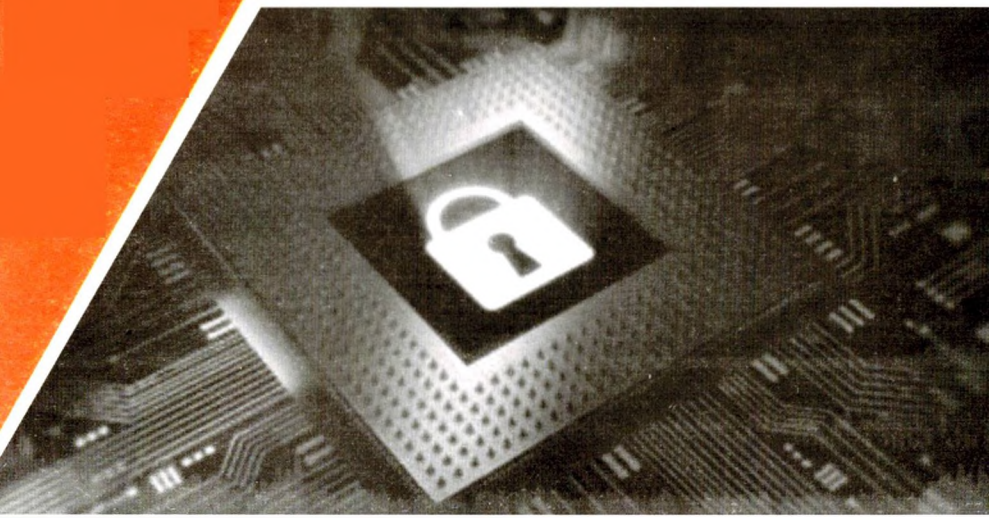
S.K. GANIYEV,
M.M. KARIMOV, K.A. TASHEV



AXBOROT XAVFSIZLIGI

TOSHKENT

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

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

S.K. GANIYEV, M.M. KARIMOV, K.A. TASHEV

AXBOROT XAVFSIZLIGI

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi tomonidan oliy o‘quv yurtlarining “5330500 – Kompyuter injiniringi”, “5330600 – Dasturiy injiniringi”, “5330100 – Telekommunikatsiya texnologiyalari”, “5350200 – Televizion texnologiyalar”, “5350300 – Axborot kommunikatsiya texnologiyalari sohasida iqtisodiyot va menejment”, “5350400 – Axborot texnologiyalari sohasida kasb ta’lim”, “5350500 – Pochta aloqasi texnologiyasi”, “5350600 – Axborotlashtirish va kutubxonashunoslik” ta’lim yo‘nalishlari talabalari uchun darslik sifatida tavsiya etilgan

Professor S.K.Ganiyev tahriri ostida

TOSHKENT – 2017

UO'K: 004.056 (075.8)
KBK 32.973-018.2
G-19

G-19 **S.K. Ganiyev, M.M. Karimov, K.A. Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2017, 372 bet.**

ISBN 978–9943–11–366–4

"Axborot xavfsizligi" fani bo'yicha darslik tayanch oliy o'quv yurti Toshkent axborot texnologiyalari universitetining "Axborot xavfsizligi" kafedrasi professor-o'qituvchilari tomonidan tayyorlangan bo'lib, unda axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo'ladigan tahdidlar, hujumlar va zaifliklar, axborot xavfsiligi sohasiga oid xalqaro va milliy me'yoriy-huquqiy baza, xavfsizlik modellari, axborotni kriptografik himoyalash, identifikatsiya va autentifikatsiya, kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlari, axborotni himoyalashda tarmoqlararo ekranlarning o'rni, operatsion tizim himoyasi, axborot sirqib chiqish kanallari va ularni aniqlash hamda obyektlarni injener himoyalash va texnik qo'riqlash masalalari keltirilgan.

Darslik oliy o'quv yurti talabalari uchun mo'ljallangan bo'lib, undan axborot texnologiyalari, kompyuter tizimlari xavfsizligi sohasida faoliyat ko'rsatuvchilar ham foydalanishlari mumkin.

***

Учебник по дисциплине "Информационная безопасность" подготовлен профессорско-преподавательским составом кафедры "Информационная безопасность" Ташкентского университета информационных технологий, являющимся базовым высшим учебным заведением по данному направлению. В учебнике раскрыто понятие информационной безопасности, рассмотрены задачи обеспечения безопасности, виды угроз, атак и присущие средствам защиты недостатки. Рассмотрены также международные и национальные нормативно-правовые документы по безопасности, модели безопасности, криптографическая защита информации, вопросы идентификации и аутентификации, методы и механизмы борьбы с компьютерными вирусами и вредоносными программами, роль межсетевых экранов, методы защиты операционных систем, каналы утечки информации и способы их выявления, методы инженерной защиты объектов и их технической охраны.

