratori bu ulanishni qabul qiladi va kanal PPPni o'rnatadi. So'ngra foydalanuvchi konsentratori LAC oxirgi uzel va uning foydalanuvchisini qisman autentifikatsiyalaydi. Provayder ISP faqat foydalanuvchining ismidan foydalangan holda unga L2TP tunnellash servisining kerakligini hal qiladi. Agar bunday servis kerak bo'lsa, foydalanish konsentratori LAC tunneli ulanish o'rnatilishi lozim bo'lgan tarmoq serveri LNS adresini aniqlashga o'tadi. Foydalanuvchi va foydalanuvchi tarmog'iga xizmat ko'rsatuvchi server LNS orasidagi muvofiqlikni aniqlashning qulayligini ta'minlash maqsadida provayder ISP tomonidan o'zining mijozlari uchun madadlanuvchi ma'lumotlar bazasidan foydalanish mumkin.



7.16-rasm. L2TP protokoli asosida tunnellash sxemasi.

Birinchi bosqichda lokal tarmoqning masofadan foydalanish serveri bilan ulanishni o'rnatish uchun masofadagi foydalanuvchi provayder ISP bilan PPP – ulashni boshlab beradi. Provayder serveri ISPda ishlovchi foydalanish konsentratori bu ulanishni qabul qiladi va kanal PPPni o'rnatadi. So'ngra foydalanuvchi konsentratori LAC oxirgi uzel va uning foydalanuvchisini qisman autentifikatsiyalaydi. Provayder ISP faqat foydalanuvchining ismidan foydalangan holda unga L2TP tunnellash servisining kerakligini hal qiladi. Agar bunday servis kerak bo'lsa, foydalanish konsentratori LAC tunnelli ulanish o'rnatilishi lozim bo'lgan tarmoq serveri LNS adresini aniqlashga o'tadi. Foydalanuvchi va foydalanuvchi tarmog'iga xizmat ko'rsatuvchi server LNS orasidagi muvofiqlikni aniqlashning qulayligini ta'minlash maqsadida provayder ISP tomonidan o'zining mijozlari uchun madadlanuvchi ma'lumotlar bazasidan foydalanish mumkin.

LNS serverining IP-adresi aniqlanganidan so'ng L2TPning bu server bilan tunneli bor yoki yo'qligi tekshiriladi. Agar bunday tunnel bo'lmasa, u o'rnatiladi. Provayderning foydalanish konsentratori LAC va lokal tarmoqning tarmoq serveri LNS orasida L2TP protokol bo'yicha sessiya o'rnatiladi.

Transportga o'zaro aloqanning «nuqta-nuqta» paket rejimini madadlash talabi qo'yiladi. LAC va LNS orasida tunnel yaratishda bu tunnel doirasida yangi ulanishga chaqirish identifikatori Call ID deb

ataluvchi identifikator beriladi. Konsentrator LAC tarmoq serveriga ushbu Call ID bilan chaqiriq xususidagi bildirish bo'lgan paket jo'natadi. LNS serveri chaqiriqni qabul qilishi yoki rad etishi mumkin.

Ikkinchi bosqichda lokal tarmoqning tarmoq serveri LNS foydalanuvchini autentifikatsiyalash jarayonini bajaradi. Buning uchun autentifikatsiyalashning standart algoritmlaridan biri, xususan, CHAP algoritmi ishlatilishi mumkin. Ta'kidlash lozimki, L2TP protokolining spetsifikatsiyasida autentifikatsiyalash usullarining tavsifi keltirilmagan. Chaqiriq xususidagi bildirish tarkibida tarmoq serveri LNS tomonidan foydalanuvchini autentifikatsiyalash uchun axborot bo'lishi mumkin. Bu axborotni konsentrator LAC foydalanuvchi bilan muloqot jarayonida yig'adi. Autentifikatsiyalashning CHAP protokolidan foydalanilganda bildirish paketida chaqirish-so'zi, foydalanuvchi ismi va uning javobi bo'ladi. PAP protokoli uchun bu axborot foydalanuvchi ismi va shifrlanmagan paroldan iborat bo'ladi. Tarmoq serveri LNS bu axborotdan, masofadagi foydalanuvchini o'z ma'lumotlarini qaytadan kiritishga majbur qilmaslik va autentifikatsiyalashning qo'shimcha siklini bajarmaslik maqsadida, autentifikatsiyalash uchun birdaniga foydalanishi mumkin.

Autentifikatsiya natijasi jo'natilishida tarmoq serveri LNS ham foydalanish konsentratori LACga foydalanuvchi uzelining IP-adresini uzatishi mumkin. Mohiyati bo'yicha foydalanish konsentratori LAC masofadagi foydalanuvchi uzeli va lokal tarmoqning tarmoq serveri orasida vositachi vazifasini bajaradi. Masofadagi uzelga korporativ tarmoqning adreslar pulidan adresning ajratilishi foydalanuvchiga provayder adreslar pulidan oddiy adres olinishidagi noqulayliklardan qutilishiga imkon beradi.

Uchinchi bosqichda provayderning foydalanish konsentratori LAC va lokal tarmoqning serveri LNS orasida himoyalangan tunnel yaratiladi. Natijada, inkapsulatsiyalangan kadrlar PPP tunnel orqali konsentrator LAC va tarmoq serveri LNS orasida ikkala yo'nalishda uzatilishi mumkin. Masofadagi foydalanuvchidan PPP kadri kelganida konsentrator LAC undan kadrni qoplagan baytlarni, nazorat yig'indi baytlarini chiqarib tashlaydi, so'ngra uni L2TP protokol yordamida tarmoq protokoliga inkapsulatsiyalaydi va tunnel orqali tarmoq serveri LNSga jo'natadi. LNS server L2TP protokoldan foydalanib, kelgan paketdan PPP kadrni chiqarib olib ishlaydi.

Tunnelning zaruriy qiymatlarini sozlash boshqarish xabarlari yordamida amalga oshiriladi. L2TP protokoli har qanday paketni kommu-

tatsiyalovchi transport ustidan ishlashi mumkin. Umumiy holda, bu transport, masalan, UDP protokoli, paketlarni kafolatli yetkazishni ta'minlamaydi. Shu sababli, L2TP protokoli bu masalalarni har bir masofadagi foydalanuvchi uchun tunnel ichida ulanishlarni o'rnatish muolajalaridan foydalanib, mustaqil hal etadi.

Ta'kidlash lozimki, L2TP protokoli kriptohimoyaning muayyan usullarini belgilamaydi va shifrlashni turli standartlaridan foydalanish mumkinligini faraz qiladi. Agar himoyalangan tunnelning IP-tarmoqda shakllantirilishi rejalashtirilgan bo'lsa, kriptohimoyani amalga oshirishda IPSec protokolidan foydalaniladi. L2TP protokoli PPP algoritmiga nisbatan ma'lumotlarni himoyalashning yuqori saviyasini ta'minlaydi, chunki unda 3DES (Triple Data Encryption Standard) shifrlash algoritmi ishlatiladi. Agar himoyaning bundan yuqori saviyasi kerak bo'lmasa, bitta 56 xonali kalitli DES algoritmidan foydalanish mumkin. Undan tashqari, L2TP protokoli HMAC (Hash Massage Authentication Code) algoritmi yordamida ma'lumotlarni autentifikatsiyalashni ta'minlaydi. Autentifikatsiyalash uchun bu algoritm uzunligi 128 xonaga teng bo'lgan «xesh»ni yaratadi.

Shunday qilib, PPTP va L2TP protokollarining funksional imkoniyatlari turlicha, PPTP protokoli faqat IP-tarmoqlarda ishlatilishi mumkin va unga tunnelni yaratishi va ishlatishi uchun alohida TCP ulanish zarur. L2TP protokoli nafaqat IP-tarmoqlarda ishlatilishi mumkin, tunnelni yaratish va u orqali ma'lumotlarni tashishda xizmatchi xabarlar bir xil format va protokollardan foydalanadi. L2TP protokoli tashkilot uchun muhim bo'lgan ma'lumotlarning qariyb 100%li xavfsizligini kafolatlashi mumkin.

L2TP protokolining kamchiligi sifatida quyidagilarni ko'rsatish mumkin:

– L2TP protokolini amalga oshirishda ISP provayderlarning madadi zarur;

– L2TP trafikni tanlangan tunnel doirasida chegaralaydi va foydalanuv-chilarning Internetning boshqa qismlaridan foydalanishiga imkon bermaydi;

– L2TP protokolida IP protokolining joriy versiyasi uchun axborot almashinuvning oxirgi nuqtalari orasida kriptohimoyalangan tunnel yaratish ko'zda tutilmagan;

– L2TPning taklif etilgan spetsifikatsiyasi standart shifrlashni faqat IP-tarmoqlarda IPSec protokoli yordamida ta'minlaydi.

Seans sathida himoyalangan virtual kanallarni shakllantirish protokollari

Himoyalangan virtual kanallarini shakllantirish mumkin bo'lgan OSI modelining eng yuqori sathi – beshinchi seans sathidir. Seans sathida himoyalangan virtual tarmoqni qurishda axborot almashinuvini kriptografik himoyalash, jumladan, autentifikatsiyalash hamda o'zaro aloqa tomonlari orasida vositachilikning qator funksiyalarini amalga oshirish imkoniyati paydo bo'ladi. Haqiqatan, OSI modelining seans sathi mantiqiy ulanishlarni o'rnatishga va bu ulanishlarni boshqarishga javobgar. Shu sababli, bu sathda so'ralgan ulanishlarning joizligini tekshiruvchi va tarmoqlararo harakatlar himoyasining boshqa funksiyalarining bajarilishini ta'minlaovchi dastur-vositachilardan foydalanish imkoniyati mavjud.

Seans sathida himoyalangan virtual kanalni shakllantirish protokoli himoyaning tatbiqiy protokollari hamda turli servislarni taqdim etuvchi yuqori sath protokollari (HTTP, FTP, POPS, SMTP va h. protokollar) uchun shaffofdir. Ammo seans sathida yuqori sathli protokollarni amalga oshiruvchi ilovalarga bevosita bog'liqlik boshlanadi. Shuning uchun mazkur sathga mos keluvchi axborot almashish protokolini amalga oshirish ko'p hollarda yuqori sathli ilovalarga o'zgartirishlar kiritilishini talab etadi.

Seans sathida axborot almashishda SSL protokoli keng tarqalgan. Seans sathida o'zaro aloqa tomonlari orasida vositachilik funksiyalarini bajarish uchun IETF tashkiloti tomonidan standart sifatida SOCKS protokoli qabul qilingan.

SSL protokoli Netscape Communication kompaniyasi tomonidan mijoz-server ilovalarida axborotni himoyalangan almashishni amalga oshirish uchun ishlab chiqilgan. Hozirda SSL protokoli OSI modelining seans sathida ishlovchi himoyalangan kanal protokoli sifatida ishlatiladi. Bu protokol axborot almashish xavfsizligini ta'minlashda axborotni himoyalashning kriptografik usullaridan foydalanadi. SSLprotokoli tarmoqning ikkita abonenti orasida himoyalangan kanal qurishning barcha funksiyalarini, jumladan, ularni autentifikatsiyalash, uzatiluvchi

ma'lumotlarning konfidensialligini va yaxlitligini ta'minlash funksiyalarini bajaradi. Asimmetrik va simmetrik kriptotizimlardan kompleks foydalanish texnologiyasi SSL protokolining yadrosi hisoblanadi.

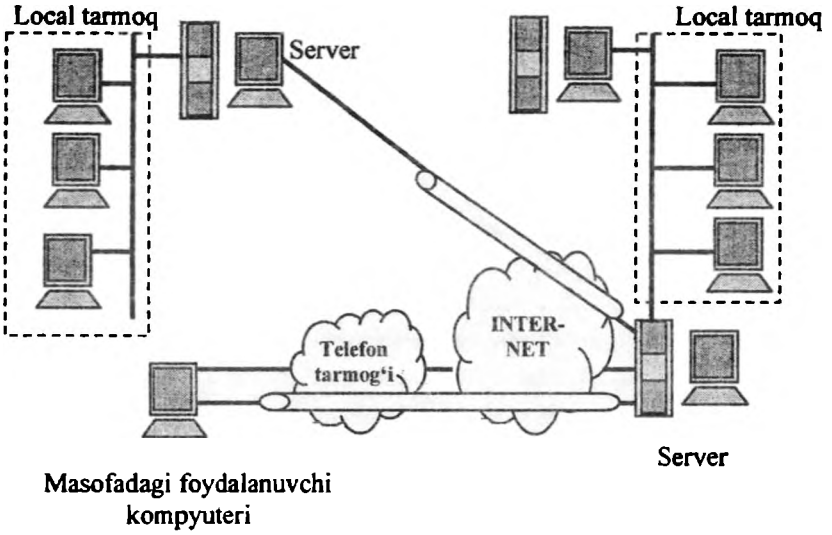
SSLda ikkala tomonning o'zaro autentifikatsiyalash foydalanuvchilarning (mijoz va server) maxsus sertifikatsiya markazlarining raqamli imzosi bilan tasdiqlangan ochiq kalitlarining raqamli sertifikatlari bilan almashish orqali bajariladi. SSL protokoli hamma qabul qilgan X.509 standartlarga mos keluvchi sertifikatlarni hamda sertifikatlarni berishda va haqiqiyligini tekshirishda ishlatiluvchi PKI ochiq kalitlari infratuzilmalarining standartini madadlaydi.

Konfidensiallik ulanish o'rnatilishida tomonlar almashinadigan simmetrik sessiya kalitlarida uzatiluvchi xabarlarni shifrlash orqali ta'minlanadi. Sessiya kalitlari ham shifrlangan ko'rinishda uzatiladi. Bunda ular abonentlarning sertifikatlaridan chiqarib olingan ochiq kalitlarda shifrlanadi. Axborotlarni shifrlashda simmetrik kalitlarning ishlatilishiga asosiy sabab-simmetrik kalitlarda shifrlash va rasshifrovka qilish jarayonining tezligi asimmetrik kalitlar ishlatilishidagiga qaraganda yuqoriligi.

Aylanuvchi axborotning haqiqiyligi va yaxlitligi elektron raqamli imzoni shakllantirish va tekshirish evaziga ta'minlanadi.

Asimmetrik shifrlash algoritmlari sifatida RSA hamda Diffi-Xellman algoritmlari ishlatiladi. Simmetrik shifrlash algoritmlari sifatida esa RC2, RC4, DES hamda Triple DES algoritmlari ishlatiladi. Xesh funksiyalarini hisoblashda MD5 va SHA-1 standartlari ishlatilishi mumkin. SSL protokolining 3.0 versiyasida kriptografik algoritmlari to'plami kengaytiriluvchi hisoblanadi.

SSL protokoliga muvofiq kriptohimoyalangan tunnellar virtual tarmoqning oxirgi nuqtalari orasida yaratiladi. Har bir himoyalangan tunnelni boshlab beruvchilari-tunnel oxirgi nuqtalaridagi kompyuterlarda ishlovchi mijoz va server (7.17-rasm).



7.17-rasm. SSL protokoli asosida shakllangan kriptohimoyalangan tunnellar.

Himoyalangan ulanishni shakllantirishda va madadlashda SSL protokoli mijoz va server o'zaro aloqasining quyidagi bosqichlarini ko'zda tutadi:

– SSL sessiyasini o'rnatish;

– himoyalangan o'zaro aloqa.

SSL sessiyani o'rnatish jarayonida quyidagi masalalar yechiladi:

– tomonlarni autentifikatsiyalash;

– himoyalangan axborot almashinuvida ishlatiluvchi kriptografik algoritmlar va zichlashtirish algoritmlarini muvofiqlashtirish;

– umumiy maxfiy master-kalitni shakllantirish;

– axborot almashishni kriptografik himoyalash uchun shakllantirilgan master-kalit asosida umumiy maxfiy seans kalitlarini generatsiyalash.

Qo'l berishish muolajasi deb ham ataluvchi SSL-sessiyani o'rnatish muolajasi axborot almashishni bevosita himoyalashdan oldin puxta ishlanadi va SSL protokoli tarkibiga kiruvchi boshlang'ich salomlash (HandShake Protocol) protokoli bo'yicha bajariladi.

Mijoz va server orasida qayta ulanish o'rnatilishida tomonlar, o'zaro kelishuv bo'yicha, oldingi umumiy sir asosida yangi seans kalit-

larini shakllantirishlari mumkin (ushbu muolaja SSL-sessiyaning davomi deb ataladi).

SSL 3.0 protokoli autentifikatsiyalashning quyidagi uchta rejimini madadlaydi:

– tomonlarni o'zaro autentifikatsiyalash;

– mijozni autentifikatsiyalamasdan serverni bir tomonlama autentifikatsiyalash;

– to'liq anonimlik.

Oxirgi variantdan foydalanilganda tomonlarning haqiqiyligini kafolatlamasdan axborot almashish xavfsizligi ta'minlanadi. Bu holda o'zaro aloqadagi tomonlar, aloqa qatnashchilarini almashtirib qo'yish bilan bog'liq hujumlardan himoyalanmaydilar.

SSL protokoliga muvofiq o'zaro aloqadagi tomonlarni autentifikatsiyalashda va umumiy maxfiy kalitni shakllantirishda ko'pincha RSA algoritmidan foydalaniladi.

Ochiq kalitlar va ularning egalari orasidagi muvofiqlik maxsus sertifikatsiya markazlari tomonidan beriluvchi raqamli sertifikatlar yordamida o'rnatiladi. Sertifikat tarkibida quyidagi axborot bo'lgan ma'lumotlar blokidir:

– sertifikatsiya markazining nomi;

– sertifikat egasining ismi;

– sertifikat egasining ochiq kaliti;

– sertifikatning ta'sir muddati;

– sertifikatni ishlashda foydalaniladigan identifikator va kriptoalgoritmning parametrlari;

– sertifikat tarkibidagi barcha ma'lumotlarni tasdiqlovchi sertifikatsiya markazining raqamli imzosi.

Sertifikat tarkibidagi sertifikatsiya markazining raqamli imzosi ochiq kalit va uning egasining haqiqiyligini va bir ma'noda mosligini ta'minlaydi. Sertifikatsiya markazi ochiq kalitlarning haqiqiyligini tasdiqlovchi notarius rolini o'taydi. Natijada, bu kalit egalariga himoyalangan o'zaro aloqa xizmatidan, oldindan shaxsiy uchrashuvsiz foydalanishlariga imkon beradi.

1999-yili SSL 3.0 versiyasi o'rniga, SSL protokoliga asoslangan va hozirda Internet standarti hisoblangan TLS protokoli keldi. SSL 3.0 va TLS protokollari orasidagi farq juda ham jiddiy emas.

SSL va TLS protokollarining kamchiligi – o'zlarining xabarlarini tashishda tarmoq sathidagi faqat bitta – IP-protokolidan foydalanishlari va demak, faqat IP-tarmoqlarda ishlay olishlari. Undan tashqari,

SSL/TLSning amalda qo'llanishi tatbiqiy protokollar uchun to'la shaffof emas.

SSLning yana bir salbiy tomoni shundan iboratki, agar mijoz va server ulanishni uzsalar, ular uni ma'lumotlarning minimal hajmini almashish yo'li bilan tiklashlari va Session ID ning eski parametrlaridan foydalanishlari mumkin. Niyati buzuq odam oldingi sessiyalardan birini obro'sizlantirib uni tiklash muolajasini server bilan o'tkazishi mumkin. Natijada, bu sessiyada uzatiladigan keyingi barcha ma'lumotlar obro'sizlantiriladi.

Undan tashqari, SSLda autentifikatsiyalashda va shirflashda bir xil kalitdan foydalaniladi. Bu esa ma'lum bir holatlarda zaiflikka olib kelishi mumkin. Bunday yechim turli kalitlar ishlatilganiga nisbatan ko'p statistik ma'lumotlarni yig'ishga imkon beradi.

SOCKS protokli OSI modelining seans sathida mijoz-server ilovalari-ning o'zaro aloqa muolajasini server-vositachi yoki proxy-server orqali tashkil etadi.

Umumiy holda, tarmoqlararo ekranlarda an'anaviy ishlatiluvchi dastur-vositachilar quyidagi funksiyalarni bajarishi mumkin:

– foydalanuvchini identifikatsiyalash va autentifikatsiyalash;

– uzatiluvchi ma'lumotlarni kriptohimoyalash;

– ichki tarmoq resurslaridan foydalanishni chegaralash;

– axborotlar oqimini filtrlash va o'zgartirish, masalan, viruslarni qidirish va axborotni shaffof shifrlash;

– chiqadigan axborot oqimlari uchun ichki tarmoq adreslarini translatsiyalash.

Avval SOCKS protokoli faqat mijoz ilovalarining serverga so'rovlarini qayta yo'naltirish hamda bu ilovalarga olingan javobni qaytarish uchun ishlab chiqilgan edi. Ushbu muolajalarning o'zi tarmoq IP-adreslari NATni (Network Address Translation) translatsiyalash funksiyalarini amalga oshirish imkoniyatini beradi. Chiquvchi paketlardagi jo'natuvchilarning IP-adreslarini shlyuzining bitta IP-adresi bilan almashtirish ichki tarmoq topologiyasini tashqi foydalanuvchilardan berkitishga imkon beradi va natijada, ruxsatsiz foydalanish masalasi murakkablashadi. Tarmoq adreslarini translatsiyalash xavfsizlikni

oshirish bilan bir qatorda xususiy adreslash tizimini madadlash imkoniyati hisobiga tarmoq ichki adresi makonini kengaytirishga imkon beradi.

SOCKS protokoli asosida tarmoqli o'zaro aloqani himoyalash bo'yicha vositachilikning boshqa funksiyalari ham amalga oshirilishi mumkin. Masalan, SOCKS axborot oqimlari yo'nalishni nazoratlashda va foydalanuvchilar va axborotlar atributlariga bog'liq holda foydalanishni chegaralashda ishlatilishi mumkin. SOCKS protokolining vositachilik funksiyalarini bajarishdagi samarali ishlatilishi uning OSI modelining seans sathiga mo'ljallanganligi bilan ta'minlanadi. Tatbiqiy sathdagi vositachilarga qaraganda, seans sathida eng yuqori tezkorlikka, yuqori sath protokollariga (HTTP, FTP, POPS, SMTP va h.) bog'liq bo'lmaslikka erishiladi. Undan tashqari, SOCKS protokoli IP protokolga bog'lanmagan va operatsion tizimga bog'liq emas. Masalan, mijoz ilovalari va vositachi orasida axborot almashishda IPX protokoli ishlatilishi mumkin.

SOCKS protokoli tufayli tarmoqlararo ekranlar va virtual xususiy tarmoqlar turli tarmoqlar orasida xavfsiz o'zaro aloqani va axborot almashinuvini tashkil etishlari mumkin. SOCKS protokoli ushbu tizimlarni xavfsiz boshqarishni unifikatsiyalangan strategiya asosida amalga oshirishga imkon beradi. Ta'kidlash lozimki, SOCKS protokoli asosida har bir ilova va har bir seans uchun alohida himoyalangan tunnel yaratilishi mumkin.

SOCKS protokoli spetsifikatsiyasiga muvofiq tarmoq shlyuziga (tarmoqlararo ekranga) o'rnatiluvchi SOCKS – *server* va har bir foydalanuvchi kompyuterga o'rnatiluvchi SOCKS – *mijoz* farqlanadi. SOCKS-server har qanday tatbiqiy server bilan bu serverga mos keluvchi tatbiqiy mijoz nomidan o'zaro aloqani ta'minlaydi. SOCKS-mijoz mijoz tomonidan tatbiqiy serverga bo'lgan barcha so'rovlarni ushlab qolib ularni SOCKS-serverga uzatishga atalgan. Ta'kidlash lozimki, mijoz ilovalarining so'rovlarini va SOCKS-server bilan o'zaro aloqani ushlab qolishni bajaruvchi SOCKS-mijozlar universal mijoz dasturlariga o'rnatilishi mumkin. SOCKS-serverga seans (soket) sathidagi trafik ma'lum, shuning uchun u sinchiklab nazoratlashi, xususan, foydalanuvchilarning muayyan ilovalari ishini, agar ularning axborot almashishga zarur vakolatlari bo'lmasa, blokirovka qilishi mumkin. SOCKS protoko-

lining 4- va 5- versiyalari keng tarqalgan. Hozirda SOCKS protokolining 5-versiyasi IETF tashkiloti tomonidan Internetning standarti sifatida ma'qullangan.

SOCKS protokolining 4-versiyasiga binoan, ulanishni o'rnatishning umumiy sxemasi quyidagicha:

– tarmoqdagi qandaydir server bilan bog'lanishni istagan mijoz SOCKS-server (ixtisoslashtirilgan proxy-server) bilan ulanib unga maxsus so'rov yuboradi. Bu so'rovda IP-adres va u ulanishi kerak bo'lgan masofadagi server porti bo'ladi;

– SOCKS-server masofadagi server-adresat bilan ulanadi;

– mijoz va masofadagi server ulanish zanjiri bo'yicha o'zaro aloqa qiladi, SOCKS-server ma'lumotlarni retranslatsiyalaydi.

SOCKS protokolining 5-versiyasi to'rtinchi versiyaning jiddiy rivoji hisoblanadi. U quyidagi qo'shimcha imkoniyatlarni amalga oshiradi:

– nomlaridan SOCKS-mijozlar murojaat etuvchi foydalanuvchilarni autentifikatsiyalash ko'zda tutilgan. SOCKS-server SOCKS-mijoz bilan autentifikatsiyalash usulini kelishib olishlari mumkin. Autentifikatsiyalash kompyuter resurslaridan foydalanishni chegaralashga imkon beradi. Ikki tomonlama autentifikatsiyalash ham joiz hisoblanadi, ya'ni foydalanuvchi, o'z navbatida, kerakli SOCKS-server bilan ulanganiga ishonch hosil qilishi mumkin;

– domenli ismlarni ishlatish joiz hisoblanadi: SOCKS-mijoz SOCKS-serverga nafaqat ulanishni o'rnatishda kerak bo'lgan kompyuterning IP-adresini, balki uning DNS ismini ham uzatishi mumkin;

– nafaqat TCP-protokol, balki UDP protokol ham madadlanadi.

SOCKS protokolining 5-versiyasiga binoan, ulanishni o'rnatishning umumiy sxemasi quyidagicha tavsiflanishi mumkin:

– tarmoqdagi qandaydir tatbiqiy server bilan ulanish o'rnatishni istagan tatbiqiy mijozning so'rovini mana shu kompyuterda o'rnatilgan SOCKS-mijoz ushlab qoladi;

– SOCKS-server bilan ulangan SOCKS-mijoz unga o'zi madadlovchi autentifikatsiyalashning barcha usullarining identifikatorlarini bildiradi;

– SOCKS-server autentifikatsiyalashning qaysi usulidan foydalanishni hal qiladi (agar SOCKS-server SOCKS-mijoz tomonidan taklif etilgan autentifikatsiyalash usullaridan birortasini ham madadlamasa, ulanish uziladi);

– taklif etilgan autentifikatsiyalash usulidan birortasi madadlansa, SOCKS server tanlangan usul bo'yicha foydalanuvchini (uning nomidan SOCKS-mijoz qatnashadi) autentifikatsiyalaydi; muvaffaqiyatsiz autentifikatsiyalashda SOCKS-server ulanishni uzadi;

– muvaffaqiyatli identifikatsiyalashdan keyin SOCKS-mijoz SOCKS-serverga tarmoqdagi so'ralayotgan tatbiqiy server DNS ismini yoki IP-adresini uzatadi, so'ngra SOCKS-server foydalanishni chegaralashning mavjud qoidalari asosida ushbu tatbiqiy server bilan ulanishni o'rnatish bo'yicha qaror qabul qiladi;

– ulanish o'rnatilgan holda tatbiqiy mijoz va tatbiqiy server bir-birlari bilan ulanish zanjiri orqali aloqa qiladilar, SOCKS-server ma'lumotlarni retranslatsiyalaydi hamda tarmoqli o'zaro aloqa xavfsizligi bo'yicha vositachilik funksiyalarini bajarishi mumkin; masalan, autentifikatsiyalash jarayonida SOCKS-mijoz va SOCKS-server seans kalitlarini almashtirishgan bo'lsalar, ular orasidagi barcha trafik shifrlanishi mumkin.

Foydalanuvchilarni SOCKS-server tomonidan autentifikatsiyalash X.509 formatidagi raqamli sertifikatlarga yoki parollarga asoslanishi mumkin. SOCKS-mijoz va SOCKS-server orasidagi trafikni shifrlash uchun OSI modelining seansli yoki pastroq sathlariga mo'ljallangan protokollar ishlatilishi mumkin. SOCKS-server foydalanuvchilarni autentifikatsiyalash, IP-adreslarini translatsiyalash va trafikni kriptohimoyalashdan boshqa yana quyidagi funksiyalarni bajarishi mumkin:

– ichki tarmoq resurslaridan foydalanishni chegaralash;

– tashqi tarmoq resurslaridan foydalanishni chegaralash;

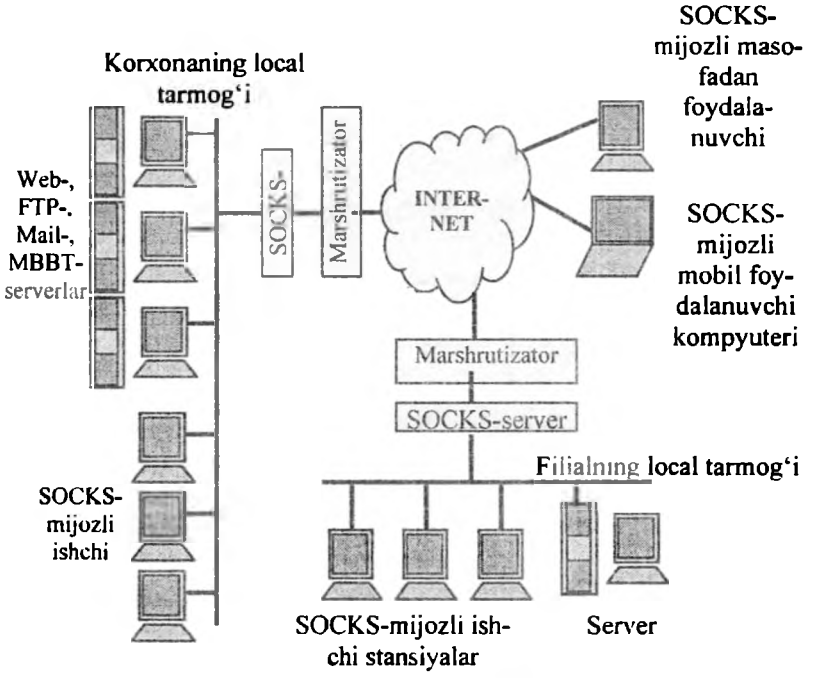
– xabarlar oqimini filtrlash, masalan, viruslarni dinamik qidirish;

– hodisalarni qaydlash va ularga reaksiya ko'rsatish;

– tashqi tarmoqdan so'ralgan ma'lumotlarni keshlash.

Shunday qilib, SOCKS protokoli bo'yicha himoyalangan virtual tarmoqlarni shakllantirish uchun har bir lokal tarmoq bilan Internet ulangan nuqtadagi kompyuter-shlyuzda SOCKS-server, lokal tarmoq-

dagi ishchi stansiyalarda va masofadan foydalanuvchilarning kompyuterlarida esa SOCKS-mijoz o'rnatiladi. Mohiyati bo'yicha, SOCKS-serverga SOCKS protokolini madadlovchi tarmoqlararo ekran sifatida qarash mumkin (7.18-rasm).



7.18 rasm. SOCKS protocoli bo'yicha o'zaro aloqa sxemasi.

Masofadagi foydalanuvchilar Internet ga kommutatsiyalanuvchi yoki ajratilgan liniyalar orqali ulanishlari mumkin. Himoyalangan virtual tarmoq foydalanuvchisi qandaydir tatbiqiy server bilan ulanishga uringanida SOCKS-mijoz SOCKS-server bilan o'zaro aloqani boshlaydi. O'zaro aloqaning birinchi bosqichi tugaganidan so'ng foydalanuvchi autentifikatsiyalanadi, foydalanish qoidasi esa uning ko'rsatilgan adresdagi kompyuterda ishlaydigan muayyan tarmoq ilovalariga ulanish huquqiga ega ekanligini ko'rsatadi. Keyingi o'zaro aloqalar kriptografik himoyalangan kanal bo'yicha yuz berishi mumkin.

SOCKS-serverga, lokal tarmoqlarni ruxsatsiz foydalanishdan himoyalashdan tashqari, bu lokal tarmoq foydalanuvchilarining Internetning ochiq resurslaridan (Telnet, WWW, SMTP, POP va h.) foydalanishlarining nazorati ham yuklanishi mumkin. Foydalanish butunlay avtorizatsiyalangan, chunki foydalanuvchining kompyuteri emas, balki o'zi identifikatsiyalanadi va autentifikatsiyalanadi. Foydalanish qoidalar muayyan xodimning vakolatiga ko'ra Internetning ma'lum resurslari bilan bog'lanishga ruxsat berishi yoki bermasligi mumkin. Foydalanish qoidalarining ta'siri boshqa parametrlar, masalan, autentifikatsiyalash usuli yoki sutka vaqtiga bog'liq bo'lishi mumkin. Tarmoqli o'zaro aloqa xavfsizligining yanada yuqori darajasiga erishish uchun Internet tomonidan foydalanishga ruxsat berilgan lokal tarmoq serverlari, SOCKS-serverga ulanuvchi, himoyalangan ochiq qism tarmoqni hosil qiluvchi alohida segmentga ajratilishi lozim.

7.5. IPSec protokollar stekini himoyalangan virtual xususiy tarmoqlar qurishda ishlatilishi

IPSec protokoli (Internet Protocol Security), asosan IP tarmoqlarda ma'lumotlarni xavfsiz uzatishni ta'minlashga atalgan. IPSecning ishlatilishi quyidagilarni kafolatlaydi:

– uzatilayotgan ma'lumotlarning yaxlitligini, ya'ni ma'lumotlar uzatilishida buzilmaydi, yo'qolmaydi va takrorlanmaydi;

– jo'natuvchining autentligini, ya'ni ma'lumotlar haqiqiy jo'natuvchi tomonidan uzatilgan;

– uzatiladigan ma'lumotlarning konfidensialligini, ya'ni ma'lumotlar shunday shaklda uzatiladiki, ularni ruxsatsiz ko'zdan kechirishning oldi olinadi.

Ta'kidlash lozimki, ma'lumotlar xavfsizligi tushunchasiga, odatda, yana bir talab-ma'lumotlarning foydalanuvchanligi kiritiladi. Ma'lumotlarning foydalanuvchanligi deganda ma'lumotlar yetkazilishining kafolati tushuniladi. IPSec protokollari bu masalani hal etmaydi va uni transport sathi ISPga qoldiradi. IPSec protokollar steki tarmoq sathida axborot himoyasini ta'minlaydi. Bu himoyaning ishlovchi ilovalarga ko'rinmasligiga olib keladi.

IP-paket IP tarmoqlarda kommunikatsiyaning fundamental birligi hisoblanadi. Uning tuzilmasi 7.19-rasmda keltirilgan. IP-paket tarkibida manba adresi S va axborot qabul qiluvchining adresi D, transport sar-

lavhasi, bu paketda tashiluvchi ma'lumotlar xili xususidagi axborot va ma'lumotlarning o'zi bo'ladi.

IP- sarlavha		Transport sarlavhasi TCP yoki UDP	Ma'lumotlar
Adres-S	Adres-D		

7.19-rasm. IP-paket tuzilmasi.

Autentifikatsiyalashni, uzatiluvchi ma'lumotlarning konfidensialligi va yaxlitligini ta'minlash maqsadida, IPSec protokollarining steki qator standartlashtirilgan kriptografik texnologiyalar asosida qurilgan:

– kalitlarni almashtirish ochiq tarmoqdan foydalanuvchilar orasida maxfiy kalitlarni taqsimlashning Diffi-Xellman algoritmi bo'yicha amalga oshiriladi;

– ikkala tomonning haqiqiyligini kafolatlash va main-in-the-midle (o'tadagi odam) xilidagi hujumlarni oldini olish maqsadida Diffi-Xellman algoritmi bo'yicha almashishlarni imzolashda ochiq kalitlar kriptografiyasidan foydalaniladi;

– ochiq kalitlarning haqiqiyligini tasdiqlashda raqamli sertifikatlar ishlatiladi;

– ma'lumotlarni shifrlashda blokli simmetrik algoritmlardan foydalaniladi;

– xeshlash funksiyalari asosida axborotlarni autentifikatsiyalash algoritmlari ishlatiladi.

Himoyalangan kanalni o'rnatish va madadlashdagi asosiy masalalar quyidagilar:

– foydalanuvchilar yoki kompyuterlarni autentifikatsiyalash;

– himoyalangan kanalning oxirgi nuqtalari orasida uzatiluvchi ma'lumotlarni shifrlash va autentifikatsiyalash;

– kanalning oxirgi nuqtalarini ma'lumotlarni autentifikatsiyalashda va shifrlashda kerak bo'ladigan maxfiy kalitlar bilan ta'minlash.

Yuqorida sanab o'tilgan masalalarni hal etishda IPSec tizimi axborot almashish xavfsizligi vositalarining kompleksidan foydalanadi.

IPSec protokolining aksariyat amalga oshirilishida quyidagi komponentlardan foydalaniladi:

– IPSecning asosiy protokoli. Ushbu komponent himoyani inkapsulatsiyalovchi protokol ESP (Encapsulation Security Payload)ni va sar-

lavhani autentifikatsiyalovchi protokoli AH(Authentication Header)ni amalga oshiradi. U sarlavhalarni ishlaydi; paketga qo'llaniladigan xavfsizlik siyosatini aniqlash uchun SPD va SAD ma'lumotlar bazasi bilan o'zaro aloqa qiladi;

– kalit axborotlarini almashishni boshqarish protokoli IKE. IKE, odatda, foydalanish sathida qo'llaniladi (operatsion tizimga o'rnatilgani bundan istisno);

– xavfsizlik siyosatlarining ma'lumotlar bazasi SPD (Security Policy Database). Bu eng muhim komponentlardan biri bo'lib, paketga qo'llaniladigan xavfsizlik siyosatini belgilaydi. SPD dan asosiy protokol IPSec tomonidan kiruvchi va chiquvchi paketlarni ishlashda foydalaniladi;

– xavfsiz assotsiatsiyalarning ma'lumotlar bazasi SPD (Security Assocition Database). Bu ma'lumotlar bazasi kiruvchi va chiquvchi axborotni ishlash uchun xavfsiz assotsiatsiyalar SA(Security Association) ro'yxatini saqlaydi. Chiquvchi SA lardan chiquvchi paketlarni himoyalashda, kiruvchi SAlardan esa IPSec sarlavhali paketlarni ishlashda foydalaniladi. SAD ma'lumotlar bazasi SA bilan qo'lda yoki kalitlarni boshqarish protokollari IKE yordamida to'ldiriladi;

– xavfsizlik siyosatini va xavfsiz assotsiatsiyalarni boshqarish. Bu – xavfsizlik siyosatini va SA ni boshqaruvchi ilovalar.

Asosiy protokol IPSec (ESP va AH ni amalga oshiruvchi) TCP/IP protokollarining transport va tarmoq steklari bilan o'zaro uzviy aloqada bo'ladi. IPSec ni tarmoq sathining qismi deyish mumkin. IPSecning asosiy moduli ikkita interfeysni – kirish yo'li va chiqish yo'li interfeyslarni ta'minlaydi. Kirish yo'li interfeysi kiruvchi paketlar tomonidan, chiqish yo'li interfeysi esa chiquvchi paketlar tomonidan foydalaniladi. IPSecning amalga oshirilishi TCP/IP protokollar stekining transport va tarmoq sathlari orasidagi interfeysga bog'liq bo'lmasligi lozim.

SPD va SAD ma'lumotlar bazasi IPSec ishlashiga jiddiy ta'sir ko'rsatadi. Ulardagi ma'lumotlar tuzilmasini tanlash IPSec ishlashining unumdorligiga ta'sir etadi.

IPSecdagi barcha protokollarni ikkita guruhga ajratish mumkin:

– uzatiluvchi ma'lumotlarni bevosita ishlovchi (ularning xavfsizligini ta'minlash uchun) protokollar;

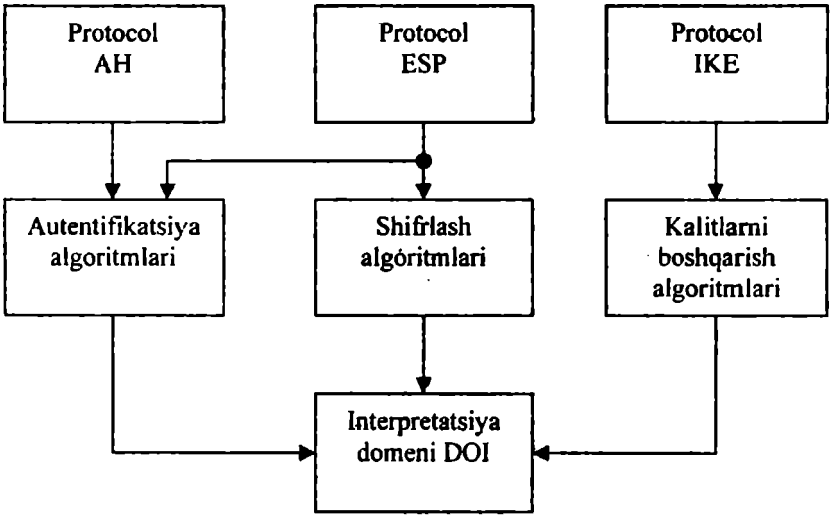
– birinchi guruh protokollariga kerakli himoyalangan ulanishlar parametrlarini avtomatik tarzda muvofiqlashtirishga imkon beruvchi protokollar.

IPSec yadrosini uchta AH, ESP va virtual kanal va kalitlarni boshqarish IKE parametrlarini muvofiqlashtiruvchi protokollar tashkil etadi.

IPSecning xavfsizlik vositalarining arxitekturasi 7.20-rasmda keltirilgan.

Arxitekturaning *yuqori sathida* quyidagi protokollar joylashgan:

– virtual kanal parametrlarini muvofiqlashtiruvchi va kalitlarni boshqarish protokoli IKE. Bu protokol himoyalangan kanalni initsializatsiyalash usulini, jumladan, ishlatiluvchi kriptohimoyalash algoritmlarini muvofiqlashtirishni hamda himoyalangan ulanish doirasida maxfiy kalitlarni almashish va boshqarish muolajalarini belgilaydi;



7.20-rasm. IPSec protokollari stekining arxitekturasi.

– sarlavhani autentifikatsiyalovchi protokol AH. Bu protokol ma'lumotlar manbaini autentifikatsiyalashni, ularning, qabul qilinganidan so'ng, yaxlitligini va haqiqiyligini tekshirish va takroriy axborotlarning tiqishtirilishidan himoyani ta'minlaydi;

– himoyani inkapsulatsiyalovchi protokol ESP. Bu protokol uzatiluvchi ma'lumotlarni kriptografik berkitishni, autentifikatsiyalashni va yaxlitligini ta'minlaydi hamda takroriy axborotlarning tiqishtirilishidan himoyalaydi.

AH va ESP protokollari har biri alohida va birgalikda ishlatilishi mumkin. Bu protokollar vazifalarining qisqacha bayonidan ko'rinib turibdiki, ularning imkoniyatlari qisman bir xil.

AH protokoli faqat ma'lumotlarni yaxlitligini va autentifikatsiyalashni ta'minlashga javob beradi. ESP protokoli quvvatliroq hisoblanadi, chunki u ma'lumotlarni shifrlashi mumkin, undan tashqari, AH protokoli vazifasini ham bajarishi mumkin.

IKE, AH va ESP protokollarining o'zaro aloqalari quyidagicha kechadi. Avval IKE protokoli bo'yicha ikkita nuqta orasida mantiqiy ulanish o'rnatiladi. Bu ulanish IPSec standartlarida «xavfsiz assotsiatsiya»- Security Association, SA nomini olgan. Ushbu mantiqiy kanal o'rnatilishida kanalning oxirgi nuqtalarini autentifikatsiyalash bajariladi hamda ma'lumotlarni himoyalash parametrlari, masalan, shifrlash algoritmi, sessiya maxfiy kaliti va h. tanlanadi. So'ngra xavfsiz assotsiatsiya SA tomonidan o'rnatilgan doirada AHva ESP protokoli ishlay boshlaydi. Bu protokollar yordamida uzatiluvchi ma'lumotlarning istalgan himoyasi, tanlangan parametrlardan foydalanilgan holda bajariladi.