Учебник предназначен для студентов высших учебных заведений, также будет полезен для всех специалистов, профессиональная деятельность которых связана с обеспечением информационной безопасности в компьютерных системах и сетях.

***

Textbook based on subject "Information security" for higher educational institution of the Tashkent University of Information Technologies which is prepared by the department "Information security", there was given concept of information security and its objectives, threats, attacks and vulnerabilities in information security, international and national normative-juridical base which related to information security sphere, security models, cryptographic protection of information, identification and authentication, mechanisms to combat with computer viruses and harmful programs, the role firewalls to protect information, protection of operation system, information leakage channels and determine them also engineer protection and technical defending of objects.

Students and people who works in information technologies, security of computer systems sphere.

UO'K: 004.056 (075.8)
KBK 32.973-018.2

Taqrizchilar:

Igamberdiyev X.Z. – Toshkent davlat texnika universiteti "Boshqarishda axborot texnologiyalari" kafedrasi professori, texnika fanlari doktori;

Ahmedova O.P. – "Unicon.UZ" DUK, Kriptografiya ilmiy-tadqiqot bo'limi boshlig'i, t.f.n.

ISBN 978–9943–11–366–4

MUQADDIMA

Kompyuter texnikasi va axborot tizimlarining iqtisodda, boshqarishda, aloqada, ilmiy tadqiqotlarda, ta'limda, xizmat ko'rsatish sohasida, tijorat, moliya va inson faoliyatining boshqa sohalarida qo'llanilishining rivoji axborotlashtirish va, umuman, jamiyat rivojini belgilovchi yo'nalish hisoblanadi. Kompyuter texnikasining qo'llanishi evaziga erishiluvchi samara axborot ishlanishi ko'lamining oshishi bilan ortib boradi. Ushbu texnikaning qo'llanish sohalari va ko'lami uning ishlashining ishonchliligi va barqarorligi muammolari bilan bir qatorda unda aylanuvchi axborot xavfsizligini ta'minlash muammosini tug'diradi.

Axborot xavfsizligi – axborotning nomaqbul (axborot munosabatlarining tegishli subyektlari uchun) oshkor qilinishidan (konfidensialligining buzilishidan), buzilishidan (yaxlitligining buzilishidan), sirqib chiqishidan, yo'qotilishidan, modifikatsiyalanishidan yoki foydalanuvchanlik darajasining pasayishidan hamda noqonuniy tirajlanishidan himoyalanganligi. Ushbu hodisalarning sababchisi tasodifiy ta'sirlar yoki buzg'unchining (niyati buzuqning) atayin ruxsatsiz foydalanishi natijasidagi ta'sirlar bo'lishi mumkin.

Jamiyatning jadal sur'atlarda axborotlashtirilishi sababli axborot xavfsizligi muammosi nihoyatda dolzarb va doimo shunday bo'lib qoladi.

Kitobning birinchi bobida axborot xavfsizligi tushunchasi va uning vazifalari bayon etilgan. Milliy xavfsizlik tushunchasiga ta'rif berilib, uning tashkil etuvchilari batafsil yoritilgan. Axborot xavfsizligini ta'minlashning asosiy vazifalari keltirilib, shaxsning, jamiyatning va davlatning axborot muhitidagi manfaatlari bayon etilgan. Xavfsizlik siyosati, axborot xavfsizligi arxitekturasi va strategiyasi va ular orasidagi bog'liqlik masalalari ham ushbu bobdan o'rin olgan.

Kitobning ikkinchi bobi axborot xavfsizligiga bo'ladigan tahdidlar, hujumlar va zaifliklarga bag'ishlangan. Axborot xavfsizligiga tahdidlar va zaifliklari tahlil etilib, ularning aktivlarga zarar

yetkaza olishlari uchun birlashishlari lozimligi misollar yordamida ko‘rsatilgan. Axborotning maxfiyligini, yaxlitligini va foydalanuvchanligini buzish usullariga alohida e’tibor berilgan.