IPSec arxitekturasining *o'rta sathini* IKE protokolida qo'llaniluvchi parametrlarni muvofiqlashtirish va kalitlarni boshqarish algoritmlari hamda AH va ESP protokollarida ishlatiluvchi autentifikatsiyalash va shifrlash algoritmlari tashkil etadi.

Ta'kidlash lozimki, IPSec arxitekturasining yuqori sathidagi virtual kanalni himoyalash protokollari (AH va ESP) muayyan kriptografik algoritmlarga bog'liq emas. Autentifikatsiyalash va shifrlashning ko'p sonli turli-tuman algoritmlaridan foydalanish imkoniyati tufayli IPSec tarmoqni himoyalashni tashkil etishning yuqori darajadagi moslanuvchanligini ta'minlaydi. IPSecning moslanuvchanligi deganda har bir masala uchun uning yechilishining turli usullari tavsiya etilishi tushuniladi. Bir masala uchun tanlangan usul, odatda, boshqa masalalarni amalga oshirish usullariga bog'liq emas. Masalan, shifrlash uchun DES algoritmining tanlanishi ma'lumotlarni autentifikatsiyalashda ishlatiluvchi daydjestni hisoblash funksiyasini tanlashga ta'sir qilmaydi.

IPSec arxitekturasining *pastki sathi* interpretatsiyalash domeni DOI (Domain of Interpretation)dan iborat. Interpretatsiyalash domenining qo'llanish zaruriyatiga quyidagilar sabab bo'ldi. AH va ESP protokollari

modulli tuzilmaga ega, ya'ni foydalanuvchilar o'zaro kelishilgan holda shifrlash va autentifikatsiyalashning turli kriptografik algoritmlaridan foydalanishlari mumkin. Shu sababli, barcha ishlatiluvchi va yangi kiritiluvchi protokol va algoritmlarning birgalikda ishlashini ta'minlovchi modul zarur. Aynan shu vazifalar interpretatsiyalash domeniga yuklatilgan.

Interpretatsiyalash domeni ma'lumotlar bazasi sifatida IPSecda ishlatiladigan protokollar va algoritmlar, ularning parametrlari, protokol identifikatorlari va h. xususidagi axborotlarni saqlaydi. Mohiyati bo'yicha interpretatsiyalash domeni IPSec arxitekturasida fundament rolini bajaradi. AH va ESP protokollarida autentifikatsiyalash va shifrlash algoritmlari sifatida milliy standartlarga mos keluvchi algoritmlardan foydalanish uchun bu algoritmlarni interpretatsiyalash domenida ro'yxatdan o'tkazish lozim.

AH yoki ESP protokollari uzatiluvchi ma'lumotlarni quyidagi ikkita rejimda himoyalashi mumkin:

– tunnel rejimda; IP paketlar butunlay, ularning sarlavhasi bilan birga himoyalanadi;

– transport rejimida; IP paketlarning faqat ichidagilari himoyalanadi.

Tunnel rejimi asosiy rejim hisoblanadi. Bu rejimda dastlabki paket yangi IP paketga joylanadi va ma'lumotlarni tarmoq bo'yicha uzatish yangi IP-paket sarlavhasi asosida amalga oshiriladi. Tunnel rejimida ishlashda har bir oddiy IP-paket kriptohimoyalangan ko'rinishda butunlaycha IPSec konvertiga joylanadi. IPSec konverti, o'z navbatida, boshqa himoyalangan IP-paketga inkapsulatsiyalanadi. Tunnel rejimi odatda maxsus ajratilgan xavfsizlik shlyuzlarida – marshrutizatorlar yoki tarmoqlararo ekranlarda amalga oshiriladi. Bunday shlyuzlar orasida himoyalangan tunnellar shakllantiriladi.

Tunnelning boshqa tomonida qabul qilingan himoyalangan IP-paketlar «ochiladi» va olingan dastlabki IP-paketlar qabul qiluvchi lokal tarmoq kompyuterlariga standart qoidalar bo'yicha uzatiladi. IP-paketlarni tunnellash tunnellarni egasi bo'lmish lokal tarmoqdagi oddiy kompyuterlar uchun shaffof hisoblanadi. Oxirgi tizimlarda tunnel rejimi masofadagi va mobil foydalanuvchilarni madadlash uchun ishlatilishi mumkin. Bu holda foydalanuvchilar kompyuterida IPSecning tunnel rejimini amalga oshiruvchi dasturiy ta'minot o'rnatilishi lozim.

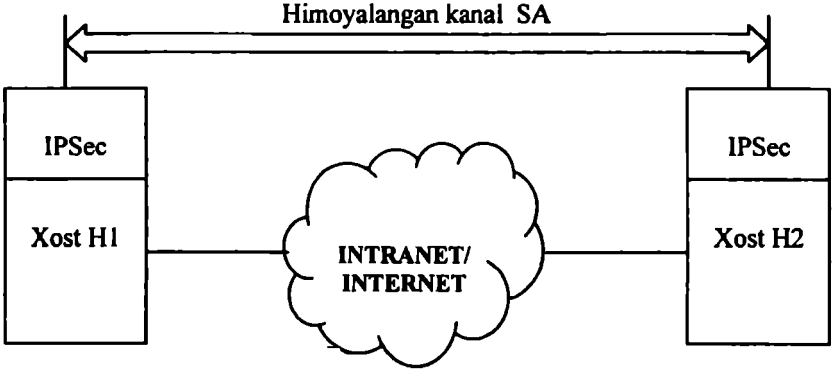
Transport rejimida tarmoq orqali IP-paketni uzatish bu paketning dastlabki sarlavhasi yordamida amalga oshiriladi. IPSec konvertiga krip-

tohimoyalangan ko'rinishda faqat IP-paket ichidagi joylanadi va olingan konvertga dastlabki IP-sarlavha qo'shiladi. Transport rejimi tunnel rejimiga nisbatan tezkor va oxirgi tizimlarda qo'llanish uchun ishlab chiqilgan. Ushbu rejim masofadagi va mobil foydalanuvchilarni hamda lokal tarmoq ichidagi axborot oqimini himoyalashni madadlashda ishlatilishi mumkin. Ta'kidlash lozimki, transport rejimida ishlash himoyalangan o'zaro aloqa guruhiga kiruvchi barcha tizimlarda o'z aksini topadi va aksariyat hollarda tarmoq ilovalarini qayta dasturlash talab etiladi.

Tunnel yoki transport rejimidan foydalanish ma'lumotlarni himoyalashga qo'yiladigan talablarga hamda IPSec ishlovchi uzel roliga bog'liq. Himoyalanuvchi kanalni tugallovchi uzel-xost (oxirgi uzel) yoki shlyuz (oraliqdagi uzel) bo'lishi mumkin. Mos holda, IPSecni qo'llashning quyidagi uchta asosiy sxemasi farqlanadi:

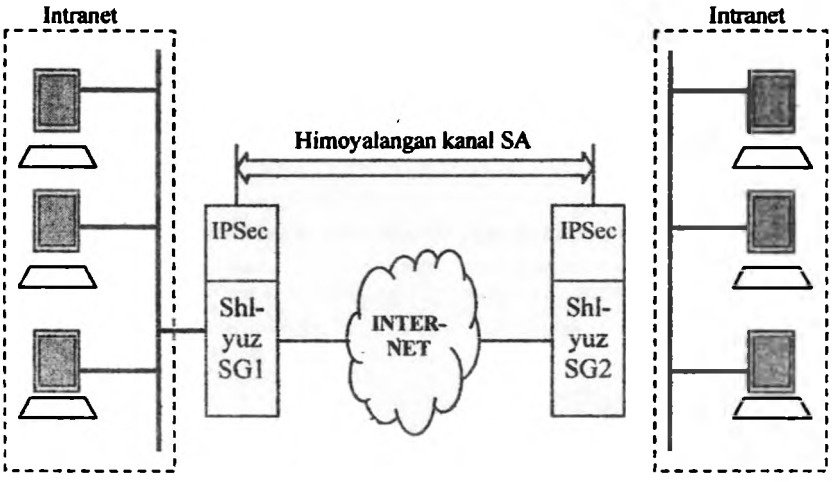
– «xost – xost»;
– «shlyuz – shlyuz»;
– «xost – shlyuz».

Birinchi sxemada himoyalangan kanal tarmoqning oxirgi ikkita uzeli, ya'ni H1 va N2 xostlar orasida o'rnatiladi (7.21-rasm), IPSecni madadlovchi xostlar uchun transport, ham tunnel rejimlaridan foydalanishga ruxsat beriladi.



7.21-rasm. «Xost-xost» sxemasi.

Ikkinchi sxemaga binoan, himoyalangan kanal har birida IPSec protokoli ishlovchi, *xavfsizlik shlyuzlari SG1 va SG2* (Security Gateway) deb ataluvchi oraliqdagi ikkita uzellar orasida o'rnatiladi (7.22-rasm).

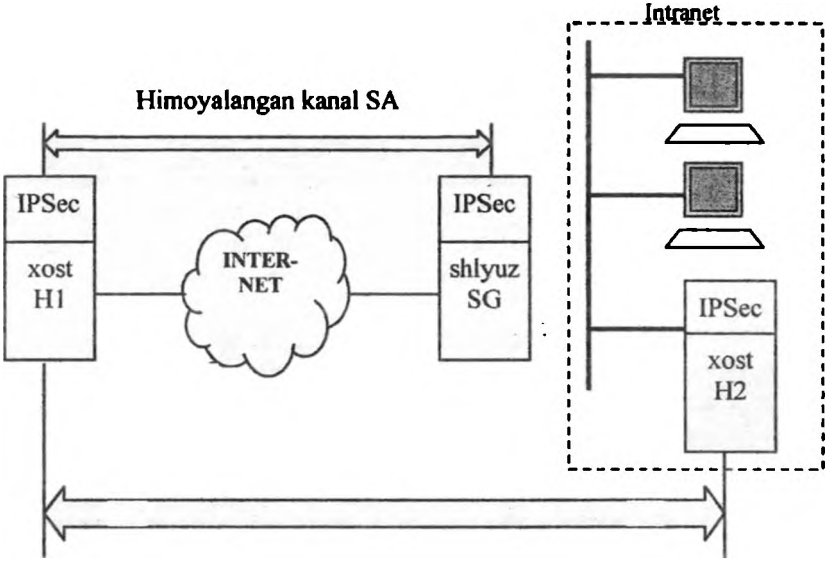


7.22-rasm. «Shlyuz-shlyuz» sxemasi.

Xavfsizlik shlyuzi ikkita tarmoqqa ulanuvchi tarmoq qurilmasi bo'lib, o'zidan keyin joylashgan xostlar uchun shifrlash va autentifikatsiyalash funksiyalarini bajaradi. VPNning xavfsizlik shlyuzi alohida dasturiy mahsulot, alohida apparat qurilma hamda VPN funksiyalari bilan to'ldirilgan marshrutizator yoki tarmoqlararo ekran ko'rinishida amalga oshirilishi mumkin.

Ma'lumotlarni himoyalangan almashish tarmoqlarga ulangan, xavfsizlik shlyuzlaridan keyin joylashgan har qanday ikkita oxirgi uzellar orasida ro'y berishi mumkin. Oxirgi uzellardan IPSec protokolni madadlash talab qilinmaydi, ular o'zlarining trafigini himoyalanmagan holda korxonaning ishonchli tarmog'i Internet orqali uzatadi. Umumfoydalanuvchi tarmoqqa yuboriluvchi trafik xavfsizlik shlyuzi orqali o'tadi va bu shlyuz o'zining nomidan IPSec yordamida trafikni himoyalashni ta'minlaydi. Shlyuzlarga faqat tunnel rejimida ishlashga ruxsat beriladi, vaholanki ular transport rejimini ham madadlashlari mumkin (bu holda samara kam bo'ladi).

«Xost –shlyuz» sxemasi ko'pincha himoyalangan masofadan foydalanishda ishlatiladi (7.23-rasm).



7.23-rasm. «Xost-xost» kanali bilan to'ldirilgan «xost-shlyuz» sxemasi.

Bu yerda himoyalangan kanal IPSec ishlovchi masofadagi N1 xost va korxona Intranet tarmog'iga kiruvchi barcha xostlar uchun trafikni himoyalovchi SG shlyuz orasida tashkil etiladi. Masofadagi xost shlyuzga paketlarni jo'natishda ham transport va ham tunnel rejimlaridan foydalanishi mumkin, shlyuz esa xostga paketlarni faqat tunnel rejimida jo'natadi.

Bu sxemani masofadagi N1 xost va shlyuz tomonidan himoyalanuvchi ichki tarmoqqa tegishli biror N2 xost orasida parallel yana bir himoyalangan kanalni yaratib modifikatsiyalash mumkin. Ikkita SAdan bunday kombinatsiyalab foydalanish ichki tarmoqdagi trafikni ham ishonchli himoyalashga imkon beradi.

Ko'rilgan IPSec asosida himoyalangan kanalni qurish sxemalari turli-tuman virtual himoyalangan tarmoqlarni (VPN) yaratishda keng qo'llaniladi. IPSec asosida turli arxitekturaga ega bo'lgan virtual himoyalangan tarmoqlar, jumladan, masofadan foydalanuvchi VPN (Re-

mote Access VPN), korporatsiya ichidagi VPN(Intranet VPN) va korporatsiyalararo VPN(Extranet VPN) quriladi.

IPSec asosidagi VPN-texnologiyalarining jozibaliligini quyidagi sabablar orqali izohlash mumkin:

– tarmoq sathining himoyasi tarmoqda ishlovchi barcha tatbiqiy tizimlar uchun shaffof, ya'ni barcha ilovalar himoyalangan tarmoqda hech qanday tuzatishsiz va o'zgarishsiz xuddi ochiq tarmoqda ishlaganidek ishlayveradi;

– himoyalash tizimining masshtablanuvchanligi ta'minlanadi, ya'ni murakkabligi va unumdorligi turlicha bo'lgan obyektlarni himoyalash uchun murakkabligi, unumdorligi, narxi darajasi bo'yicha adekvat bo'lgan himoyalashning dasturiy yoki dasturiy-apparat vositalaridan foydalanish mumkin;

– masshtablanuvchi qatordagi axborotni himoyalash mahsulotlari birga ishlay oladilar, shu sababli, ularni turli sathdagi obyektlarda (masofadagi yagona terminallardan to ixtiyoriy masshtabli lokal tarmoqlargacha) resurslaridan va trafigidan barcha begonalar foydalana olmaydigan yagona korporativ tarmoqqa birlashtirish mumkin.

VIII bob. OCHIQ KALITLARNI BOSHQARISH INFRATUZILMASI PKI

8.1. PKIning ishlash prinsipi

Tarixan axborot xavfsizligini boshqaruvchi har qanday markazning vazifalari doirasiga axborot xavfsizligining turli vositalari tomonidan ishlatiluvchi kalitlarni boshqarish kirgan. Bu kalitlarni berish, yangilash, bekor qilish va tarqatish.

Simmetrik kriptografiyadan foydalanilganda kalitlarni tarqatish masa-lasi eng murakkab muammoga aylangan, chunki:

– N foydalanuvchi uchun himoyalangan N(N-1)/2 kalitni tarqatish lozim edi. N bir necha yuzga teng bo'lganida bu sermashaqqat vazifaga aylanishi mumkin;

– bunday tizimning murakkabligi (kalitlarning ko'pligi va tarqatish kanalining maxfiyligi) xavfsizlik tizimini qurish qoidalarining biri- tizim oddiyligiga to'g'ri kelmaydi, natijada zaif joylarning paydo bo'lishiga olib keladi.

Asimmetrik kriptografiya faqat N maxfiy kalitni tavsiya etib, bu muammoni chetlab o'tishga imkon yaratadi. Bunda har bir foydalanuvchida faqat bitta maxfiy kalit va maxsus algoritm bo'yicha maxfiy kalitdan olingan ochiq kalit bo'ladi.

Ochiq kalitdan maxfiy kalitni olib bo'lmasligi sababli ochiq kalitni himoyalanmagan holda barcha o'zaro aloqa qatnashchilariga tarqatish mumkin. O'zining maxfiy kaliti va o'zaro aloqadagi sherigining ochiq kaliti yordamida har qanday foydalanuvchi har qanday kriptoamallarni bajarishi mumkin: bo'linuvchi sirni hisoblash, axborotning konfidensialligi va yaxlitligini himoyalash, elektron raqamli imzoni yaratish.

Shunday qilib, simmetrik kriptografiyaning ikkita asosiy muammosi hal etiladi:

– kalitlar sonining ko'pligi – ular endi atigi Nta;

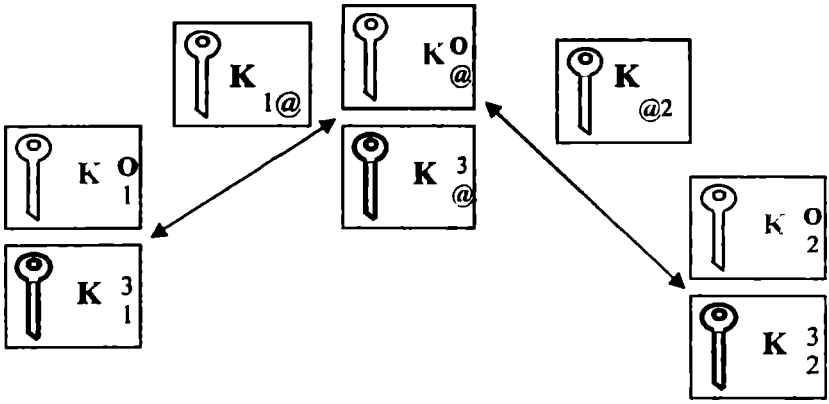
– tarqatishning murakkabligi – ularni ochiq tarqatish mumkin.

Ammo bu texnologiyaning bitta kamchiligi – hujum qiluvchi niyati buzuq odam o'zaro aloqa qatnashchilari o'rtasida joylashganida man-in-the-middle (o'rtadagi odam) hujumiga moyilligi.

Ochiq kalitlarni boshqarish infratuzilmasi PKI ushbu kamchilikni bartaraf qilishga imkon beradi va man-in-the-middle hujumidan samarali himoyalanishni ta'minlaydi. Ochiq kalitlar infratuzilmasi korporativ axborot tizimlarining ishonchli ishlashi uchun atalgan ichki va tashqi foydalanuvchilarga ishonchli munosabatlar zanjiri yordamida xavfsiz axborot almashishga imkon beradi. Ochiq kalitlar infratuzilmasi foydalanuvchining shaxsiy maxfiy kalitini uning ochiq kaliti bilan bog'lovchi elektron pasportga o'xshab ishlovchi raqamli sertifikatlarga asoslanadi.

Man-in-the-middle hujumidan himoyalash. Man-in-the-middle hujumi amalga oshirilganida niyati buzuq odam ochiq kanal orqali uzatiluvchi o'zaro aloqaning qonuniy ishtirokchilari kalitlarini sekingina o'zining ochiq kalitiga almashtirib, qonuniy ishtirokchilarning har biri bilan bo'linuvchi sir yaratishi va so'ngra ularning barcha axborotlarini ushlab qolishi va rasshifrovka qilishi mumkin.

Hujum qiluvchining harakatini va bu hujumdan himoyalanish usulini misol orqali (8.1-rasm) ko'rib chiqaylik. Faraz qilaylik, foydalanuvchilar 1 va 2 o'zlariga umumiy bo'lgan bo'linuvchi sirni Diffi-Xellman sxemasi bo'yicha hisoblab, himoyalangan ulanishni o'rnatishga qaror qildilar. Ammo 1- va 2- foydalanuvchilarning K_1 va K_2 kalitlari ochiq kanal orqali uzatilayotgan onda niyati buzuq, odam @ bu kalitlarni adresatga yetkazmay ushlab qoldi. Niyati buzuq odam o'zining maxfiy va ochiq kalitini yaratib, ochiq K kalitini 1 va 2-foydalanuvchilarga sekingina ularning haqiqiy ochiq K_1 va K_2 kalitlarining o'rniga jo'natadi. Natijada 1 va 2 - foydalanuvchilar bo'linuvchi sirni o'zaro emas, balki 1-@ va 2-@ sxemalari bo'yicha yaratadilar, chunki ular o'zlarining maxfiy kalitlaridan va niyati buzuq odam @ning ochiq kaliti $K_@$ dan foydalanadilar.



8.1-rasm. «Man-in-the-middle» hujumini amalga oshirish.

1-foydalanuvchi 2-foydalanuvchiga shifrlangan axborotni jo'natgan vaqtida niyati buzuq odam @ uni ushlab qolishi va rasshifrovka qilishi mumkin (unda 1-foydalanuvchi bilan bo'linuvchi sir $K_{1@}$ bor). So'ngra niyati buzuq odam @ axborotni (o'zgartirilgani bo'lishi mumkin) o'zi va 2- foydalanuvchi hisoblagan bo'linuvchi sir $K_{@2}$ dan foydalanib yangidan shifrlaydi. Natijada, 2-foydalanuvchi 1-foydalanuvchi bilan himoyalangan kanalga egaman deb o'ylab, niyati buzuq odam jo'natgan axborotni oladi, rasshifrovka qiladi va ishlatadi.

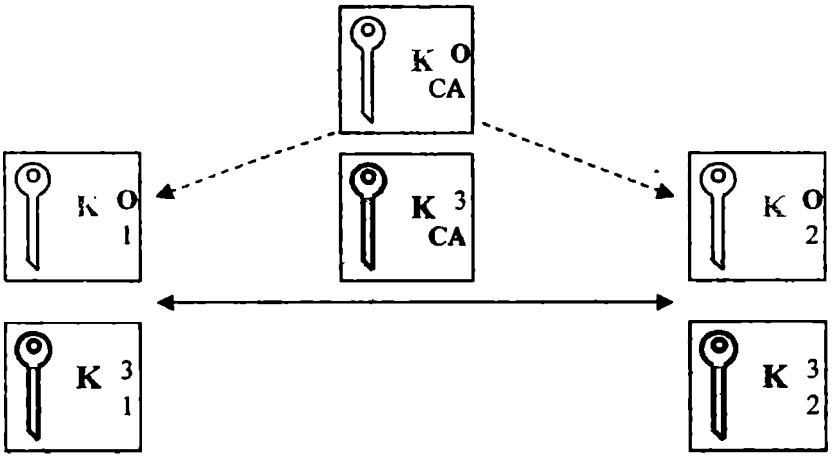
Bu hujumga qarshi samarali vosita – notarius yoki sertifikatsiyalash idorasi CA (Certificate Authority). Ochiq kalitlarning notarial tasdiqlangan sertifikatlarini qo'llash man-in-the-middle hujumini oldini olishga imkon beradi.

1-foydalanuvchi notariusga boradi, notarius 1-foydalanuvchining ochiq kalitini o'zining maxfiy kalitidan foydalanib, elektron raqamli imzosi bilan imzolaydi. Bunda notarius raqamli imzosi bilan nafaqat 1-foydalanuvchining ochiq kalitini, balki foydalanuvchi xususidagi qator aniq axborotni (F.I.SH., ish joyi va h.) hamda imzoning ta'sir muddatini imzolaydi. Hosil bo'lgan hujjat (fayl) 1-foydalanuvchi *ochiq kalitining sertifikati* deb ataladi. Notariusdan o'zining ochiq kaliti uchun sertifikat olishning xuddi shu muolajasini 2-foydalanuvchi ham bajaradi.

1 va 2-foydalanuvchi imzo chekilgan ochiq kalitlarini almashishganidan so'ng, ular notariusning elektron raqamli imzosini va sertifikat haqiqatan 1- yoki 2- foydalanuvchiga berilganligini tekshiradi. No-

tariusning elektron raqamli imzosini tekshirish foydalanuvchilar notariusga tashrif buyurganlarida ehtiyotdan olib quyilgan notariusni ochiq kaliti yordamida sherigidan olgan sertifikatni rasshifrovka qilish orqali bajariladi. Natijada, notarius CA orqali foydalanuvchilar orasida oddiy ishonch zanjiri paydo bo'ladi (8.2-rasm).

Niyati buzuq odam @ notariusga borib 1-foydalanuvchining sertifikatini ololmaydi, chunki unga bu sertifikatni olish vaqtida pasportini ko'rsatishiga va u 1- foydalanuvchi ekanligini isbotlashiga to'g'ri keladi.



8.2-rasm. Notarius CA orqali foydalanuvchilar orasidagi oddiy ishonch zanjiri.

Ochiq kalit sertifikatlari. Ochiq kalit sertifikatlarini shakllantirish X.509 standart tarafidan tavsiya etilgan *qat'iy autentifikatsiyalash* prinsipiga va ochiq kalitli kriptotizim xususiyatlariga asoslanadi.

Ochiq kalit sertikati deganda ma'lumotlar bo'limi va imzo bo'limidan tashkil topgan ma'lumotlar tuzilmasi tushuniladi. Ma'lumotlar bo'limida ochiq kalit xususidagi va kalit egasini identifikatsiyalovchi ma'lumotlar bo'ladi. Imzo bo'limida ochiq kalitli ma'lumotlar bo'limi uchun generatsiyalangan ochiq kalit egasini autentifikatsiyalovchi elektron raqamli imzo bo'ladi. Sertifikatsiya markazi CA sertifikatlardagi ochiq kalitlarni autentifikatsiyalashni ta'minlovchi ishonchli uchinchi tomon hisoblanadi.

Sertifikatsiyalash markazi o'zining juft (ochiq-maxfiy) kalitiga ega bo'lib, maxfiy kalit sertifikatlarni imzolash uchun ishlatilsa, ochiq kalit chop etiladi va undan foydalanuvchilar sertifikatdagi ochiq kalitning haqiqiyligini tekshirishda foydalanadilar. Ta'kidlash lozimki, sertifkatsiya markazining ochiq kalitini xavfsiz uzatish nafaqat sertifkatsiya markaziga shaxsan murojaat asosida, balki bu ochiq kalitni kerakli vakolatga ega bo'lgan boshqa sertifkatsiya markazi tomonidan sertifikatsiyalash asosida ham amalga oshirish mumkin. Sertifikatsiya markazi foydalanuvchining ochiq kaliti sertifikatini ma'lumotlarning ma'lum to'plamini raqamli imzo bilan tasdiqlash orqali shakllantiradi.

Odatda, ma'lumotlarning bu to'plamiga quyidagilar kiradi:

– ochiq kalitning ta'sir davri: davrning boshlanishi va nihoyasi sanalarini o'z ichiga oladi;

– kalitning nomeri va seriyasi;

– foydalanuvchining noyob ismi;

– foydalanuvchining ochiq kaliti xususidagi axborot: ushbu kalit atalgan algoritmning identifikatori va ochiq kalitning o'zi;

– elektron raqamli imzoni tekshirish muolajasida ishlatiluvchi algoritm (masalan, elektron raqamli imzoni generatsiyalovchi algoritm identifikatori);

– sertifikatsiya markazining noyob ismi.

Ochiq kalit sertifikati quyidagi xususiyatlarga ega:

– sertifikatsiya markazining ochiq kalitidan foydalanuvchining har biri sertifikatga kiritilgan ochiq kalitni chiqarib olishi mumkin;

– sertifikatsiya markazidan tashqari hech bir tomon sertifikatni bilintirmasdan o'zgartiraolmaydi (sertifikatlarni soxtalashtirish mumkin emas).

Sertifikatlarni soxtalashtirish mumkin emasligi, ularni umumfoydalanuvchi ma'lumotnomalarda, himoyalamasdan chop etishga imkon tug'diradi.

Ochiq kalit sertifikatini yaratish juft kalitni (ochiq-maxfiy) yaratishdan boshlanadi. Kalitni generatsiyalash muolajasi quyidagi ikkita usul orqali amalga oshirilishi mumkin:

– sertifikatsiya markazi kalitlar juftini yaratadi. Ochiq kalit sertifikatga kiritiladi, uning jufti-maxfiy kalit esa foydalanuvchiga uzatiladi (foydalanuvchini autentifikatsiyalashni va kalit uzatilishining konfidensialligini ta'minlagan holda).

– foydalanuvchi kalitlar juftini o'zi yaratadi. Maxfiy kalit foydalanuv-chida saqlanadi, ochiq kalit esa himoyalangan kanal orqali sertifikatsiya markaziga yuboriladi.

Har bir foydalanuvchi sertifikatsiya markazi tomonidan shakllantirilgan bitta yoki bir nechta kalitlarning egasi bo'lishi mumkin. Foydalanuvchi bir necha turli sertifikatsiya markazlaridan olingan sertifikatlarga ham ega bo'lishi mumkin.

Amalda boshqa sertifikatsiya markazidan sertifikat oladigan foydalanuvchilarni autentifikatsiyalash ehtiyoji tug'iladi.

Sertifikatlarni boshqarish tizimlarining bazaviy tuzilmalari. Sertifikatlarni boshqarish tizimi-o'zaro axborot almashishda xavfsizlikni ta'minlash maqsadida ochiq kalitli kriptografik texnologiyalardan foydalanishga zarur bo'lgan dasturiy-apparat vositalari hamda tashkiliy-texnik tadbirlar kompleksi.

Ochiq kalitlarni boshqarish infratuzilmasi PKI man-in-the-middle hujumlaridan ishonchli himoyalashni amalga oshirishga imkon beruvchi notariuslar tarmog'idan iborat. Notarius orqali foydalanuvchilar orasidagi oddiy ishonch zanjiri (8.2-rasm) bitta notariusga, unga tashrif buyurgan foydalanuvchilarning ochiq kalitlarini, imzolangan sertifikatlarni yaratish yo'li bilan himoyalashga imkon beradi.

Bu tizimning samarali ishlashi quyidagilarga bog'liq:

– o'zaro aloqa ishtirokchilari sertifikatsiya markazi ochiq sertifikatining haqiqiy nusxasiga ega bo'lishlari shart;

– o'zaro aloqa ishtirokchilari ishlatadigan axborotni himoyalash vositalari o'zaro aloqadagi sherigining har qanday sertifikatini sertifikatsiya markazining ochiq sertifikatidan foydalanib, avtomatik tarzda tekshira olishi lozim.

Ba'zida o'zaro aloqadagi sheriklar sertifikatsiya markazidan juda uzoqda bo'lishligi mumkin. Bu holda SA–notariuslarining taqsimlangan qatlamlari yaratiladi.

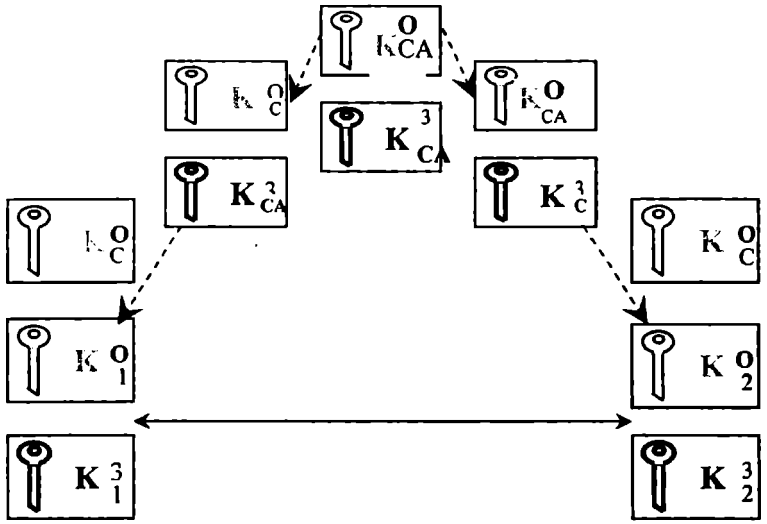
Sertifikatsiyalashning uchta bazaviy modeli farqlanadi:

– sertifikatlarning ierarxik (shajara) zanjiriga asoslangan sertifikatsiyalashning ierarxik modeli;

– kross-sertifikatsiyalash modeli (o'zaro sertifikatsiyalashni ko'zda tutadi);

– sertifikatsiyalashning tarmoq (gibrid) modeli (ierarxik va o'zaro sertifikatsiyalash elementlarini o'z ichiga oladi);

Ierarxik modelda SA lar boshqa SA larga sertifikatlar beruvchi ildiz sertifikatsiya markaziga ierarxik tobelikda joylashgan (8.3-rasm).



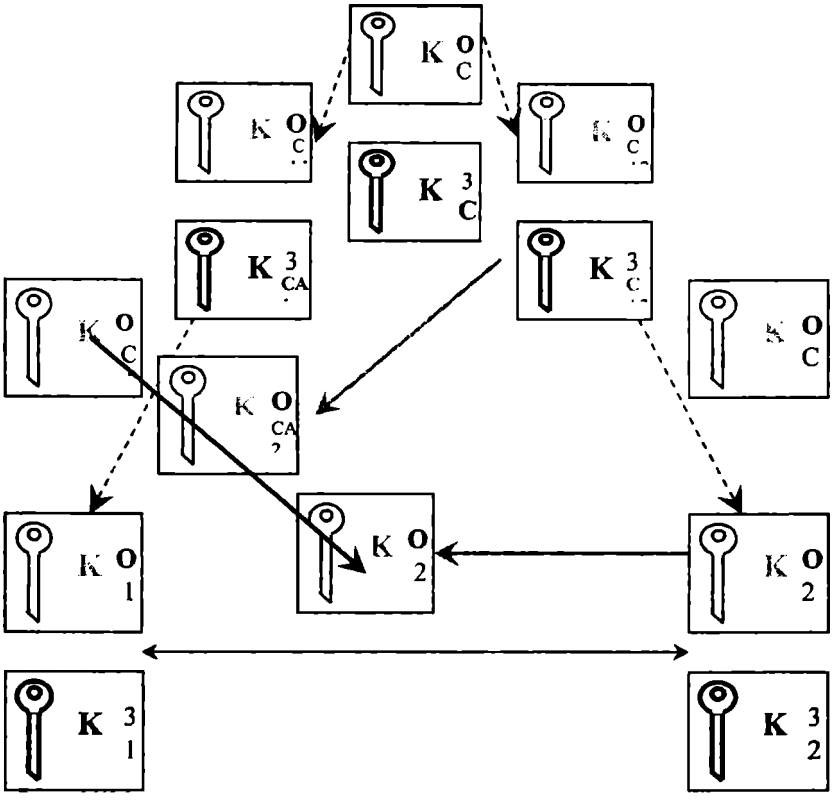
8.3-rasm. CAning ikki sathli ierarxiyasi.

Ildiz sertifikatsiya markazining vazifasi tobe SA1 va SA2larni qaydlashdan iborat. Har bir SA xavfsizlikning yagona darajasini ta'minlash maqsadida sertifikatsiyalashning berilgan siyosatiga muvofiq ishlaydi. 8.3-rasmda keltirilgan misolda SA notariuslarning yana bir ierarxik sathi yaratiladi. Notariuslar:

– foydalanuvchilarga o'xshab sertifikatlarini markaziy SAda imzolashadi;

– markaziy CAga o'xshab oddiy foydalanuvchilarning sertifikatlarini maxfiy kalitlari bilan imzolaydilar.

Masofadagi sherikning haqiqiyligini tekshirish mantiqi quyidagicha quriladi (8.4-rasm):



8.4-rasm. Masofadagi abonent sertifikatini tekshirish sxemasi.

– foydalanuvchi sherigining sertifikatini olib, uni notanish CA imzolaganini aniqlaydi;

– u sherigidan ushbu SAning sertifikatini so'raydi;

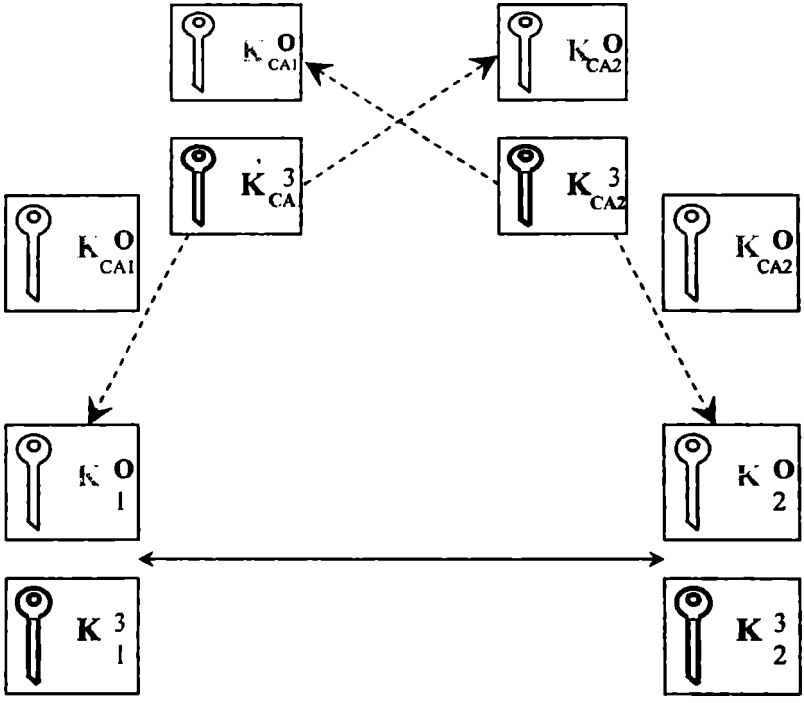
– SAning sertifikatini olib, uni markaziy SA sertifikati bilan tekshiradi;

– muvaffaqiyatli tekshirishdan so'ng foydalanuvchi bu SAga ishona boshlaydi va uning sertifikati bilan masofadagi foydalanuvchi sertifikatini tekshiradi.

Xuddi shunday tekshirishni ikkinchi sherik ham bajaradi. Muhimi, ishlatiladigan axborotni himoyalash tizimlari bunday murakkab ierarxik

tekshirishlarni avtomatik tarzda bajaraolsinlar. Tavsiflangan ierarxik sxemani, zaruriyat tug'ilganda ierarxiyaning yangi sathlarini kiritib, davom ettirish mumkin.

Kross-sertifikatsiyalash modelida ierarxiyaning bir shohida bo'lmagan mustaqil SAlar sertifikatsiya markazlari tarmog'ida o'zaro sertifikatsiyalanadilar. Tekshirish sxemasi o'zgarmaydi, chunki foydalanuvchiga begona notarius uning notariusiga tobedek tuyuladi (8.5-rasm).



8.5-rasm. Kross-sertifikatsiyalash sxemasi.

Ta'kidlash lozimki, kross-sertifikatsiyalash modeli sertifikatlarni boshqarish tizimining tarmoqli arxitekturasining xususiy holi hisoblanadi.

Sertifikatlarni boshqarish tizimining ierarxik va tarmoq arxitekturalarining umumlashtirilgan sxemalari 8.6-rasmda keltirilgan.

Sertifikatlarni boshqarish tizimining *ierarxik tuzilmasi* quyidagi afzalliklarga ega:

– u mavjud federal va idora tashkiliy-boshqaruv tuzilmalarga o'xshash va ularning prinsiplari bo'yicha qurilishi mumkin;

– u ismlarning ierarxik daraxtiga osongina bog'lanishi mumkin;

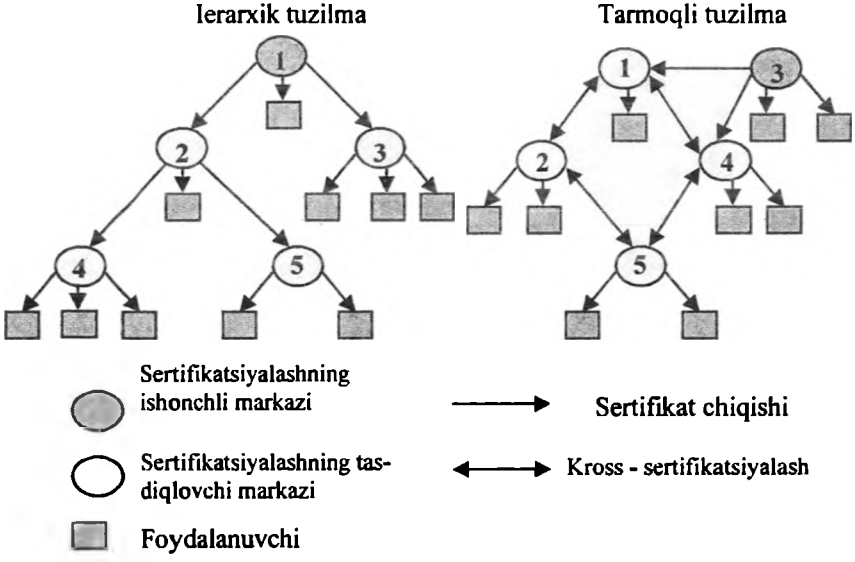
– u o'zaro aloqadagi barcha tomonlar uchun sertifikatlar zanjirini qidi-rish, qurish va verifikatsiyalashning oddiy algoritmini aniqlaydi;

– ikkita foydalanuvchining o'zaro aloqani ta'minlashi uchun ulardan birining ikkinchisiga o'zining sertifikatlar zanjirini taqdim etishi kifoya, bu o'zaro aloqa bilan bog'liq muammolarni kamaytiradi.

Ierarxik arxitekturaga quyidagi kamchiliklar xarakterli:

– barcha oxirgi foydalanuvchilarning o'zaro aloqasini ta'minlash uchun faqat bitta ildizli ishonchli CA bo'lishi shart;

– tijorat tuzilmalarining o'zaro aloqasi ierarxikdan ko'ra ko'proq to'g'ri xarakterga ega.



8.6-rasm. Sertifikatlarni boshqarish tizimining ierarxik va tarmoqli arxitekturalari.

Sertifikatlarni boshqarish tizimining *tarmoq arxitekturasi* quyidagi afzalliklarga ega:

– u anchagina moslashuvchan va zamonaviy biznesda mavjud bo'lgan bevosita ishonchli o'zaro munosabatlarning o'rnatilishiga imkon beradi;

– oxirgi foydalanuvchi hech bo'lmaganda uning sertifikatini bosib chiqargan markazga ishonishi shart va tizimdagi ishonch munosabatlari mana shunga asoslangan;

– foydalanuvchilari o'zaro tez-tez aloqa qiluvchi turli tasdiqlovchi SAlarni bevosita kross-sertifikatsiyalash mumkin, bu zanjirlarni verifikatsiyalash jarayonini qisqartiradi;

– tasdiqlovchi SA kaliti obro'sizlantirilganidan so'ng tiklash jarayoni ierarxik tuzilmaga qaraganda tarmoq tuzilmasida oddiyroq.

Ammo sertifikatlarni boshqarishning tarmoq arxitekturasi quyidagi kamchiliklarga ega:

– barcha o'zaro aloqa tomonlar uchun sertifikatlar zanjirini qidirish va qurish algoritmi juda murakkab bo'lishi mumkin;

– foydalanuvchi uning sertifikatini boshqa barcha foydalanuvchilar tomonidan tekshirilishini ta'minlovchi zanjirni taqdim etaolmaydi.

Ehtimol, yaqin orada sertifikatsiyalash ierarxiyasining eng yuqori sathida turli tashkilotlarning ishonch zanjirlari aloqasini ta'minlovchi davlat notariusi bo'ladi.

8.2. Ochiq kalitlarni boshqarish infratuzilmasining mantiqiy tuzilmasi va komponentlari

Ochiq kalitlarni boshqarish infratuzilmasi PKIning asosiy vazifalari quyidagilar:

– raqamli kalitlar va sertifikatlarning hayot siklini madadlash (ya'ni kalitlarni generatsiyalash, sertifikatlarni yaratish va imzolash, ularni taqsimlash va h.);

– obro'sizlantirish faktlarini qaydlash va chaqirib olingan sertifikatlar-ning «qora» ro'yxatini chop etish;

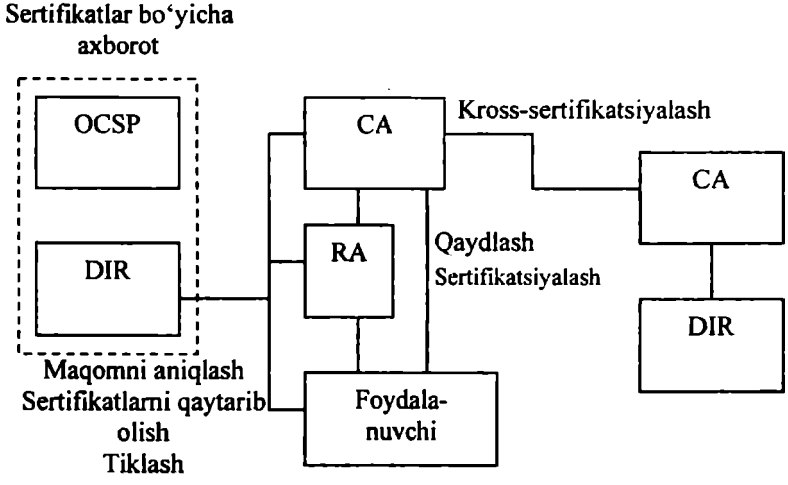
– foydalanuvchining tizimdan foydalanish vaqtini imkoni boricha kamaytiruvchi identifikatsiyalash va autentifikatsiyalash jarayonlarini madadlash:

– mavjud ilovalar va xavfsizlik qism tizimining barcha komponentlarini integratsiyalash mexanizmini (PKIga asoslangan) amalga oshirish;

– barcha foydalanuvchilar va ilovalar uchun bir xil va tarkibida barcha zaruriy kalit komponentlari va sertifikatlar bo'lgan xavfsizlikning yagona tokenidan foydalanish imkoniyatini taqdim etish.