Kitobning uchinchi bobi axborot kommunikatsiya tizimlarida axborot xavfsizligini ta’minlash, boshqarish sohasiga oid xalqaro va milliy me‘yoriy-huquqiy bazaga bag‘ishlangan. Davlat va xususiy korxona hamda tashkilotlarda mavjud axborot kommunikatsiya tizmlarida axborot xavfsizligini ta’minlashda qo‘llaniladigan me’yoriy huquqiy hujjatlar ko‘rib chiqilgan.

Kitobning to‘rtinchi bobi xavfsizlik modellari – diskretsion, mandatli va rolli modellarga bag‘ishlangan. Diskretsion modellarda foydalanishni boshqarish foydalanuvchilarga ma’lum obyektlar ustida ma’lum amallarni bajarish vakolatini berish yo‘li bilan amalga oshirilishi, mandatli modellarning foydalanishni xufiya holda – tizimning barcha subyekt va obyektlariga xavfsizlik sathlarini belgilash orqali boshqarishi, rolli modelning xavfsizlikning tatbiqiy siyosatini akslantirishi batafsil bayon etilgan.

Kitobning beshinchi bobi axborotni kriptografik himoyalash usullari va vositalariga bag‘ishlangan bo‘lib, uzatiladigan ma’lumotlarni himoyalashda qo‘llaniladigan simmetrik shifrlash tizimlarining strukturasi, algoritmlari va ular uchun foydalaniladigan kalitlarni taqsimlash sxemalari keltirilgan. Asimmetrik shifrash tizimlariga oid kriptografik o‘zgartirish sxemalari va shifrlash algoritmlarining matematik asoslari haqida so‘z yuritilib, asimmetrik algoritmlar misol tariqasida keltirilgan. Elektron raqamli imzolarni shakllantirish va haqiqiyligini tasdiqlash jarayonlarini tashkil etuvchi algoritmlar tavsiflangan, rivojlangan davlatlarning elektron raqamli imzolari haqidagi standartlari keltirib o‘tilgan. Undan tashqari ushbu bobda kriptografiyaning steganografik usullari, ularning turlari va texnologiyalari haqida qisqacha to‘xtalib o‘tilgan. Ushbu bobdan kriptografik algoritmlarni tahlillash usullari va vositalari ham o‘rin olgan.

Kitobning oltinchi bobida tizimning foydalanuvchilar bilan o‘zaro aloqasidagi asosiy jarayonlar – foydalanuvchi harakatini autentifikatsiyalash, avtorizatsiyalash va ma’murlash, bir va ko‘p martali parollar hamda raqamli sertifikatlar asosidagi autentifikatsiyalash xususiyatlarining tahlili o‘rin olgan. Foydalanuvchini

identifikatsiyalash va autentifikatsiyalashning namunaviy sxemalari keltirilgan. Simmetrik va asimmetrik kriptoalgoritmlarga asoslangan qat'iy autentifikatsiyalashga alohida e'tibor berilib, jumladan, Kerberos protokoli muhokama etilgan. Ushbu bobdan biometrik identifikatsiyalash va autentifikatsiyalash vositalarining tavsifi ham o'rin olgan.

Kitobning yettinchi bobi kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlariga bag'ishlangan. Kompyuter viruslarining tasnifi keltirilib, virus hayot sikli bosqichlari tahlil-langan, viruslar va boshqa zarar keltiruvchi dasturlarning asosiy tarqalish kanallari ko'rilgan. Virusga qarshi dasturlarning asosiylari muhokama etilib, himoyaning profilaktik choralari yoritilgan. Virusga qarshi himoya tizimini qurishdagi asosiy bosqichlar batafsil bayon etilgan.

Kitobning sakkizinchi bobi axborotni himoyalashda tarmoq-lararo ekranlarning o'rniga bag'ishlangan. Tarmoqlararo ekranlar-ning funksiyalari tahlili, ularning OSI modelining sathlarida ishlashi bo'yicha, xususiyatlari muhokama etilgan. Tarmoqlararo ekranlar asosidagi tarmoq himoyasining sxemalari keltirilgan.

Kitobning to'qqizinchi bobi operatsion tizim xavfsizligini ta'minlash muammolariga bag'ishlangan bo'lib, himoyalangan operatsion tizim tushunchasi, himoyalangan operatsion tizimni yaratishdagi yondashishlar va himoyalashning ma'muriy choralari bayon etilgan. Operatsion tizimni himoyalash qismtizimining asosiy funksiyalari hamda axborotni himoyalashda dasturiy ilovalarning qo'llanilishi masalalariga alohida e'tibor berilgan.