Xavfsizlik tokeni – foydalanuvchining tizimdagi barcha huquqlari va qurshovini aniqlovchi xavfsizlikning shaxsiy vositasi, masalan, smart-karta.

8.7-rasmda ochiq kalitlarni boshqarish infratuzilmasining mantiqiy tuzilmasi va asosiy komponentlari keltirilgan.



8.7-rasm. PKIning mantiqiy tuzilmasi va asosiy komponentlari.

Rasmda quyidagi belgilashlar qabul qilingan:

– SA – sertifikatsiyalash markazi;

– RA – qaydlash markazi;

– OCSP – joriy sertifikat maqomining protokoli (Online Certificate Status Protocol);

– DIR – X.511, X.519, DAP, LDAP foydalanish protokollari bo'yicha direktoriya xizmati.

Qaydlash markazi RA – PKI elementi, qaydlashni amalga oshiruvchi vakil, ya'ni foydalanuvchiga sertifikatni himoyalangan holda berish imkoniyatini ta'minlash maqsadida foydalanuvchilarni autentifikatsiyalashni va ularni qaydlashni amalga oshiradi. Qaydlash markazining xususiyati shundan iboratki, u funksional nuqtai nazaridan sertifikatsiya markaziga qaraganda foydalanuvchiga yaqinroq. Undan tashqari, aynan

qaydlash markazi PKIning o'zaro aloqaga layoqatligini ta'minlovchi samarali interfeys hisoblanadi.

Sertifikatsiya markazi CA – PKIning elementi (sertifikatlarning ishonchli manbai, notarius), unga sertifikatlarni yaratish va/yoki tasdiqlash ishonib topshirilgan. Sertifikatsiya markazining ishlash sxemasi quyidagicha:

– SA shaxsiy kalitlarini generatsiyalaydi va foydalanuvchilar sertifikatlarini tekshirishga atalgan SA sertifikatlarini shakllantiradilar;

– foydalanuvchilar sertifikatsiyalashga so'rovlarni shakllantiradilar va ularni u yoki bu usul bo'yicha SAga yetkazadi;

– SA foydalanuvchilar so'rovlari asosida ularning sertifikatlarini shakllantiradi;

– SA bekor qilingan sertifikat ro'yxatlarini (CRL) shakllantiradi va vaqti-vaqti bilan yangilaydi;

– foydalanuvchi sertifikatlari, SA sertifikatlari va bekor qilinganlar ro'yxati CRL sertifikatlar markazi tomonidan chop etiladi (foydalanuvchilarga tarqatiladi yoki umumfoydalanuvchi ma'lumotnomaga joylashtiriladi).

PKI bajaradigan funksiyalarni shartli ravishda bir necha guruhlarga ajratish mumkin:

– sertifikatlarni boshqarish funksiyalari;

– kalitlarni boshqarish funksiyalari;

– qo'shimcha funksiyalar (xizmatlar).

Sertifikatlarni boshqarish funksiyalariga quyidagilar kiradi:

– *qaydlash.* Nafaqat funksiyalarning bir qismi, balki PKIning xavfsizligi ham to'g'ri qaydlashga va identifikatsiyalashga asoslangan. Foydalanuvchilar sifatida fizik foydalanuvchilar, tatbiqiy dastur, tarmoq qurilmasi va h. ishtirok etishi mumkin. Identifikatsiyalashda ishlatiladigan usullarni sertifikatsiyalash siyosati belgilaydi. Shunday qilib, foydalanuvchilarni identifikatsiyalash va qaydlash PKI tizimining minimal to'liq komponentlari hisoblanadi;

– *ochiq kalitlarni sertifikatsiyalash.* Sertifikatsiyalash jarayoniga sertifkatsiyalash markazi SA javob beradi. Mohiyatan, sertifikatsiyalash jara-yoni foydalanuvchi ismini ochiq kalit bilan bog'lashdan iborat.

SA quyidagi harakatlarni bajargan holda foydalanuvchi va pastroq sathdagi SA sertifikatlarini imzolaydi:

– foydalanuvchilarning haqiqiyligini tekshirish;

– sertifikatga identifikator berish;

– ma'lumotlarni sertifikatga kiritish;

– harakat vaqtini (boshlanishi-nihoyasi) o'rnatish;

– sertifikatni imzolash;

– sertifikatni sertifikatlarning ochiq serverida chop etish.

SAning maxfiy kalitini saqlash. Bu tizimning eng nozik nuqtasi. SA maxfiy kalitini *obro'sizlantirilishi* uning ixtiyoridagi butun tizimni buzadi. SAning maxfiy kaliti joylashgan kompyuter ishonchli qo'riqlanishi lozim;

– *sertifikatlar bazasini saqlash va sertifikatlarni taqsimlash.* Tizim ishlashining qulayligini ta'minlash maqsadida foydalanuvchilarning va oraliq SAlarning (eng yuqori sath SAsidan bo'lak) barcha sertifikatlari sertifikatlar serveri deb ataluvchi umumfoydalanuvchi serverga olib qo'yiladi. Bu holda foydalanuvchilar abonentning sertifikatini, hatto u tarmoqda vaqtincha bo'lmagan holda ham olishlari mumkin;

– *sertifikatni yangilash.* Ushbu jarayon sertifikat ta'siri muddati o'tgan holda faollashadi va foydalanuvchi ochiq kaliti uchun yangi sertifikatni berishdan iborat bo'ladi. Agar kalitlar jufti obro'sizlantirilgan bo'lsa yoki yangi sertifikat siyosat, kengayish yoki xususiyat atamalarida oldingisidan farqlansa, bu usul ishlatilmaydi. Yaroqlilik muddati davrida sertifikatning ismi va mansubligi (foydalanuvchining boshqa bo'limga o'tishi) kabi jiddiy bo'lmagan xususiyatlarining o'zgarishi ham sertifikatni oldingi ochiq kalit bilan yangilashni (regeneratsiyalashni) talab etishga olib kelishi mumkin;

– *kalitlarni yangilash.* Foydalanuvchilar yoki uchinchi tomon kalitlarning yangi juftini generatsiyalaganlarida yangi ochiq kalitga mos keluvchi sertifikatni yaratish zarur. Bu usuldan sertifikatni yangilash mumkin bo'lmagan hollarida ham foydalaniladi;

– *sertifikatni qaytarib olish maqomini aniqlash.* Ushbu jarayon foydalanuvchiga sertifikatining qaytarib olingan emasligini tekshirishga imkon beradi. Bu jarayon sertifikatning ochiq kalitlar katalogi PKDda (Public Key Directory) va sertifikatlarni qaytarib olish ro'yxati CRLda (Certificate Revocation List) borligini tekshirish orqali yoki bu masalani yechishga vakolati bo'lgan uchinchi tomonga so'rov yordamida tashkil etilishi mumkin;

– *sertifikatni qaytarib olish.* Bu jarayon turli holatlar natijasida xavfsizlikning muayyan siyosatiga bog'liq holda (masalan, kalitlarning obro'sizlantirilishi, ismlarning o'zgarishi, foydalanishning to'xtashi va h.) bo'lishi mumkin;

– *kalitlarni boshqarish funksiyasi* – kalitlarni generatsiyalash va taqsimlash asosiy qism guruhlariga bo'linadi.

Kalitlarni taqsimlash funksiyalari, o'z navbatida, ochiq kalitlarni taqsimlash va tokenlarni personallashtirishga bo'linadi. Tokenlarni personallashtirishda fizik qurilmalar – tokenlardan foydalanib maxfiy kalitlarni va qo'shimcha ma'lumotlarni saqlash tashkil etiladi; tokenlarning personalizatsiyasi CA, RA va foydalanuvchi tomonidan madadlanishi lozim. Masalan, smart-kartaning personalizatsiyasi o'rnatish (fayl tizimini yaratish) muolajasini, tasodifiy PIN-kodni yoki parolni tanlash, bu smart-kartaga tegishli barcha ma'lumotlarni yetkazish va saqlashni o'z ichiga olishi mumkin.

Qo'shimcha funksiyalar (xizmatlar) guruhi tarkibiga quyidagilar kiradi:

– o'zaro sertifikatsiyalash (turli CAlarda kross-sertifikatsiyalash);

– ochiq kalitni uning unga qo'yiladigan arifmetik talablarga mos kelishini, ya'ni ochiq kalit haqiqiy ekanligini tekshirish;

– sertifikatni tekshirish; agar foydalanuvchi boshqa foydalanuvchining raqamli imzosiga ishonishni xohlasa va mos sertifikatni tekshiraolmasa, tekshirishni ishonchli uchinchi tomondan iltimos qilishi mumkin;

– arxivlash xizmatlari va h.

Ochiq kalitlar infratuzilmasi PKI quyidagi qator ilovalar va standartlarni madadlaydi:

– ochiq kalit sertifikatlarini madadlovchi vositalar o'rnatilgan Linux, FreeBSD, HP-UX, Microsoft Windows, Novell Netware, Sun Solaris ope-ratsion tizimlari;

– ochiq kalit sertifikatlari asosida foydalanuvchilarni autentifikatsiyalash mexanizmini madadlovchi ma'lumotlar bazasini boshqarish tizimlari, xususan, Oracle, DB2, Informix, Sybase;

– IP protokoli asosida amalga oshiriluvchi virtual himoyalangan tarmoqlarni (VPN) tashkil etish vositalari, xususan, Cisco Systems, Nortel Network kompaniyalarining telekommunikatsiya asbob-uskunalari hamda ixtisoslashtirilgan dasturiy ta'minot;

– elektron hujjat aylanishi tizimlari, masalan, Lotus Notes, Microsoft Exchange hamda himoyalangan pochta almashish standarti S/MIMEni madadlovchi pochta tizimlari;

– Microsoft Active Directory, Novell NDS, Netscape iPlanet kataloglarining xizmati;

– SSL standarti asosida amalga oshiriluvchi Web-resurslardan foydalanish tizimlari.

– foydalanuvchilarni autentifikatsiyalash tizimlari, xususan, RSA kompaniyasining SecurID va h.

O'z navbatida, ochiq kalitlar infratuzilmasi sanab o'tilgan funksional sohalarni integratsiyalashi mumkin. Natijada, ochiq kalitlar infratuzilmalarini kompaniya axborot tizimiga integratsiyalash va umumiy standartlar va ochiq kalit sertifikatlaridan foydalanish yo'li bilan axborot xavfsizligining kompleks tizimini yaratish mumkin.

Yuqorida keltirilganlar ochiq kalitlar infratuzilmasini yaratish va madadlash xizmatlari ahamiyatini oshishiga olib keladi.

IX bob. AXBOROT-KOMMUNIKATSION TIZIMLARDA SUQILIB KIRISHLARNI ANIQLASH

9.1. Xavfsizlikni adaptiv boshqarish konsepsiyasi

Tashkilotlarda himoyalash bilan bog'liq bo'lgan muammolarni yechish uchun aksariyat hollarda qisman yondashishlardan foydalanishadi. Bu yondashishlar, odatda, avvalo, foydalana oluvchi resurslarning joriy darajasi orqali aniqlanadi. Undan tashqari, xavfsizlik ma'murlari ko'pincha o'zlariga tushunarli bo'lgan xavfsizlik xavf-xatarlariga reaksiya ko'rsatishadi. Aslida xavf-xatarlar juda ko'p bo'lishi mumkin. Korporativ axborot tizimini faqat qat'iy joriy nazorati va xavfsizlikning umumiy siyosatini ta'minlovchi kompleks yondashish xavfsizlik xavf-xatarlarini anchagina kamaytirishi mumkin.

Oxirgi vaqtda turli kompaniyalar tomonidan qator yondashishlar ishlab chiqildiki, bu yondashishlar nafaqat mavjud zaifliklarni aniqlashga, balki o'zgargan eski yoki paydo bo'lgan yangi zaifliklarni aniqlashga va ularga mos himoyalash vositalarini qarshi qo'yishga imkon beradi. Xususan, ISS(Internet Security Systems) kompaniyasi tomonidan *xavfsizlikni adaptiv boshqarish modeli* ANS (Adaptive Network Security) ishlab chiqildi.

Xavfsizlikka adaptiv yondashish, to'g'ri loyihalangan va yaxshi boshqariluvchi jarayon va vositalar yordamida xavfsizlik xavf-xatarlarini real vaqt rejimida nazoratlash, aniqlash va ularga reaksiya ko'rsatishga imkon beradi.

Tarmoqning adaptiv xavfsizligi quyidagi asosiy uchta element orqali ta'minlanadi:

– xavf-xatarlarni baholash;
– himoyalanishni tahlillash;
– hujumlarni aniqlash.

Xavf-xatarlarni baholash. Zaifliklarni (keltiradigan zararning jiddiylik darajasi bo'yicha), tarmoq qism tizimlarini (jiddiylik darajasi bo'yicha), tahdidlarni (ularning amalga oshirilishi ehtimolligi bo'yicha) aniqlash va rutbalashdan iborat. Tarmoq konfiguratsiyasi muttasil o'zgarishi sababli, xavf-xatarlarni baholash jarayoni ham uzluksiz

o'tkazilishi lozim. Korporativ axborot tizimining himoyalash tizimini qurish xavf-xatarlarni baholashdan boshlanishi lozim.

Himoyalanishni tahlillash – tarmoqning zaif joylarini qidirish. Tarmoq ulanishlardan, uzellardan, xostlardan, ishchi stansiyalardan, ilovalardan va ma'lumot bazalaridan tarkib topgan. Bularning barchasi himoyalanish samaradorligining baholanishiga hamda noma'lum zaifliklarining aniqlanishiga muhtoj. Himoyalanishni tahlillash texnologiyasi tarmoqni tadqiqlash, nozik joylarini topish, bu ma'lumotlarni umumlashtirish va ular bo'yicha hisobot berish imkoniyatiga ega. Agar bu texnologiyani amalga oshiruvchi tizim adaptiv komponentga ham ega bo'lsa, aniqlangan zaifliklarni avtomatik tarzda bartaraf etish mumkin. Himoyalanishni tahlillash texnologiyasi tarmoq xavfsizligi siyosatini, uni tashkilot tashqarisidan yoki ichkarisidan buzishga urinishlardan oldin, amalga oshirishga imkon beruvchi ta'sirchan usul hisoblanadi.

Himoyalanishni tahlillash texnologiyasi tomonidan identifikatsiyalanuvchi muammolarning ba'zilari quyidagilar:

– tizimlardagi «teshiklar» (back door) va troyan oti xilidagi dastur;

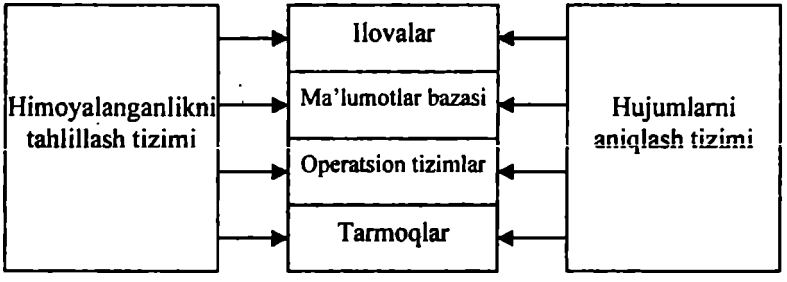
– kuchsiz parollar;

– himoyalanmagan tizimdan suqilib kirishga va «xizmat qilishdan voz kechish» xilidagi hujumlarga ta'sirchanlik;

– operatsion tizimlardagi zaruriy yangilanishlarning yo'qligi;

– tarmoqlararo ekranlarning, Web-serverlarning va ma'lumotlar bazasining noto'g'ri sozlanishi va h.

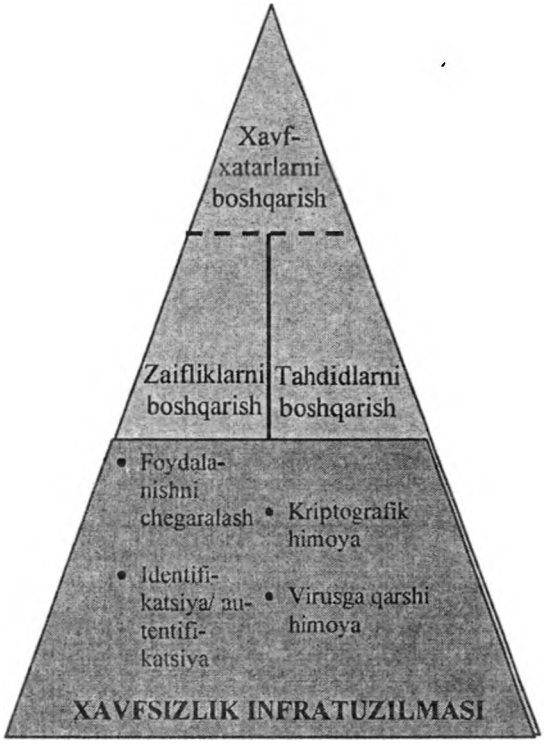
Hujumlarni aniqlash – korporativ tarmoqdagi shubhali harakatlarni baholash jarayoni. Hujumlarni aniqlash operatsion tizim va ilovalarni qaydlash jurnallarini yoki real vaqtdagi trafikni tahlillash orqali amalga oshiriladi. Tarmoq uzellari yoki segmentlarida joylashtirilgan hujumlarni aniqlash komponentlari turli hodisalarni, xususan, ma'lum zaifliklardan foydalanuvchi harakatlarni ham baholaydi (9.1-rasm).



9.1-rasm. Himoyalanganlikni tahlillash va hujumlarni aniqlash tizimlarining o'zaro aloqasi.

Xavfsizlikni adaptiv boshqarish modeli ANSning adaptiv komponenti, yangi zaifliklar xususidagi eng oxirgi axborotni taqdim qilgan holda, himoyalanishni tahlillash jarayonini modifikatsiyalashga javob beradi. U hujumlarni aniqlash komponentini ham uni hujumlar xususidagi oxirgi axborot bilan to'ldirish orqali, modifikatsiyalaydi. Adaptiv komponentning misoli sifatida yangi viruslarni aniqlash uchun virusga qarshi dasturning ma'lumotlar bazasini yangilash mexanizmini ko'rsatish mumkin.

Xavfsizlikni adaptiv boshqarish modelidan (9.2-rasm) foydalanish barcha tahdidlarni nazoratlash va ularga o'z vaqtida samarali reaksiya ko'rsatish imkonini beradi. Bu esa, o'z navbatida, nafaqat tahdidlarning amalga oshirilishiga sabab bo'luvchi zaifliklarni bartaraf qilishga, balki zaifliklar paydo bo'lish sharoitlarini tahlillashga imkon beradi.



9.2-rasm. Xavfsizlikni adaptiv boshqarish modeli.

Tarmoq xavfsizligini adaptiv boshqarish modeli tarmoqda suiiste'mol qilishni kamaytirishga, tarmoqdagi hodisalardan foydalanuvchilar, ma'murlar va kompaniya rahbariyatining xabardorlik darajasini oshishiga ham imkon beradi. Ta'kidlash lozimki, ushbu model oldin ishlatiluvchi himoyalash mexanizmlaridan (foydalanishni chegaralash, autentifikatsiyalash va h.) voz kechmaydi. Ularning funksionalligini yangi texnologiya evaziga kengaytiradi. O'zlarining axborot xavfsizligini ta'minlash tizimlarini zamonaviy talablarga mos kelishini xohlovchi tashkilotlar mavjud yechimlarni uchta yangi komponent-himoyalanishni tahlillash, hujumlarni aniqlash va xavf-xatarni baholash bilan to'ldirishi lozim.

9.2. Himoyalanishni tahlillash

Himoyalanishni tahlillash vositalari zaifliklarni topib va o'z vaqtida yo'q qilib hujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishiga bo'ladigan barcha sarf-xarajatlar kamayadi.

Himoyalanishni tahlillash vositalari tarmoq sathida, operatsion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko'paytirish, axborot tizimiga «ichkarilab borish» va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin.

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

Himoyalanishni tahlillash tizimi zaifliklarni aniqlash bo'yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga hujumlarida qo'llanilganiga o'xshash.

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

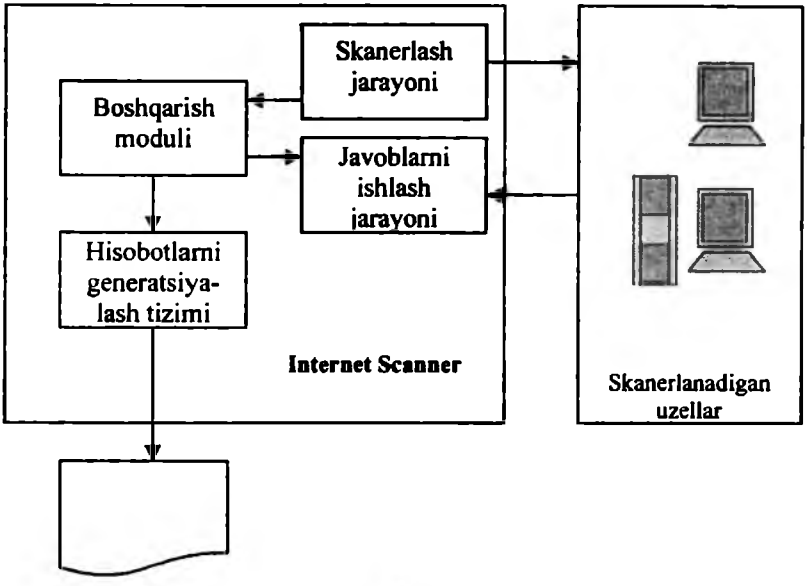
Himoyalanishni tahlillash vositalari yordamida tarmoq sathida nafaqat Internet ning korporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichki tarmog'ida tekshirishni amalga oshirish mumkin. Tarmoq sathida himoyalanishni tahlillash tizimi tashkilot xavfsizlik darajasini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

Himoyalanishni tahlillashni amalga oshiruvchi (Internet Scanner tizimi misolida) namunaviy sxema 9.3-rasmda keltirilgan.

Himoyalanishni tahlillash vositalarining bu sinfi nafaqat tarmoq protokollari va servislari, balki tarmoq bilan ishlashga javobgar tizimli va tatbiqiy dasturiy ta'minoti zaifiklarini ham tahlillaydi. Bunday ta'minot qatoriga Web-, FTP- va pochta serverlarini, tarmoqlararo ekranlami, brauzerlarni va h. kiritish mumkin.

Ba'zi vositalar dasturiy ta'minotni tahlillash bilan bir qatorda apparat vositalarini skanerlaydi. Bunday vositalarga kommutatsiyalovchi va marshrutlovchi asbob-uskunalar kiradi.

Operatsion tizim himoyalanishini tahlillash vositalari. Vositalarning bu sinfi operatsion tizim himoyalanishiga ta'sir etuvchi uning sozlanishlarini tekshirishga atalgan. Bunday sozlashlar quyidagilarni aniqlaydi:



9.3-rasm. Internet Scanner tizimi misolida himolanganlikni tahlillash sxemasi.

– foydalanuvchilarning hisob yozuvi, masalan, parol uzunligi va uning ta'sir muddati;

– foydalanuvchilarning jiddiy tizimli fayllardan foydalanish huquqlari;

– zaif tizimli fayllar;

– o'rnatilgan patchlar va h.

Operatsion tizim sathidagi himoyalanishni tahlillash tizimlari operatsion tizimlar konfiguratsiyasini nazoratlashda ham ishlatilishi mumkin.

Tarmoq sathi himoyalanishni tahlillash vositalaridan farqli ravishda, ushbu tizimlar tahlillanuvchi tizimni tashqaridan emas, balki ichkaridan skanerlaydi, ya'ni ular tashqaridagi niyati buzuq odamlar hujumlarini imitatsiyalamaydi. Operatsion tizim sathida himoyalanishni tahlillash tizimlarining ba'zilari (masalan, Internet Security Systems kompaniyasining System Scanner tizimi) zaifliklarni aniqlash imkoniyatidan tashqari, aniqlangan muammolarning bir qismini avtomatik

tarzda bartaraf qilishga yoki tashkilotda qabul qilingan xavfsizlik siyosatini qoniqtirmaydigan tizim parametrlariga tuzatish kiritishga imkon beradi.

Tanlanuvchi himoyalashni tahlillash vositalariga quyiladigan umumiy talablar. Tanlanuvchi tizimga qo'yiladigan majburiy talab korxona tarmoq infratuzilmasini o'zgartirish zaruriyatining yo'qligi. Aks holda bunday qaytadan tashkil etishga qilinadigan xarajat himoyalanishni tahlillash tizimi narxidan oshib ketishi mumkin. Hozirda bu talabga faqat Internet Security Systems kompaniyasining Security Systems tizimi javob beradi.

Himoyalanishni tahlillash vositalarini noto'g'ri ishlatish ulardan niyati buzuq odamlarning korporativ tarmoqqa suqilib kirish uchun foydalanishlariga imkon yaratadi. Shu sababli, himoyalanishni tahlillash vositalari o'zlarining komponentlaridan va yig'llgan ma'lumotlardan foydalanishni chegaralovchi mexanizmlar bilan ta'minlanishi lozim. Bunday mexanizmlarga quyidagilar kiradi:

– faqat ma'mur huquqiga ega bo'lgan foydalanuvchi tomonidan ushbu vositalarni ishga tushirish;

– skanerlash ma'lumotlari arxivini shifrlash;

– masofadan boshqarishda ulanishni autentifikatsiyalash;

– kataloglar bilan ishlash uchun maxsus huquqlarni aniqlash va h.

Zaifliklarni aniqlash jarayonining quyidagi imkoniyatlariga e'tiborni qaratish lozim:

– bir necha qurilma yoki servislarni parallel ishlash evaziga skanerlash tezligini oshirish;

– tizimdan ruxsatsiz foydalanishni oldini olish uchun har bir skanerlanuvchi uzelga bildirish qog'ozini yuborish;

– yolg'on ishlashlarni minimallashtirish uchun tarmoqni ekspluatatsiya talablariga to'g'rilash.

Korporativ tarmoq holatining doimo o'zgarib turishi, uning himoyalanishiga ta'sir ko'rsatadi. Shu sababli, himoyalanishni tahlillashning yaxshi tizimi jadval bo'yicha ishlash rejimiga ega bo'lib, ma'mur uni eslagunicha o'zi tarmoq uzellari zaifliklarini tekshirishi va paydo bo'lgan muammolar xususida nafaqat ma'murni ogohlantirishi, balki aniqlangan zaifliklarni yo'qotish usullarini tavsiya etishi lozim.

E'tibor berish zarur bo'lgan xarakteristikalardan biri–hisobotlarni generatsiyalash tizimining mavjudligi. Bu tizim foydalanuvchilarning turli kategoriyalari – texnik mutaxassislardan tortib to tashkilotlar rah-

barlari uchun tafsiloti turli darajada bo'lgan hujjatlarni yaratishga imkon berishi lozim.

Hujjatlarda ma'lumotlarni ifodalash shakli ham muhim hisoblanadi. Faqat matnli axborot bilan to'ldirilgan hujjatlarning foydasi bo'lmaydi. Grafiklardan foydalanish esa ma'murga tashkilot tarmog'idagi barcha muammolarni yaqqol namoyish etishga imkon beradi. Hisobotlarda aniqlangan muammolarni yo'qotish bo'yicha tavsiyalarning mavjudligi himoyalanishni tahlillash vositalarini tanlashdagi majburiy shart hisoblanadi.

Doimo yangi zaifliklarning aniqlanishi himoyalanishni tahlillash tizimining zaifliklar ma'lumotlari bazasini to'ldira olishi imkoniyatiga ega bo'lishini taqozo etadi. Bu zaifliklarni tavsiflovchi maxsus til yordamida yoki tizim ishlab chiqaruvchilari tomonidan zaifliklarni vaqti-vaqti bilan to'ldirish yo'li bilan amalga oshiriladi. Korporativ tarmoq uzellarining himoyalanish darajasining o'zgarishini tahlillash uchun tanlanuvchi vosita o'tkazilgan skanerlash seanslari xususidagi axborotni to'planishiga imkon berishi lozim.

9.3. Hujumlarni aniqlash

Tarmoq axborotini tahlillash usullari. Mohiyati bo'yicha, hujumlarni aniqlash jarayoni korporativ tarmoqda bo'layotgan shubhali harakatlarni baholash jarayonidir. Boshqacha aytganda hujumlarni aniqlash hisoblash yoki tarmoq resurslariga yo'naltirilgan shubhali harakatlarni identifikatsiyalash va ularga reaksiya ko'rsatish jarayoni. Hozirda hujumlarni aniqlash tizimida quyidagi usullar ishlatiladi:

– statistik usul;
– ekspert tizimlari;
– neyron tarmoqlari.

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

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

1. Statistik tizimlar hodisalar kelishi tartibiga sezuvchanmaslar; ba'zi hollarda bir hodisaning o'zi, kelishi tartibiga ko'ra anomal yoki normal faoliyatni xarakterlashi mumkin.

2. Anomal faoliyatni adekvat identifikatsiyalash maqsadida hujumlarni aniqlash tizimi tomonidan kuzatiluvchi xarakteristikalar uchun chegaraviy (bo'sag'aviy) qiymatlarni berish juda qiyin.

3. Statistik usullar vaqt o'tishi bilan buzg'unchilar tomonidan shunday «o'rganilishi» mumkinki, hujum harakatlari normal kabi qabul qilinadi.

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

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

Ekspert tizimlarining kamchiliklari ichida eng asosiysi – noma'lum hujumlarni akslantira olmasligi. Bunda oldindan ma'lum hujumning hatto ozgina o'zgarishi hujumlarni aniqlash tizimining ishlashiga jiddiy to'siq bo'lishi mumkin.

Neyron tarmoqlari. Hujumlarni aniqlash usullarining aksariyati qoidalar yoki statistik yondashish asosida nazoratlanuvchi muhitni tahlillash shakllaridan foydalanadi. Nazoratlanuvchi muhit sifatida qaydlash jurnallari yoki tarmoq trafigi ko'rilishi mumkin. Bunday tahlillash ma'mur yoki hujumlarni aniqlash tizimi tomonidan yaratilgan, oldindan aniqlangan qoidalar to'plamiga tayanadi.

Hujumni vaqt bo'yicha yoki bir necha niyati buzuq odamlar o'rtasida har qanday bo'linishi ekspert tizimlar yordamida aniqlashga qiyinchilik tug'diradi. Hujumlar va ular usullarining turli-tumanligi tufayli, ekspert tizimlari qoidalarining ma'lumotlar bazasining, hatto do-

imiy yangilanishi ham hujumlar diapazonini aniq identifikatsiyalashni kafolatlamaydi.

Neyron tarmoqlaridan foydalanish ekspert tizimlarining yuqorida keltirilgan muammolarni bartaraf etishning bir usuli hisoblanadi. Ekspert tizimlari foydalanuvchiga ko'rilayotgan xarakteristikalar ma'lumotlar bazasidagi qoidalarga mos kelishi yoki mos kelmasligi xususida aniq javob beraolsa, neyrotarmoq axborotni tahlillaydi va ma'lumotlarni aniqlashga o'rgangan xarakteristikalariga mos kelishini baholash imkoniyatini taqdim etadi. Neyrotarmoqli ifodalashning moslik darajasi 100%ga yetishi mumkin, ammo tanlash haqiqiyligi tamoman qo'yilgan masala misollarini tahlillash sifatiga bog'liq.

Avval predmet sohasining oldindan tanlab olingan misolida neyrotarmoqni to'g'ri identifikatsiyalashga «o'rgatishadi». Neyrotarmoq reaksiyasi tahlillanadi, qoniqarli natijalarga erishish maqsadida tizim sozlanadi. Neyrotarmoq ham vaqt o'tishi bilan, predmet sohasi bilan bog'liq ma'lumotlarni tahlillashni o'tkazishiga qarab «tajriba orttiradi».

Neyrotarmoqlarning suiiste'mol qilinishni aniqlashdagi muhim afzalligi, ularning atayin qilinadigan hujumlar xarakteristikalarini «o'rganish» va tarmoqda oldin kuzatilganiga o'xshamagan elementlarni identifikatsiyalash qobiliyatidir.

Yuqorida tavsiflangan hujumlarni aniqlash usullarining har biri afzalliklarga va kamchiliklarga ega. Shu sababli, hozirda tavsiflangan usullarning faqat bittasidan foydalanuvchi tizimni uchratish qiyin. Odatda, bu usullar birgalikda ishlatiladi.

Hujumlarni aniqlash tizimlarining turkumlanishi. Hujumlarni aniqlash tizimlari IDS(Intrusion Detection System)da ishlatiluvchi hujumlarni aniqlovchi mexanizmlar bir necha umumiy usullarga asoslangan. Ta'kidlash lozimki, bu usullar bir-birini inkor etmaydi. Aksariyat tizimlarda bir necha usullarning kombinatsiyasidan foydalaniladi.

Hujumlarni aniqlash tizimlari quyidagi alomatlari bo'yicha turkumla-nishi mumkin:

– reaksiya ko'rsatish usuli bo'yicha;

– hujumlarni fosh etish usuli bo'yicha;

– hujum xususidagi axborotni yig'ish usuli bo'yicha.

Reaksiya ko'rsatish usuli bo'yicha passiv va aktiv IDSlar farqlanadi. Passiv IDS lar hujum faktlarini qaydlaydi, ma'lumotlarni jurnal fayliga yozadi va ogohlantirishlar beradi. Aktiv IDSlar, masalan, tarmoqlararo ekranni qayta konfiguratsiyalash yoki marshrutizatordan foy-

dalanish ro'yxatini generatsiyalash bilan hujumga qarshi harakat qilishga urinadi.

Hujumlarni fosh etish usuli bo'yicha IDSlarni quyidagi ikkita kategoriyaga ajratish qabul qilingan:

– anomal xatti-harakatni aniqlash (anomaly-based);

– suiiste'molliklarni aniqlash (misuse detection yoki signature-based).

Anomal xatti-harakatni aniqlash yo'li bilan hujumlarni aniqlash texnologiyasi quyidagi gipotezaga asoslangan. Foydalanuvchining anomal xatti-harakati (ya'ni hujumi yoki qandaydir g'arazli harakati) – normal xatti-harakatdan chetlashish. Anomal xatti-harakatga misol tariqasida qisqa vaqt oralig'ida ulanishlarning katta sonini, markaziy protsessorning yuqori yuklanishini va h. ko'rsatish mumkin.

Agar foydalanuvchining normal xatti-harakati profilini bir ma'noda tavsiflash mumkin bo'lganida, undan har qanday chetlanishlarni anomal xatti-harakat sifatida identifkatsiyalash mumkin bo'lar edi. Ammo anomal xatti-harakat har doim ham hujum bo'lavermaydi. Masalan, tarmoq ma'muri tomonidan yuborilgan ko'p sonli so'rovlarni hujumlarni aniqlash tizimi «xizmat ko'rsatishdan voz kechish» xilidagi hujum sifatida identifikatsiyalashi mumkin.

Ushbu texnologiya asosidagi tizimdan foydalanilganda ikkita keskin holat yuz berishi mumkin:

– hujum bo'lmagan anomal xatti-harakatni aniqlash va uni hujumlar sinfiga kiritish;

– anomal xatti-harakat ta'rifiga mos kelmaydigan hujumlarni o'tkazib yuborish. Bu holat hujum bo'lmagan anomal xatti-harakatni hujumlar sinfiga kiritishga nisbatan xavfliroq hisoblanadi.

Bu kategoriya tizimlarini sozlashda va ekspluatatsiyasida ma'mur quyidagi qiyinchiliklarga duch keladi:

– foydalanuvchi profilini qurish sermehnat masala bo'lib, ma'murdan katta dastlabki ishlarni talab etadi.

– yuqorida keltirilgan ikkita keskin harakatlardan birining paydo bo'lishi ehtimolligini pasaytirish uchun foydalanuvchi xatti-harakatining chegaraviy qiymatlarini aniqlash zarur.

Anomal xatti-harakatlarni aniqlash texnologiyasi hujumlarning yangi xilini aniqlashga mo'ljallangan. Uning kamchiligi - doimo «o'rganish» zaruriyati.

Suiiste'molliklarni aniqlash yo'li bilan hujumlarni aniqlash texnologiyasining mohiyati hujumlarni signatura ko'rinishida tavsiflash va

ushbu signaturani nazoratlanuvchi makonda (tarmoq trafigida yoki qaydlash jurnalida) qidirishdan iborat. Hujum signaturasi sifatida anomal faoliyatni xarakterlovchi harakatlar shabloni yoki simvollar satri ishlatilishi mumkin. Bu signaturalar virusga qarshi tizimlarda ishlatiluvchi ma'lumotlar bazasiga o'xshash ma'lumotlar bazasida saqlanadi. Ta'kidlash lozimki, virusga qarshi rezident monitorlar hujumlarni aniqlash tizimlarining xususiy xoli hisoblanadi. Ammo bu yo'nalishlar boshidan parallel rivojlanganlari sababli, ularni ajratish qabul qilingan. Ushbu xil tizimlar barcha ma'lum hujumlarni aniqlasa-da, yangi, hali ma'lum bo'lmagan hujumlarni aniqlay olmaydi.

Bu tizimlarni ekspluatatsiyasida ham ma'murlar muammolarga duch keladi. Birinchi muammo – signaturalarni tavsiflash mexanizmlarini, ya'ni hujumlarni tavsiflovchi tillarni yaratish. Ikkinchi muammo, birinchi muammo bilan bog'liq bo'lib, hujumlarni shunday tavsiflash lozimki, uning barcha modifikatsiyalarini qaydlash imkoni tug'ilsin.

Hujum xususidagi axborotni yig'ish usuli bo'yicha turkumlash eng ommaviy hisoblanadi:

– tarmoq sathida hujumlarni aniqlash (network-based);

– xost sathida hujumlarni aniqlash (host-based);

– ilova sathida hujumlarni aniqlash (application-based).

Tarmoq sathida hujumlarni aniqlash tizimida tarmoqdagi trafikni eshitish orqali niyati buzuq odamlarning mumkin bo'lgan harakatlari aniqlanadi. Hujumni qidirish «xostdan-xostgacha» prinsipi bo'yicha amalga oshiriladi. Ushbu xilga taalluqli tizimlar, odatda, hujumlar signaturasidan va «bir zumda» tahlillashdan foydalanib, tarmoq trafigini tahlillaydi. «Bir zumda» tahlillash usuliga binoan tarmoq trafigi real yoki unga yaqinroq vaqtda monitoringlanadi va mos aniqlash algoritmlaridan foydalaniladi. Ko'pincha ruxsatsiz foydalanish faoliyatini xarakterlovchi trafikdagi ma'lum satrlarni qidirish mexanizmlaridan foydalaniladi.

Xost sathida hujumlarni aniqlash tizimi ma'lum xostda niyati buzuq odamlarni monitoringlash, detektirlash va harakatlariga reaksiya ko'rsatishga atalgan. Tizim himoyalangan xostda joylashib, unga qarshi yo'naltirilgan harakatlarni tekshiradi va oshkor qiladi. Bu tizimlar operatsion tizim yoki ilovalarning qaydlash jurnallarini tahlillaydi. Qaydlash jurnallarini tahlillash usulini amalga oshirish oson bo'lsa-da, u quyidagi kamchiliklarga ega:

– jurnalda qayd etiluvchi ma'lumotlar hajmining kattaligi nazoratlanuvchi tizim ishlashi tezligiga salbiy ta'sir ko'rsatadi;

– qaydlash jurnalini tahlillashni mutaxassislar yordamisiz amalga oshirib bo'lmaydi;

– hozirgacha jurnallarni saqlashning unifikatsiyalangan formati mavjud emas;

– qaydlash jurnallaridagi yozuvni tahlillash real vaqtda amalga oshirilmaydi.

IDSning uchinchi xili ma'lum ilovadagi muammolarni qidirishga asoslangan.

Hujumlarni aniqlash tizimining komponentlari va arxitekturasi

Mavjud yechimlarning tahlili hujumlarni aniqlashning namunaviy tizimi komponentlarining ro'yxatini keltirishga imkon beradi.

Kuzatish moduli nazoratlanuvchi makondan (qaydlash jurnali yoki tarmoq trafigi) ma'lumotlarni yig'ishni ta'minlaydi. Uning quyidagi nomlari ham uchraydi: sensor (sensor), monitor (monitor), zond(probe) va h. Hujumlarni aniqlash tizimi arxitekturasining qurilishiga bog'liq holda kuzatish moduli boshqa komponentlardan alohida, boshqa kompyuterda joylashishi mumkin.

Hujumlarni aniqlash qism tizimi asosiy modul bo'lib, kuzatish modulidan olinadigan axborotni tahlillaydi. Ushbu tahlillash natijasi bo'yicha qism tizim hujumlarni identifikatsiyalash, reaksiya ko'rsatish variantlari bo'yicha to'xtamga kelishi, ma'lumotlar omborida hujumlar xususidagi axborotni saqlashi mumkin va h.

Bilimlar bazasida, hujumlarni aniqlash tizimlarida ishlatiladigan usullarga bog'liq holda, foydalanuvchilar va hisoblash tizim profillari, ruxsatsiz foydalanishlarni xarakterlovchi hujum signaturalari yoki shubhali satrlar saqlanishi mumkin. Bilimlar bazasi hujumlarni aniqlash tizimlarini ishlab chiqaruvchilari, tizimdan foydalanuvchilar yoki uchinchi tomon, masalan, bu tizimni madadlovchi autsorsing kompaniyasi tomonidan to'ldirilishi mumkin.

Ma'lumotlar ombori hujumlarni aniqlash tizimi ishlashi jarayonida yig'ilgan ma'lumotlarning saqlanishini ta'minlaydi.

Grafik interfeys tizimning nihoyatda zaruriy komponenti bo'lib, hujumlarni aniqlash tizimi ishlashini boshqaruvchi operatsion tizimga bog'liq holda de-fakto Windows va Unix standartlariga mos kelishi lozim.

Reaksiya ko'rsatish qism tizimi aniqlangan hujumlar va boshqa nazoratlanuvchi hodisalarga reaksiya ko'rsatishni amalga oshiradi. Mavjud tizimlarda ishlatiladigan reaksiya ko'rsatish usullarini quyidagi uchta kategoriyaga ajratish mumkin:

– bildirish;

– saqlash;

– faol reaksiya ko'rsatish.

Bildirish usuli bo'yicha hujum xususidagi axborot xavfsizlik ma'muriga tizimning konsoliga yoki elektron pochta bo'yicha, peydjerga faks yoki telefon orqali jo'natilishi mumkin.

Saqlash usuliga reaksiya ko'rsatishning quyidagi variantlari taalluqli:

– hodisalarni ma'lumotlar bazasida qaydlash;

– hujumlarni real vaqt masshtabida tiklash.

Birinchi variant himoyalashning boshqa tizimlarida ham keng qo'llaniladi: Ikkinchi variantni amalga oshirish uchun hujum qiluvchini kompaniya tarmog'iga o'tkazib yuborish va uning barcha harakatlarini qaydlash lozim. Bu xavfsizlik ma'muriga keyin vaqtning real masshtabida (yoki berilgan tezlikda) hujum qiluvchi tomonidan qilingan barcha harakatlarni tiklashga, muvaffaqiyatli tahlillashga va ularni keyinchalik bartaraf etishga hamda muhokama qilish jarayonida yig'Ilgan axborotdan foydalanishga imkon beradi.

Faol reaksiya ko'rsatish kategoriyasiga quyidagi variantlar taalluqli:

– hujum qiluvchi ishini blokirovka qilish;

– hujum qilinuvchi uzel bilan seansni tugallash;

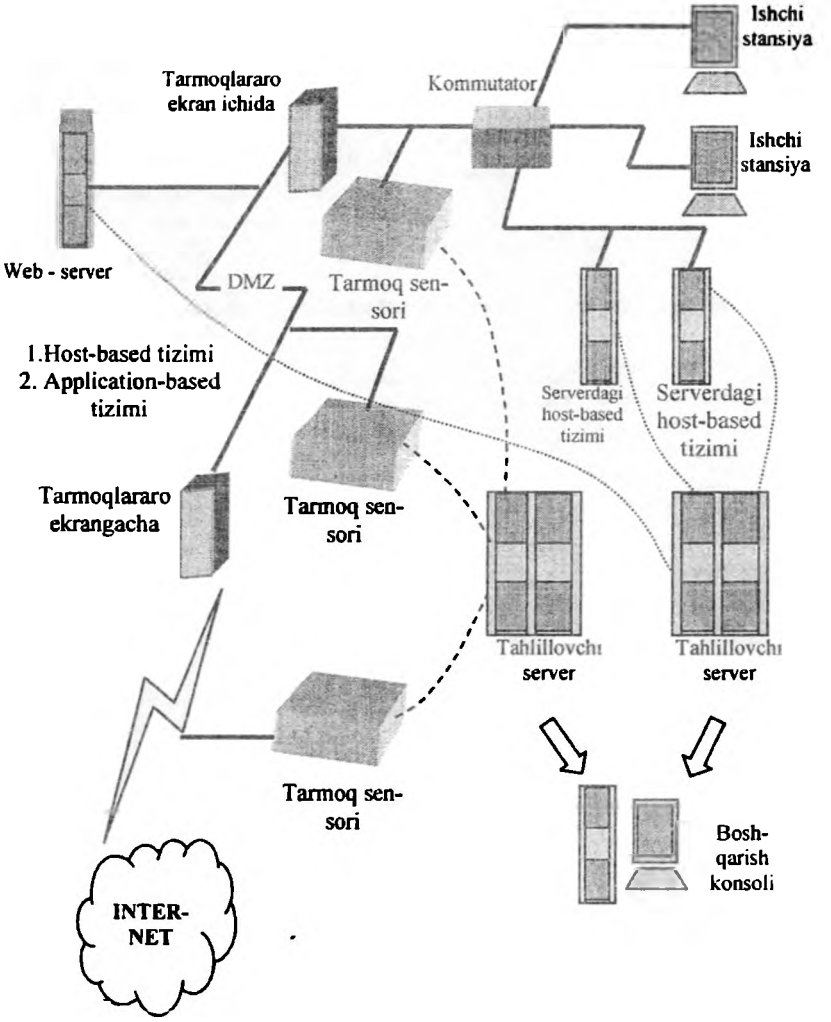
– tarmoq asbob-uskunalari va himoya vositalarini boshqarish.

Reaksiya ko'rsatish mexanizmlarining ushbu kategoriyasi bir tomondan yetarlicha samarali bo'lsa, ikkinchi tomondan ulardan juda ehtiyotlik bilan foydalanish zarur, chunki ularni noto'g'ri ishlatish butun korporativ axborot tizimi ishga layoqatligining buzilishiga olib kelishi mumkin.

Komponentlarni boshqarish qism tizimi hujumlarni aniqlash tizimining turli komponentlarini boshqarishga atalgan. «Boshqarish» atamasi orqali hujumlarni aniqlash tizimining turli komponentlari (masalan, kuzatish modullari) uchun xavfsizlik siyosatini o'zgartirish hamda ushbu komponentlardan axborotni (masalan, qaydlangan hujum xususidagi) olish tushuniladi. Boshqarish ichki protokollar va interfeyslar va ishlab chiqilgan standartlar (masalan, SNMP) yordamida amalga oshirilishi mumkin.

Hujumlarni aniqlash tizimlari ikkita arxitektura – «avtonom agent» va «agent-menejer» arxitekturalari asosida quriladi. Birinchi holda tarmoqning har bir himoyalanuvchi uzel va segmentlariga tizim agentlari o'rnatilib, bu agentlar o'zaro axborot almasha olmaydilar hamda ularni yagona konsol orqali markazlashtirilgan holda boshqarib bo'lmaydi. «Agent-menejer» arxitekturasi bu kamchiliklardan xoli. Bu holda katta tarmoqning turli qismlarida joylashgan ko'pgina IDSdan iborat hujumlarni aniqlashning taqsimlangan tizimi dIDS (distributed IDS)da ma'lumotlarni yig'ish serverlari va markaziy tahlillovchi server qaydlanuvchi ma'lumotlarni markazlashtirilgan yig'ishni va tahlillashni amalga oshiriladi. dIDS modullarini boshqarish boshqarishning markaziy konsoli orqali amalga oshiradi. Filiallari turli hududlar, hatto shaharlar bo'yicha tarqalgan yirik tashkilotlar uchun bunday arxitekturaning ishlatilishi jiddiy ahamiyatga ega.

dIDS ishlashining umumiy sxemasi 9.4-rasmda keltirilgan.



9.4-rasm. Taqsimlangan IDS ishlashining umumiy sxemasi.

Bunday tizim turli IDSlardan hujumlar xususidagi axborotlarni markazlashtirilishi evaziga korporativ qism tarmoq himoyalanishini kuchaytirishga imkon beradi. Hujumlarni aniqlovchi taqsimlangan tizim

dIDS quyidagi qism tizimlardan tashkil topgan: boshqarish konsoli, tahlillovchi serverlar, tarmoq agentlari, hujum xususidagi axborotni yig'uvchi server. Markaziy tahlillovchi server, odatda, ma'lumotlar bazasi va Web-serverdan tashkil topgan bo'lib, hujumlar xususidagi axborotni saqlashga va qulay Web-interfeys yordamida ma'lumotlarni manipulatsiyalashga imkon beradi. Tarmoq agenti dIDSning eng muhim komponentlaridan biri hisoblanib, maqsadi markaziy tahlillovchi serverga hujum xususida xabar berish bo'lgan kichkina dasturdir. Hujum xususidagi axborotni yig'uvchi server markaziy tahlillovchi serverga mantiqiy tayangan va tarmoq agentlaridan olingan ma'lumotlarni guruhlashda foydalaniladigan parametrlarni belgilaydi.

Ma'lumotlarni guruhlashni quyidagi parametrlar bo'yicha amalga oshirish mumkin:

– hujum qiluvchining IP-adresi;
– qabul qiluvchining porti;
– agent nomeri;
– sana, vaqt;
– protokol;
– hujum xillari va h.

IDSdan foydalanish samaradorligiga qandaydir shubhalar bo'lishiga qaramay, foydalanuvchilar IDSning bemalol tarqatiluvchi va tijorat vositalaridan keng foydalanadilar.

9.4. Kompyuter viruslari va virusdan himoyalanish muammolari

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

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

– asliga mos kelishi shart bo'lmagan, ammo aslining xususiyatlariga (o'z-o'zini tiklash) ega bo'lgan nusxalarni yaratish qobiliyati;

– hisoblash tizimining bajariluvchi obyektlariga yaratiluvchi nusxalarning kiritilishini ta'minlovchi mexanizmlarning mavjudligi.

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

Viruslarni quyidagi asosiy alomatlari bo'yicha turkumlash mumkin:

– yashash makoni;

– operatsion tizim;

– ishlash algoritmi xususiyati;

– destruktiv imkoniyatlari.

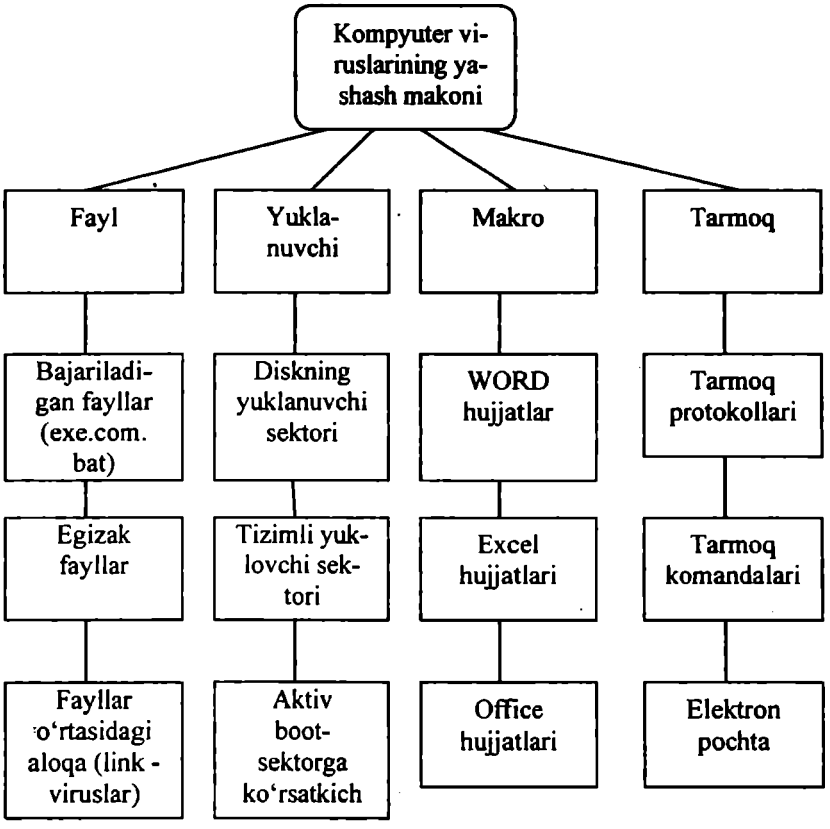
Kompyuter viruslarini yashash makoni, boshqacha aytganda, viruslar kiritiluvchi kompyuter tizimi obyektlarining xili bo'yicha turkumlash asosiy va keng tarqalgan turkumlash hisoblanadi (9.5-rasm).

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

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

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

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



9.5-rasm. Yashash makoni bo'yicha kompyuter viruslarining turkumlanishi.

Kompyuter viruslarining ko'pgina kombinatsiyalangan xillari ham mavjud, masalan – tarmoqli makrovirus tahrirlanuvchi hujjatlarni zaharlaydi hamda o'zining nusxalarini elektron pochta orqali tarqatadi. Boshqa bir misol sifatida fayl-yuklama viruslarini ko'rsatish mumkinki, ular fayllarni hamda disklarning yuklanadigan sektorini zaharlaydi.

Viruslarning hayot davri. Har qanday dasturdagidek, kompyuter viruslari hayoti davrining ikkita asosiy bosqichini – saqlanish va bajarilish bosqichlarini ajratish mumkin.

Saqlanish bosqichi virusning diskda u kiritilgan obyekt bilan birgalikda shundaygina saqlanish davriga to'g'ri keladi. Bu bosqichda virus virusga qarshi dastur ta'minotiga zaif bo'ladi, chunki u faol emas va himoyalanish uchun operatsion tizimni nazorat qila olmaydi.

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

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

Virusni xotiraga yuklash. Virusni xotiraga yuklash operatsion tizim yordamida virus kiritilgan bajariluvchi obyekt bilan bir vaqtda amalga oshiriladi. Masalan, agar foydalanuvchi virus bo'lgan dasturiy faylni ishga tushirsa, ravshanki, virus kodi ushbu fayl qismi sifatida xotiraga yuklanadi. Oddiy holda, virusni yuklash jarayoni-diskdan tezkor xotiraga nusxalash bo'lib, so'ngra boshqarish virus devori kodiga uzatiladi. Bu harakatlar operatsion tizim tomonidan bajariladi, virusning o'zi passiv holatda bo'ladi. Murakkabroq vazifalarda virus boshqarishni olganidan so'ng o'zining ishlashi uchun qo'shimcha harakatlar bajarishi mumkin. Bu bilan bog'liq ikkita jihat ko'riladi.

Birinchisi viruslarni aniqlash muolajasining maksimal murakkablashishi bilan bog'liq. Saqlanish bosqichida ba'zi viruslar himoyalanishni ta'minlash maqsadida yetarlicha murakkab algoritmdan foydalanadi. Bunday murakkablashishga virus asosiy badanini shifrlashni kiritish mumkin. Ammo faqat shifrlashni ishlatish chala chora hisoblanadi, chunki yuklanish bosqichida rasshifrovkani ta'minlovchi virus qismi ochiq ko'rinishda saqlanishi lozim. Bunday holatdan qutilish uchun viruslarni ishlab chiquvchilar rasshifrovka qiluvchi kodini «mutatsiyalash» mexanizmidan foydalanadi. Bu usulning mohiyati shundan iboratki, obyektga virus nusxasi kiritilishida uning rasshifrovka qiluvchiga taalluqli qismi shunday modifikatsiyalanadiki, original bilan matnli farqlanish paydo bo'ladi, ammo ish natijasi o'zgarmaydi.

Kodni mutatsiyalash mexanizmidan foydalanuvchi viruslar *polimorf viruslar* nomini olgan. Polifmorf viruslar (polymorphic)-qiyin aniqlanadigan viruslar bo'lib, signaturalarga ega emas, ya'ni tarkibida

birorta ham kodining doimiy qismi yo'q. Polimorfizm faylli, yuklamali va makroviruslarda uchraydi.

Stels-algoritmlardan foydalanilganda viruslar o'zlarini tizimda to'la yoki qisman berkitishlari mumkin. Stels-algoritmlaridan foydalanadigan viruslar – *stels-viruslar* (Stealth) deb yuritiladi. Stels viruslar operatsion tizimning shikastlangan fayllarga murojaatini ushlab qolish yo'li bilan o'zini yashash makonidaligini yashiradi va operatsion tizimni axborotni shikastlanmagan qismiga yo'naltiradi.

Ikkinchi jihat *rezident viruslar* deb ataluvchi viruslar bilan bog'liq. Virus va u kiritilgan obyekt operatsion tizim uchun bir butun bo'lganligi sababli, yuklanishdan so'ng ular, tabiiy, yagona adres makonida joylashadi. Obyekt ishi tugaganidan so'ng u tezkor xotiradan ozod bo'ladi. Bunda bir vaqtning o'zida virus ham bo'shalib saqlanishning passiv bosqichiga o'tadi. Ammo ba'zi viruslar xili xotirada saqlanish va virus eltuvchi ishi tugashidan so'ng faol qolish qobiliyatiga ega. Bunday viruslar rezident nomini olgan. *Rezident viruslar*, odatda, faqat operatsion tizimga ruxsat etilgan imtiyozli rejimlardan foydalanib, yashash makonini zaharlaydi va ma'lum sharoitlarda zararkunandalik vazifasini bajaradi. Rezident viruslar xotirada joylashadi va kompyuter o'chirilishigacha yoki operatsion tizim qayta yuklanishigacha faol holda bo'ladi.

Rezident bo'lmagan viruslar faqat faollashgan vaqtlarida xotiraga tushib zaharlash va zararkunandalik vazifalarini bajaradi. Keyin bu viruslar xotirani butunlay tark etib, yashash makonida qoladi.

Ta'kidlash lozimki, viruslarni rezident va rezident bo'lmaganlarga ajratish faqat fayl viruslariga taalluqli. Yuklanuvchi va makroviruslar rezident viruslarga tegishli.

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

Topilgan qurbonni zaharlash. Oddiy holda zaharlash deganda qurbon sifatida tanlangan obyektda virus kodining o'z-o'zini nusxalashi tushuniladi.

Avval fayl viruslarining zaharlash xususiyatlarini ko'raylik. Bunda ikkita sinf viruslari farqlanadi. Birinchi sinf viruslari o'zining kodini dasturiy faylga bevosita kiritmaydi, balki fayl nomini o'zgartirib, virus badani bo'lgan yangi faylni yaratadi. Ikkinchi sinfga qurbon fayllariga

bevosita kiruvchi viruslar taalluqli. Bu viruslar kiritilish joylari bilan xarakterlanadi. Quyidagi variantlar bo'lishi mumkin:

1. *Fayl boshiga kiritish.* Ushbu usul MS-DOSning *com*-fayllari uchun eng qulay hisoblanadi, chunki ushbu formatda xizmatchi sarlavhalar ko'zda tutilgan.

2. *Fayl oxiriga kiritish.* Bu usul eng ko'p tarqalgan bo'lib, viruslar kodiga boshqarishni uzatish dasturning birinchi komandasi (*com*) yoki fayl sarlavhasini (*exe*) modifikatsiyalash orqali ta'minlanadi.

3. *Fayl o'rtasiga kiritish.* Odatda bu usuldan viruslar tuzilmasi oldindan ma'lum fayllarga (masalan, *Command.com* fayli) yoki tarkibida bir xil qiymatli baytlar ketma-ketligi bo'lgan, uzunligi virus joylashishiga yetarli fayllarga tatbiqan foydalanadi.

Yuklama viruslar uchun zaharlash bosqichining xususiyatlari ular kiritiluvchi obyektlar – qayishqoq va qattiq disklarning yuklanish sektorlarining sifati va qattiq diskning bosh yuklama yozuvi (MBR) orqali aniqlanadi. Asosiy muammo-ushbu obyekt o'lchamlarining chegaralanganligi. Shu sababli, viruslar o'zlarining qurbon joyida sig'magan qismini diskda saqlashi hamda zaharlangan yuklovchi original kodini tashishi lozim.

Makroviruslar uchun zaharlash jarayoni tanlangan hujjat-qurbonda virus kodini saqlashdan iborat. Ba'zi axborotni ishlash dasturlari uchun buni amalga oshirish oson emas, chunki hujjat fayllari formatining makroprogrammalarni saqlashi ko'zda tutilmagan bo'lishi mumkin.

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

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

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

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

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

Boshqarishni virus dastur – eltuvchisiga o'tkazish. Ta'kidlash lozimki, viruslar buzuvchilar va buzmaydiganlarga bo'linadi.

Buzuvchi viruslar dasturlar zaharlanganida ularning ishga layoqatligini saqlash xususida qayg'urmaydilar, shu sababli, ularga ushbu bosqichning ma'nosi yo'q.

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

Zarar keltiruvchi dasturlarning boshqa xillari. Viruslardan tashqari zarar keltiruvchi dasturlarning quyidagi xillari mavjud:

– troyan dasturlari;

– mantiqiy bombalar;

– masofadagi kompyuterlarni yashirincha ma'murlovchi xaker utilitalari;

– Internetdan va boshqa konfidensial axborotdan foydalanish parollarini o'g'irlovchi dasturlar.

Ular orasida aniq chegara yo'q: troyan dasturlari tarkibida viruslar bo'lishi, viruslarga mantiqiy bombalar joylashtirilishi mumkin va h.

Troyan dasturlar o'zlari ko'paymaydi va tarqatilmaydi. Tashqaridan troyan dasturlar mutlaqo beozor ko'rinadi, hatto foydali funksiyalarni tavsiya etadi. Ammo foydalanuvchi bunday dasturni kompyuteriga yuklab, ishga tushirsa, dastur bildirmay zarar keltiruvchi funksiyalarni bajarishi mumkin. Ko'pincha troyan dasturlar viruslarni dastlabki tarqatishda, Internet orqali masofadagi kompyuterdan foydalanishda, ma'lumotlarni o'g'irlashda yoki ularni yo'q qilishda ishlatiladi.

Mantiqiy bomba – ma'lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari. Mantiqiy bomba, masalan, ma'lum sana kelganda yoki ma'lumotlar bazasida yozuv paydo bo'lganida yoki yo'q bo'lganida va h. ishga tushishi mumkin. Bunday bomba viruslarga, troyan dasturlarga va oddiy dasturlarga joylashtirilishi mumkin.

Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari. Kompyuterlar va korporativ tarmoqlarni himoyalovchi samarador tizimni yaratish uchun qayerdan xavf tug'llishini aniq tasavvur etish lozim. Viruslar tarqalishning juda xilma-xil kanallarini topadi. Buning ustiga eski usullarga yangisi qo'shiladi.

Tarqatishning klassik (mumtoz) usullari. Fayl viruslari dastur fayllari bilan birgalikda disketlar va dasturlar almashishda, tarmoq katologlaridan, Web- yoki FTP – serverlardan dasturlar yuklanishida tarqatiladi. Yuklama viruslar kompyuterga foydalanuvchi zaharlangan disketani diskovodda qoldirib, so'ngra operatsion tizimni qayta yuklashida tushib qoladi. Yuklama virus kompyuterga viruslarning boshqa xili

orqali kiritilishi mumkin. Makrokomanda viruslari MicroSoft Word, Excel, Access fayllari kabi ofis hujjatlarining zaharlangan fayllari almashinishida tarqaladi.

Agar zaharlangan kompyuter lokal tarmoqqa ulangan bo'lsa, virus osongina fayl-server disklariga tushib qolishi, u yerdan kataloglar orqali tarmoqning barcha kompyuterlariga o'tishi mumkin. Shu tariqa virus epidemiyasi boshlanadi. Virus tarmoqda shu virus tushib qolgan kompyuter foydalanuvchisi huquqlari kabi huquqqa ega ekanligini tizim ma'muri unutmasligi lozim. Shuning uchun u foydalanuvchi foydalanadigan barcha kataloglarga tushib qolishi mumkin. Agar virus tarmoq ma'muri ishchi stansiyasiga tushib qolsa, oqibati juda og'ir bo'lishi mumkin.

Elektron pochta. Hozirda Internet global tarmog'i viruslarning asosiy manbai hisoblanadi. Viruslar bilan zaharlanishlarning aksariyati MicroSoft Word formatida xatlar almashishda sodir bo'ladi. Elektron pochta makrokomanda viruslarini tarqatish kanali vazifasini o'taydi, chunki axborotlar bilan bir qatorda ko'pincha ofis hujjatlari jo'natiladi.

Viruslar bilan zaharlash bilmasdan va yomon niyatda amalga oshirilishi mumkin. Masalan, makrovirus bilan zaharlangan muharrirdan foydalanuvchi o'zi shubha qilmagan holda, adresatlarga zaharlangan xatlarni jo'natishi mumkin. Ikkinchi tarafdan niyati buzuq odam atayin elektron pochta orqali har qanday xavfli dasturiy kodni jo'natishi mumkin.

Troyan Web-saytlar. Foydalanuvchilar virusni yoki troyan dasturni Internet saytlarining oddiy kuzatishda, troyan Web-saytni ko'rganida olishi mumkin. Foydalanuvchi brauzerlaridagi xatoliklar ko'pincha troyan Web-saytlari faol komponentlarining foydalanuvchi kompyuterlariga zarar keltiruvchi dasturlarni kiritishiga sabab bo'ladi. Troyan saytni ko'rishga taklifni foydalanuvchi oddiy elektron xat orqali olishi mumkin.

Lokal tarmoqlar. Lokal tarmoqlar ham tezlikda zaharlanish vositasi hisoblanadi. Agar himoyaning zaruriy choralari ko'rilmasa, zaharlangan ishchi stansiya lokal tarmoqqa kirishda serverdagi bir yoki bir necha xizmatchi fayllarni zaharlaydi. Bunday fayllar sifatida Login.com xizmatchi faylni, firmada qo'llaniluvchi Excel-jadvallar va standart hujjat-shablonlarni ko'rsatish mumkin. Foydalanuvchilar bu tarmoqqa kirishida serverdan zaharlangan fayllarni ishga tushiradi, natijada virus foydalanuvchi kompyuteridan foydalana oladi.

Zarar keltiruvchi dasturlarni tarqatishning boshqa kanallari. Viruslarni tarqatish kanallaridan biri dasturiy ta'minotning qaroqchi nus-

xalari hisoblanadi. Disketlar va CD-disklardagi noqununiy nusxalarda ko'pincha turli-tuman viruslar bilan zaharlangan fayllar bo'ladi. Viruslarni tarqatish manbalariga elektron anjumanlar FTP va BBS fayl-serverlar ham taalluqli.

O'quv yurtlarida va Internet-markazlarida o'rnatilgan hamda umum-foydalanish rejimida ishlovchi kompyuterlar ham osongina viruslarni tarqatish manbaiga aylanishi mumkin. Agar bunday kompyuterlardan biri navbatdagi foydalanuvchi disketidan zaharlangan bo'lsa, shu kompyuterda ishlovchi boshqa foydalanuvchilar disketlari ham zaharlanadi.

Kompyuter texnologiyasining rivojlanishi bilan kompyuter viruslari ham o'zining yangi yashash makoniga moslashgan holda, takomillashadi. Har qanday onda yangi, oldin ma'lum bo'lmagan yoki ma'lum bo'lgan, ammo yangi kompyuter asbob-uskunasiga mo'ljallangan kompyuter viruslari, troyan dasturlari va qurtlar paydo bo'lishi mumkin. Yangi viruslar ma'lum bo'lmagan yoki oldin mavjud bo'lmagan tarqatish kanallaridan hamda kompyuter tizimlarga tatbiq etishning yangi texnologiyalaridan foydalanishi mumkin. Virusdan zaharlanish xavfini yo'qotish uchun korporativ tarmoqning tizim ma'muri, nafaqat virusga qarshi usullardan foydalanishi, balki kompyuter viruslari dunyosini doimo kuzatib borishi shart.

9.5. Virusga qarshi dasturlar

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

Viruslarga qarshi dasturlar foydalanadigan viruslarni aniqlashning asosiy usullari quyidagilar:

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

Etalon bilan taqqoslash usuli eng oddiy usul bo'lib, ma'lum viruslarni qidirishda niqoblardan foydalanadi. Virusning niqobi–mana shu muayyan virusga xos kodning qandaydir o'zgarmas ketma-ketligidir. Virusga qarshi dastur ma'lum virus niqoblarini qidirishda tekshiriluvchi fayllarni ketma-ket ko'rib chiqadi (skanerlaydi). Virusga qarshi skanerlar faqat niqob uchun belgilangan, oldindan ma'lum viruslarni topa oladi. Oddiy skanerlar kompyuterni yangi viruslarning suqilib kirishidan himoyalamaydi. Yangi dasturni yoki yuklama sektorini zaharlashda kodini to'la o'zgartira oluvchi shifrlanuvchi va polimorf viruslar uchun niqob ajratish mumkin emas. Shu sababli, skaner ularni aniqlamaydi.

Evristik tahlil. Kompyuter virusi ko'payishi uchun xotirada nusxalanish, sektorga yozilish kabi qandaydir muayyan harakatlarni amalga oshirishi lozim. Evristik tahlillagichda bunday harakatlarning ro'yxati mavjud. Evristik tahlillagich dasturlarni, disk va disket yuklama sektorlarini, ularda virusga xos kodlarni aniqlashga uringan holda, tekshiradi. Tahlillagich zaharlangan faylni topib, monitor ekraniga axborot chiqaradi va shaxsiy yoki tizimli jurnalga yozadi. Evristik tahlil oldin ma'lum bo'lmagan viruslarni aniqlaydi.

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

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

Kompyuterlarning kiritish-chiqarish bazaviy tizimiga (BIOSga) virusga qarshi vositalarni o'rnatish. Kompyuterlarning tizimli platasiga

viruslardan himoyalashning oddiy vositalari o'rnatiladi. Bu vositalar qattiq disklarning bosh yuklama yozuviga hamda disklar va disketlarning yuklama sektorlariga barcha murojaatlarni nazoratlashga imkon beradi. Agar qandaydir dastur yuklama sektorlar tarkibini o'zgartirishga urinsa, himoya ishga tushadi va foydalanuvchi ogohlantiriladi. Ammo bu himoya juda ham ishonchli emas.

Virusga qarshi dasturlarning xillari. Virusga qarshi dasturlarning qu-yidagi xillari farqlanadi:

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

Dastur-faglar eng ommaviy va samarali virusga qarshi dastur hisoblanadi. Samaradorligi va ommaviyligi bo'yicha ikkinchi o'rinda dastur-taftishchilar turadi. Odatda, bu ikkala dastur xillari bitta virusga qarshi dasturga birlashtiriladi, natijada, uning quvvati anchagina oshadi. Turli xil blokirovka qiluvchilar va immunizatorlar ham ishlatiladi.

Dastur-faglar (skanerlar) viruslarni aniqlashda etalon bilan taqqoslash usulidan, evristik tahlillashdan va boshqalardan foydalanadi. Dastur-faglar tezkor xotira va fayllarni skanerlash yo'li bilan muayyan virusga xarakterli bo'lgan niqobni qidiradi. Dastur-faglar nafaqat viruslar bilan zaharlangan fayllarni topadi, ba'lki ularni davolaydi ham, ya'ni fayldan dastur-virus badanini olib tashlab, faylni dastlabki holatiga qaytaradi. Dastur-faglar avval tezkor xotirani skanerlaydi, viruslarni aniqlaydi va ularni yo'qotadi, so'ngra fayllarni davolashga kirishadi. Fayllar ichida viruslarni katta sonini qidirishga va yo'q qilishga atalgan dastur-faglar, ya'ni polifaglar ham mavjud.

Dastur-faglar ikkita kategoriyaga bo'linadi: universal va ixtisoslashtirilgan skanerlar. Universal skanerlar skaner ishlashi mo'ljallangan operatsion tizim xiliga bog'liq bo'lmagan holda, viruslarning barcha xillarini qidirishga va zararsizlantirishga mo'ljallangan. Ixtisoslashtirilgan skanerlar viruslarning chegaralangan sonini yoki ularning bir sinfini, masalan, makroviruslarni zararsizlantirishga atalgan. Faqat makroviruslarga mo'ljallangan ixtisoslashtirilgan skanerlar MS WORD va Excel muhitlarida hujjat almashinish tizimini himoyalashda eng qulay va ishonchli yechim hisoblanadi.

Dastur-faglar skanerlashni «bir zumda» bajaruvchi monitoringlashning rezident vositalariga va faqat so'rov bo'yicha tizimni tekshirishni ta'minlovchi rezident bo'lmagan skanerlarga ham bo'linadi. Monitorin-

lashning rezident vositalari tizimni ishonchliroq himoyalashgi ta'minlaydi, chunki ular viruslar paydo bo'lishiga darrov reaksiya ko'rsatadi, rezident bo'lmagan skaner esa virusni aniqlash qobiliyatiga faqat navbatdagi ishga tushirilishida ega bo'ladi.

Dastur-faglarning afzalligi sifatida ularning universalligini ko'rsatish mumkin. Dastur-faglarning kamchiligi sifatida viruslarni qidirish tezligining nisbatan katta emasligini va virusga qarshi bazalarning nisbatan katta o'lchamlarini ko'rsatish mumkin. Undan tashqari, yangi viruslarning doim paydo bo'lishi sababli dastur-faglar tezdan eskiradi va ular versiyalarining muntazam yangilanishi talab etiladi.

Dastur-taftishchilar (CRC-skanerlar) viruslarni qidirishda o'zgarishlarni aniqlovchi usuldan foydalanadi. CRC-skanerlar diskdagi fayllar/tizimli sektordagilar uchun CRC-yig'indini (siklik nazorat kodini) hisoblashga asoslangan. Bu CRC-yig'indilar virusga qarshi ma'lumotlar ba'zasida fayllar uzunligi, sanalar va oxirgi modifikatsiyasi va boshqa parametrlar xususidagi qo'shimcha axborotlar bilan bir qatorda saqlanadi. CRC-skanerlar ishga tushirilishida ma'lumotlar bazasidagi ma'lumot bilan real hisoblangan qiymatlarni taqqoslaydi. Agar ma'lumotlar bazasidagi yozilgan fayl xususidagi axborot real qiymatlarga mos kelmasa, CRC-skanerlar fayl o'zgartirilganligi yoki virus bilan zaharlanganligi xususida xabar beradi. Odatda, holatlarni taqqoslash operatsion tizim yuklanishdan so'ng darhol o'tkaziladi.

CRC-skanerlarning kamchiligi sifatida ularning yangi fayllardagi viruslarni aniqlay olmasligini ko'rsatish mumkin, chunki ularning ma'lumotlar bazasida bu fayllar xususidagi axborot mavjud emas.

Dastur-blokirovka qiluvchilar virusga qarshi monitoringlash usulini amalga oshiradi. Virusga qarshi blokirovka qiluvchilar rezident dasturlar bo'lib, virus xavfi vaziyatlarini to'xtatib qolib, u xususida foydalanuvchiga xabar beradi. Virus xavfi vaziyatlariga viruslarning ko'payishi onlaridagi xarakterli chaqiriqlar kiradi. Blokirovka qiluvchilarning afzalliklari sifatida viruslar ko'payishining ilk bosqichida ularni to'xtatib qolishini ko'rsatish mumkin. Bu ayniqsa, ko'pdan beri ma'lum virusning muntazam paydo bo'lishida muhim hisoblanadi. Ammo ular fayl va disklarni davolamaydi. Blokirovka qiluvchilarning kamchiligi sifatida ular himoyasining aylanib o'tish yo'llarining mavjudligini va ularning «xiralikligini» (masalan, ular bajariluvchi fayllarning har qanday nusxalanishiga urinish xususida muntazam ogohlantiradi) ko'rsatish mumkin. Ta'kidlash lozimki, kompyuter apparat komponenti sifatida yaratilgan virusga qarshi blokirovka qiluvchilar mavjud.

Dastur-immunizatorlar – fayllar zaharlanishini oldini oluvchi dasturlar ikki xilga bo'linadi: zaharlanish xususida xabar beruvchi va virusning qandaydir xili bo'yicha zaharlanishni blokirovka qiluvchi. Birinchi xil immunizatorlar, odatda, fayl oxiriga yoziladi va fayl ishga tushirilganda bir necha marta uning o'zgarishini tekshiradi. Bunday immunizatorlar bitta jiddiy kamchilikka ega. Ular stels-virus bilan zaharlanishni aniqlay olmaydilar. Shu sababli, bu xil immunizatorlar hozirda ishlatilmaydi.

Ikkinchi xil immunizatorlar tizimni virusning ma'lum turi bilan zaharlanishdan himoyalaydi. Bu immunizator dastur yoki diskni shunday modifikatsiyalaydiki, bu modifikatsiyalash ularning ishiga ta'sir etmaydi, virus esa ularni zaharlangan deb qabul qiladi va suqilib kirmaydi. Immunizatsiyalashning bu xili universal bo'la olmaydi, chunki fayllarni barcha ma'lum viruslardan immunizatsiyalash mumkin emas. Ammo bunday immunizatorlar chala chora sifatida kompyuterni yangi noma'lum virusdan, u virusga qarshi skanerlar tomonidan aniqlanishiga qadar, ishonchli himoyalashi mumkin.

Virusga qarshi dasturning sifat mezonlari. Virusga qarshi dasturni bir necha mezonlar bo'yicha baholash mumkin. Quyida bu mezonlar muhimligi darajasi pasayishi tartibda keltirilgan:

– ishonchlilik va ishlash qulayligi foydalanuvchilardan maxsus harakatlarni talab etuvchi texnik muammolarning yo'qligi; virusga qarshi dasturning ishonchliligi eng muhim mezon hisoblanadi, chunki eng yaxshi virusga qarshi dastur skanerlash jarayonini oxirigacha olib bora olmasa, u befoyda hisoblanadi;

– viruslarni barcha tarqalgan xillarini aniqlash fazilati, ichki fayl-hujjatlar/jadvallarni (MS Office), joylashtirilgan va arxivlangan fayllarni skanerlash, virusga qarshi dasturning asosiy vazifasi-100% viruslarni aniqlash va ularni davolash;

– barcha ommaviy platformalar (DOS, Windows 95/NT, Novell NetWare, OS/2, Alpha, Linux va h.) uchun virusga qarshi dastur versiyalarining mavjudligi; so'rov bo'yicha skanerlash va «bir zumda» skanerlash rejimlarining borligi, tarmoqni ma'murlash imkoniyatli server versiyalarining mavjudligi. Virusga qarshi dasturning ko'p platformaliligi muhim mezon hisoblanadi, chunki muayyan operatsion tizimga mo'ljallangan dasturgina bu tizim funksiyalaridan to'la foydalanish mumkin. Fayllarni «bir zumda» tekshirish imkoniyati ham virusga qarshi dasturlarning yetarlicha muhim mezoni hisoblanadi. Kompyuterga keluvchi fayllarni va qo'yiluvchi disketlarni bir lahzada va majburiy

tekshirish virusdan zaharlanmaslikka 100%-li kafolat beradi. Agar virusga qarshi dasturning server variantida tarmoqni ma'murlash imkoniyati bo'lsa, uning qiymati yanada oshadi;

– ishlash tezligi. Virusga qarshi dasturning ishlash tezligi ham uning muhim mezoni hisoblanadi. Turli virusga qarshi dasturlarda virusni qidirishning har xil algoritmlaridan foydalaniladi. Bir algoritm tezkor va sifatli bo'lsa, ikkinchisi sust va sifati past bo'lishi mumkin.

Himoyaning profilaktika choralari. Har bir kompyuterda viruslar bilan zaharlangan fayllar va disklarni o'z vaqtida aniqlash, aniqlangan viruslarni tamomila yo'qotish virus epidemiyasining boshqa kompyuterlarga tarqalishining oldini oladi. Har qanday virusni aniqlashni va yo'q qilishni kafolatlovchi mutlaq ishonchli dasturlar mavjud emas. Kompyuter viruslari bilan kurashishning muhim usuli o'z vaqtidagi profilaktika hisoblanadi.

Virusdan zaharlanish ehtimolligini jiddiy kamaytirish va disklardagi axborotni ishonchli saqlanishini ta'minlash uchun quyidagi profilaktika choralarini bajarish lozim:

– faqat qonuniy, rasmiy yo'l bilan olingan dasturiy ta'minotdan foydalanish;

– kompyuterni zamonaviy virusga qarshi dasturlar bilan ta'minlash va ular versiyalarini doimo yangilash;

– boshqa kompyuterlarda disketda yozilgan axborotni o'qishdan odin bu disketda virus borligini o'zining kompyuteridagi virusga qarshi dastur yordamida doimo tekshirish;

– axborotni ikkilash. Avvalo dasturiy ta'minotning distributiv eltuvchilarini saqlashga va ishchi axborotni saqlanishiga e'tibor berish;

– kompyuter tarmoqlaridan olinuvchi barcha bajariluvchi fayllarni nazoratlashda virusga qarshi dasturdan foydalanish;

– kompyuterni yuklama viruslardan zaharlanishiga yo'l qo'ymaslik uchun, operatsion tizim ishga tushirilganida yoki qayta yuklanishida diskovod cho'ntagida disketani qoldirmaslik.

Virusga qarshi dasturlarning har biri o'zining afzalliklariga va kamchiliklariga ega. Faqat virusga qarshi dasturlarning bir necha xilini kompleks ishlatilishi maqbul natijaga olib kelishi mumkin.

Quyida virusdan zaharlanish profilaktikasiga, viruslarni aniqlash va yo'qotishga mo'ljallangan ba'zi dasturiy komplekslar tavsiflangan.

AVP (Antivirus Kasperskogo Personal) – Rossiyaning virusga qarshi paketi. Paket tarkibiga quyidagilar kiradi:

– Office Guard – blokirovka qiluvchi, makrovirusdan 100% himoyala-nishni ta'minlaydi;

– Inspector – taftishchi, kompyuterdagi barcha o'zgarishlarni kuzatadi, virus faolligi aniqlanganida diskning asl nusxasini tiklashga va zarar keltiruvchi kodlarni chiqarib tashlashga imkon beradi;

– Monitor – viruslarni ushlab qoluvchi, kompyuter xotirasida doimo hozir bo'lib, fayllar ishga tushirilganida, yaratilishida yoki nusxalanishida ularni virusga qarshi tekshiradi;

– Scanner – virusga qarshi modul, lokal va tarmoq disklar tarkibini keng ko'lamli tekshirish imkonini beradi. Skanerni qo'l yordamida yoki berilgan vaqtda avtomatik tarzda ishga tushirish mumkin.

Paket yordamida elektron pochtani virusga qarshi filtrlash va pochta korrespondensiyasini kompleks tekshirish amalga oshiriladi. Virusga qarshi bazani yangilash Internet orqali bajariladi.

Dr.Web – Rossiyaning virusga qarshi ommaviy dasturi, Windows 9x/NT/2000/XP uchun mo'ljallangan bo'lib, faylli yuklama va fayl-yuklama viruslarni qidiradi va zararsizlantiradi. Dastur tarkibida rezident qorovul SplDer Guard, Internet orqali virus bazalarini yangilashning avtomatik tizimi va avtomatik tekshirish jadvalini rejalashtiruvchi mavjud. Pochta fayllarini tekshirish amalga oshirilgan.

Dr.Web da ishlatiluvchi algoritmlar haqida ma'lum bo'lgan barcha virus xillarini aniqlashga imkon beradi. Dr.Web dasturining muhim xususiyati – oddiy signaturli qidirish natija bermaydigan murakkab shifrlangan va polimorf viruslarni aniqlash imkoniyatidir.

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

Symantec mahsulotidan ishchi joylarining umumiy soni 100 va undan ortiq bo'lganida va bo'lmaganda bitta Windows NT/2000/NetWare serveri mavjudligida foydalanish maqsadga muvofiq hisoblanadi. Ushbu paketning bashqalardan ajralib turadigan xususiyati quyidagilar:

– boshqarishning ierarxik modeli;

– yangi virus paydo bo'lishiga reaksiya qilish mexanizmining mavjudligi.

AntiVir Personal Edition – virusga qarshi dastur AVP, Dr.Web va h.lar imkoniyatlaridek imkoniyatlarga ega. Dastur komplektiga quyidagilar kiradi:

– disklarni skanerlovchi;
– rezident qorovul;
– boshqarish dasturi;
– rejalashtiruvchi.

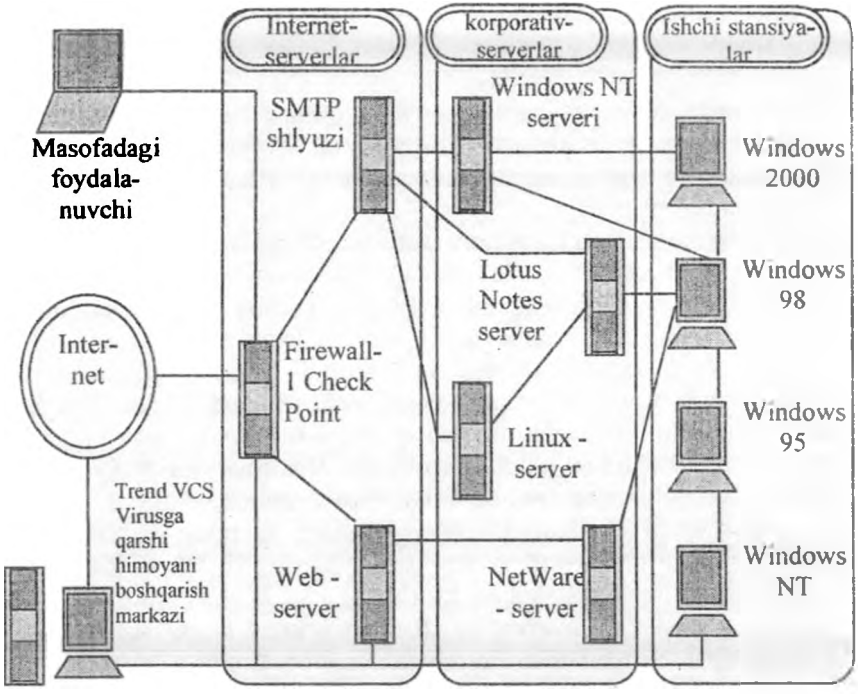
Dastur Internet dan yuklanuvchi fayllarni skanerlaydi. Internet orqali yangilanishiarni avtomatik tarzda tekshirish va yuklash funksiyasi ham mavjud. Dastur xotirani, yuklanish sektorini tekshirishda va unda viruslar bo'yicha keng ko'lamdagi ma'lumotnoma mavjud.

9.6. Virusga qarshi himoya tizimini qurish

Hozirda o'rtacha kompaniyaning korporativ kompyuter tarmog'i tarkibida o'nlab va yuzlab ishchi stansiyalari, o'nlab serverlar, telekommunikatsiyaning turli faol va passiv asbob-uskunalari mavjud bo'lgan yetarlicha murakkab tuzilmaga ega (10.6-rasm).

Korporativ tarmoqdan foydalanuvchilar tarmoqqa viruslarning suqilib kirish fayllari bilan doimo to'qnashadilar. Internet/intranet korporativ tizimlariga virus hujumlari muntazam bo'lib turadi, foydalanuvchi ishchi stansiyasining zaharlangan axborot eltuvchisi tomonidan zaharlanishi esa odat tusini olgan.

Korporativ tarmoq viruslar va boshqa zarar keltiruvchi dasturlar hujumlariga duchor bo'lganida tarmoqning virusga qarshi himoyasi ko'pincha virusga qarshi lokal dasturiy ta'minot yordamida, skanerlash va qator ishchi stansiyalarni davolash bilan tugaydi va himoya ta'minlanadi deb hisoblanadi. Aslida muammoning bunday lokalizatsiyalash minimal chora hisoblanadi va korporativ tarmoqning keyingi barqaror ishlashini kafolatlamaydi. Boshqacha aytganda, virusga qarshi lokal yechimlarning ishlatilishi korxonani virusdan samarali himoyalash uchun zaruriy, ammo yetarli vosita hisoblanmaydi.



9.6-rasm. Korporativ tarmoqning namunaviy arxitekturasi.

Virusga qarshi himoyaning samarali korporativ tizimi-«mijoz-server» texnologiyasi bo'yicha amalga oshirilgan, tarmoqdagi har qanday shubhali harakatni sezgirlik bilan fahmlab oluvchi, teskari bog'lanishli moslanuv-chan tizimdir. Bunday tizim korporativ tarmoqning ichki tuzilmasi doirasida viruslarning va boshqa g'anim dasturlarning tarqalishiga yo'l qo'ymaydi. Virusga qarshi himoyaning samarali korporativ tizimi turli virus hujumlarini, ma'lumlarini, ham noma'lumlarini, ular namoyon bo'lishining dastlabki bosqichida, aniqlaydi va betarflashtiradi.