Kitobning o'ninchi bobi axborot sirqib chiqish kanallariga bag'ishlangan bo'lib, axborot sirqib chiqadigan texnik kanallar va ularning tasnifi keltirilgan. Axborot sirqib chiqadigan radioelektron, akustik, optik, moddiy kanallarning axborot eltuvchilari, infor-mativligi, davriyligi va strukturalari yoritilgan. Axborot sirqib chiqadigan texnik kanallarni aniqlash usullari va vositalari bayon etilgan. Ushbu bobdan obyektlarni injener himoyalash va texnik qo'riqlash masalalari ham o'rin olgan.

Ilovalarda axborotni himoyalashning dasturiy vositalarini yaratish namunalari va atamalarning o'zbek, rus, ingliz tillaridagi izohli lug'ati keltirilgan.

I BOB. AXBOROT XAVFSIZLIGI TUSHUNCHASI VA UNING VAZIFALARI

1.1. Milliy xavfsizlik tushunchasi

Hozirda 29-avgust 1997-yili qabul qilingan "O'zbekiston Respublikasining milliy xavfsizligi konsepsiyasini tasdiqlash to'g'risida" qonuni amalda. Ushbu qonunga asoslanib, milliy xavfsizlik tushunchasiga quyidagicha ta'rif berish mumkin.

O'zbekiston Respublikasining milliy xavfsizligi deganda O'zbekiston Respublikasining suverenitetini ifodalovchi va hokimiyatning yagona manbai hisoblanuvchi ko'p millatli xalqining xavfsizligi tushuniladi.

Milliy xavfsizlikning, shartli ravishda, quyidagi tashkil etuvchilarini ko'rsatish mumkin:

- iqtisodiy xavfsizlik;
- ichki siyosiy xavfsizlik;
- ijtimoiy xavfsizlik;
- ma`naviy xavfsizlik;
- xalqaro xavfsizlik;
- axborot xavfsizligi;
- harbiy xavfsizlik;
- chegaraviy xavfsizlik;
- ekologik xavfsizlik.

Iqtisodiy xavfsizlik – shaxs, jamiyat va davlatning iqtisodiy sohadagi hayotiy muhim manfaatlarining ichki va tashqi tahdidlardan himoyalanganligi. Iqtisodiy xavfsizlikka binoan xalq o'zining iqtisodiy rivojlanish yo'llari va shakllarini tashqaridan aralashishsiz va bosimsiz mustaqil ravishda aniqlay oladi.

Ichki siyosiy xavfsizlik – hokimiyat institutlarining barqarorligi va samaradorligi, hokimiyat tuzilmalarining siyosiy jarayonlarni nazoratlash qobiliyati, aksariyat fuqarolar tomonidan madadlashga erishish, jamiyatda siyosiy barqarorlikni ta'minlovchi, samarali faoliyat yurituvchi nodavlat siyosiy institutlarning mavjudligi bilan

xarakterlanadi. Ichki siyosiy xavfsizlikka binoan siyosiy munosabatlar sohasida qarama-qarshilik, siyosiy ekstremizmning ommaviy tus olishi, hokimiyat bilan xalq orasida qarama-qarshilik bo'lmaydi. Fuqarolarning siyosiy ongi holati va jamiyatning siyosiy madaniyati jamiyatning xavfsiz siyosiy rivojiga jiddiy ta'sir ko'rsatadi.

Ijtimoiy xavfsizlik – shaxs, oila va jamiyatning hayotiy muhim manfaatlarining ichki va tashqi tahdidlardan himoyalanganligi. Ijtimoiy xavfsizlikning obyekti - milliy va ijtimoiy siyosat tomonidan tartibga solinuvchi xalq turmushi sifati va darajasini ta'minlovchi ijtimoiy tizimning barcha asosiy elementlari. Ijtimoiy rivojlanish strategiyasi, ularning uzoqligiga, kambag'allik darajasiga, turmush darajasidagi mintaqaviy mutanosibligiga, ta'lim va sog'liqni saqlash sifatiga, jamiyatdagi ma'naviyat va madaniyatning umumiy darajasiga va nihoyat, demografik muammolariga ta'siri ma'lum.