Albatta, turli vaziyatlar bo'lishi mumkin, masalan, masofadan foydalanuvchining zaharlangan kompyuterini korporativ serverga ulaganda yoki makroviruslar bo'lgan WORD yoki Excel faylli disketlardan ish joylarida foydalanishda tarmoq zaharlanishi mumkin. Ammo sifatli qurilgan virusga qarshi himoyaning korporativ tizimi uchun bu jiddiy emas, chunki birinchidan, zaharlanishning ko'rsatilgan holatlari kam-

dan-kam uchraydi, ikkinchidan, viruslar vaqtida aniqlanadi va betaraflashtiriladi. Natijada, ularning ko'payishiga va korporativ tarmoq doirasida tarqalishiga yo'l qo'yilmaydi.

Ulanadigan ishchi stansiyalari soni oshgan sari korporativ tarmoqning xizmat ko'rsatish narxi osha boradi. Korporativ tarmoqni viruslardan himoyalash xarajatlari korxona umumiy xarajatlari ro'yxatida oxirgi bandni egallamaydi.

Ushbu xarajatlarni korporativ tarmoqni virusga qarshi himoyalashni vaqtning real masshtabida markazlashtirilgan boshqarish orqali optimallashtirish va kamaytirish mumkin. Bunday yechim korxona tarmog'i ma'murlariga virusni barcha suqilib kirish nuqtalarini boshqarishning yagona konsoli orqali kuzatishga va korporativ tarmoqdagi barcha virusga qarshi vositalarni samarali boshqarishga imkon beradi. Virusga qarshi himoyani markazlashtirilgan boshqarish maqsadi juda oddiy – viruslarning barcha suqilib kirish nuqtalarini blokirovka qilish. Quyidagi suqilib kirishlarni va zaxarlanishlarni ko'rsatish mumkin:

– tashuvchi manbalardan (floppi-disklar, kompakt-disklar, Zip, Jazz, Floptical va h.) oxirgi zaharlangan fayllardan foydalanishda ishchi stansiyalarga viruslarning suqilib kirishi;

–Web yoki FTP Internet orqali olingan lokal ishchi stansiyasida saqlangan zaharlangan tekin dasturiy ta'minot yordamida zaharlanish;

– masofadagi yoki mobil foydalanuvchilarning zaharlangan ishchi stansiyalari korporativ tarmoqqa ulanganida viruslarning suqilib kirishi;

– korporativ tarmoqqa ulangan masofadagi serverdagi viruslar bilan zaharlanish.

– ilovalarida makroviruslar bilan zaharlangan Excel va Word fayllar bo'lgan elektron pochtaning tarqalishi.

Viruslardan va boshqa zarar keltiruvchi dasturlardan himoyalovchi korporativ tizimni qurish quyidagi bosqichlarni o'z ichiga oladi.

Birinchi bosqichda himoyalanuvchi tarmoqning o'ziga xos xususiyatlari aniqlanadi va bir necha virusga qarshi himoya variantlari tanlanadi va asoslanadi. Bu bosqichda quyidagilar bajariladi:

– kompyuter tizimi va virusga qarshi himoya vositalarining auditi;

– axborot tizimini tekshirish va *kartirlash*;

– viruslarning suqilib kirishi bilan bog'liq tahdidlarning amalga oshirish ssenariysini tahlillash.

Natijada, virusga qarshi himoyaning umumiy holati baholanadi.

Ikkinchi bosqichda virusga qarshi xavfsizlik siyosati ishlab chiqiladi. Bu bosqichda quyidagilar bajariladi:

– axborot resurslarini turkumlashning turi;

– virusga qarshi xavfsizlikni ta'minlovchi kuchlarni yaratish- vakolatlarni taqsimlash;

– virusga qarshi xavfsizlikni tashkiliy-huquqiy madadlash;

– virusga qarshi xavfsizlik instrumentlariga talablarni aniqlash;

– virusga qarshi xavfsizlikni ta'minlash xarajatlarini hisoblash.

Natijada, korxonaning virusga qarshi xavfsizlik siyosati ishlab chiqiladi.

Uchinchi bosqichda dasturiy vositalari, axborot resurslarini inventarizatsiyalash va monitoringini avtomatlashtirish vositalari tanlanadi. Virusga qarshi xavfsizlikni ta'minlash bo'yicha tashkiliy tadbirlar ro'yxati ishlab chiqiladi.

Natijada, korxonaning virusga qarshi xavfsizligini ta'minlovchi reja ishlab chiqiladi.

To'rtinchi bosqichda virusga qarshi tanlangan va tasdiqlangan xavfsizlik rejasi amalga oshiriladi. Bu bosqichda virusga qarshi vositalar yetkazib beriladi, joriy etiladi va madadlanadi.

Natijada, korporativ virusga qarshi himoyalashning samarali tizimi yaratilishiga imkon tug'iladi.

X bob. MA'LUMOTLARNI UZATISH TARMOG'IDA AXBOROTNI HIMOYALASH

10.1. Ma'lumotlarni uzatish tarmoqlarida axborot himoyasini ta'minlash

Ma'lumotlarni uzatish tarmoqlarida axborot himoyasini ta'minlash masalasi ma'lumotlar uzatish tarmog'ining muayyan arxitekturasini amalga oshiruvchi va uning barqaror ishlashini ta'minlovchi apparat-dasturiy vositalari bilan bog'liq holda yechilishi lozim.

Ma'lumotlarni uzatish tarmoqlarida axborot xavfsizligini ta'minlashga quyidagi talablar qo'yiladi:

– ma'lumotlarni uzatish tarmoqlarida axborot xavfsizligiga bo'ladigan ma'lum tahdidlardan himoyalash xizmati va mexanizmlarini belgilovchi *funksional talablar*;

– axborot xavfsizligiga bo'ladigan ma'lum tahdidlardan himoyalash mexanizmini ma'lumotlarni uzatish tarmog'i arxitekturasiga qay tarzda joriy etilishi lozimligini belgilovchi *arxitekturaviy talablar*;

– boshqarishning qanday funksiyalari ishlab chiqilishi va ular qay tarzda ma'lumotlarni uzatish tarmog'iga joriy etilishini belgilovchi *boshqarish (ma'murlash) talablari.*

Funksional talablar. Ma'lumotlarni uzatish tarmog'i komponentlariga va arxitekturasiga real ta'sir etuvchi umumiy funksional talablar quyidagilar:

– *foydalanuvchini autentifikatsiyalash.* Ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlovchi tizim axborotni (ma'lumotlarni) uzatish jarayonida ishtirok etuvchi komponentining (obyekt, subyekt va foydalanuvchining) haqiqiyligini aniqlash imkoniyatini ta'minlashi lozim;

– *nazoratlanuvchi foydalanish.* Ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlovchi tizim tarmoq subyektlari va foydalanuvchilarining ruxsat etilmagan axborot resurslaridan foydalana olmasliklarini kafolatlashi lozim;

– *konfidensiallikni ta'minlash.* Konfidensiallikni ta'minlash xizmati asosan ma'lumotlarni uzatish tarmog'ini axborot muhitini ochish, ax-

berotdan ruxsatsiz foydalanish va o'g'irlash imkoniyatlaridan himoyalash uchun zarur hisoblanadi;

– *ma'lumotlar yaxlitligini ta'minlash.* Ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlovchi tizim tarkibida foydalanuvchi va boshqarish axboroti bo'lgan ma'lumotlarning saqlanish va uzatilish yaxlitligini kafolatlashi lozim. Ma'lumotlarning buzilishi, soxtalashtirilishi, kechiktirilishi, ruxsatsiz qaytalanishi axborot uzatilishininig blokirovka qilinishiga olib kelishi mumkin;

– *qat'iy hisob-kitob.* Ma'lumotlarni uzatish tarmog'i resurslaridan foydalanuvchi har qanday subyekt bajargan har qanday amallari uchun javob berishi lozim. Ma'lumotlarni uzatish tarmog'i ustida qilingan barcha harakatlar va tarmoqda sodir bo'lgan barcha hodisalar xususidagi axborotning saqlanish imkoniyati ta`minlanishi lozim;

– *xavfni bildiruvchi signalni generatsiyalash.* Ma'lumotlarni uzatish tarmog'i tarmoq axborot xavfsizligi obyektlari tomonidan xavfsizlikning buzilishi xususidagi signalni generatsiyalash imkonini ta'minlashi lozim;

– *audit.* Audit tizimni boshqarishning samaradorligini baholash hamda axborot xavfsizligining buzilishini aniqlash maqsadida tizimli yozuvlarni va amallarni mustaqil tahlillash va tadqiqlash sifatida ko'rilishi lozim;

– *tiklash.* Ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlash tizimi xavfsizlikning buzilishini tiklash qobiliyatiga ega bo'lishi lozim. Har doim, qachon axborot xavfsizligini buzishga urinish sodir bo'lganida, tizim ushbu urinish xususidagi axborotni shunday ishlashi lozimki, ushbu urinish ma'lumotlarni uzatish tarmog'ining o'tkazish qobiliyatini va foydalanuvchanligini jiddiy pasayishiga olib kelmasin;

– *moslanuvchanlik.* Ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlash tizimiga qo'yiladigan muhim konseptual talab– moslanuvchanlik talabi, ya'ni aloqa tarmog'ining tuzilmasi. texnologiyasi va ishlash sharoiti o'zgarganida moslashuv qobiliyati talabidir.

Arxitekturaviy talablar. Ma`lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlash tizimi axborot xavfsizligining turli siyosatini madadlashi, ya'ni moslanuvchan bo'lishi lozim. Tizimga quyidagi asosiy xizmatlar kiritilishi mumkin:

– shifrlash kalitlarini va parollarni shakllantirish, saqlash va taqsimlash xizmati;

– shifrlash xizmati;

– foydalanuvchilarni va xabarlarni autentifikatsiyalash xizmati;
– foydalanishni boshqarish xizmati;
– xabarlar yaxlitligini ta'minlash xizmati;
– foydalanuvchanlikni ta'minlash xizmati;
– yetkazilganlikni tasdiqlash xizmati;
– rad qilmaslik xizmati;
– qo'shimcha trafikni shakllantirish xizmati;
– ma'murlash xizmati.

Bu xizmatlarning har biri axborot xavfsizligini ta'minlash bo'yicha masalalarni mustaqil tarzda u yoki bu himoya mexanizmlaridan foydalanib yechilishi mumkin. Bunda himoyaning bitta mexanizmi axborot xavfsizligining turli xizmatlarida qo'llanilishi mumkin.

Boshqarish (ma'murlash) talablari. Ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ma'murlash xizmati himoyaning texnik vositalarini to'ldiruvchi himoya choralarining ma'lum kompleksini o'z ichiga oladi. Bu himoya choralari buzg'unchining tarmoq axborot xavfsizligiga tahdidni kuchaytirishga qaratilgan u yoki bu ta'sirni o'tkazishini qiyinlashtirish maqsadida mavjud himoya tizimiga tezkor tarzda o'zgartirishlar kiritishga imkon yaratadi.

Ma'murlash xizmatining asosiy vazifalari quyidagilar:
– himoya xizmati va mexanizmiga zarur axborotni tarqatish;
– himoya xizmati va mexanizmining ishlashi xususidagi axborotni yig'ish va tahlillash;
– himoyalanuvchi obyektlarni aniqlash;
– xizmat funksiyalarini samarali amalga oshirish maqsadida himoya mexanizmlarini kombinatsiyalash;
– ma'lumotlarni uzatish tarmog'ining ishonchli va barqaror ishlashini ta'minlash xizmatlariga javobgar boshqa ma'murlar bilan o'zaro aloqa;
– ma'lumotlarni uzatuvchi tarmoqning buzilgan ishlash jarayonini tiklash.

Xavfsizlik ma'muri ma'murlash xizmatining muhim elementi hisoblanadi. Axborot xavfsizligining har qanday vositalaridan foydalanilmasin, ma'lumotlarni uzatish tarmog'ida axborot xavfsizligini ta'minlash sifati ma'murning qobiliyatiga, uning tirishishiga, texnik jihozlanganligiga bog'liq.

Ta'kidlash lozimki, birorta ham real himoyalangan ma'lumotlarni uzatish tarmog'i mutlaq himoyalangan bo'lmaydi. Shunga qaramasdan himoyaning adekvat choralari buzg'unchi ta'siri samarasini (zarar kelti-

rish xarajatining kutilayotgan zarar o'lchamiga nisbatini) anchagina pasaytiradi.

10.2. Aloqa kanallarida ma'lumotlarni himoyalash usullari

Ma'lumotlarni uzatishni himoyalash masalasini yechish usullarining uchta asosiy guruhi mavjud: kanalga mo'ljallangan himoyalash usullari, chekkalararo himoyalash usullari va ulanishga mo'ljallangan himoyalash usullari. Birinchisi har bir kanal uchun mustaqil ravishda ma'lumotlar oqimini himoyalashni ta'minlasa, ikkinchisi har bir xabarni, uni manbadan adresatgacha uzatishda umumiy himoyalashni ta'minlaydi. Uchinchi usul ikkinchi usulning bir turi hisoblanadi.

Kanalga mo'ljallangan usullar manba va adresatga bog'liq bo'lmagan holda, alohida uzellar orasidagi alohida aloqa kanali bo'yicha uzatilayotgan xabarlar oqimini himoyalashni ta'minlaydi. Bu xil himoyani ta'minlashda buzg'unchining uzelga (paketni kommutatsiyalovchi markazga) qaraganda kanalga ta'sir etish qulayligi faraz qilinadi. Undan tashqari, ma'lumotlarni uzatish tarmog'idagi uzellarni foydalanuvchi terminallarini himoyalagandek himoyalash mumkin emas yoki iqtisod nuqtai nazaridan foydasiz. Ushbu guruh usullarining kamchiligi–qism tarmoq uzellaridan birining ochilishi tarmoq orqali o'tayotgan xabarlar oqimining talaygina qismini ochilishiga olib kelishi mumkin.

Terminallar va tarmoqlar o'rtasidagi aloqa kanallarini kanalga mo'ljallangan himoyalash xarajatlari bevosita daxldor taraflar tomonidan qoplansada, ma'lumotlarni uzatish qism tarmog'i ichidagi kanalga mo'ljallangan himoyalash usullarining umumiy narxi qism tarmoqdan foydalanuvchilarning barchasi o'rtasida hisoblab chiqilishi mumkin.

Chekkalararo himoyalash usullari xabarlarni manba uzellari va qabul qiluvchi orasida uzatish jarayonida shunday himoyalaydiki, manba va adresat orasidagi aloqa kanallaridan birining ochilishi xabarlar oqimining ochi-lishiga olib kelmaydi. Ushbu usullarning asosiy afzalligi – ulardan foydalanish masalasi alohida foydalanuvchilar orasida, boshqa foydalanuv-chilarni jalb etmasdan, yechilishi mumkin.

Ulanishga mo'ljallangan usullar. Aksariyat qo'llanish sohalarida ma'lumotlarni uzatish tarmog'ini manbadan adresatgacha ulanishni yoki virtual kanalni o'rnatish uchun foydalanuvchiga taqdim etiluvchi muhit sifatida tasavvur etish mumkin. Bunday tasavvur etishda himoyaning ulanishga mo'ljallanishi faraz qilinadi, ya'ni har bir ulanish yoki virtual kanal alohida himoyalanadi. Shunday qilib, ulanishga mo'ljallangan

usullar chekkalararo himoyalash usullarining bir turi hisoblanadi. Ulanishga mo'ljallangan usullar turli sharoitlarda umumiy himoyaning yuqori darajasini ta'minlaydi va himoyaga qo'yiladigan talablar xususidagi foydalanuvchining idrokiga mos keladi. Chunki, ulanishga mo'ljallangan axborot konfidensialligini himoyalash usullari asbob-uskunani himoyalashni, masalan, faqat xabarlar manbaida va qabul qiluvchida axborotdan ruxsatsiz foydalanishdan himoyalashni ko'zda tutadi. Ayni vaqtda himoyalashning kanalga mo'ljallangan usullari ruxsatsiz foydalanishdan himoyalashning ma'lumotlarni uzatish tarmog'idagi har bir uzeli tomonidan ta'minlanishini talab etishi mumkin. Ammo ba'zida ikkala usulni qo'llaganda himoyalashning tejamli darajasiga erishiladi.

Ma'lumotlarni uzatishni himoyalashning u yoki bu usulidan foydala-nishdagi asosiy vazifalar quyidagilar:

– xabarlar mazmunining fosh qilinishini oldini olish;
– xabarlar oqimining tahlillanishini oldini olish;
– xabarlar oqimi haqiqiyligini buzilganligini aniqlash;
– yolg'on ulanishni aniqlash.

Axborot tizimlari yoki ma'lumotlarni uzatish tarmoqlarida axborot xavfsizligini ta'minlash maqsadida ma'lumotlarni uzatishni himoyalash usullaridan nafaqat buzg'unchi ta'siri oqibatlarini aniqlashni, balki, agar oqibatlar vaqtincha xarakterga ega bo'lganida, uzilgan (buzilgan) uzatish jarayonini avtomatik tarzda tiklashni talab etish kerak.

Hozirda yuqorida keltirilgan vazifalarning bajarilishini ta'minlovchi himoyalashning standartlashtirilgan mexanizmlari mavjud emas. Har bir muayyan holda ma'lumotlarni uzatish xavfsizligi masalalari axborotlarni kriptografik o'zgartirish usullari, axborotlarni halallarga bardosh kodlash usullari, xabarlarning haqiqiyligini ta'minlovchi usullar, tizimlar ishlashining ishonchliligini, yashovchanligini va barqarorligini ta'minlovchi usullarga asoslangan himoyalashning turli mexanizmlarini birgalikda ishlatish orqali hal etiladi.

Xabarlar mazmunining fosh qilinishini oldini olishda himoyalashning kanalga mo'ljallangan hamda ulanishga mo'ljallangan usullaridan foydalanish mumkin.

Yuqorida aytib o'tilganidek, kanalli shifrlash aloqa tarmog'ining har bir kanalida mustaqil tarzda bajarilishi mumkin. Kanalli shifrlashda, odatda, oqimli shifrlash ishlatiladi va uzellar orasida shifrlangan matn bitlarining uzluksiz oqimi madadlanadi. Tarmoqlarda kommutatsiyalash (marshrutlash) vazifalari faqat uzellarda bajarilishi sababli, aloqa

kanalida paketning sarlavhalari bilan birga axborot qismini ham shifrlash mumkin.

Ammo ma'lumotlar faqat kanalda (kanallar orqali ulangan uzellarda emas) shifrlanishi sababli, barcha oraliq uzellar himoyalanishi lozim. Buning ustiga uzellarni nafaqat fizik himoyalanishi, balki bu uzellarning apparat-dasturiy vositalari tomonidan uzellar orqali o'tuvchi har bir ulanishdagi axborotni yakkalashi kafolatlanishi zarur.

Chekkalararo shifrlashda marshrutizatorda ishlanuvchi har bir xabar (sarlavhaning ba'zi ma'lumotlari bundan istisno) yo'l boshida shifrlanadi va belgilangan joyga yetmaguncha rasshifrovka qilinmaydi. Har bir ulanish uchun o'zining kaliti ishlatilishi mumkin.

Xabarlar oqimini tahlillanishidan himoyalash, odatda, turli sinflarga mansub xabarlar uzunligi va chastotasining qiymatlarini, manba adreslarini va xabarlar oqimi adreslarini berkitishga yo'naltirilgan. Agar kanalli shifrlash ishlatilsa, uzellar orasida ma'lumotlar uzatilganida shifrlangan matn bitlarining uzluksiz oqimi o'rnatilishi mumkin. Bu esa chastota qiymatlarini va ulanishning davomligini berkitishga imkon beradi. Bunday yondashishda tarmoqning samarali o'tkazish qobiliyati pasaymaydi, chunki hech qanday qo'shimcha axborot talab etilmaydi. Ammo uzel ochilsa, bu uzel orqali o'tuvchi xabarlarning butun oqimi tahlillash mavzuiga aylanadi.

Himoyalashning chekkalararo usullaridan foydalanilganda uzatiluvchi xabarlarning haqiqiy chastotasi va uzunligini berkitish uchun turli uzunlikdagi «bo'sh» xabarlar generatsiyalanishi, haqiqiy xabar esa bo'sh simvollar bilan to'ldirilishi mumkin. Qabul qiluvchi begona kengayishlarni va «bo'sh» xabarlarni aniqlashda xabardagi shifrlangan hoshiyadan foydalanishi mumkin.

Aksariyat ilovalarda oqimni tahlillash orqali axborotni chiqarib olish ikkinchi darajali xavf sifatida talqin qilinishi va maxsus qarshi choralar ko'rilmasligi mumkin.

Xabarlar sathida haqiqiylikni tasdiqlash xabarlarni kechiktirish, ularni yo'q qilish, almashtirib qo'yish yoki qaytalash kabi ta'sirlardan himoyalashni ta'minlamaydi. Shunga qaramasdan, bunday tahdidlardan himoyalashning turli usullari mavjud:

– xabarlarni nomerlash. Har bir xabarni nomerlab, nomerni xabar tarkibiga kiritib, demak, shifrlab uzatish orqali xabarning haqiqiyligiga ishonch hosil qilish mumkin. Tarmoqning har bir obyekti u bilan aloqada bo'luvchi obyektlarning har biri uchun alohida sanagichlarga

(schyotchiklarga) ega bo'lishi lozimligi bu muolajaning kamchiligi hisoblanadi.

– vaqtni belgilash. Qabul qiluvchi har bir uzatilgan xabarning kuni va vaqtini bilgan holda uning adekvatligini tekshirishi mumkin. Bunday belgilashning intervali va aniqligi shunday tanlanishi lozimki, bir tomondan xatoli xabarlar, ikkinchi tomondan. uzatish kanaliga xos bo'lgan tabiiy kechikish aniqlanishi mumkin bo'lsin.

– tasodifiy sonlardan foydalanish. Vaqtning real masshtabida ikki tomonlama aloqa ishlatilganida qabul qiluvchi jo'natuvchiga xabar jo'natilmasdan oldin tasodifiy son yuboradi. Jo'natuvchi bu sonni shifrlangan xabarga shunday o'rnatadiki, qabul qiluvchi uni tekshirishi mumkin bo'lsin. Shu tarzda yolg'on xabarlar chiqarib tashlanishi mumkin.

– har bir ulanish uchun alohida kalitdan foydalanish. Natijada, olingan xabarda ulanishning oshkor bo'lmagan identifikatsiyalanishi amalga oshiriladi.

Xabarlar oqimi uzilishini aniqlash masalasini «so'rov-javob» protokolidan foydalanib hal etish mumkin. Bunday protokolning tarkibida ulanishning vaqtinchalik yaxlitligini va maqomini o'rnatuvchi xabarlar juftini almashish muolajasi bo'ladi. Ulanishning har bir chekkasida «xabar-so'rov» uzatishni vaqti-vaqti bilan ishga tushiruvchi taymer ishlatiladi va «xabar-so'rov» uzatishga ulanishning boshqa chekkasidan javob olinadi. Har bir «xabar-so'rov»da peredatchik axboroti mavjud bo'lib, bu axborot ulanishdagi xabar yo'qotilishini aniqlashga imkon beradi.

Yolg'on ulanishni aniqlash uchun har bir chekkadagi «ulanishga javobgar»ning haqiqiyligini va ulanishning vaqtinchalik yaxlitligini tekshirishga ishonchli asosni ta'minlovchi qarshi choralar ishlab chiqilgan.

Ulanish boshlanishi vaqtida har bir chekkada ulanishga javobgarning haqiqiyligini tekshirish keyingi xabarlar oqimining haqiqiyligi xususida qaror qabul qilishga asos hisoblanadi.

Ulanishning vaqtinchalik yaxlitligini tekshirish buzg'unchining oldingi qonuniy ulanish yozuvidan foydalanib, foydalanuvchini xato fikrga solishidan yoki adashtirishidan, ma'lumotlar uzatish jarayonini buzishidan himoyalaydi.

XI bob. SIMSIZ ALOQA TIZIMLARIDA AXBOROT HIMOYASI

11.1. Simsiz tarmoq konsepsiyasi va tuzilmasi

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

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

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

– simsiz shaxsiy tarmoq (Wireless personal-area network, PAN);

– simsiz lokal tarmoq (Wireless local-area network, LAN);

– simsiz regional tarmoq (Wireless metropolitan-area network, MAN);

– simsiz global tarmoq (Wireless Wide-area network, WAN).

Jadvalda ushbu tarmoqlarning qisqacha tavsifi keltirilgan.

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

Bunday tarmoq, masalan, foydalanuvchi PDA sida va uning shaxsiy kompyuterida yoki noutbukida ma'lumotlarni simsiz sinxronlashni ta'minlashi mumkin. Xuddi shu tariqa priner bilan simsiz ulanish

ta'minlanadi. Kompyuterni tashqi qurilmalar bilan ulovchi simlar chigalliklarining yo'qolishi yetarlicha jiddiy afzallik bo'lib, buning evaziga tashqi qurilmalarning boshlang'ich o'rnatilishi va keyingi, zaruriyat tug'ilganda, joyining o'zgartirilishi anchagina osonlashadi.

jadval

Tarmoq xili	Ta'sir doirasi	Xarakteristikasi	Standartlar	Qo'llanish sohasi
Shaxsiy simsiz tarmoqlar	Foydalanuvchidan bevosita yaqinlikda	O'rtacha	Bluetooth, IEEE, 802.15, IRDA	Tashqi qurilmalar kabellarining o'rnida
Lokal simsiz tarmoqlar	Binolar va kampuslar doirasida	Yuqori	IEEE 802.15, Wi-Fi, HiperLAN	Simli tarmoqlarni mobil kengaytirish
Regional simsiz tarmoqlar	Shahar doirasida	Yuqori	Patentli, IEEE 802.16, WIMAX	Binolar va korxonalar va Internet orasida belgilangan simsiz bog'lanish
Global simsiz tarmoqlar	Butun dunyo bo'yicha	Past	CDPD va 2, 2.5 va 3-avlod uyali telefon orqali tizimlar	Binodan tashqarida Internet dan mobil foydalanish

Simsiz shaxsiy tarmoqlarning aksariyat uzatuvchi-qabul qiluvchilarning (transceiver) kam quvvat iste'mol qilishi va ixchamligi mikroprotsessorlar bilan ta'minlangan, katta bo'lmagan foydalanuvchi qurilmalarini samarali madadlashga hamda kompyuter qurilmasini uzoq vaqt mobaynida bitta batareyada (yoki akkumulatorda) ishlashiga imkon beradi. Undan tashqari, kam quvvat iste'mol qilinishi simsiz shaxsiy tarmoqlarni uyali telefonlarga, PDA larga va naushniklarga tatbiq etishga sabab bo'ldi.

Simsiz shaxsiy tarmoqlar Internet ga va ilovalarga ulanishdan birgalikda foydalanish maqsadida noutbuklar va shaxsiy kompyuterlarning

o'zaro aloqasini ta'minlashi mumkin. Bu ta'sir doirasi bitta xona bilan chegaralangan tarmoqlarga to'g'ri keladi.

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

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

Simsiz Internet xizmatlari bilan ta'minlovchilar (Wireless Internet Service Provider, WISP) uyda foydalanuvchilar va kompaniyalar uchun doimiy simsiz ulanishlarni ta'minlash maqsadida shaharlarda va qishloq joylarda simsiz regional tarmoqlarni mijozlar ixtiyoriga taqdim etadi. Bunday tarmoqlar, ko'pincha simli ulanishlarni yotqizish bilan bog'liq chegaralanishlarga ega bo'lgan oddiy simli ulanishlarga nisbatan samarali hisoblanadi.

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

Simsiz global tarmoqlar mobil ilovalarning, ulardan mamlakat yoki hatto kontinent masshtabida foydalanishni ta'minlash bilan ishlanishini ta'minlaydi. Iqtisodiy mulohazalarga tayangan holda, telekommunikatsiya kompaniyalari ko'pgina foydalanuvchilar uchun uzoq masofadan ulanishni ta'minlovchi simsiz global tarmoqning nisbatan qimmat in-

fratuzilmasini yaratadilar. Bunday yechimning xarajati barcha foydalanuvchilar o'rtasida taqsimlanadi, natijada, abonent to'lovi unchalik yuqori bo'lmaydi.

Ko'pgina telekommunikatsiya kompaniyalarining kooperatsiyasi tufayli simsiz global tarmoqlarining ta'sir doirasi chegaralanmagan. Telekommunikatsiya xizmatini ta'minlovchilarning biriga to'lab, simsiz global tarmoq orqali dunyoning har qanday nuqtasidan qator Internet xizmatidan foydalanish mumkin.

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

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

Simsiz global tarmoqlar texnologiyasini tatbiq etishdagi muammolardan biri uning bino ichidagi foydalanuvchilar uchun bog'lanishni ta'minlay olmasligi. Chunki bunday tarmoq infratuzilmalari bino tashqarisida joylashgan va radiosignallar binoda aytarlicha susayadi. Simsiz global tarmoqlarni bino ichiga o'rnatilishi esa qimmatga tushadi va texnik nuqtai nazaridan asoslanmagan.

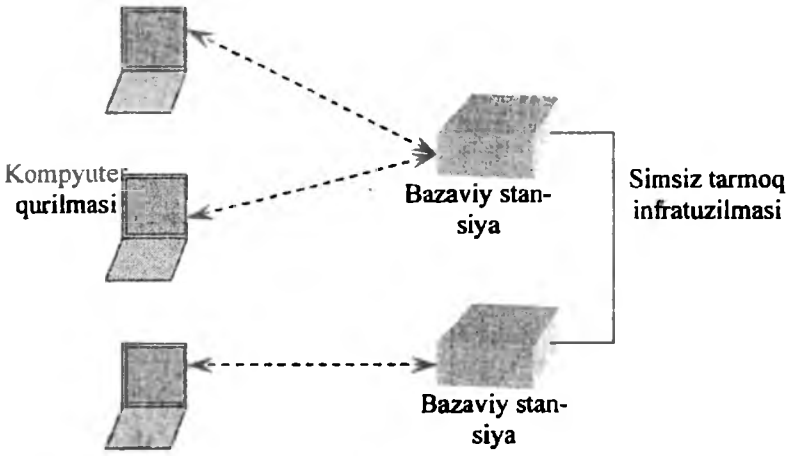
Simsiz shaxsiy, lokal, regional va global tarmoqlar bir-birini to'ldiruvchi bo'lib, turli talablarni qondiradi. Ammo ba'zida bir tarmoqni ikkinchisidan farqlab bo'lmaydi. Masalan, bino ichidagi simsiz lokal tarmoq foydalanuvchi PDAsi bilan shaxsiy kompyuterini simsiz shaxsiy tarmoq kabi ulashni ta'minlashi mumkin. Turli simsiz tarmoqlar orasidagi farqni aniqlashda ularda ishlatiladigan texnologiyalar va standartlardan foydalanishadi (jadvalga qaralsin).

Agar foydalanuvchi nuqtai nazaridan istiqbol xususida so'z yuritilsa, simsiz tarmoqlar orasida chegaraning yo'qolishi shart. Turli xil simsiz tarmoq ishini madadlovchi kompyuter qurilmalari tarmog'i interfeysining platalari paydo bo'lmoqda. Masalan, sayyohda yoki tijoratchida ham simsiz lokal ham simsiz global tarmoq bilan o'zaro aloqa qiluvchi zamonaviy uyali telefon bo'lishi mumkin.

Simsiz tarmoq tuzilmasi. Simsiz tarmoqlarda simli tarmoqda ishlatiladigan komponentlar ishlatiladi. Ammo simsiz tarmoqlarda axborot

havo muhiti (medium) orqali uzatishga yaroqli ko'rinishga o'zgartirilishi lozim.

11.1-rasmda simsiz tarmoqlarda ishlatiladigan komponentlarning asosiylari ko'rsatilgan. Ularga foydalanuvchilar, kompyuter qurilmalari, bazaviy stansiyalar va simsiz infratuzilma kiradi.



11.1-rasm. Simsiz tarmoqda ishlatiladigan asosiy komponentlar.

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

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

Ba'zi foydalanuvchilarga faqat kompyuter qurilmasining portativligi zarur, ya'ni ular vaqtning ma'lum oralig'ida simsiz tarmoq bilan

ishlaganida bir joyda bo'ladilar. Bunday foydalanishga misol tariqasida majlislar zalida simsiz tarmoqqa ulangan noutbukda ishlovchi xodimni ko'rsatish mumkin.

Kompyuter qurilmalari. Kompyuter qurilmalarining (ba'zida ularni mijozlar deb atashadi) ko'pgina xillari simsiz tarmoq bilan ishlayoladi. Ba'zi kompyuter qurilmalari foydalanuvchilar uchun atayin qurilgan bo'lsa, boshqalari oxirgi tizim hisoblanadi. 11.2-rasmda simsiz tarmoqlarning kompyuter qurilmalari keltirilgan.

Printer

Mobil telefon

Noutbuk

Ma'lumotlarni yig'uvchi qurilma

Shaxsiy kompyuter

PDA

Oddiy telefon

11.2-rasm. Simsiz tarmoqlarning kompyuter qurilmalari.

Mobil ilovalar ishini ta'minlash va odamlarga o'zlari bilan uzoq vaqt mobaynida olib yurishlarida qulaylik tug'dirish uchun kompyuter qurilmalari ixcham bo'lishi lozim. Odatda, ular katta bo'lmagan ekranga, kam sonli tugmachalarga va o'lchamlari kichik batareyaga ega. Kompyuter qurilmalari mobillikka ega bo'lgan holda faqat ba'zi

ilovalarni madadlaydi. Nisbatan yuqori xarakteristikalarni talab etuvchi ilovalarni bajarishda katta ekranga va katta klaviaturaga ega bo'lgan o'lchamlari katta kompyuter qurilmalaridan foydalaniladi. Ammo ular massasining kattaligi va bir joydan ikkinchi joyga ko'chirishning noqulayligi muammo hisoblanadi. Simsiz tarmoqlarning kompyuter qurilmalari serverlar, ma'lumotlar bazasi va Web-uzellar kabi oxirgi tizimlarni ham o'z ichiga oladi.

Foydalanuvchilar mavjud kompyuter qurilmalarini simsiz tarmoqda ishlatish uchun (masalan, simsiz tarmoq interfeysi platasini noutbukka o'rnatish orqali) moslashtirishlari mumkin. *Tarmoq interfeysi platasi* yoki *tarmoq adapteri* (network interface card) kompyuter qurilmasi va simsiz tarmoq infratuzilmasi orasida interfeysni ta'minlaydi. Bu plata kompyuter qurilmasi ichiga o'rnatiladi, ba'zida tashqi tarmoq adapteri ham ishlatiladi. Bunday adapterlar, ishga tushirilishi bilan kompyuter qurilmasi tashqarisida qoladi.

Kompyuter qurilmalari Windows-XP, Linux yoki MAC OS kabi operatsion tizimga ham ega bo'lib, bu operatsion tizim simsiz tarmoq ilovalarini amalga oshirish uchun zarur bo'lgan dasturiy ta'minotni ishga tushiradi.

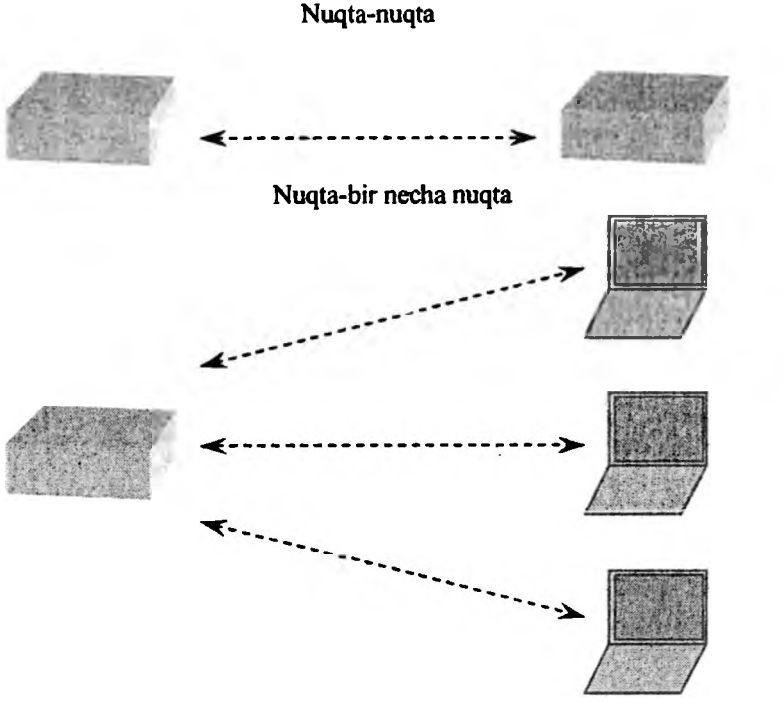
Havo muhiti. Havo kompyuter qurilmalari va simsiz infratuzilmaga orasida axborot oqimini uzatish kanali hisoblanadi. Simsiz tarmoqlar orqali aloqani nutq orqali muloqotga o'xshatish mumkin. Agar suhbatdoshlar orasidagi masofa oshaversa, ular bir-birlarini yomon eshita boshlaydilar.

Simsiz tarmoqlarning axborot signallari ham havo orqali tarqaladi, ammo o'zining xususiyati evaziga nutq signalariga qaraganda anchagina katta masofaga tarqalishi mumkin. Bu signallar odamga eshitilmaydi, shu sababli, ularni so'zlashga xalaqit berishidan qo'rqmay, yanada yuqori sathlargacha kuchaytirish mumkin. Ammo aloqa sifati to'siqlarning mavjudligiga bog'liq. To'siqlar signallar tarqalishiga xalaqit qiladi yoki ularni susaytiradi, natijada, signallar sathi pasayadi, ularning tarqalish uzoqligi kamayadi.

Yomg'ir, qor, tuman, tutun (smog) simsiz tarmoqlarda axborot signallarini tarqalishiga ta'sir etuvchi obi-havo sharoitlari hisoblanadi. Masalan, kuchli jala aloqa uzunliginl ikki martaga kamaytirishi mumkin. Binolar va daraxtlar kabi boshqa to'siqlar tarqalish sharoitlariga va simsiz tarmoq xarakteristikalariga ta'sir etishi mumkin. Simsiz regional va global tarmoqlarni joylashtirishni rejalashtirishda bu muammolarning muhimligi ortadi.

Simsiz tarmoq infratuzilmasi. Simsiz tarmoq infratuzilmasi foydalanuvchilar va oxirgi tizimlarning o'zaro simsiz aloqalarini ta'minlaydi. Uni bazaviy stansiyalar, foydalanish kontrollerlari, ulanish o'rnatilishini ta'minlovchi ilovalarning dasturiy ta'minoti va taqsimlovchi tizim tashkil etishi mumkin.

Bazaviy stansiya infratuzilmaning tarqalgan komponenti hisoblanadi. U havo muhiti orqali tarqaluvchi simsiz tarmoq axborot signallarining simli tarmoqqa uzatilishini ta'minlaydi. Bazaviy stansiyani ba'zida *taqsimlovchi tizim* deb ham yuritishadi. Demak, bazaviy stansiya Web-sahifalarni ko'zdan kechirish servislari, elektron pochta va ma'lumotlar bazasi kabi tarmoq xizmati yo'nalishidan foydalanishni ta'minlaydi. Bazaviy stansiyada ko'pincha simsiz tarmoq interfeysi platasi bo'lib, bu plata foydalanuvchi kompyuteridagi simsiz tarmoq interfeysi platasining ishlash prinsipidan foydalanadi. Bazaviy stansiya «nuqta-nuqta» yoki «nuqta-bir necha nuqta» kabi ulanishlarni madadlashi mumkin (11.3-rasm).



11.3-rasm. Bazaviy stansiyaning «nuqta-nuqta» va «nuqta-bir necha nuqta» ulanishlarini madadlashi.

«Nuqta-nuqta» tizimi signallar oqimini bir bazaviy stansiyadan ikkinchisiga yoki bir kompyuterdan ikkinchisiga uzatish imkoniyatiga ega. «Nuqta-bir necha nuqta» konfiguratsiyasi holida bazaviy stansiya bittadan ortiq kompyuter qurilmasi yoki bir necha bazaviy stansiyalar bilan bog'lanishi mumkin. Bunday xil bog'lanishni, masalan, simsiz lokal tarmoq tarkibidagi foydalanish nuqtasi ta'minlaydi. Foydalanish nuqtasi bitta qurilma bo'lib, ko'pgina kompyuter qurilmalari bir-birlari bilan hamda simsiz tarmoq infratuzilmasidagi tizimlar bilan bog'lanish maqsadida u bilan ulanishni o'rnatadi.

Foydalanish kontrolleri. Foydalanish kontrolleri, odatda, tarmoqning o'tkazuvchi qismida, foydalanish nuqtasi va tarmoqning himoyalanish qismi orasida joylashgan apparat uzeli hisoblanadi. Foydalanish kontrollerlari ochiq simsiz tarmoq va muhim resurslar orasida trafikni tartibga solish maqsadida foydalanish nuqtalarini markazlashtirilgan nazoratini ta'minlaydi. Ba'zi hollarda foydalanishni boshqarish vazifasini foydalanish nuqtasi bajaradi.

Foydalanish kontrollerlari keng qo'llaniladi. Umumfoydalanuvchi simsiz lokal tarmoqda, foydalanish kontrolleri foydalanuvchilarni autentifikatsiyalash va avtorizatsiyalash bilan Internetdan foydalanishni tartibga soladi.

Ulanish o'rnatilishini ta'minlovchi ilovalarning dasturiy ta'minoti. Internet dan va elektron pochtadan simsiz tarmoq orqali, odatda, oson foydalaniladi. Buning uchun *mijoz qurilmasida* brauzer va elektron pochta dasturi o'rnatilishi lozim. Foydalanuvchilar vaqti-vaqti bilan simsiz ulanishdan mahrum bo'lishlari mumkin, ammo nisbatan murakkab bo'lmagan ilovalarni bajarishda ishlatiluvchi protokollar yetarlicha barqaror hisoblanadi.

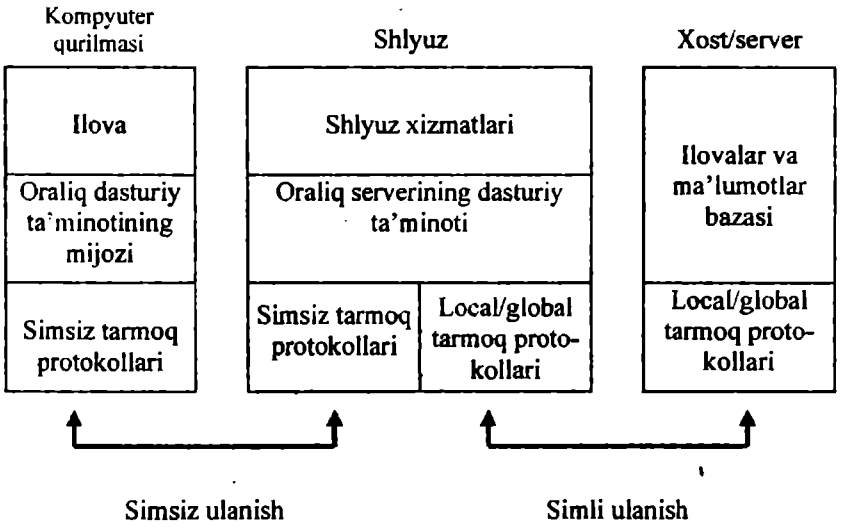
Ammo bunday oddiy ilovalar bilan bir qatorda maxsus, yanada murakkab ilovalar ishlashini ta'minlovchi dasturiy ta'minot zarur. Quyida ulanishni ta'minlovchi ilovalarning asosiylari keltirilgan.

Terminal emulyatori (therminal emulation). Terminal emulyatorining dasturiy ta'minoti kompyuter qurilmasida bajarilib, uni foydalanuvchini nisbatan sodda interfeys bilan ta'minlashga imkon beruvchi terminal kabi ishlashga majbur etadi. Bu sodda interfeys foydalanuvchiga boshqa kompyuterda bajariluvchi ilovalar bilan o'zaro aloqa qilishga imkon beradi.

Ma'lumotlar bazasi bilan to'g'ridan-to'g'ri ulanish (direct database connectivity). Ma'lumotlar bazasi bilan to'g'ridan-to'g'ri ulanishda (ba'zida mijoz-server texnologiyasi deb ataladi) ilova foydalanuvchi

kompyuterida bajariladi. Bunday konfiguratsiyada oxirgi foydalanuvchi qurilmasidagi dasturiy ta'minot ilovaga yuklangan barcha vazifalarni bajaradi va odatda, markaziy serverda joylashgan ma'lumotlar bazasi bilan o'zaro aloqada bo'ladi.

Oraliq dasturiy ta'minot (Wireless middleware). Oraliq dasturiy ta'minot foydalanuvchining kompyuter qurilmasi va ilova dasturiy ta'minoti yoki serverdagi ma'lumotlar bazasi orasida oraliq ulanishni amalga oshiradi (11.4-rasm).



11.4-rasm. Oraliq dasturiy ta'minoti.

Oraliq dastur simli tarmoqqa ulangan qo'shimcha kompyuterda (oraliq shlyuzida) bajariladi. U foydalanuvchining kompyuter qurilmasi va serverlar orasida aylanuvchi paketlarni ishlaydi. Bu dasturiy ta'minot simsiz tarmoqda samarali va ishonchli bog'lanishni yaratishga imkon beradi, chunki ma'lumotlar bazasiga ulanish va ilovalarning dasturiy ta'minoti bilan o'zaro aloqa yanada ishonchli simli tarmoq orqali amalga oshiriladi. Ba'zida bu texnologiyani chidamli bog'lanish (session persistence) deb atashadi.

Taqsimlangan tizim. Simsiz tarmoq kamdan-kam to'la ma'noda simsiz ishlatiladi. Tarkibida ko'pincha simli ulanishlar bo'lgan taqsim-

lovchi tizim, odatda, foydalanish nuqtalarini, foydalanish kontrollerlarini va serverlarni bir butunga birlashtirish uchun zarur bo'ladi. Aksariyat hollarda taqsimlovchi vazifasini oddiy Internet tarmog'i bajaradi.

11.2. Simsiz tarmoqlar xavfsizligiga tahdidlar

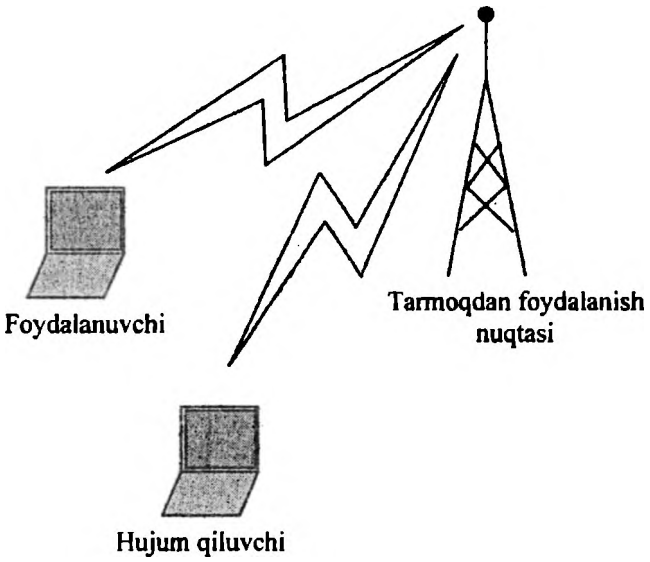
Simsiz texnologiyadan foydalanilib juda katta afzalliklarga erishish mumkin. Bu texnologiya foydalanuvchilarga aloqani yo'qotmasdan bemalol harakatlanish hissiyotini bersa, tarmoq yaratuvchilariga bog'lanishlarni tashkil etish uchun katta imkoniyatlarni yaratadi. Undan tashqari, tarmoqdan foydalanish uchun ko'pgina yangi qurilmalarning paydo bo'lishiga imkon beradi. Ammo simsiz texnologiya oddiy simli tarmoqlarga qaraganda o'zida ko'proq tahdidlarni eltadi. Xavfsiz simsiz ilovani yaratish uchun simsiz «hujumlar» o'tuvchi bo'lishi mumkin bo'lgan barcha yo'nalishlarni aniqlash lozim. Afsuski, ilovalar hech qachon butunlay xavfsiz bo'lmaydi, ammo simsiz texnologiyalardagi xavf-xatarni sinchiklab o'rganish har holda himoyalanish darajasini oshishiga yordam beradi. Demak, mumkin bo'lgan tahdidlarni tahlillab, tarmoqni shunday qurish lozimki, hujumlarga xalaqit berish va nostandart «hujumlar»dan himoyalanishga tayyor turish imkoni bo'lsin.

Nazoratlanmaydigan hudud. Simli va simsiz tarmoqlar orasidagi asosiy farq tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan zona bilan bog'liq. Uyali tarmoqlarning yetarlicha keng makonida simsiz muhit aslo nazoratlanmaydi. Zamonaviy simsiz texnologiyalar tarmoq makonini boshqarish vositalarining chegaralangan to'plamini taqdim etadi. Bu simsiz tuzilmalarning yaqinidagi hujum qiluvchilarga simli dunyoda mumkin bo'lmagan hujumlarni amalga oshirishga imkon beradi.

Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda eng tarqalgan muammo – anonim hujumlarning mumkinligi. Anonim zararkunandalar 11.5-rasmda ko'rsatilganidek, radiosignallarni ushlab qolib, uzatiluvchi ma'lumotlarni rasshifrovka qilishi mumkin.

Uzatishni ushlab qolish uchun niyati buzuq odam uzatgich (peredatchik) oldida bo'lishi lozim. Ushlab qolishning bunday turlarini umuman qaydlash mumkin emas va ularga xalaqit berish undan ham qiyin. Antennalar va kuchaytirgichlardan foydalanish, ushlab qolish jarayonida niyati buzuq odamlarga nishondan aytarlicha uzoq masofada bo'lishlariga imkon beradi.

Yashirincha eshitishning yana bir usuli – simsiz tarmoqqa ulanish. Lokal simsiz tarmoqda yashirincha faol eshitish, odatda, *Adress Resolution Protocol* (ARP) protokolidan noto'g'ri foydalanishga asoslangan. Boshida bu texnologiya tarmoqni «eshitish» maqsadida yaratilgan edi. Aslida, biz ma'lumotlar bog'lanishi sathida «man in the middle» (MITM – «o'rtada odam», pastroqqa qaralsin) xilidagi hujum bilan ish ko'ramiz. Hujum qiluvchi lokal simsiz tarmoqning nishon stansiyasiga so'ralmagan ARP-javoblarni yuboradi, nishon stansiyasi esa hujum qiluvchiga o'zidan o'tayotgan barcha trafikni jo'natadi. So'ngra niyati buzuq odam paketlarni ko'rsatilgan adresatlarga yo'llaydi. Shunday qilib, simsiz stansiya boshqa simsiz mijozning (yoki lokal tarmoqdagi simli mijozning) trafigini ushlab qolishi mumkin.

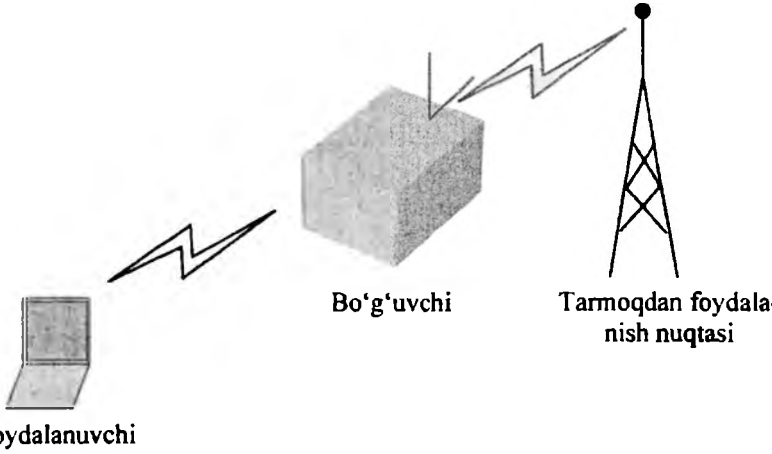


11.5-rasm. Simsiz kommunikatsiyalarda yashirincha eshitish.

Bo'g'ish. Tarmoqlarda bo'g'ish atayin yoki atayin bo'lmagan interferensiyaning aloqa kanalidagi jo'natuvchi va qabul qiluvchi imkoni-

yatidan oshganida sodir bo'ladi. Natijada, bu kanal ishdan chiqariladi. Hujum qiluvchi bo'g'ishning turli usullaridan foydalanishi mumkin.

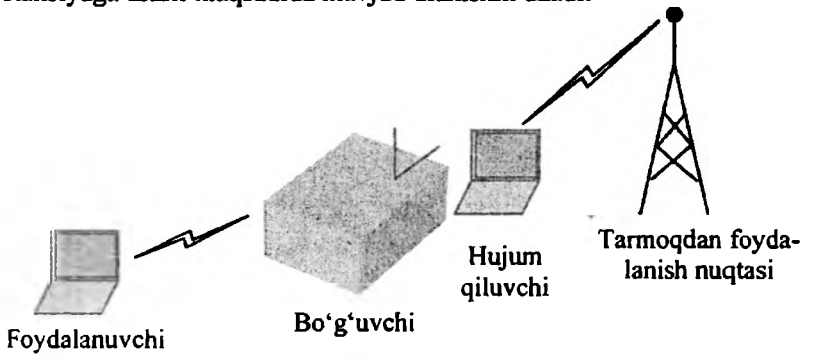
Xizmat ko'rsatishdan voz kechish. DoS (Denial of Service – xizmat ko'rsatishdan voz kechish) xilidagi hujum tarmoqni butunlay ishdan chiqarishi mumkin. Butun tarmoqda, jumladan, bazaviy stansiyalarda va mijoz terminallarida, shunday kuchli interferensiya paydo bo'ladiki, stansiyalar bir-birlari bilan bog'lana olmaydilar (11.6-rasm). Bu hujum ma'lum doiradagi barcha kommunikatsiyani o'chiradi. Simsiz tarmoqqa bo'ladigan DoS hujumni oldini olish yoki to'xtatish qiyin. Simsiz tarmoq texnologiyalarining aksariyati litsenziyalanmagan chastotalardan foydalanadi, demak, bir qancha elektron qurilmalardan interferensiya bo'lishi mumkin.



11.6-rasm. Simsiz kommunikatsiyalarda bo'g'ish hujumlari.

Mijozlarni bo'g'ish. Mijoz stansiyasini bo'g'ish firibgarga o'zini bo'g'ilgan mijoz o'rniga qo'yishiga imkon beradi (11.7-rasm). Mijoz ulanishni amalga oshira olmasin degan maqsadda unga xizmat ko'rsatishdan voz kechish uchun ham bo'g'ishdan foydalaniladi. Juda

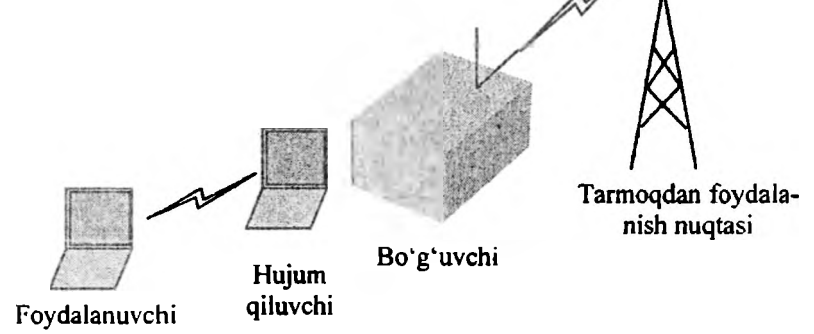
mohirlik bilan qilingan hujumlar niyati buzuq odam stansiyasini bazaviy stansiyaga ulash maqsadida mavjud ulanishni uzadi.



11.7-rasm. Ulanishni ushlab qolish maqsadida mijozni bo'g'ish hujumi.

Bazaviy stansiyani bo'g'ish. Bazaviy stansiyani bo'g'ish uni hujum qiluvchi stansiya bilan almashtirishga imkon beradi (11.8-rasm).

Bunday bo'g'ish foydalanuvchilarni xizmatlardan foydalanishdan, telekommunikatsiya kompaniyalarini esa foydadan mahrum qiladi.



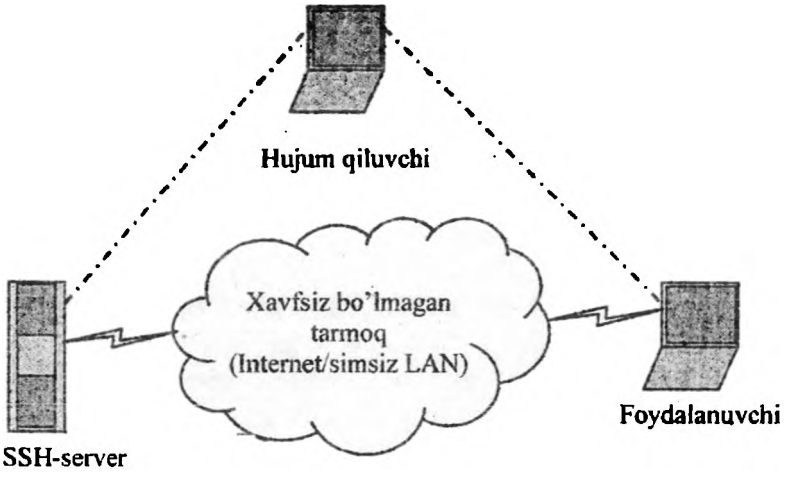
11.8-rasm. Ulanishni ushlab qolish maqsadida bazaviy stantsiyani bo'g'ish hujumi.

Yuqorida qayd etilganidek, aksariyat simsiz texnologiyalar litsenziyalanmagan chastotalardan foydalanadi. Shu sababli, ko'pgina qurilmalar – radiotelefonlar, kuzatish tizimlari va mikroto'lqinli o'choqlar – simsiz tarmoq ishiga ta'sir etishi va simsiz ulanishni bug'ishi mumkin. Bunday atayin bo'lmagan bo'g'ish hollarini oldini olish uchun, qimmatbaho simsiz asbob-uskunani sotib olishdan avval u o'rnatiladigan joyni sinchiklab tahlillash lozim. Bunday tahlil kommunikatsiyalarga begona qurilmalarning ta'sir etmasligiga ishonch hosil qilishga imkon beradi va ma'nosiz xarajatlardan asraydi.

Bostirib kirish va ma'lumotlarni modifikatsiyalash. Niyati buzuq odam ulanishni ushlab qolish, ma'lumotlarni yoki komandalarni uzatish maqsadida ma'lumotlarning mavjud oqimiga axborotni qo'shganida bostirib kirish sodir bo'ladi. Hujum qiluvchi paketlarni bazaviy stansiyaga yuborib boshqarish komandalari va axborot oqimlari ustida manipulatsiyani amalga oshirishi mumkin. Boshqarish komandalarini kerakli boshqarish kanaliga yuborish orqali foydalanuvchini tarmoqdan uzishga erishish mumkin.

Bostirib kirish xizmat ko'rsatishdan voz kechish uchun ishlatilishi mumkin. Hujum qiluvchi tarmoqdan foydalanish nuqtalarini ulanish komandalari bilan to'lib-toshiradi. Natijada, boshqa foydalanuvchilarga tarmoqdan foydalanishga ruxsat berilmaydi.

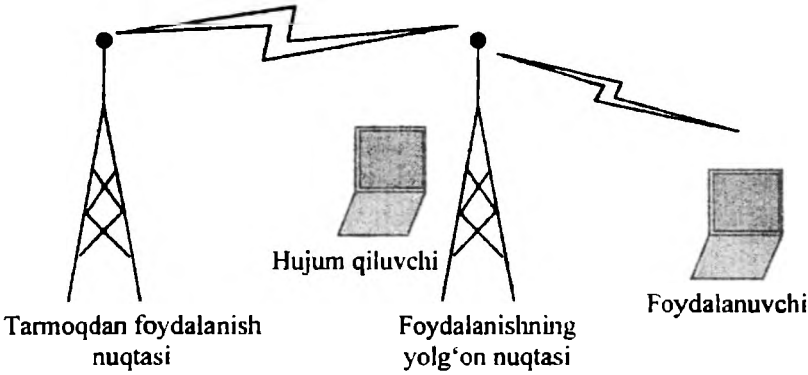
MITM(man in the middle) hujumi. MITM hujumi yuqorida tavsiflangan bostirib kirishlarga o'xshash. Ular turli shakllarni olishlari mumkin va aloqa seansining konfidensialligini va yaxlitligini buzish uchun ishlatiladi. MITM hujumlar anchagina murakkab, chunki ularni amalga oshirish uchun tarmoq xususida batafsil axborot talab etiladi. Niyati buzuq odam, odatda, tarmoq resurslaridan birining identifikatsiyasini bajaradi. Hujum qurboni ulanishni boshlaganida, firibgar uni ushlab qoladi va istalgan resurs bilan ulanishni tugallaydi, so'ngra ushbu resurs bilan barcha ulanishlarni o'zining stansiyasi orqali o'tkazadi (11.9-rasm). Bunda hujum qiluvchi axborotni jo'natishi, jo'natilganini o'zgartirishi yoki barcha muzokaralarni yashirincha eshitishi va so'ngra rasshifrovka qilishi mumkin.



11.9-rasm. MITM xilidagi hujum.

Abonent-firibgar. Tarmoq abonentining ishini sinchiklab o'rganib chiqqan hujum qiluvchi o'zini «tarmoq abonenti» qilib ko'rsatib, tarmoq va uning xizmatlaridan foydalanishga urinadi. Undan tashqari, foydalanishda qo'llaniladigan qurilmaning o'g'irlanishi tarmoqqa kirishga yetarli bo'ladi. Barcha simsiz qurilmalarning xavfsizligini ta'minlash oson ish emas, chunki ular foydalanuvchilarning harakatlanishida qulaylik tug'dirish maqsadida atayin kichkina qilib yaratiladi.

Tarmoqdan foydalanishning yolg'on nuqtalari. Tajribali hujum qiluvchi tarmoq resurslarini imitatsiya qilish bilan foydalanishning yolg'on nuqtalarini tashkil etishi mumkin. Abonentlar, hech shubhalanmasdan foydalanishning ushbu yolg'on nuqtasiga murojaat etadilar va uni o'zining muhim rekvizitlaridan, masalan, autentifikatsiya axborotidan xabardor qiladilar. Hujumning bu xili tarmoqdan foydalanishning haqiqiy nuqtasini «bo'g'ish» maqsadida ba'zida to'g'ridan-to'g'ri bo'g'ish bilan birgalikda amalga oshiriladi (11.10-rasm).



11.10-rasm. Foydalanishning yolg'on nuqtasi.

Simli tarmoqdan foydalanuvchilar ham bilmasdan tarmoqni hujumga ochib berib foydalanishning yolg'on nuqtalarining o'rnatilishiga sababchi bo'lishlari mumkin. Ba'zida foydalanuvchi, qulaylikka intilib, simsiz aloqa taqdim etuvchi foydalanishning simsiz nuqtalarini o'rnatadi, ammo xavfsizlik muammosini o'ylamaydi. Bu nuqtalar simli tarmoqqa kirish uchun «orqa eshik» vazifasini bajarishi mumkin, chunki ular turli hujumlarga duchor bo'ladigan konfiguratsiyada o'rnatiladi.

Hujumlarning anonimligi. Simsiz foydalanish hujumning to'liq anonimligini ta'minlaydi. O'rnatilgan joyni aniqlovchi mos tarmoq asbob-uskunasi bo'lmasa, hujum qiluvchi anonimlikni osongina saqlashi va simsiz tarmoq ta'siri hududidagi har qanday joyda berkinishi mumkin. Bunday holda niyati buzuq odamni tutish qiyin, ishni sudga oshirish esa undan ham qiyin.

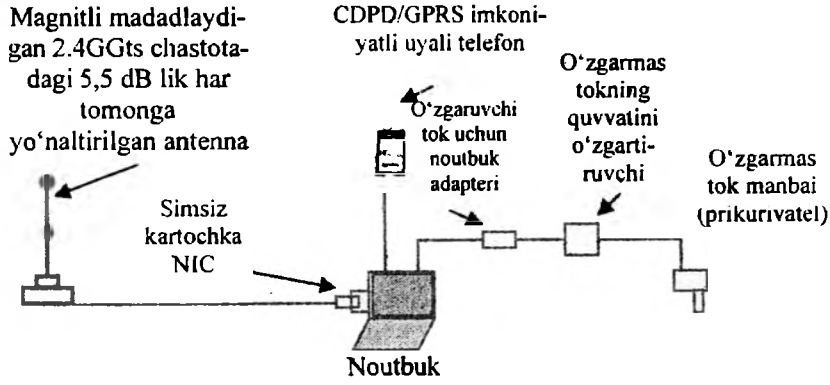
Ta'kidlash lozimki, aksariyat firibgarlar tarmoqni, ularning ichki resurslariga hujum qilish uchun emas, balki Internetdan tekin anonim foydalanish uchun o'rganadilar va Internet himoyasida boshqa tarmoqlarni hujumlaydilar.

«Mijoz-mijoz» xilidagi hujumlar. Tarmoqning barcha abonentlari hujumlanishi mumkin. Birinchi muvaffaqiyatdan so'ng hujum qiluvchi korporativ yoki telekommunikatsion tarmoqdan foydalanish huquqiga ega bo'ladi. Aksariyat tarmoq ma'murlari xavfsizlik rejimiga talabni oshirishga yoki shaxsiy tarmoqlararo ekranlarni (brandmauerlarni)

o'rnatishga yetarlicha e'tibor bermaydilar. Shu sababli, simsiz tarmoq mijozlariga muvaffaqiyatli hujumlar niyati buzuq odamlarga foydalanuvchilarning ismini va parolini ochish, demak, boshqa tarmoq resurslaridan foydalanish imkonini berishi mumkin.

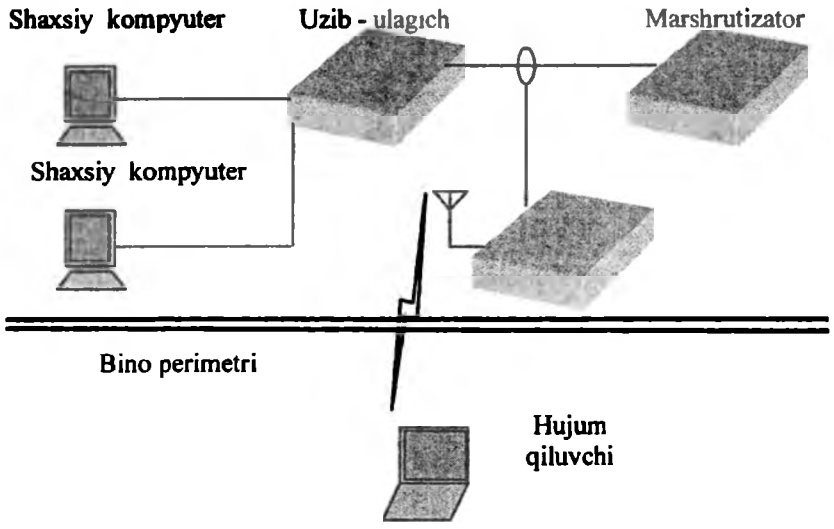
Tarmoq asbob-uskunalariga hujumlar. Noto'g'ri konfiguratsiyalangan asbob-uskunalar hujum qiluvchilar uchun birinchi «xo'rak» hisoblanadi va tarmoqqa keyingi suqilib kirishga yo'l ochadi. Hujumlarning asosiy obyektlari – marshrutizatorlar, uzib-ulagichlar, arxivlarni saqlovchi serverlar va foydalanish serverlari.

Maxfiy simsiz kanallar. Simsiz tarmoq foydalanuvchilari tarmoqni yaratish yoki baholash jarayonida yana bir omilni hisobga olishlari zarur. Simsiz foydalanish nuqtasining narxi past hamda dasturiy ta'minot, standart noutbuk va NIC-kartalar asosida foydalanish nuqtasini yaratish yetarlicha oson bo'lganligi sababli, nokorrekt konfiguratsiyalangan yoki simli tarmoqda o'ylamasdan joylashtirilgan simsiz asbob-uskunani ziyraklik bilan kuzatish talab etiladi. Bu asbob-uskuna (11.11-rasm) simli infratuzilmada juda sezilarli «raxnalar» hosil qilishi mumkinki, ular tarmoqdan bir necha kilometr uzoqdagi hujum qiluvchilar diqqatini tortishi mumkin.



11.11-rasm. «Simsiz urushni» olib borish asbob-uskunasi.

Xuddi shunga o'xshash konstruksiya yordamida o'ziga xos «simsiz ko'prik» o'tkazish va foydalanish nuqtalarining butun zanjirini tashkil qilgan holda tarmoqdan ma'lumotlarni himoyalangan bino tashqarisida chiqarib olish mumkin (11.12-rasm).



11.12-rasm. «Orqa eshik» ko'rinishidagi tarmoqdan foydalanish nuqtasi.

Rouming muammosi. Simsiz tarmoqning simli tarmoqdan yana bir muhim farqi foydalanuvchining tarmoq bilan aloqani uzmasdan joyini o'zgartirish qobiliyatidir. Rouming konsepsiyasi turli simsiz aloqa standartlari CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) va simsiz Ethernet uchun bir xil. TCP/IPning ko'pgina tarmoq ilovalari server va mijoz IP-adreslarining o'zgarmasligini talab etadi, ammo tarmoqdagi rouming jarayonida abonent, albatta, uning bir joyini tark etib, boshqa joyiga qo'shiladi. Simsiz tarmoqlarda mobil IP-adreslarning va boshqa rouming mexanizmlarining ishlatilishi ushbu talabga asoslangan.

Mobil IP-aloqaning asosiy g'oyasi – foydalanuvchining turgan joyini qaydlash va trafikni qayta yo'naltirish. Abonent turgan joyiga bog'liq bo'lmagan adres TCP/IP – ulanishni madadlaydi, foydalanuvchi turgan joyiga bog'liq bo'lgan vaqtincha adres esa lokal tarmoq resurslari bilan ulanishni ta'minlaydi. IP mobil tizimi uchun uchta tartibga soluvchi talablar mavjud: mobil uzeli (foydalanuvchining simsiz qurilmasi), uy agenti (uy tarmog'ida joylashgan server) va ajnabiy agent (rouming

uzatiluvchi tarmoqda joylashgan server). Mobil uzeli yangi tarmoqqa o'tganida, u turgan joyiga bog'liq bo'lgan vaqtincha IP-adresni oladi va ajnabiy agentda qaydlanadi. So'ngra ajnabiy agent uy agenti bilan bog'lanib mobil agentning o'ziga bog'langanligini xabar qiladi. Shu ondan boshlab barcha paketlar ajnabiy agent-rouming orqali uy agentiga yo'naltiriladi.

Kriptohimoyalash tahdidlari. CDMA, GSM uyali tarmoqlarda va simsiz Ethernet-tarmoqda axborotning konfidensialligini va yaxlitligini ta'minlash maqsadida kriptografik vositalar ishlatiladi. Ammo xatoliklarga yo'l qo'yish kommunikatsiyaning buzilishiga va axborotning yomon niyatda ishlatilishiga olib keladi.

WEP(Wired Equivalent Privacy – simsiz tarmoq darajasidagi maxfiylik) – 802.11 xilidagi tarmoq xavfsizligini ta'minlash uchun yaratilgan kriptografik mexanizm. WEPni tatbiq etishdagi xatoliklar va boshqarish muammolari uni befoyda qilib qo'ydi. Ushbu mexanizm barcha foydalanuvchilar ishlatadigan yagona statik kalitga ega. Internet tarmoqda niyati buzuq odamga bir necha soat mobaynida kalitni tiklashga imkon beruvchi vositalar mavjud. Shu sababli, WEPga autentifikatsiya va konfidensiallik vositasi sifatida ishonish mumkin emas. Tavsiflangan kriptografik usullarni ishlatilgani, umuman ishlatilmaganiga qaraganda yaxshiroq, ammo yuqorida keltirilgan hujumlardan himoyalashning boshqa usullari zarur.

11.3. Simsiz tarmoqlar xavfsizligi protokollari

SSL/TLS protokollari. Himoyalangan ulanishlar protokoli – Secure Sockets Layer (SSL) Internet brauzerlarining xavfsizligi muammosini yechish uchun yaratilgan. SSL taklif etgan birinchi brauzer – Netscape Navigator tijorat tranzaksiyalari uchun Internet tarmog'ini xavfsiz qildi, natijada ma'lumotlarni uzatish uchun xavfsiz kanal paydo bo'ldi. SSL protokoli shaffof, ya'ni ma'lumotlar tayinlangan joyga shifrlash va rasshifrovka qilish jarayonida o'zgarmasdan keladi. Shu sababli, SSL ko'pgina ilovalar uchun ishlatilishi mumkin.

SSL o'zidan keyingi TLS (Transport Layer Security – transport sathi himoyasi protokoli) bilan Internet da keng tarqalgan xavfsizlik protokolidir. Netscape kompaniyasi tomonidan 1994-yili tatbiq etilgan SSL/TLS hozirda har bir brauzerga va elektron pochtaning ko'pgina

dasturlariga o'rnatiladi. SSL/TLS xavfsizlikning boshqa protokollari, masalan, Private Communication Technology (PCT – xususiy kommunikatsiya texnologiyasi), Secure Transport Layer Protocol (STLP– xavfsiz sathning transport protokoli) va Wireless Transport Layer Security (WTLS – simsiz muhitda transport sathini himoyalash protokoli) uchun asos vazifasini o'taydi.

SSL/TLSning asosiy vazifasi tarmoq trafigini yoki gipermatnni uzatish protokoli HTTPni himoyalashdir. SSL/TLS aloqa jarayonining asosida yotadi. Oddiy HTTP–kommunikatsiyalarda TCP–ulanish o'rnatiladi, hujjat xususida so'rov yuboriladi, so'ngra hujjatning o'zi yuboriladi.

SSL/TLS ulanishlarni autentifikatsiyalash va shifrlash uchun ishlatiladi. Bu jarayonlarda simmetrik va asimmetrik algoritmlarga asoslangan turli texnologiyalar kombinatsiyalari ishtirok etadi. SSL/TLSda mijozni va serverni identifikatsiyalash mavjud, ammo aksariyat hollarda server autentifikatsiyalanadi.

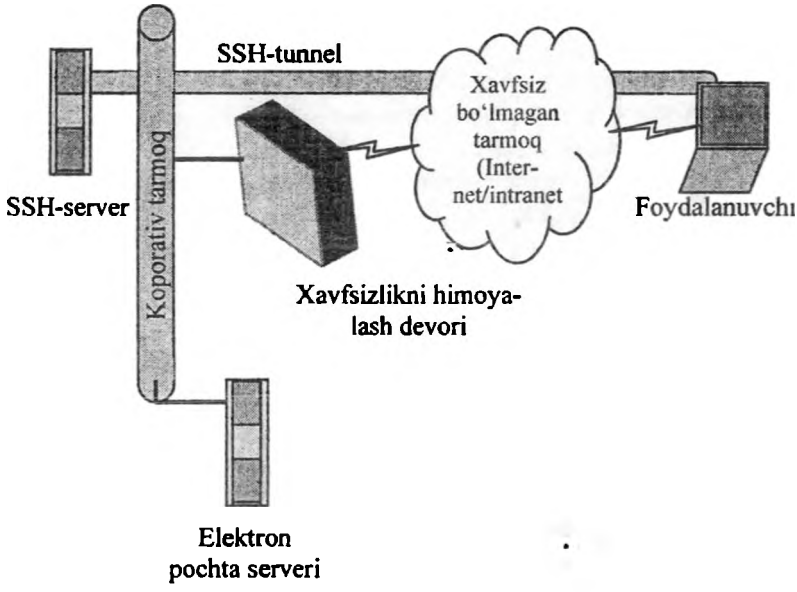
SSL/TLS turli tarmoq kommunikatsiyalar xavfsizligini ta'minlashi mumkin. Protokolning juda keng tarqalishi elektron pochta, yangiliklar, Telnet va FTP (File Transfer Protocol – fayllarni uzatish protokoli) kabi mashhur TCP-kommunikatsiyalar bilan bog'liq. Aksariyat hollarda SSL/TLS yordamida kommunikatsiya uchun alohida portlar ishlatiladi.

SSH protokoli. Secure Shell protokoli, SSL/TLSkabi kommunikatsiyalarni himoyalash uchun 1995-yili yaratilgan. O'zining moslanuvchanligi va ishlatilishining soddaligi tufayli SSH ommaviy xavfsizlik protokoliga aylandi va hozirda aksariyat operatsion tizimlarda standart ilova hisoblanadi.

SSHda aloqa seansi jarayonida ma'lumotlarni uzatish uchun simmetrik kalitdan foydalaniladi. Serverni ham mijozni autentifikatsiyalash uchun SSHni osongina qayta konfiguratsiyalash mumkin.

Ko'pincha SSH tarmoq xostlarini boshqarishda ishlatiladigan, ko'p tarmqalgan ilova – telnetni almashtirish uchun ishlatiladi.

Ba'zida ishlab chiqaruvchilar SSHni telnet yoki FTPni almashtiruvchi sifatida madadlamaydilar. Bunday hollarda SSHni telnet, FTP, POP (Post Office Protocol - pochta xabarlari protokoli) yoki hatto HTTP kabi xavfsiz bo'lmagan ilovalar xavfsizligini ta'minlash uchun ishlatish mumkin. 11.13-rasmda trafikni xavfsiz bo'lmagan tarmoqdan SSH serverga o'tkazish uchun konfiguratsiyalangan brandmauer keltirilgan.



11.13-rasm. SSH-tunnel.

Xavfsiz bo'lmagan tarmoqdan SSH serverga va aksincha hech qanday trafik o'tkazilmaydi. SSH-serverning SSH dan terminal foydalanishidan tashqari, portning qayta yo'naltirilishi elektron pochta trafigini SSH-serverga xavfsiz tarmoq bo'yicha uzatilishini ta'minlashi mumkin. So'ngra SSH-server paketlarni elektron pochta serveriga qayta yo'naltiradi. Elektron pochta serveriga trafik SSH-serverdan kelganidek tuyuladi va paketlar SSH-serverga, foydalanuvchiga tunnellash uchun yuboriladi.

WLTS protokoli. SSL/TLSga asoslangan WLTS protokoli WAP (Wireless Application Protocol – simsiz ilovalar protokoli) qurilmalarida, masalan, uyali telefonlarda va cho'ntak kompyuterlarida ishlatiladi. SSL va WLTS bir-biridan transport sathi bilan farqlanadi. SSL yo'qolgan paketlarni qayta uzatishda yoki nostandart paketlarni

uzatishda TCP ishiga ishonadi. WLTSdan foydalanuvchi WAP qurilmalari o'z funksiyalarini bajarishida TCPni qo'llay olmaydilar, chunki faqat UDP (user Datagram Protocol) bo'yicha ishlaydilar. UDP protokoli esa ulanishga mo'ljallanmagan, shu sababli, bu funksiyalar WLTSga kiritilishi lozim.

«Qo'l berib ko'rishish» jarayonida quyidagi uchta sinf faollashishi mumkin:

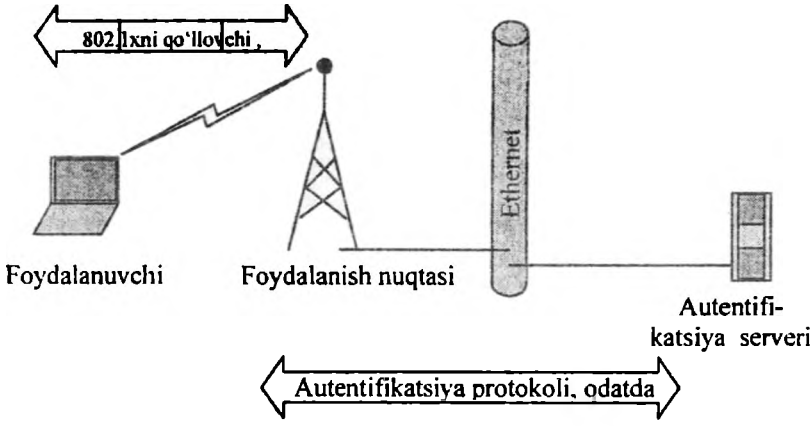
– WLTS – 1-sinf. Sertifikatsiz;

– WLTS – 2-sinf. Sertifikatlar serverda;

– WLTS – 3-sinf. Sertifikatlar serverda va mijozda.

1-sinfda autentifikatsiyalash bajarilmaydi, protokol esa shifrlangan kanalni tashkil etishda ishlatiladi. 2-sinfda mijoz (odatda, foydalanuvchi terminal) serverni autentifikatsiyalaydi, aksariyat hollarda sertifikatlar terminalning dasturiy ta'minotiga kiritiladi. 3-sinfda mijoz va server autentifikatsiyalanadi.

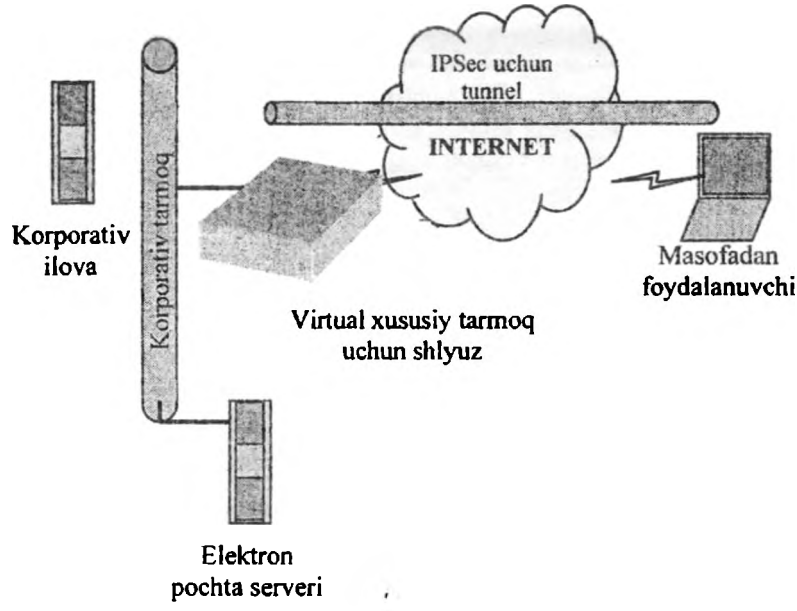
802.1x protokoli. Bu protokolning asosiy vazifasi – autentifikatsiyalashdir; ba'zi hollarda protokoldan shifrlovchi kalitlarni o'rnatishda foydalanish mumkin. Ulanish o'rnatilganidan so'ng undan faqat 802.1x. trafigi o'tadi, ya'ni DHCP (Dynamic Host Configuration Protocol – xostlarni dinamik konfiguratsiyalash protokoli), IP va h. kabi protokollarga ruxsat be-rilmaydi. Extensible Authentification Protocol (EAP) (RFC 2284) foydalanuvchilarni autentifikatsiyalashda ishlatiladi. Boshlanishida EAP «nuq-ta-nuqta» (PPP, Point-to-Point Protocol) prtokoli yordamida autentifikatsiyalashning ba'zi muammolarini hal etish uchun ishlab chiqilgan edi, ammo uning asosiy vazifasi simsiz aloqa muammolarini hal etishga qaratilishi lozim. EAPning autentifikatsiyalash paketlari foydalanuvchi ma'lumotlarini kiritgan foydalanish nuqtasiga yuboriladi; aksariyat hollarda bu ma'lumotlar foydalanuvchi ismi (login) va paroldan iborat bo'ladi. Foydalanish nuqtasi tarmoq yaratuvchisi tanlagan vositalarning biri bilan foydalanuvchini identifikatsiyalashi mumkin. Foydalanuvchi identifikatsiyalanganidan va shifrlash uchun kanal o'rnatilganidan so'ng aloqa mumkin bo'ladi va DHCP kabi protokollarning o'tishiga ruxsat beriladi (11.14-rasm).



11.14-rasm. 802.1x protokolining ko'rinishi.

IPSec protokoli. Protokollar stekida IPSec protokoli SSL/TLS, SSH yoki WLTS protokollaridan pastda joylashgan. Xavfsizlikni ta'minlash IP-sathida va Internet-modelda amalga oshiriladi. IPSec ni tatbiq qilish usullaridan ko'p tarqalgani tunnellash bo'lib, u bitta sessiyada IP-trafikni shifrlash va autentifikatsiyalash imkonini beradi. IPSec hozirda Internetda ishlatiluvchi aksariyat virtual xususiy tarmoqlardagi (VPN-Virtual Private Network) asosiy texnologiya hisoblanadi. IP-Secning moslashuvchanligi va ilovalar tanlanishining kengligi sababli, ko'pchilik aynan bu sxemadan simsiz ilovalar xavfsizligini ta'minlashda foydalanadi.

IPSecni ilovalarga asoslangan qo'llanishining juda ko'p imkoniyatlari mavjud. Xavfsiz kommunikatsiyalar uchun IPSecning qo'llanishi ko'pincha Internet orqali masofadan foydalanish virtual xususiy tarmog'i VPN bilan bog'liq. Qachonki umumfoydalanuvchi tarmoq xususiy tarmoq funksiyalarini amalga oshirish uchun ishlatilsa, uni VPN deb atash mumkin. Bunday ta'rifga ATM (Asynchronous Transfer Mode - uzatishning asinxron usuli), Frame Relay va X.25 kabi tarmoq texnologiyalari ham tushadi, ammo aksariyat odamlar Internet bo'yicha shifrlangan kanalni tashkil etish xususida gap ketganida VPN atamasini ishlatishadi. Korporativ tarmoq perimetri bo'yicha 11.15-rasmda ko'rsatilganidek shlyuzlar o'rnatiladi va IPSec-tunnel orqali shlyuzdan masofadan foydalanish amalga oshiriladi.



11.15-rasm. IPSec VPN-tunnel.

11.4. Simsiz qurilmalar xavfsizligi muammolari

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

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

Fizik xavfsizlik noutbuklar uchun jiddiy muammo hisoblanadi. Bunday kompyuterlarni xarid qilishdagi parametrlardan biri–uning o'lchami. Noutbuk qanchalik kichkina bo'lsa, u shunchalik qimmat turadi. Boshqa tarafdan, noutbuk qanchalik kichkina bo'lsa, uni o'g'irlash shunchalik osonlashadi. Shifrlash kalitlarining, masalan, WEP-kalitlar (Wired Equivalent Privacy), dasturiy kalitlar, parollar yoki shaxsiy kalitlarning (PGP, Pretty Good Privace kabilar) yo'qotilishi katta muammo hisoblanadi va uni ilovalar yaratilishi bosqichidayoq hi-

sobga olish zarur. Niyati buzuq odam noutbukni o'z ixtiyoriga olganidan so'ng aksariyat xavfsizlik mexanizmlari buzilishi mumkin.

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

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

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

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

Axborotning chiqib ketishi noutbuk egasining ko'p odamlar to'plangan joylarda ham sodir bo'lishi mumkin. Samolet – kompaniya menejerlari foydalanadigan odatdagi transport vositasidir. Samolyotda qo'shni kreslodagi yo'lovchi noutbuk egasining elkasi ustidan muhim axborotni o'qib olishi mumkin. Hatto «uy sharoitidagi» noutbuklar ham himoyalanishi zarur. Bu holda kompyuterning himoyasi server himoyasidan farqlanmaydi. Juda ham zarur bo'lmagan servislarning o'chirilishi qurilma ishlashini yaxshilaydi.

O'zining dasturiy ta'minotini noutbukka o'rnatgan niyati buzuq odam xavfsizlikning barcha mexanizmlarini chetlab o'tish imkoniyatiga ega bo'ladi. Kompyuterni o'z ixtiyoriga olgan o'g'ri unga o'zining das-

turini o'rnatganida uni to'xtatib bo'lmaydi. BIOSda (Basic Input/Output System-kiritish/chiqarishning bazaviy tizimi) va qattiq diskda o'rnatilgan parollar o'g'rilangan noutbukdan foydalanishga to'sqinlik qilishi mumkin.

Ushbu barcha vositalar, afsuski, tajribali xaker uchun to'siq bo'laolmaydi.

Cho'ntak kompyuterlari. PDA(Personal Digital Assistans – «shaxsiy raqamli yordamchilar»)ning ko'pgina xillaridan simsiz ilovalar bilan ishlashda foydalaniladi. Maxsus qurilgan PDAlarda tibbiyot, sanoat yoki aviatsiya ilovalari ishga tushiriladi. Cho'ntak kompyuterlari ham mavjud bo'lib, ularda simsiz aloqa uchun o'rnatilgan kartochka, shtrix kodlarning skaneri, xizmat muddati uzoq bo'lgan batareyalar yoki magnit hoshiyali kartalarni o'quvchi qurilma kabi qo'shimcha qurilmalar bilan birgalikda Palm OS yoki Windows SE operatsion tizim o'rnatilgan. Bunday kompyuterlardan foydalanish uchun maxsus texnik tayyorgarlik talab etilmaydi. Shunga o'xshash qurilmalarni yoki ilovalarni himoyalash, ayniqsa, murakkab masala hisoblanadi.

PDAdan foydalanishga xohish bildirgan hujum qiluvchi uchun undagi axborot kiritish mexanizmlarining barchasi nishon hisoblanadi. Undan tashqari, aksariyat cho'ntak kompyuterlari shunday ishlab chiqilganki, ularni ishlab chiquvchilari uchun ilovalardagi xatoliklarni osongina aniqlash yo'llari ta'minlangan. Xatoliklarni aniqlashda ishlatiluvchi interfeyslar niyati buzuq odamlar uchun haqiqiy «teshik» xizmatini o'tashi mumkin.

Cho'ntak kompyuteri ishlaydigan axborotni himoyalash uchun axborotni cho'ntak kompyuterida emas, balki ma'lumotlarning xavfsiz rezerv bazasida saqlash lozim. Yana bir variant – JAVA tili ilovasidan yoki foydalanuvchi uchun maxsus yaratilgan ilovalardan foydalanish. Bu holda axborot qurilmada saqlanmaydi, ammo PDAning displeyida akslantiriladi. Boshqacha aytganda, simsiz ilovalardan faqat simsiz tarmoqdan foydalanish mavjud bo'lgan joylarda foydalanish mumkin.

Aksariyat PDAlarda parol yordamida blokirovka va razblokirovka qi-lish imkoniyati mavjud. Bu usullarga butunlay ishonmaslik lozim, ammo ular niyati buzuq odamlarni vaqtincha to'xtatib turishi mumkin. Undan tashqari, PDAni blokirovka qilish tizimi qurilmadagi ilovalardan yoki axborotdan niyati buzuq odamlarning foydalanishni qiyinlashtiradi. PDAning zarur bo'lmagan barcha funksiyalarini o'chirib qo'yish lozim, chunki har bir o'chirilgan kiritish mexanizmi bo'lishi mumkin bo'lgan hujumlar sonini kamaytiradi.

Cho'ntak kompyuterida muhim axborotni saqlash uchun shifrlashni qo'llash va unga qo'shimcha sifatida manbani ulash va ekranni blokirovka qilish uchun parollar o'rnatish tavsiya etiladi.

Simsiz infratuzilma. Simsiz infratuzilma qurilmalari, odatda, odamlar yig'ilgan yerda joylashtiriladi. Ularga kafelar, aeroportlar, korporativ tadbirlarni o'tkazish joylari va h. kiradi. Turli xil odamlar EAP(Extensible Authentification Protocol – autentifikatsiyalashning kengaytiriluvchi protokoli) yoki WEP kabi xavfsizlik vositalarini ishdan chiqarish yoki tarmoqqa suqilib kirish uchun tarmoq konfiguratsiyasi xususidagi axborotni qo'lga kiritish maqsadida ushbu komponentlardan foydalanishni xohlashlari mumkin.

Simsiz infratuzilma qurilmalarida tarmoqni boshqarish funksiyalari-ning xavfsizligini ta'minlash uchun ulardan foydalanishda SSH, SSL (Secure Sockets Layer) yoki SNMP3 (Simple Network Management Protocol 3 – tarmoqni oddiy boshqarish protokoli, 3-versiya) kabi xavfsiz protokollardan foydalanish lozim. Undan tashqari, telnet, HTTP dagi to'g'ri matn va SNMP (birinchi versiya) kabi xavfsizlikning yetarli darajasini madadlamaydigan protokollar o'chirilishi lozim. Xavfsiz boshqarishni ta'minlash iloji bo'lmasa, foydalanishning ba'zi bir nuqtalarini ketma-ket portlar orqali boshqarish mantiqan to'g'ri hisoblanadi. Foydalanish nuqtalarini yuqoriga qo'l yetmaydigan joyga mahkamlab qo'yish ham ularni o'g'irlanishdan saqlaydi.

Uyali telefonlar. Uyali telefonlar uchun xavfsizlik mulohazalari noutbuk va PDAlarga nisbatan keltirilgan mulohazalarga o'xshash. Qurilmalar-ning o'zi va mos dasturiy ta'minot uchun xavfsizlik muammosi ham hech nimasi bilan farq qilmaydi.

Uyali telefonlar ham boshqa simsiz qurilmalarga bo'ladigan hujumlarga duchor bo'ladi. Odatda, buferning to'lib-toshishi, qator formatiga hujumlash, grammatik xatoliklar ishlatiladi, natijada hujum qiluvchi o'g'irlangan qurilmada o'zining dasturini ishga tushirishga erishadi. Misol sifatida SMSning qisqa xabarlarini ko'rsatish mumkin. O'zining telefoni orqali SMS jo'natgan foydalanuvchiga hujumga duchor bo'lishi xavfi tug'iladi. Bu hujum natijasida xizmat qilish to'xtatiladi yoki foydalanuvchi terminalida begonaning komandalari bajariladi.

Undan tashqari, SIM-kartalarni (Subscriber Idenity Module – abonent identifkatsiyasi moduli) ishlab chiqaruvchilari qurilmalariga uyali telefonga simsiz interfeys orqali yuklanilishi ruxsat etiladigan qo'shimcha funksiyalarni kirita boshladilar. Misol tariqasida Sim Toolkit va MEXEni ko'rsatish mumkin. Zararli ilovalarni boshqa foydalanuv-

chiga uzatishni oldini oluvchi usullar tashqi hujumlarga duchor bo'ladi. Bunday ilovalarning mohiyati shundaki u niyati buzuq odamga foydanuvchining adres kitobini yoki telefondagi butun SMS ro'yxatini uzatishi mumkin. Ba'zi yechimlar DES standarti asosida ishlaydi, ammo xuddi shunday DES-kalitlar har bir SIM-kartalar uchun ishlatiladi.

Terminallar uchun parol yoki PIN-kodlarni ishlatish tavsiya etiladi. GSM(Global System for Mobile Communications – mobil kommunikatsiyalarning global tizimi) tarmoqlarida ishlovchi telefonlar xavfsizligini ta'minlashda SIM PIN kerak bo'ladi. Bu funksiyadan maksimal foydalanish uchun barcha bo'lishi mumkin bo'lgan PIN lardan foydalanish hamda IMEI (International Mobile Equipment Identity – mobil qurilmaning xalqaro nomeri)ning ishonchli joyda yozilishi tavsiya etiladi.

Muhim axborotni uzatish uchun terminaldan foydalanishda axborotni, albatta, shifrlash zarur. Kredit kartochkalar nomerlarini yoki boshqa shaxsiy axborotni uzatish uchun, albatta, SSL-himoyali WTLS-ulanish xizmatidan foydalanish zarur. Undan tashqari GSM ichidagi algoritmlarga bo'ladigan aksariyat hujumlar niyati buzuq odamga foydalanuvchining telefon nomerini o'ylab chiqarishga (klonirovka) imkon beradi. Bu hujumlar, odatda, telefon mavjudligini talab qiladi, shu sababli, telefonni xavfsiz joyda saqlash, yo'qotilgan yoki o'g'irlangan holda tezlik bilan operatorga xabar berish lozim.

XII bob. XAVFSIZLIKNI BOSHQARISH VA HIMOYA TIZIMINI QURISH

12.1. Boshqarishning funksional masalalari

Zamonaviy axborot texnologiyalaridan muvaffaqiyatli foydalanish uchun nafaqat tarmoqlarning o'zini, balki tarmoq xavfsizligi vositalarini ham ishonchli va samarali boshqarish zarur. Hozirgi vaqtda kompaniyaning butun infratuzilmasini qamrab oluvchi boshqarishning kompleks tizimini yaratish birinchi galdagi vazifa hisoblanadi. Bunday boshqarish tizimi axborot tizimining murakkabligi va masshtabidan qat'i nazar, quyidagilarga imkon yaratadi:

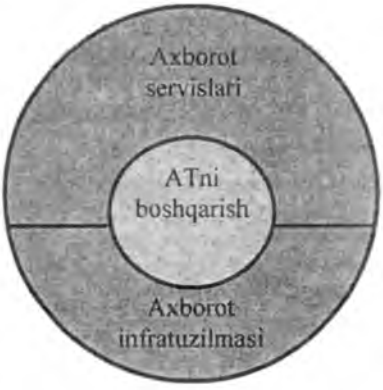
– butun axborot infratuzilmasiga markazlashtirilgan va tezkor boshqa-rish ta'sirni ko'rsatish;

– tezkor yechimlarni qabul qilish uchun axborot xavfsizligi holati xususidagi obyektiv axborotni beruvchi muntazam auditni va keng ko'lamdagi monitoring o'tkazish;

– axborot infratuzilmasi rivojini bashoratlash uchun uning ishlashi xususidagi statistik ma'lumotlarni to'plash.

Axborot tizimlarini boshqarishning ITIL metodologiyasi

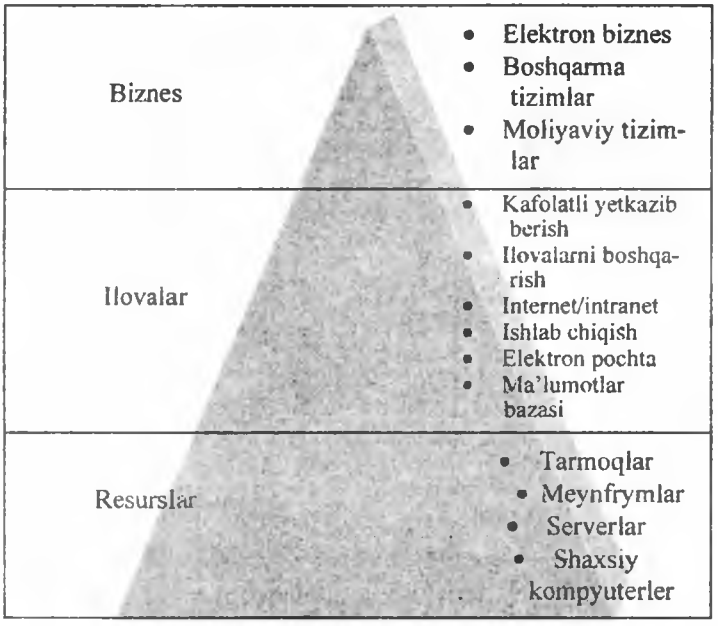
ITIL (IT Infrasructure Library) metodologiyasiga muvofiq axborot tizimi ikkita yirik blokdan – axborot infratuzilmasi va axborot servislaridan iborat (12.1-rasm).



12.1-rasm. ITIL metodologiyasi nuqtai nazaridan axborot tizimining ko'rinishi.

Axborot infratuzilmasi axborot servislari ishlovchi moddiy asos, muhit hisoblanadi. Axborot servislariga Internet-servislar, ilovalar servisi, boshqarish, yechim qabul qilish servislari va h. kiradi. Axborot infratuzilmasi servislar ishlashini ta'minlovchi texnik vositalar, aloqa liniyalari, muolajalar, me'yoriy hujjatlar va h. majmuidir. Axborot servislarining sifati bevosita axborot infratuzilmasi va uni boshqarish sifatiga bog'liq.

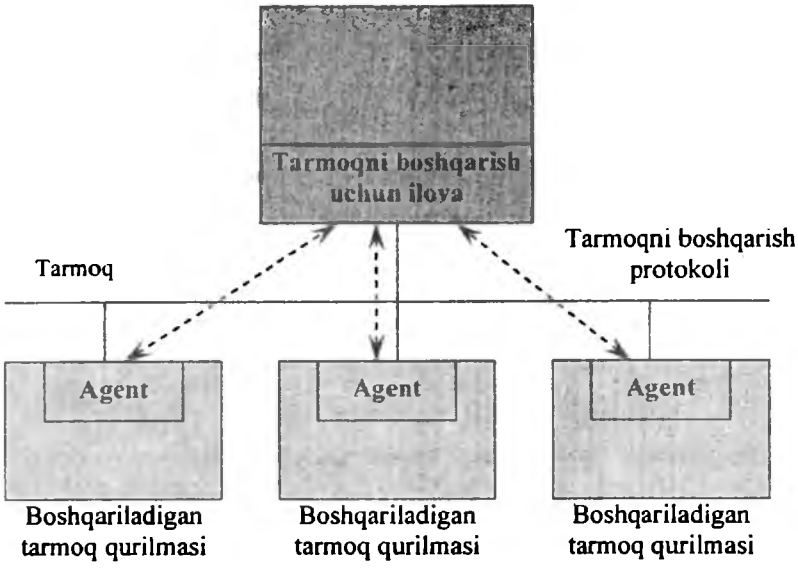
Axborot infratuzilmasini asosida axborot resurslari (hisoblash platformalari, serverlar, shaxsiy kompyuterlar, ma'lumotlarni uzatish tarmoqlari, aloqa liniyalari) yotuvchi piramida sifatida tasavvur etish mumkin (12.2-rasm).



12.2-rasm. Axborot infratuzilmasining tashkil etuvchilari.

Piramidaning ikkinchi sathini turli ilovalar tashkil etadi. Bu ilovalar birinchi sath resurslaridan foydalanib tatbiqiy dastur ta'minoti, elektron pochta, kafolatlangan yetkazish tizimi, ma'lumotlar bazasi, Web-serverlar va h. kabi muayyan ilovalar ishlashini ta'minlaydi. Va nihoyat, eng yuqori sathda biznes va ishlab-chiqarish jarayonlarining o'tishini ta'minlovchi ilovalar ishlaydi. Ikkala pastki sathdan foydalanuvchi bu ilovalar ishlab chiqarishni boshqarish, buyurtmachilar va ta'minlovchi bilan o'zaro aloqa, moliyaviy hisob va yechimni qabul qilishni madadlash kabi biznes-masalalarni yechishga yo'naltirilgan.

Umumiy holda, tarmoqni boshqarish tizimining arxitekturasi 12.3-rasmda keltirilgan ko'rinishga ega. Tarmoqni boshqarish ilovasi tarmoq ma'murining ish joyida yoki boshqa kompyuterda bajarilishi mumkin. Uning vazifasi boshqariluvchi qurilmalarda bajariladigan *agent* – ilovalardan yoki operatsion tizim servislaridan keluvchi boshqariluvchi obyekt xususidagi axborotni yig'ish.



12.3-rasm. Tarmoqni boshqarish tizimining umumlashtirilgan arxitekturasi.

Bunday ilovalarni agentlar bilan o'zaro aloqasi uchun odatda, SNMP (Simple Network Management Protocol) yoki CMIP (Common Management Information Protocol) protokollaridan foydalaniladi. Birinchisi, odatda, lokal tarmoqda ishlatilsa, ikkinchisi, telekommunikatsiyadan foydalanuvchi taqsimlangan tarmoqlarda ishlatiladi. Ammo dastur ta'minotini ba'zi ishlab chiqaruvchilari tarmoqni boshqarishda xususiy tarmoq protokollaridan foydalanishadi.

Tarmoqni boshqaruvchi zamonaviy vositalar quyidagi vazifalarni bajara oladi:

– boshqariluvchi kompyuter va qurilmalardagi buzilishlarni kuzatish, sabablarni aniqlash va bartaraf etish (ko'pincha avtomatik tarzda), oqibatlarini tuzatish va buzilishlarni oldini olish (masalan, tashxislash amalini bajarish orqali);

– kompyuterlarning va tarmoq qurilmalarining konfiguratsiyalanishini boshqarish (xususan, initsializatsiyalash, qayta konfiguratsiyalash va tarmoq qurilmalari va kompyuterlarni uzib qo'yish);

– foydalanuvchilar va foydalanuvchilar guruhi tomonidan tarmoq resurslaridan foydalanishni tartibga solish (masalan, diskli va boshqa kvotalarni tartibga solish);

– tarmoq qurilmalari va servislar unumdorligini boshqarish (tarmoq qurilmalari ishlatilishi jadalligi statistikasini va xatoliklar chastotasini yig'ish va tahlillash hamda olingan ma'lumotlar asosida ular unumdorligi darajasini sun'iy tarzda o'rnatish);

– oldindan belgilangan xavfsizlik siyosati asosida tarmoq resurslaridan foydalanishni nazoratlashdan foydalanib, ma'lumotlar himoyasini boshqa-rish va ularni buzishga urinishlardan ma'murni xabardor etish.

Korxona axborot xavfsizligi tizimi korporativ tarmoqni boshqarish tizimining eng muhim komponenti hisoblanadi. Korxona masshtabidagi taqsimlangan tarmoqda axborotni himoyalash vositalarini boshqaruvchi tizim quyidagi vazifalarni bajarishi lozim:

– korxona tarmog'i doirasida xavfsizlik siyosatini boshqarish, alohida qurilmalar xavfsizligining lokal siyosatini shakllantirish va uni axborotni himoyalovchi barcha qurilmalarga yetkazish;

– foydalanish obyektlarini va subyektlarini konfiguratsiyalashni boshqarish; himoya qurilmalari va dasturiy ta'minoti tarkibini, versiyasini, komponentlarini boshqarishni o'z ichiga oladi;

– taqsimlangan tatbiqiy tizimlarga himoya servislarini taqdim etish, himoyalangan ilovalar va ular resurslarini ro'yxatga olish. Ilovalarning bu guruhi, avvalo, tatbiqiy tizimlar tomonidan himoya servislarini boshqarish uchun interfeysni ta'minlashi lozim;

– kriptovositalarni boshqarish, xususan, kalitli boshqarish (kalitli infrastruktura). Kalitli infratuzilma infratuzilma xizmati tarkibida ishlashi lozim;

– hodisaviy protokollash; turli qurilmalarga *loglarni* berishni sozlashni, loglarni detallashtirish sathini boshqarishni, protokol olib boriluvchi hodisalarni tarkibini boshqarishni o'z ichiga oladi;

– axborot tizimi xavfsizligini auditlash; axborot tizimlari himoyalanishining joriy holati xususidagi obyektiv ma'lumotlarni baholashni ta'minlaydi;

– tizim xavfsizligini monitoringlash; qurilmalar va qurilmalarda kechuvchi hodisalar (himoyalash konteksti bo'yicha) holati, faolligi xususida, masalan, bo'lishi mumkin bo'lgan hujumlar xususida real vaqtda axborot olinishini ta'minlaydi;

– maxsus himoyalangan ilovalar, masalan, amallar ustidan notarial nazorat ishini ta'minlash hamda reglamentda ko'zda tutilgan tadbirlarni (kalitlarni, parollarni, himoya qurilmalarini almashtirish, smart-kartalarni ishlab chiqarish va h.) madadlash;

– ilovalarning loyiha-inventarizatsiyalash guruhi ishini ta'minlash. Ilovalarning bu guruhi korxona tarmog'iga himoya vositalarini o'rnatishni, qo'llaniladigan himoya vositalarini hisobga olishni, himoya vositalarining modul tarkibini nazoratlashni, himoya vositalari holatini nazoratlashni va h. bajaradi.

Tarmoqlarni an'anaviy boshqarish tizimi va tarmoqdagi axborotni himoyalash vositalarini boshqarish tizimi orasida o'zaro aloqani kompleks-lash va tashkil etish muammosi mavjud.

12.2. Xavfsizlik vositalarini boshqarish arxitekturasi

Kompaniya taqsimlangan axborot tizimida xavfsizlik siyosatini muvaffaqiyatli amalga oshirishi uchun xavfsizlikni boshqarish markazlishtirilgan bo'lishi va ishlatiladigan operatsion tizimga va tatbiqiy tizimlarga bog'liq bo'lmasligi lozim. Undan tashqari, korporativ axborot tizimida kechuvchi jarayonlarni (ruxsatsiz foydalanish, foydalanuvchilar imtiyozini o'zgarishi va h.) ro'yxatga olish tizimi yagona bo'lishi va ma'murga korporativ axborot tizimidagi barcha o'zgarishlarning to'liq ko'rinishini tasavvur etishiga imkon berishi lozim.

Korporativ axborot tizimi xavfsizligini markazlashtirilgan boshqarish asosida global boshqarish konsepsiyasi GSM (Global Security Man-

agement) yotadi. Ushbu Konsepsiya korxona axborot resurslarini quyidagi xususiyatlarga ega bo'lgan kompleks boshqarish tizimini qurishga imkon beradi:

– korxonaning barcha resurslari (xavfsizlik siyosati obyektlari) uchun himoyalashning yaxlitligini, ziddiyatlik emasligini va qoidalar to'plamining to'laligini ta'minlovchi, barcha mavjud himoya vositalarini korxona xavfsizligi siyosati asosida boshqarish;

– resurslarni tavsiflovchi shaxsiy vositalar hamda korxonaning boshqa kataloglari bilan aloqasi bo'yicha faollashuvchi korxona muhitining yagona (taqsimlangan) katalogi orqali korxonaning barcha resurslarini aniqlash;

– xavfsizlik siyosatiga asoslanib, axborotni himoyalashning lokal vositalarini markazlashtirilgan boshqarish;

– korxona muhitida siyosat obyektlarini tokenlar va ochiq kalitlar infratuzilmasidan foydalanib qat'iy autentifikatsiyalash;

– katalogda belgilangan korxona resurslaridan yoki butun katalog qismlaridan foydalanishni ma'murlashning kengaytirilgan imkoniyatlari;

– hisob-kitoblikni (korporativ tarmoq masshtabida tizimning taqsimlangan obyektlarining o'zaro aloqasidagi barcha amallarini ro'yxatga olish) va auditni, xavfsizlik monitoringini, xavotirli signalizatsiyani ta'minlash;

– umumiy boshqarish tizimlari va xavfsizlikning infratuzilma tizimlari bilan integratsiyalanishi.

Ushbu Konsepsiya doirasida «xavfsizlik siyosatiga asoslangan PBM (Policy Based Management) boshqarish» deganda korxona biznes-obyekti uchun ta'riflangan qoidalar to'plami tushuniladi. Bu qoidalar to'plami obyektlarning biznes-sohani to'liq qamrab olishini va ishlatiluvchi boshqarish qoidalarining ziddiyatlik emasligini kafolatlaydi.

PBM prinsiplariga asoslangan, korxona xavfsizligini boshqarishga mo'ljallangan GSM boshqarish tizimi quyidagi talablarga javob beradi:

– korxona xavfsizligi siyosati mantiqiy va semantik bog'langan, shakllanuvchi, tahrirlanuvchi va tahlillanuvchi ma'lumotlarning bir butun tuzilmasidan iborat;

– korxona xavfsizligi siyosati yagona kontekstda himoyaning barcha sathlari uchun himoyaning tarmoq siyosati va korxona axborot resurslari xavfsizlik siyosatining bir butuni sifatida belgilanadi;

– korxona resurslarini va xavfsizlik siyosatini ma'murlashni yengillashtirish maqsadida siyosat parametrlari soni minimallashtiriladi.

GSM boshqarish tizimi xavfsizlik siyosatining korxona xavfsizligi konsepsiyasi modeliga mosligini tekshiruvchi ko'p mezonli vositalar evaziga xavfsizlik siyosatini tahlillashning turli-tuman mexanizmlarini ta'minlaydi.

Xavfsizlikning global va lokal siyosatlari

Korxona xavfsizligining global siyosati axborot xavfsizligi kontekstida korporativ tarmoq obyektlari o'zaro aloqasining parametrlarini tavsiflovchi xavfsizlik qoidalarining chekli to'plamidir.

Bunda xavfsizlikning global siyosati obyekti sifatida alohida ishchi stansiyalari va qism tarmoqlar hamda o'z ichiga kompaniyaning butun tuzilmaviy bo'limlarini oluvchi (masalan, marketing bo'limi yoki moliyaviy departament) obyektlar guruhi yoki hatto alohida kompaniya ko'rilishi mumkin.

Xavfsizlikning global siyosati tarmoqdagi o'zaro aloqaga hamda tizimning nazoratlash va boshqarish funksiyalariga taalluqli bo'lishi mumkin. Bajaradigan funksiyalari bo'yicha xavfsizlikning global siyosati quyidagi guruhlarga bo'linadi:

– *VPN qoidalari.* Qoidalarning bu guruhi IPSec protokollari yordamida amalga oshiriladi;

– *paketli filtrlash qoidalari.* Bu qoidalar Stateful va Statles xilidagi paketli filtrlashni ta'minlaydi.

– *proxy-qoidalar.* Bu qoidalar berilgan tatbiqiy protokllar boshqaruvida uzatiluvchi trafikni filtrlashga javob beradi;

– *autentifikatsiyalangan/avtorizatsiyalangan foydalanish qoidalari;*

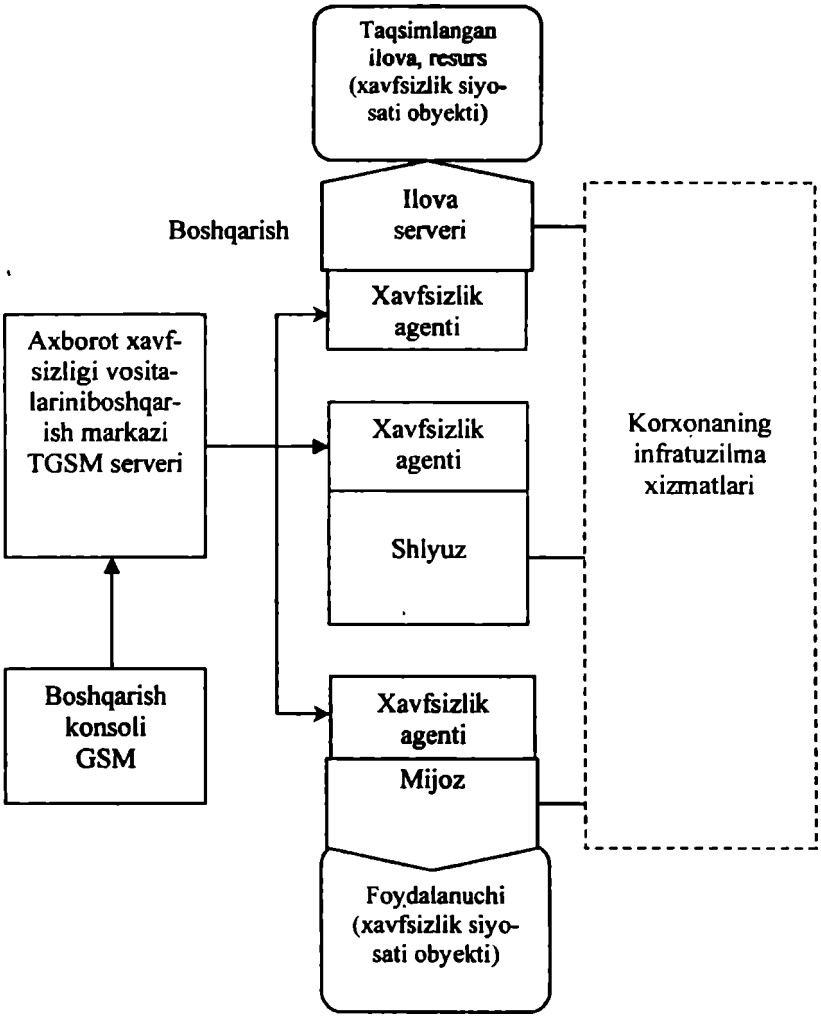
– *signalizatsiyaga va hodisaviy protokollashga javob beruvchi qoidalar.*

Xavfsizlikning global siyosati tarmoq sathida xavfsizlik siyosatining mantiqiy yaxlit va semantik to'liq tavsifi bo'lib, uning asosida alohida qurilmalar xavfsizligining lokal siyosati qurilishi mumkin.

Xavfsizlikning lokal siyosati axborot xavfsizligining qandaydir servi-sini amalga oshiruvchi har qanday himoyalash vositasiga zarur hisoblanadi. An'anaviy yondashishda ma'murga har bir himoya vositasini alohida sozlashga yoki eng oddiy soziashni uzellarning katta soniga qaytarishga (replikatsiyalashga) to'g'ri kelar edi. Ravshanki, bu ma'murlashning katta sonli xatoligiga olib kelar va natijada, korporativ tarmoqning himoyalanish darajasi jiddiy pasayar edi.

Ma'mur tomonidan xavfsizlikning global siyosati shakllantirilganidan so'ng boshqarish markazi uning asosida har bir himoya vositasi uchun avtomatik tarzda himoyalashning alohida lokal siyosatini hisoblaydi va mos himoya vositasining boshqarish moduliga zaruriy sozlashlarni avtomatik tarzda yuklaydi.

Tarmoqda xavfsizlikning global siyosatini va muayyan qurilmada xavfsizlikning lokal siyosatini amalga oshirish qoidalarining bir-biridan farqi shundaki, xavfsizlikning global siyosatidagi qoidalardan foydalanish obyektlari va subyektlari tarmoq chegarasida ixtiyoriy ravishda taqsimlanishi mumkin, xavfsizlikning iokai siyosatidagi qoidalardan esa faqat tarmoq qurilmalaridan birining muhiti chegarasida foydalanish mumkin.



12.4-rasm. Axborot xavfsizligi vositalarini boshqarish tizimining umumiy tuzilma sxemasi.

Axborot xavfsizligi vositalarini boshqarish tizimining umumiy tuzilma sxemasi 12.4-rasmda keltirilgan. Asosiy xavfsizlik vositalarining vazifalari quyidagicha. Mijoz shaxsiy kompyuterida o'rnatilgan

xavfsizlik agenti, odatda, «mijoz-server» ilovalarida mijoz sifatida qatnashuvchi alohida foydalanuvchini himoyalashga mo'ljallangan.

Ilovalar serveriga o'rnatilgan *xavfsizlik agenti* taqsimlangan ilovalarning server komponenti xavfsizligini ta'minlashga mo'ljallangan. Shlyuz kompyuteriga o'rnatilgan *xavfsizlik agenti* turli tarmoq xavfsizligi siyosatini muvofiqlashtirish masalasini yechgan holda, korxona ichida yoki korxonalar orasida tarmoq agentlarini ajratilishini ta'minlaydi.

Boshqarish markazi tarmoq masshtabida xavfsizlikning global siyosatini tavsiflashni, global siyosatni himoyalash qurilmasi xavfsizligining lokal siyosatiga translatsiyalashni, himoyalash qurilmasini yuklashni va tizimning barcha agentlari holatini nazoratlashni ta'minlaydi.

Boshqarish konsoli ma'mur (ma'murlar) ish joyini tashkil etishga mo'ljallangan. GSMning har bir serveri uchun bir necha konsollar o'rnatilishi mumkin.

Xavfsizlikning lokal agenti oxirgi qurilmada (mijozda, serverda, shlyuzda) joylashtiriluvchi dastur bo'lib, quyidagi funksiyalarni bajaradi:

– xavfsizlik siyosati obyektlarini autentifikatsiyalash, jumladan, auten-tifikatsiyalashning turli servislarini integratsiyalash;

– tizimdagi foydalanuvchini va u bilan bog'liq hodisalarni aniqlash;

– xavfsizlik vositalarini markazlashtirilgan boshqarishni va foydalanish nazoratini ta'minlash;

– ilovalar manfaati uchun resurslarni boshqarish, tatbiqiy sath resurslaridan foydalanishni boshqarishni madadlash;

– trafikni himoyalash va autentifikatsiyalash;

– trafikni filtrlash;

– hodisaviy protokollash, monitoring, xavotirli signalizatsiya.

Lokal agentning markaziy elementi – xavfsizlikning lokal siyosatining protsessori (LSP processor) xavfsizlikning lokal siyosatini izohlaydi va boshqa komponentlar orasida chaqirishlarni taqsimlaydi.

12.3. Axborot tizimlarining auditi va monitoringi

Axborot xavfsizligi tizimi amalga oshirilganida tarmoq infratuzilmasini murakkabligi, ma'lumotlar va ilovalarning turli-tumanligi sababli ko'pgina tahdidlar xavfsizlik ma'murining e'tiboridan chetda qolishi mumkin. Shuning uchun axborot tizimlarining muntazam auditi va doimiy monitoringi amalga oshirilishi zarur.

Axborot tizimlari xavfsizligining auditi. Audit-korxonaning alohida sohalarini mustaqil ekspertizasi. Korxona auditining tashkil etuvchilaridan biri uning axborot tizimi auditi hisoblanadi. Axborot tizimlarining auditi – axborot tizimining himoyalanishining joriy holati, undagi harakatlar va hodisalar xususidagi obyektiv ma'lumotlarni olish va baholash, ular sathining belgilangan mezonga mosligini aniqlovchi tizimli jarayondir. Audit o'tkazilishi axborot tizimi joriy xavfsizligini baholashga, xavf-xatarni baholashga, ularning tashkilot biznes-jarayonlariga ta'sirini bashoratlashga va boshqarishga, tashkilot axborot resurslari xavfsizligini ta'minlash masalasiga asosli yondashishga imkon beradi.

Axborot tizimlari xavfsizligining auditi quyidagi bosqichlarni o'z ichiga oladi:

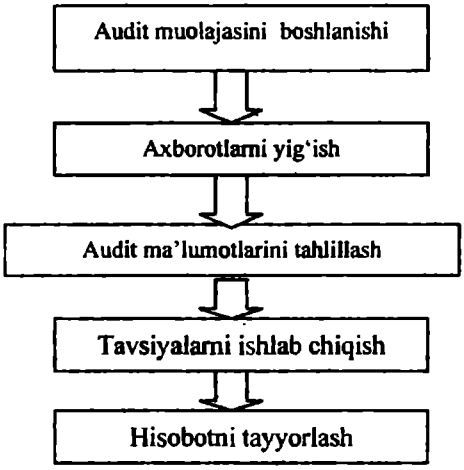
– audit muolajasining boshlanishi;
– audit axborotini yig'ish;
– audit ma'lumotlarini tahlillash;
– tavsiyalar ishlab chiqish;
– hisobot tayyorlash.

Audit bosqichlarining bajarilish ketma-ketligi 12.5-rasmda kelitirilgan.

Audit muolajasining boshlanishi. Audit, bu masalada manfaatdor hisoblanuvchi, kompaniya rahbariyati tashabbusi bilan o'tkaziladi. Audit tadbirlarning kompleksi bo'lib, unda auditor bilan birga kompaniyaning aksariyat tuzilmaviy bo'linmalarining vakillari qatnashadi. Bu jarayonda ishtirok etuvchilarining harakatlari aniq muvofiqlashtirilishi shart. Shu sababli, audit muolajasining boshlanishi bosqichida audit o'tkazish re-

jasini tayyorlash va tasdiqlash, auditor huquqi va majburiyatini belgilash bilan bog'liq tashkiliy masalalar yechilishi lozim.

Audit muolajasining boshlanishi bosqichida tekshirish doirasi aniqla-nishi lozim. Kompaniyaning axborot qismi tizimining birini konfidensiallik nuqtai nazaridan auditga tortib bo'lmasa, ikkinchisini, yetarlicha jiddiy bo'lmaganligi sababli, audit doirasidan chiqarish mumkin.



12.5-rasm. Audit bosqichlarining bajarilishi ketma - ketligi.

Audit axborotini yig'ish. Bu bosqich eng murakkab va uzoq davom etadi. Bunga sabab, axborot tizimiga kerakli hujjatlarning yo'qligi va auditorning tashkilotning ko'pgina lavozimli shaxslari bilan bevosita o'zaro muloqotda bo'lishi zaruriyati. Auditor tashkilot, axborot tizimining ishlashi va joriy holati xususidagi axborotni kompaniyaning javobgar shaxslari bilan maxsus tashkil etilgan suhbat orqali, texnikaviy va tashkiliy-boshqarish hujjatlarni o'rganish yo'li bilan hamda ixtisoslashtirilgan dasturiy vositalar yordamida axborot tizimini tadqiqlash orqali oladi.

Audit ma'lumotlarini tahlillash. Tahlillash axborot tizimlarining auditida eng mas'uliyatli bosqich hisoblanadi. Tahlillashda noaniq, eskirgan ma'lumotlardan foydalanish nojoizdir, shu sababli

ma'lumotlarga aniqlik kiritilishi va axborotlar jiddiy yig'ilishi mumkin. Audit ma'lumotlarini tahlillashda quyidagi uchta yondashishdan foydalaniladi.

Birinchi yondashish xavf-xatarlarni tahlillashga asoslanadi. Xavf-xatarlarni tahlillashdan maqsad mavjud xavf-xatarlarni aniqlash va ular kattaligini baholash (ularga sifatiy va miqdoriy baho berish). Ushbu yondashish juda murakkab bo'lib, ko'p mehnat sarf etiladi va auditorning eng yuqori malakasini talab qiladi.

Ikkinchi yondashish axborot xavfsizligi standartlaridan foydalanishga asoslangan. Standartlar axborot tizimlarining keng sinfi uchun dunyo amaliyotini umumlashtirish natijasida shakllangan xavfsizlik talablarining bazaviy to'plamini belgilaydi. Bu holda auditordan, berilgan axborot tizimi uchun standart talablari to'plamini to'g'ri tanlash talab etiladi. Soddaligi va ishonchliligi tufayli bu yondashish amalda keng qo'llaniladi. U resurslar-ning minimal sarfida axborot tizimi xususida asoslangan xulosalar qilishga imkon beradi.

Uchinchi yondashish oldingi ikkala yondashishni kombinatsiyalashni ko'zda tutadi. Axborot tizimiga quyiladigan xavfsizlikning bazaviy talablari standart orqali aniqlansa, berilgan axborot tizimi ishlashining xususiyatlarini hisobga oluvchi qo'shimcha talablar xavf-xatarlarni tahlillash asosida shakllantiriladi.

Tavsiyalar ishlab chiqish. Tahlillash natijalari tavsiyalar ishlab chiqish uchun asos bo'ladi. Auditor tavsiyalari muayyan va berilgan axborot tizimiga qo'llaniladigan, iqtisodiy asoslangan, isbotlangan (tahlillash natijalari bilan quvvatlangan) va muhimlik darajasi bo'yicha rutbalangan bo'lishi shart. Auditning muntazam o'tkazilishi axborot tizimining barqaror ishlashini kafolatlaydi. Shuning uchun professional audit natijalaridan biri keyingi tekshirishlarni o'tkazish reja-grafigini shakllantirishdan iborat.

Hisobot tayyorlash. Auditor hisoboti audit o'tkazishning asosiy hujjati hisoblanadi va uning sifati auditor ishining sifatini xarakterlaydi.

Hisobot tarkibida audit o'tkazish maqsadining tavsifi, tekshiriluvchi axborot tizimining xarakteristikasi, audit o'tkazish doirasi va ishlatiluvchi usullar bo'yicha ko'rsatma, audit-ma'lumotlari tahlilining nati-

jasi, bu natijalarni umumlashtiruvchi va axborot tizimi himoyalanish sathining standart talablariga javob berishi bo'yicha xulosalar va albatta, mavjud kamchiliklarni bartaraf etish va himoya tizimini takomillashtirish bo'yicha tavsiyalar bo'lishi lozim.

Axborot tizimlari xavfsizligining monitoringi

Hozirda tarmoqlararo ekran, virtual xususiy tarmoq, ruxsatsiz foydalanishdan himoyalash vositalari kabi himoyaning an'anaviy vositalari ishonchli va samarali axborot xavfsizligi tizimini qurishga zarur bo'lsada, yetarli emas. Chunki bu an'anaviy vositalar faqat hujumni blokirovka qilishga qodir, ammo hujumlarni oldini olish va oqibatlarini aniqlash imkoniyati ularda mavjud emas.

Ushbu muammoning yechimi asoslangan yondashish faol audit texnologiyasi yoki xavfsizlikni faol (adaptiv) boshqarish texnologiyasi nomini olgan. Xavfsizlikni faol boshqarish texnologiyasi quyidagi komponentlarni o'z ichiga oladi:

– ishchi stansiyalari, serverlar, ma'lumotlar bazasini boshqaruvchi tizimlar, tarmoq ulanishlari va Internet va boshqa global tarmoqlarga ula-nish nuqtalari kabi axborot tizimi obyektlari himoyalanishini tahlillovchi va zaifliklarini qidiruvchi vositalar;

– hujumlarni aniqlash va tahlillash vositalari;

– infratuzilma o'zgarishida yoki hujumlarda himoyalash vositalarini vaqtning real rejimida sozlashlarni moslashtirish va boshqarish vositalari.

Axborot xavfsizligi tizimi monitoringi vazifalarini himoyalanishni tahlillash va hujumlarni aniqlash vositalari bajaradi. Himoyalanishni tahlillash vositalari ishchi stansiyalarida va serverlarda, ma'lumotlar bazasida operatsion tizim himoyasi elementlarining sozlanishini tadqiqlaydi. Ular tarmoq topologiyasini tadqiqlaydi, himoyalanmagan yoki noto'g'ri tarmoq ulanishlarini qidiradi, tarmoqlararo ekranlar sozlanishini tahlillaydi. Himoyalanishni tahlillash vositalarini, ularning ishlashi bo'yicha xavfsizlik skanerlari deb ham yuritishadi. Tahlillash natijasida skaner ma'murga yuboriluvchi, tarkibida aniqlangan zaifliklar va ularni yo'qotish qoidalari bo'lgan hisobotni shakllantiradi. Agar

skaner tarkibida xavfsizlik vositalari sozlanishini boshqaruvchi vositalar bo'lsa, u mustaqil tarzda ularni qayta konfiguratsiyalashi mumkin.

Tashkilotning zamonaviy infratuzilmasini hisobga olgan holda aytish mumkinki, bunday skanerlarning mavjudligi axborot tizimlari xavfsizligi monitoringining muhim elementi hisoblanadi. Ta'kidlash lozimki, bu vositalar himoyani hujum sodir bo'lishidan avval amalga oshiradi.

Axborot tizimi xavfsizligi monitoringining yana bir zarur elementi hujumlarni aniqlovchi vositalardir. Hujumlarni aniqlash korporativ tarmoqda kechuvchi shubhali harakatlarni baholash jarayonidir. Hujumlarni aniqlash vaqtning real rejimida tarmoq trafigini hamda operatsion tizim va ilovalarning ro'yxatga olish jurnallarini tahlillash orqali amalga oshiriladi. Hujumlarni aniqlash tizimining komponentlari agentlar deb ataladi va ishchi stansiyalarda, serverlarda joylashtiriladi yoki tarmoqning qandaydir segmentini yoki butun tarmoqni qoplaydi. Agentlar o'zlarining ishida skanerlar kabi ma'lum zaifliklar ro'yxatidan foydalanib, hodisalarni ushbu zaifliklar bilan taqqoslaydi. Qandaydir uzelda shubhali faoliyat aniqlanganida hujumlarni aniqlash tizimi ushbu faoliyat faolligi xususidagi ogohlantirishni ma'murga jo'natadi. U ogohlantirishni uzelning o'ziga jo'natishi yoki uzel ishini blokirovka qilish mumkin. Ushbu tizimning farqli xususiyati – uning bo'lib o'tgan hujumlarni aniqlash uchun hodisalar jurnalini tahlillashidir.

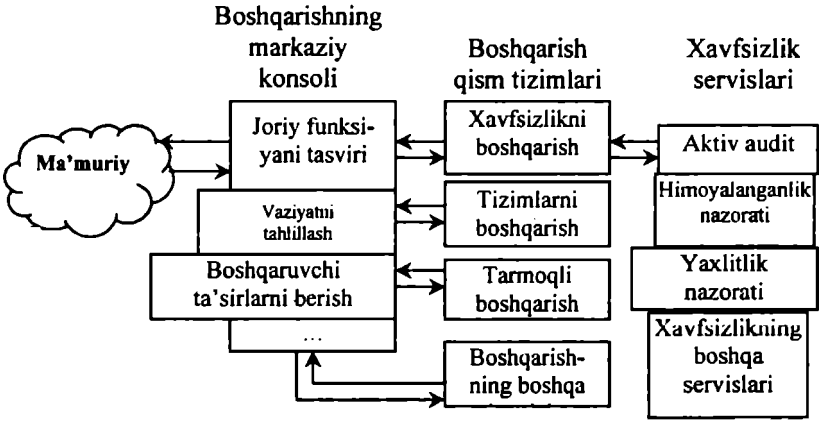
Xavfsizlik vositalarini boshqarish shakli bo'yicha passiv va faol (aktiv) bo'lishi mumkin. Passiv boshqarishda tarmoqni boshqarish tizimiga yoki ma'murga faqat xabar berilsa, faol boshqarishda hujumlovchi uzel yoki foydalanuvchi bilan mustaqil tarzda sessiya tugallanadi.

Bundan tashqari, bu tizimning vazifasiga tarmoqdagi, ilovalardagi yoki tashkilot axborot tizimining boshqa komponentlaridagi zaifliklarni yo'qotish bo'yicha ma'murga tavsiyalar ishlab chiqish kiradi.

Faol audit tizimi (monitoringi) va umumiy boshqarish o'rtasida o'zaro aloqani tashkil etish muhim masalalardan hisoblanadi. Faol audit namunaviy boshqarish funksiyalarini, ya'ni axborot tizimidagi faollik xususidami ma'lumotlarni tahlillashni, joriy vaziyatni akslantirishni, shubhali faollikka avtomatik tarzda reaksiya ko'rsatilishini bajaradi.

Tarmoqni boshqarish tizimi xuddi shunga o'xshash ishlaydi. Faol audit va umumiy boshqarishni umumiy dasturiy-texnik va tashkiliy yechimlardan foydalanib integratsiyalash maqsadga muvofiq hisoblanadi. Bu integratsiyalangan tizimga yaxlitlikni nazoratlash hamda axborot tizimi xatti-harakatlarining o'ziga xos jihatlarini kuzatuvchi boshqa yo'nalishdagi agentlar ham kiritilishi mumkin (12.6-rasm).

Boshqarishning markaziy konsoli mavjud bo'lib, unda faol audit (monitoring) yaxlitlikni nazoratlash, boshqa jihatlar bo'yicha tizim va tarmoqlarni nazoratlash tizimlaridan ma'lumotlar to'planadi. Bu konsolda joriy vaziyat akslantiriladi, undan avtomatik tarzda yoki qo'lda boshqarish komandalari beriladi. Texnik yoki tashkiliy sabablarga ko'ra, bu konsol bir necha ishchi joyi ko'rinishida fizik amalga oshirilishi mumkin (xavfsizlik ma'muriga joy ajratish bilan).



12.6-rasm. Xavfsizlik servislari va boshqarish tizimining integratsiyasi.

Tarmoq xavfsizligini adaptiv boshqarish modelidan foydalanish barcha tahdidlarni nazoratlash va ularga o'z vaqtida reaksiya ko'rsatish, nafaqat tahdidlarni amalga oshirishga sharoit yaratuvchi zaifliklarni yo'qotish, balki zaifliklarni paydo bo'lish sharoitlarini tahlillash imkonini beradi.

12.4. Xavf-xatarlarni tahlillash va boshqarish

Xavf-xatarlarni tahlillash va boshqarish axborot tizimidagi tahdidlar, zaifliklar va xavf-xatarlarni baholash hamda ushbu axborot tizimi xavfsizligining yetarli darajasini ta'minlovchi qarshi choralarni aniqlash uchun ishlatiladi.

Xavf-xatarlarni tahlillash-tahdidlarni, zaifliklarni va korporativ axborot tizimi xavfsizligiga bo'lishi mumkin bo'lgan zararlarni aniqlash jarayoni. Xavf-xatarlarni tahlillashdan maqsad mavjud xavf-xatarlarni aniqlash va ular me'yorini baholash (ularga miqdoriy baho berish). Xavf-xatarlarni tahlillash kompyuter axborot tizimi xavfsizligini tekshirish bo'yicha tadbirni o'z ichiga oladi. Bu tadbirga binoan qaysi resurslarni qaysi tahdidlardan himoyalash zarurligi hamda u yoki bu resurslar qanday darajada himoyaga muhtoj ekanligi aniqlanadi.

Xavf-xatarlarni tahlillashga turli yondashishlar mavjud. Yondashishni tanlash tashkilotda axborot xavfsizligi rejimiga quyiladigan talablar darajasiga va e'tiborga olinuvchi tahdidlar xarakteriga (tahdidlar ta'siri spektriga) bog'liq. Talablarning ikkita darajasi farqlanadi:

– axborot xavfsizligi rejimiga minimal talablar;

– axborot xavfsizligi rejimiga oshirilgan talablar.

Axborot xavfsizligi rejimiga minimal talablar *axborot xavfsizligining bazaviy darajasiga* mos keladi. Bu darajadan, odatda, namunaviy loyiha yechimlarida foydalaniladi. Xavf-xatarlarni tahlillash soddalashtirilgan sxema bo'yicha o'tkaziladi: xavfsizlikka tahdidlarning ko'p tarqalgan to'plami ularning ehtimolligini baholamasdan ko'riladi. Viruslar, asbob-uskunalarning buzilishi, ruxsatsiz foydalanish va h. kabi ehtimolligi yuqori tahdidlarning minimal to'plami ko'riladigan qator standartlar va spetsifikatsiyalar mavjud. Bunday tahdidlarni betaraflashtirish uchun ularning amalga oshirilishi ehtimolligi va resurslarning zaifligidan qat'i nazar, qarshi choralar ko'rilishi lozim, ya'ni bazaviy darajada tahdidlar xarakteristikalarini ko'rish shart emas.

Axborot xavfsizligi rejimiga oshirilgan talablar, axborot xavfsizligi rejimining buzilishi og'ir oqibatlarga sabab bo'lganida va axborot xavfsizligi rejimiga minimal talablar yetarli bo'lmaganida ishlatiladi.

Axborot xavfsizligi rejimiga oshirilgan talablarni ta'riflash uchun resurslar ahamiyatini aniqlash, tadqiqlanuvchi axborot tizimi uchun dolzarb bo'lgan tahdidlar ro'yxati bilan standart to'plamni to'ldirish, tahdidlar ehtimolligini baholash va resurslar zaifligini aniqlash zarur.

Xavf-xatarni tahlillash jarayonini quyidagi bosqichlarga ajratish mumkin:

– korporativ axborot tizimining tayanch resurslarini identifikatsiyalash;

– u yoki bu resursning muhimligini aniqlash;

– tahdidlarning amalga oshirilishiga imkon beruvchi mavjud xavfsizlik tahdidlarni va zaifliklarni identifikatsiyalash;

– xavfsizlikka tahdidlarni amalga oshirilishi bilan bog'liq xavf-xatarlarni hisoblash.

Resurslar uchta kategoriyaga – axborot resurslariga, dasturiy ta'minotga va texnik vositalarga (fayl serverlari, ishchi stansiyalar, ko'priklar, marshrutizatorlar va h.) bo'linadi. Har bir kategoriya ichida resurslarni sinflarga va qism sinflarga ajratish mumkin. Faqat korporativ axborot tizimi funksionalligini belgilovchi va xavfsizlikni ta'minlash nuqtai nazaridan muhim bo'lgan resurlar identifikatsiyalanishi lozim.

Resursning muhimligi (narxi) bu resursning konfidensialligi, yaxlitligi yoki foydalanuvchanligi buzilganida yetkazilgan zarar miqdori bilan belgilanadi. Resurslar narxini baholashda resurslarining har bir kategoriyasi uchun bo'lishi mumkin bo'lgan zarar miqdori belgilanadi.

Namunaviy xavfsizlik tahdidlariga korporativ axborot tizimi resurslariga lokal masofadan hujumlar, tabiiy ofat, xodimlar xatosi, dasturiy ta'minotdagi xatolik yoki apparaturaning nosozligi sabab bo'luvchi korporativ axborot tizim ishidagi buzilishlar taalluqli. Tahdid darajasi deganda, uning amalga oshirilishi ehtimolligi tushuniladi.

Himoyaning bo'shligi korporativ axborot tizimidagi zaifliklarga sabab bo'ladi. Zaifliklarni baholash xavfsizlik tahdidlarining muvaffaqiyatli amalga oshirilish ehtimolligini aniqlashni nazarda tutadi. Shunday qilib, zarar yetkazish ehtimolligi tahdidlarning amalga oshirilishi ehtimolligi va zaiflik miqdori orqali aniqlanadi.

Xavf-xatar darajasi resurs narxi, tahdid darajasi va zaiflik miqdori asosida aniqlanadi. Resurs narxi, tahdid darajasi va zaiflik miqdori oshishi bilan xavf-xatar darajasi ham oshadi. Xavf-xatarlar darajasini baholash asosida xavfsizlik talablari belgilanadi.

Xavf-xatarlarni boshqarish masalasi, xavf-xatar darajasini maqbul miqdorgacha kamaytirishga imkon beruvchi qarshi choralarni asosli tanlashni va amalga oshirish narxini baholashni o'z ichiga oladi. Tabiiyki, qarshi choralarni amalga oshirish narxi bo'lishi mumkin bo'lgan zarar miqdoridan kam bo'lishi kerak.

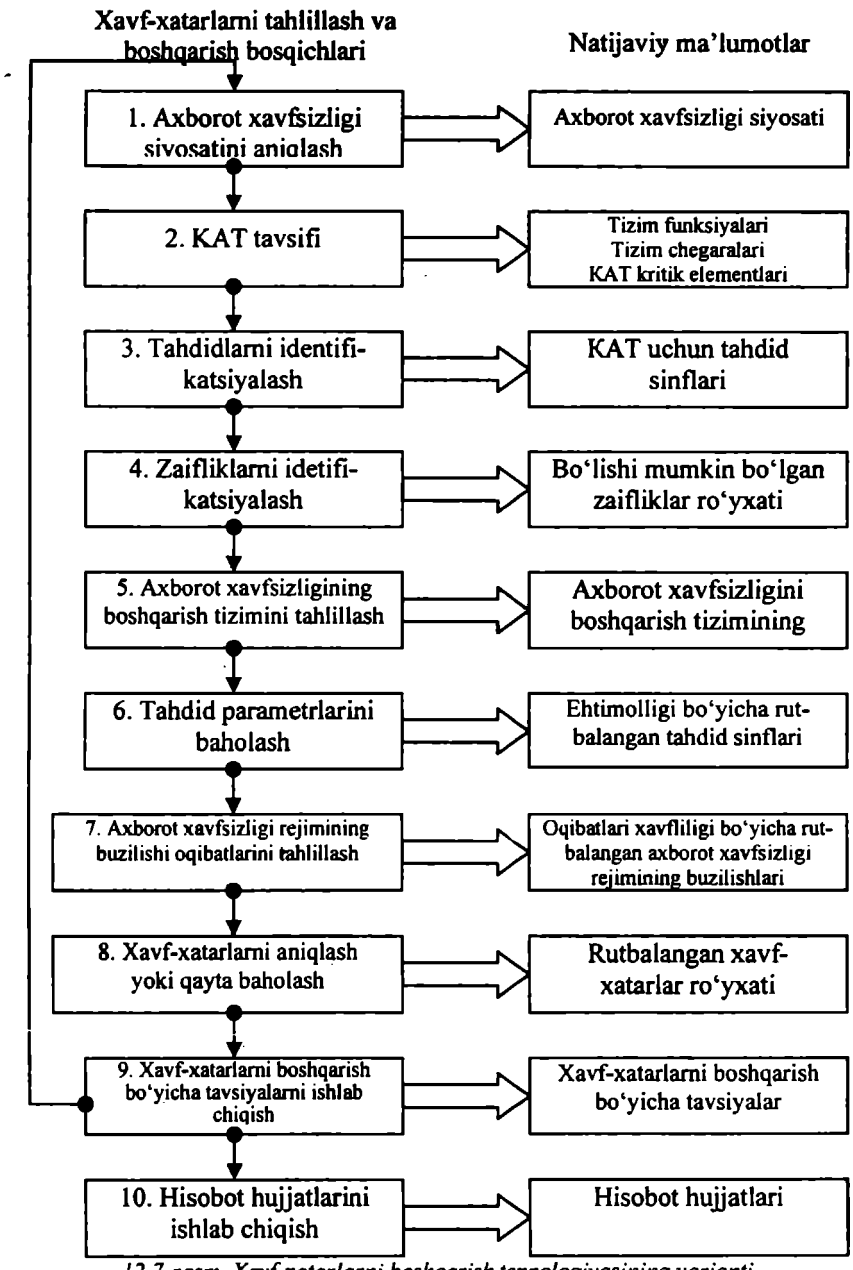
12.7-rasmda xavf-xatarlarni boshqarish texnologiyasining bosqichlari keltirilgan.

Axborot xavfsizligi siyosatini aniqlash. Bu bosqichda axborot xavfsizligi sohasidagi qo'llanma-hujjatlar, standartlar, axborot xavfsizligining asosiy qoidalari, xavf-xatarlarni boshqarishga yondashishlar aniqlanadi hamda qarshi choralar strukturizatsiyalanadi va korporativ axborot tizimini sertifikatsiyalash tartibi belgilanadi.

Korporativ axborot tizimini (KAT) tavsiflash. Ushbu bosqichda axborot xavfsizligi sohasidagi xalqaro, davlat va korporativ standartlarga binoan korporativ axborot tizimning funksional vazifalari tavsiflanadi. Kompaniyaning kritik axborot resurslari, jarayonlari va servislari tavsiflanadi; korporativ axborot tizimining chegaralari hamda boshqarish va ma'lumotlar bo'yicha eng muhim komponentlarining tarkibi va bog'lanishlari aniqlanadi.

Tahdidlarni identifikatsiyalash. Ushbu bosqichda tahdidlar ro'yxati tuziladi va ularning darajasi baholanadi. Bunda turli tashkilotlarning tahdidlar sinflari ro'yxatidan hamda berilgan tahdidni amalga oshirish ehtimolligining reytingi yoki o'rtacha qiymatidan foydalanish mumkin.

Zaifliklarni identifikatsiyalash. Ushbu bosqichda berilgan korporativ axborot tizimining zaifliklari ro'yxati, ularning amalga oshirilishidagi joiz natijalar ko'rsatilgan holda tuziladi. Mavjud korporativ axborot tizimi uchun ro'yxatlar qator manbalardan foydalanilib tuziladi. Bu manbalarga zaifliklarni tarmoq skanerlari, turli tashkilotlarning zaifliklar katalogi, xavf-xatarlarni tahlillovchi ixtisoslashtirilgan usullar kiradi.



12.7-rasm. Xavf-xatarlarni boshqarish texnologiyasining varianti.

Korporativ axborot tizimining boshqarish tizimini tahlillash. Ushbu bosqichda boshqarish tizimi, aniqlangan tahdidlarga va zaifliklarga joiz bo'lgan ta'sir nuqtai nazaridan tahlillanadi.

Tahdid parametrlarini baholash. Ushbu bosqichda hodisaga olib keluvchi zaiflikning amalga oshirilishi imkoniyati baholanadi. Baholashning namunaviy shkalasi – bir necha rutbali (masalan, past, o'rta, va yuqori sath) sifatiy (balli) shkaladir. Bunday baho ekspert tomonidan mavjud obyektiv faktorlarni hisobga olgan holda beriladi.

Axborot xavfsizligi rejimining buzilishi oqibatlarini tahlillash. Ushbu bosqichda axborot xavfsizligi rejimining buzilishi bahosi aniqlanadi. Buzi-lish oqibatlari moliyaviy yo'qotishlarga, obro'sizlanishga, rasmiy tuzilmalar tomonidan ko'ngilsizliklarga va h. sabab bo'lishi mumkin. Buzilish oqibatlarini baholash uchun mezonlar tizimi tanlanadi va oqibatlar og'irligini baholash uchun integratsiyalangan shkala belgilanadi.

Xavf-xatarlarni baholash. Ushbu bosqichda axborot resurslari xavfsizligining buzilishi xavf-xatar darajasi baholanadi. Xavf-xatar darajasi qiymati tahdidlar, zaifliklar darajasiga va bo'lishi mumkin bo'lgan oqibatlar og'lrligiga bog'liq. Xavf-xatarlarni baholashda sifatiy va miqdoriy usullardan foydalaniladi. Sifatiy usul ishlatilganda axborot xavfsizligi buzilishining bo'lishi mumkin bo'lgan xavf-xatarlar xavfliligi darajasi bo'yicha rutbalanishi lozim. Miqdoriy usul ishlatilganda xavf-xatarlar miqdoriy shkalalarda baholanishi mumkin. Bu tavsiya etilayotgan qarshi choralarning narxi – samaradorligini tahlillashni osonlashtiradi. Ammo bu holda dastlabki ma'lumotlarni o'lchash shkalalariga va ishlatilayotgan modelning adekvatligiga juda yuqori talablar quyiladi. Oddiy holda xavf-xatarni baholashda ikkita omil-hodisa ehtimolligi va bo'lishi mumkin bo'lgan oqibatlar og'irligi ishlatilishi mumkin.

Xavf-xatarlarni boshqarish bo'yicha tavsiyalarni ishlab chiqish. Ushbu bosqichda turli sathlar (tashkiliy, dasturiy-texnik) va xavfsizlikning alohida jihatlari bo'yicha strukturizatsiyalangan qarshi choralarning kompleksi tavsiya etilishi lozim. Taklif etiluvchi qarshi choralar kompleksi xavf-xatarlarni boshqarishning tanlangan strategiyasiga binoan quriladi.

Hisobot hujjatlarni ishlab chiqish. Ushbu bosqichda xavf-xatarlarni tahlillash va boshqarishning barcha bosqichlari bo'yicha ish natijalari akslantirilgan hisobot hujjatlari tayyorlanadi.

Ta'kidlash lozimki, hozirda axborot xavf-xatarlarini baholashni avtomatlashtirish maqsadida dasturiy mahsulotlar ishlab chiqilgan.

12.5. Axborot xavfsizligi tizimini qurish metodologiyasi

Axborot xavfsizligi modelini qurish. Korxonadagi axborot xavfsizligi bo'yicha tadbirlar qonun chiqarish, tashkiliy va dasturiy-texnik xarakterga ega bo'lgan qator jihatlarni qamrab oladi. Ularning har birida korxona axborot xavfsizligini ta'minlash uchun bajarilishi zarur bo'lgan qator masalalar ta'riflanadi. Masalalarni hal etishda axborot xavfsizligi sohasidagi xalqaro standartlarga asoslangan korxona axborot xavfsizligining konseptual modelidan foydalanish mumkin.

Quyidagi xalqaro standartlar korporativ axborot tizimi himoyalanishini baholash mezonini va himoyalash mexanizmlariga qo'yiladigan talablarni aniqlovchi eng muhim me'yoriy hujjatlar hisoblanadi:

– axborot texnologiyalari xavfsizligini baholashning umumiy mezonlari ISO/IEC 15408 (The Common Criteria For Information Technology Security Evalution);

– axborot xavfsizligini boshqarishning amaliy qoidalari ISO/IEC 17799 (Code of practice for Information Security Management).

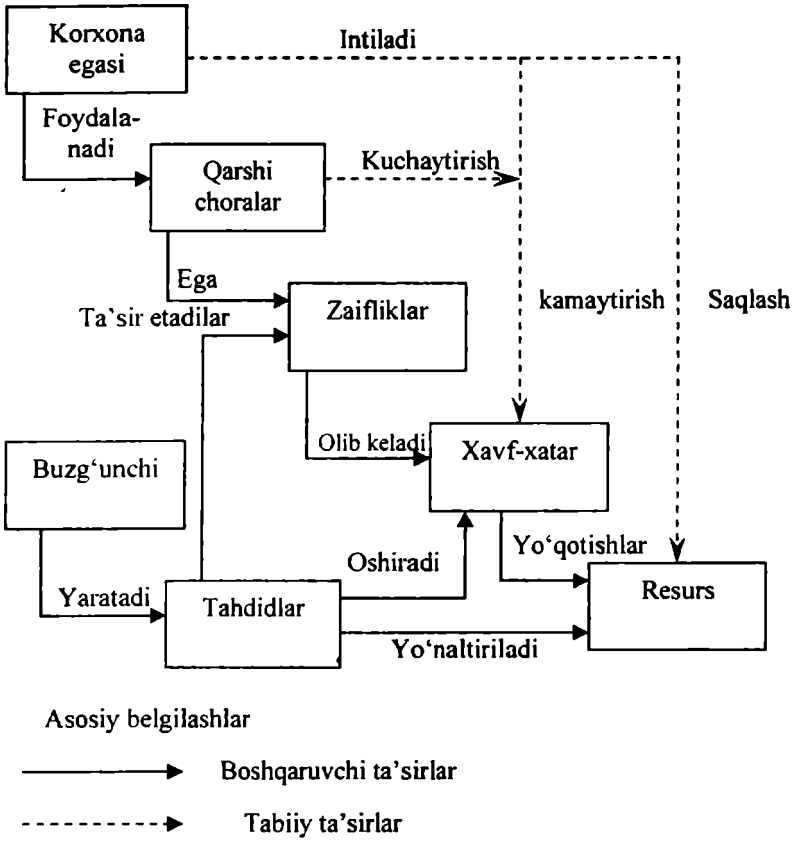
Ushbu xalqaro standartlarga to'la mos ravishda tuzilgan korxona axborot xavfsizligining konseptual modeli 12.8-rasmda keltirilgan.

Korxona axborot xavfsizligining konseptual modelida quyidagi omillar hisobga olingan:

– paydo bo'lish ehtimolligi va amalga oshirilish ehtimolligi bilan xarakterlanuvchi axborot xavfsizligi *tahdidlari*;

– tahdidlarning amalga oshirilishi ehtimolligiga ta'sir etuvchi axborot tizimi yoki qarshi chora tizimi (axborot xavfsizligi tizimi) *zaifliklari*;

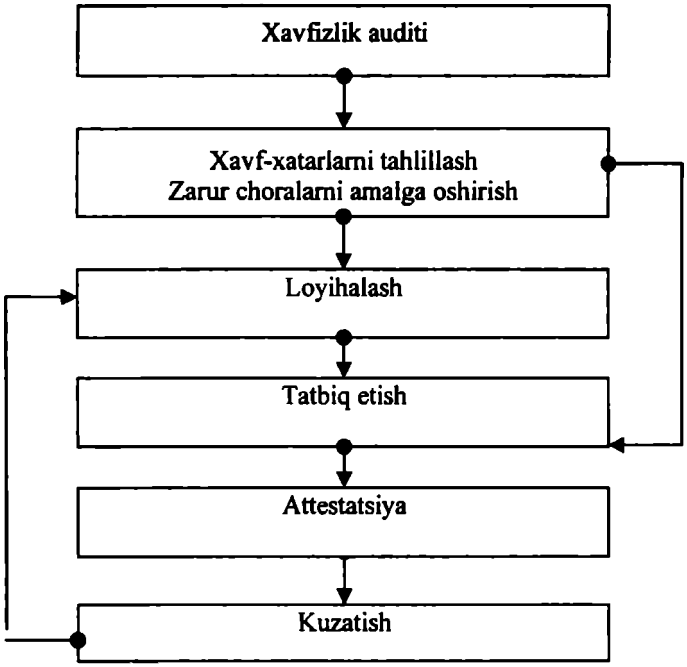
– axborot xavfsizligiga tahdidlar amalga oshirilishi natijasida korxonaga yetkaziluvchi zararni akslantiruvchi omil–*xavf-xatar*.



12.8-rasm. Korxona axborot xavfsizligi tizimining konseptual modeli.

Bu modelning harakatdagi subyektlari – Buzg'unchi (tahdidlar manbaini ifodalovchi) va ega (korxona ma'muri) obyekt-Resursga qarama-qarshi maqsadlarda ta'sir qiladilar. Resurs-korxonaning moddiy va axborot resurslarini va axborot xavfsizligi holatini ifodalaydi.

Axborot xavfsizligi tizimini qurish bosqichlari. Axborot xavfsizligi tizimini qurish bosqichlari quyidagi standartlashtirilgan ketma-ketlik amalga oshiriladi: xavfsizlik auditi; xavf-xatarlarni tahlillash, tizimni loyihalash, joriy etish, attestatsiyalash va kuzatish (12.9-rasm).



12.9-rasm. Axborot xavfsizligi tizimini qurish bosqichlari.

Xavfsizlik auditi. Hozirda «xavfsizlik auditi» tushunchasi yetarlicha keng talqin etiladi. Auditning quyidagi ko'rinishlari farqlanadi.

– axborot xavfsizligini testli buzish;
– ekspress-tekshirish;
– tizimni attestatsiyalash;
– loyihagacha tekshirish.

Axborot xavfsizligi testli buzish korporativ axborot tizimining himoyalanish darajasini aniqlash nuqtai nazaridan samarali hisoblanmaydi. «Bu-zuvchi»ning asosiy maqsadi bir ikki zaifliklarni topib, ularni tizimdan foydalanishda ishlatish. Agar «testli buzish» muvaffaqiyatli chiqsa, ushbu muayyan «buzish»ning mumkin bo'lgan ssenariysi rivojini oldini olib, zaifliklarni qidirishda davom etish kerak. «Testli

buzish»ning muvaffaqiyatsizligini babbaravar testlanuvchi tizimning himoyalanganligi va testlarning yetishmasligi kabi talqin qilish mumkin.

Ekspress-tekshirish doirasida, odatda, ko'p vaqt sarfini talab etmaydigan, standartizatsiyalangan tekshirishlar asosida korporativ axborot tizimi xavfsizlik vositalarining umumiy holati baholanadi. Ekspress-tekshirish, odatda, axborot resurslarining minimal himoyalanish darajasini ta'min-lovchi ustuvor yo'nalishlarni aniqlash zaruriyati tug'ilganda o'tkaziladi.

Tizimni attestatsiyalash tizimning axborot resurslarining himoyalanish talablariga mosligini tekshirish maqsadida amalga oshirilida. Bunda ham tashkiliy, ham texnik jihatdan talablar to'plami rasmiy tekshiriladi, xavfsizlik vositalarining amalga oshirilishining to'liqligi va yetarliligi ko'riladi.

Loyihagacha tekshirish auditning eng ko'p mehnat talab qiladigan varianti hisoblanadi. Bunday audit axborot resurslari ilovalarida korxona tashkiliy tuzilmasini va xodimlarning u yoki bu ilovalardan foydalanish qoidalarini tahlil etishni ko'zda tutadi. So'ngra ilovalarning o'zi tahlillanadi. Undan keyin bir sathdan ikkinchi sathning foydalanishdagi muayyan xizmatlar hamda axborot almashishga zarur bo'lgan xizmatlar tahlillanishi lozim. So'ngra xavfsizlikning o'rnatilgan vositalarini tahlillash bilan tasavvur to'ldiriladi.

Xavf-xatarlarni tahlillash 12.4-bo'limda batafsil ko'rilgan. Axborot xavfsizligi buzilganda loyihagacha tekshirish, xavf-xatarlarni tahlillash bilan birgalikda axborot tizimidagi mavjud xavf-xatarlarni rutbalashga va adekvat choralarni ishlab chiqishga imkon beradi.

Tizimni loyihalash. Himoyani tashkil etish strategiyasi nuqtai nazaridan resursli va servisli yondashish farqlanadi. Resursli yondashishda tizim resurslar to'plami sifatida ko'riladi va axborot xavfsizligi tizimining komponentlari bu resurslarga bog'lanadi. Resursli yondashish amalga oshirilganida axborotni himoyalash masalasi xizmatlar tuzilmasiga qo'shimcha cheklashlarsiz yechiladi. Bu esa bir jinsli bo'lmagan tizim sharoitida mumkin emas. Servisli yondashishda tizim foydalanuvchilarga taqdim etiluvchi xizmatlar to'plami kabi talqin qilinadi. Hozirgi vaqtda servisli yondashish afzalroq hisoblanadi, chunki u

tizimda amalga oshirilgan xizmatlarga bog'lanadi va «ortiqcha» xizmatlarni rad etish hisobiga qator tahdidlarni istisno qilinishiga imkon beradi. Bu esa tizimni yanada mantiqan asoslangan tizimga aylantiradi. Aynan servis yondashish xavfsizlikning zamonaviy standartlari, xususan, ISO/IEC 15408 asosida yotadi.

Axborot xavfsizligi tizimni qurishning ikkita asosiy ssenariysi mavjud: mahsulotli va loyihali. Mahsulotli ssenariy (yondashish) doirasida avval himoya vositalari to'plami tanlanadi, ularning funksiyalari tahlillanadi, so'ngra funksiyalar tahlili asosida axborot resurslaridan foydalanish siyosati belgilanadi.

Loyihaga xarajatlar nuqtai nazaridan mahsulotli ssenariy eng arzon hisoblanadi. Undan tashqari, yechimlarning tanqisligi sharoitida ko'pincha mahsulotli yondashish yagona hisoblanadi (masalan, kriptografik himoyada faqat shu yondashish qo'llaniladi).

Loyihali ssenariyda avval xavfsizlik siyosati ishlab chiqiladi, uning asosida xavfsizlik siyosatini amalga oshirishda zarur bo'lgan funksiyalar aniqlanadi, so'ngra bu funksiyalar bajarilishini ta'minlovchi himoya vositalari tanlanadi.

Loyihali ssenariy asosida qurilgan tizimlar yaxshiroq optimizatsiyalangan va attestatsiyaning yuqori natijalarini beradi. Ushbu yondashish mahsulotli yondashishdan farqli ravishda boshidan u yoki bu platforma bilan bog'lanmaganligi tufayli, katta geterogen tizimlarni qurishda afzal hisoblanadi. Undan tashqari, uzoq muddatga mo'ljallangan yechimlarni ta'minlaydi, chunki xavfsizlik siyosatini o'zgartirmasdan yechimlarni va himoya vositalarini almashtirishga imkon beradi.

Axborot xavfsizligi tizimi arxitekturasini tanlash nuqtai nazaridan obyektli, tatbiqiy yoki aralash yondashishdan foydalaniladi. Obyektli yondashish axborot xavfsizligini u yoki bu obyekt (bo'linma, filial, tashkilot) tuzilmasi asosida yaratadi. Obyektli yondashishning qo'llanishi tashkiliy choralarning bir jinsli to'plamini madadlovchi xavfsizlik mexanizmlari uchun universal yechimlar to'plamidan foydalanishni ko'zda tutadi. Bunday yondashishga misol tariqasida tashqi axborot almashish, lokal tarmoq, telekommunikatsiya tizimlarining va h. himoyalangan infratuzilmalarini qu- rishni ko'rsatish mumkin. Obyektli

yondashishning kamchiligi uning universal mexanizmlarining, ayniqsa, o'zaro murakkab bog'lanishli katta sonli ilovalarga ega bo'lgan tashkilotlar uchun tugal emasligi.

Tatbiqiy yondashish xavfsizlik mexanizmini muayyan ilovaga bog'lab yaratadi. Tatbiqiy yondashishga misol tariqasida avtomatlashtirishning alohida masalasi (buxgalteriya, kadrlar va h.) uchun qism tizimlarning himoyasini ko'rsatish mumkin. Ushbu yondashishning kamchiligi – ma'murlash va ishlatish xarajatlarini minimallashtirish maqsadida xavfsizlikning turli vositalarini uyg'unlashtirish zaruriyati.

Aralash yondashish yuqorida tavsiflangan ikkita yondashishni kombinatsiyalashni ko'zda tutadi. Bunday yondashish loyihalash bosqichida ko'proq mehnat talab qilsada, axborot xavfsizligi tizimini joriy etish va ishlatish narxi bo'yicha afzalliklarni berishi mumkin.

Joriy etish. Joriy etish bosqichi quyidagi ketma-ket o'tkaziluvchi tadbirlarni o'z ichiga oladi:

– himoya vositalarini o'rnatish va konfiguratsiyalash;

– xodimlarni himoya vositalari bilan ishlashga o'rgatish;

– dastlabki sinovni o'tkazish;

– tajribaviy ishlatishga topshirish.

Tajribaviy ishlatish, axborot xavfsizligi tizimini ishchi rejimiga tushirishdan avval, uning ishlashidagi mumkin bo'lgan kamchiliklarni aniqlashga va yo'qotishga imkon beradi. Agar tajribaviy ishlatish jarayonida komponentlarning to'g'ri ishlamasligi faktlari aniqlansa, himoya vositalari sozlanishiga va ularning ishlash rejimlariga va h. tuzatishlar kiritiladi.

Tizimni attestatsiyalash. Axborot xavfsizligi tizimini vakolatli idora tomonidan attestatsiyalash uning funksional to'liqligini va korporativ axborot tizimi himoyasining talab qilingan darajasi ta'minlanganligini tasdiqlashga imkon beradi. Tizimning attestatsiyasi xavfsizlik auditining bir ko'rinishi hisoblanadi va ishlatiluvchi choralar kompleksi va himoya vositalarining xavfsizlik darajasi talablariga mosligini baholash maqsadida himoyalanuvchi korxonani ishlatishning real sharoitlarida kompleks tekshirishni ko'zda tutadi.

Attestatsiya natijasida hisobot hujjati tayyorlanadi va moslik attestati beriladi. Bu attestat konfidensial axborot bilan attestatda ko'rsatilgan vaqt mobaynida ishlash huquqini beradi.

Kuzatish. Axborot xavfsizligi tizimining ishga layoqatligini va o'z vazifalarini tekis bajarilishini madadlash uchun xavfsizlik tizimining dasturiy va apparat ta'minotini texnik madadlash va kuzatish bo'yicha tadbirlar kompleksi ko'zda tutilishi lozim. Axborot xavfsizligi tizimini texnik madadlash va kuzatish xizmatchi xodimlarning bilimi va ko'nikmalarini talab etadi va himoyalanuvchi tizim egasi – tashkilot shtatidagi axborot xavfsizligiga javob beruvchi xodimlar tomonidan yoki ixtisoslashtirilgan tashkilot xodimlari tomonidan amalga oshirilishi mumkin.

Ko'rilgan metodologiya qoidalaridan foydalanish korporativ axborot tizimining umumiy rivoji bilan birga rivojlantirilishi va modifikatsiyalanishi mumkin bo'lgan axborot xavfsizligining samarali va ishonchli tizimini qurishga imkon beradi.

FOYDALANILGAN ADABIYOTLAR

1. S.S.Qosimov. Axborot texnologiyalari. O‘quv qo‘llanma. – T.: «Aloqachi», 2006.

2. S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tarmoqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qo‘llanma. –Toshkent Davlat texnika universiteti, 2003.

3. В.И. Завгородный. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001.

4. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.:СИНТЕГ, 2000.

5. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров.-М.: 2004.

6. А. Соколов, О. Степанюк. Защита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.

7. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент. – 2003. – №1,2.

8. А.В. Беляев. Методы и средства защитм информации // http://www.citforum.ru/internet/infsecure/its2000_01.shtml.

9. Вэк Дж., Карнахан Л. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны //Конфидент. – 2000. – №4–5.

10. А. Галатенко. Активный аудит//JetInfo.-1999.-№8.

11. А.В. Лукацкий. Адаптивная безопасность сети// Компьютер-Пресс. –1999. – №8.

12. А.В. Лукацкий. Обнаружение атак. – СПб.: БХВ-Петербург, 2001.

13. Р.Норман. Выбираем протокол VPN//Windows 2000 Magazine. – 2001. –№7.

14. В.Г. Олифер. Защита информации при работе в Интернет// Connect. – 2002. – №11.

15. Н.А. Олифер. Дифференцированная защита трафика средствами IPSec //LAN.-2001.-№04; http://www.osp.ru/lan/ 2001/04/024.htm.

16. Н.А. Олифер. Протоколы IPSec. //LAN.-2001.-№03; http://www.osp.ru/lan/2001/03/024.htm.

17. С.А. Петренко. Построение эффективной системы антивирусной защиты // Конфидент.-2002.-№3.

18. С.А. Петренко. Централизованное управление антивирусной защитой корпоративных сетей Internet/Intranet // Конфидент. – 2001. – №2.

19. А.А. Петров. Компьютерная безопасность. Криптографические методы защиты. –М.: ДМК Пресс, 2000.

20. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Уч.пособие для ВУЗов/ Авт.: П.Ю. Белкин и др. –М.:Радио и связь, 1999.

21. Н. Прокофьев. Антивирусная защита сети // Компьютер – Пресс.-2001. –№12.

22. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. – М.: Радио и связь, 2001.

23. С.В. Симонов. Анализ рисков в информационных системах. Практические советы // Конфидент. -2001. -№2.

24. А.В. Соколов, В.Ф. Шаньгин. Защита информации в распределенных корпоративных сетях и системах. –М.: ДМК Пресс, 2002.

25. Типовые решения по применению средств VPN для защиты информационных ресурсов / ООО «Конфидент». –СПб., 2001.

26. Типовые решения по применению технологии межсетевых экранов для защиты информационных ресурсов / ООО «Конфидент». –СПб., 2001.

27. Типовые решения по применению технологии централизованного управления антивирусной защитой предприятия/ ООО «Конфидент». –СПб., 2002.

28. «Axborot texnologiyasi. Ma'lumotlarni kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O'zbekiston Davlat standarti. O'z DSt 1092:2005.

29. «Axborot texnologiyasi. Axborotlarni kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi» O'zbekiston Davlat standarti. O'zDSt 1105:2006.

30. «Axborot texnologiyasi. Axborotlarni kriptografik muhofazasi. Xeshlash funksiyasi» O'zbekiston Davlat standarti. O'zDSt 1106:2006.

31. «Axborot texnologiyasi. Ochiq tizimlar o'zaro bog'liqligi. Elektron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzilmasi» O'zbekiston Davlat standarti. O'zDSt 1108:2006.

32. «Axborot texnologiyalari. Axborot xavfsizligi. Atamalar va ta'riflar» O'zbekiston Davlat standarti. O'z DSt ISO/IEC 2382–8:2007.

33. www.nasa.gov\statistics\

34. www.security.uz

35. www.cert.uz

36. www.uzinfocom.uz

QISQARTIRILGAN SO'ZLAR

ACK	Acknowledgement – Tasdiqlash
AES	Advanced Encryption Standard – Amerikaning yangi shifrlash standarti
AN	Authentication Header – Autentifikatsiyalovchi sarlavha
ANS	Adaptive Network Security – Xavfsizlikni adaptiv boshqarish modeli
ANSI	American National Standard Institute – AQSHning milliy standartlashtirish instituti
AS	Authentication Server – Autentifkatsiyalash serveri
ASA	Adaptive Security Algorithm – Xavfsizlikning adaptiv algoritmi
ASP	Applications Service Providing – Serverda iste'molchidan masofada joylashgan ilovalarga Internet yoki xususiy tarmoq orqali xizmat ko'rsatish
V2V	Business to Business – «biznes-biznes» sxemasi
V2S	Business to Consumer – «biznes – iste'molchi» sxemasi
SA	Certification Authorities – Sertifikatsiyalash markazi
SEK	Content Encryption Key – Ma'lumotlarni shifrlash kaliti
CHAP	Challenge Handshake Authentication Protocol – «Qo'l uzatish» muolajasi asosida autentifkatsiyalash protokoli
DDoS	Distributed Denial of Service – xizmat ko'rsatishdan bosh tortishga undaydigan taqsimlangan hujum
DHCP	Dynamic Host Configuration Protocol – Xostlarni dinamik konfiguratsiyalash protokoli
DNS	Domain Name Server – Domenli ismlar xizmati
e business	electronic business – Elektron biznes
e commerce	electronic commerce – Elektron tijorat
ECP	Encryption Control Protocol – Shifrlashni boshqarish protokoli

ESP	Encapsulated Security Payload – Kiritilgan uzatiladigan himoyalangan ma'lumotlar
FTP	File Transfer Protocol – Fayllarni uzatish protokoli
GSM	Global System for Mobile Communications – Mobil aloqaning global tizimi
GSP	Global Security Policy – VPN uchun global xavfsizlik siyosati
HDLC	High level Data Link Control – Yuqori sathdagi ma'lumotlarni uzatish kanalini boshqarish
NMAS	Hashing for Message Authentication – Kalitlarni xeshlash orqali xabarlarni autentifikatsiyalash
HTML	HyperText Markup Language – Web-sahifalarni gipermatnli belgilovchi til
HTTP	HyperText Transfer Protocol – Gipermatnli fayllarni uzatish protokoli
ICMP	Internet Control Message Protocol – Internet tarmog'ida xabarlarni boshqarish protokoli
IETF	Internet Engineering Task Force – Internetni loyihalash muammolari guruhi
IKE	Internet Key Exchange – Internetda kalitlarni almashish protokoli
IP	Internet Protocol – Tarmoqlararo ma'lumotlarni almashinishning Internet protokoli
IPSec	Internet Security Protocol – Tarmoqlararo ma'lumotlarni xavfsiz almashinish Internet protokoli
IRC	Internet Relay Chat – Internet da chat-anjumanlarni tashkil etish xizmati
ISO	International Standards Organization – Xalqaro standartlashtirish tashkiloti
ISP	Internet Service Provider – Internet xizmatlarini ta'minotchisi
KDC	Key Distrubution Center – kalitlarni taqsimlash markazi
KEK	Key Encryption Key – Kalitlarni shifrlash uchun kalit
KS	Kerberos Server – Kerberos tizimi serveri
L2F	Layer2 Forwarding – Ikkinchi (kanal) sathda ma'lumotlarni uzatish protokoli

L2TP	Layer2 Tunneling Protocol – Kanal sathida ma'lumotlarni tunnellash protokoli
LAC	L2TP Access Concentrator – L2TP ruxsatlar konsentratori
LAN	Local Access Network – Mahalliy tarmoq.
LCP	Link Control Protocol – Ulanishlarni boshqarish protokoli
LDAP	Lightweight Directory Access Protocol – Katalog-lardan foydalanishlarni soddalashtirilgan protokoli
LNS	L2TP Network Server – L2TP tarmoq serveri
LSP	Local Security Policy – Mahalliy xavfsizlik siyo-sati (mijoz uchun)
MAC	Message Authentication Code – Xabarlarni autentifikatsiyalash kodi
MD	Message Digest – Xabarlar daydjesti
NAT	Network Address Translation – Tarmoq adreslarini translatsiyalash
NCP	Network Control Protocol – Tarmoqni boshqarish protokoli
NIST	National Institute of Standards and Technology – AQSHning standartlar va texnologiyalari milliy in-stituti
NNTP	Network News Transfer Protocol – Tarmoq yangiliklarini uzatish protokoli
OSI	Open Systems Interconnection – Ochiq tizimlar o'zaro bog'liqligi
OTK	One Time Key – Bir marotabalik kalit
R2R	Peer to Peer ili Partner to Partner – Biznes munosa-batining «teng-teng» sxemasi
PAP	Password Authentication Protocol – Parol bo'yicha autentifikatsiyalash protokoli
PIN	Personal Identification Number – shaxsiy identifi-katsiya kodi
PKD	Public Key Directory – Ochiq kalitlar katalogi
PKI	Public Key Infrastructure – Ochiq kalitlarni boshqarish infratuzilmasi
RRR	Point to point Protocol – Ikki nuqtali bog'lanish pro-tokoli

RRTR	Point to Point Tunneling Protocol – Ikki nuqtali bog'lanish uchun tunnellash protokoli
POP	Post Office Protocol – foydalanuvchi o'ziga kelgan elektron xabarlardan foydalanishiga imkon beruvchi protokol
RADIUS	Remote Authentication Dial In User Service – Foydalanuvchilarni bog'lanadigan liniyalar bo'yicha masofadan autentifikatsiyalash tizimi
RAS	Remote Access Service –Masofadan foydalanish xizmati
RFC	Request For Comments – Izohlarni so'rovi
RMON	Remote MONitoring – Tarmoq uskunalarini masofadan monitoringlashning standart spetsifikatsiyasi
RSA	Rivest, Shamir, Adleman – Rayvest, Shamir, Adleman, Asimmetrik kriptoalgoritm
SHA	Secure Hash Algorithm – Himoyalangan xeshlash algoritmi
SKIP	Simple Key management for Internet Protocols – Internet protokoli uchun kalitlarni oddiy boshqarish
SMTP	Simple Mail Transfer Protocol – Elektron pochtaning oddiy protokoli
SNMP	Simple Network Management Protocol – Tarmoqni boshqarishning oddiy protokoli
SPD	Security Policy Database – Xavfsizlik qoidalarining ma'lumotlar bazasi
TACACS	Terminal Access Controller Access Control System – Masofadan foydalanishni markazlashtirilgan nazoratlash protokoli
TCP	Transport Control Protocol – Uzatishlarni boshqarish protokoli
TELNET	Virtual terminal protokoli – masofadagi kompyuterda dasturni bajarishga mo'ljallangan protokol
TFN	Trible Flood Net – DdoS hujumlar uchun instrumental vositalardan biri
TGS	Ticket Granting Server – Mandatlarni tarqatish serveri
TLS	Transport Layer Security – Transport sathining himoyasi
UDP	User Data Protocol – Foydalanuvchining ma'lumotlarini uzatish protokoli

VPN	Virtual Private Network – himoyalangan virtual tarmoq
WAN	Wide Area Network – Global tarmoq
WWW	World Wide Web - Internetning gipermatnli axborotlar xizmati
XML	Extended Mark-up Language – belgilashning kengaytirilgan tili
MBBT	Ma'lumotlar bazasini boshqarish tizimi

S.G'ANIYEV, M.KARIMOV, K.TASHEV

Axborot xavfsizligi

(Axborot kommunikatsion tizimlar xavfsizligi)

Toshkent – «ALOQACHI» – 2008

Muharrir: M.Mirkomilov
Tex.muharrir: A.Moydinov
Musahhih: G.Karimova
Kom.sahifalovchi: G.Arifxo'djayeva

Bosishga ruxsat etildi 30.05.08 yil. Bichimi 60x84 $^{1}/_{16}$.
«Times New Roman» garniturasi. Ofset usulida bosildi.
Shartli bosma tabog'i 22,75. Nashr bosma tabog'i 22,5. Tiraj 1000.
Buyurtma № 237.

«Aloqachi matbaa markazi» bosmaxonasida chop etildi.
700000, Toshkent sh., A.Temur ko'chasi, 108-uy.