Ma'naviy xavfsizlik – bugungi kunda inson ma'naviyatiga qarshi yo'naltirilgan, bir qarashda arzimas bo'lib tuyuladigan kichkina xabar ham axborot olamidagi globallashuv shiddatidan kuch olib, ko'zga ko'rinmaydigan, lekin zararini hech narsa bilan qoplab bo'lmaydigan ulkan ziyon yetkazishi mumkin. Ayniqsa, ommaviy madaniyat degan niqob ostida ahloqiy buzuqlik va zo'ravonlik, individualizm, egotsentrizm g'oyalarini tarqatish, kerak bo'lsa, shuning hisobidan boylik orttirish, boshqa xalqlarning necha ming yillik an'ana va qadriyatlarini, turmush tarzining ma'naviy negizlariga bepisandlik, ularni qo'porishga qaratilgan xatarli tahdidlar odamni tashvishga solmay qo'ymaydi. Hozirgi vaqtda axloqsizlikni madaniyat deb bilish va aksincha, asl ma'naviy qadriyatlarni mensimasdan, eskilik sarqiti deb qarash bilan bog'liq holatlar bugungi taraqqiyotga, inson hayoti, oila muqaddasligi va yoshlar tarbiyasiga katta xavf solmoqda va ko'pchilik butun jahonda bamisoli balo-qazodek tarqalib borayotgan bunday xurujlarga qarshi kurashish naqadar muhim ekanini anglab olmoqda.

Xalqaro xavfsizlik – xalqaro munosabatlar nazariyasida xalqaro xavfsizlik deganda dunyo hamjamiyatining barqarorligini ta'minlovchi xalqaro munosabatlar holati tushuniladi. Boshqacha aytganda, xalqaro xavfsizlik – xalqaro munosabatlar subyektlariga

urush xavfi yoki suveren hayotiga va mustaqil rivojiga tashqaridan boshqa tajovuz xavfi bo'lmagan holat. BMT Nizomiga binoan, hozirda xalqaro tinchlikni saqlashga asosiy javobgar sifatida Xavfsizlik Kengashi belgilangan. Faqat aynan ushbu Kengash agressorga nisbatan sanksiya qo'llash huquqiga ega.

Axborot xavfsizligi – mamlakat madaniy mulkining, xo'jalik subyektlari va fuqarolar intellektual mulkining, davlat va kasbiy sirga ega maxsus ma'lumotlarning ishonchli himoyalanganligi holati.

Harbiy xavfsizlik – harbiy siyosat O'zbekiston Respublikasi harbiy doktrinasida ishlab chiqilgan nizomlarga asosan yuritiladi. Harbiy doktrina – O'zbekiston Respublikasining harbiy xavfsizligining harbiy-siyosiy, harbiy-strategik va harbiy-iqtisodiy asoslarini belgilovchi rasmiy qarashlar majmui. Harbiy doktrinaning huquqiy asosini O'zbekiston Respublikasi Konstitutsiyasi, qonunlar hamda harbiy xavfsizlikni ta'minlash sohasidagi O'zbekiston Respublikasining xalqaro shartnomalari tashkil etadi. O'zbekiston Respublikasining harbiy xavfsizligini ta'minlashga rahbarlik Qurolli Kuchlarning Oliy Bosh qo'mondoni hisoblanuvchi O'zbekiston Respublikasi Prezidenti tomonidan amalga oshiriladi.

Chegaraviy xavfsizlik – O'zbekiston Respublikasi davlat chegarasi va chegara oldi hududlarining himoyalanganlik holati. Chegaraviy xavfsizlik shaxs, jamiyat va davlat xavfsizligining juda muhim tashkil etuvchilaridan biri hisoblanadi, chunki davlat barqarorligi uning chegaralarining xavfsizligi bilan uzviy bog'langan. Chegara xavfsizligini ta'minlash zaruriyati davlat chegarasi va chegara oldi hududlarda yuzaga kelgan tahdidlar tizimiga asoslangan.

Ekologik xavfsizlik. Sivilizatsiyaning atrof – muhitga faol ta'siri natijasida uning ifloslanishi yildan-yilga oshib bormoqda. Ushbu salbiy ta'sir ayniqsa ekologik halokat joylarda, mineral resurslardan va ishlab chiqarishning zararli chiqindilaridan oqilona foydalanilmaydigan joylarda kuchli bo'ladi.

Nazorat savollari:

1. Milliy xavfsizlik tushunchasi nima?
2. Milliy xavfsizlikni shartli ravishda tashkil etuvchilarini sanab o'ting.
3. Ma'naviy xavfsizlikning oqibatlarini tushuntirib bering.
4. Xalqaro xavfsizligini jahon sivilizatsiyasida tutgan o'rni?
5. Axborot xavfsizligining mohiyati nima?

1.2. Axborot xavfsizligini ta'minlashning asosiy vazifalari va darajalari

Axborot xavfsizligini ta'minlash muntazam va kompleks xarakterga ega ko'p qirrali faoliyatni amalga oshirishni ko'zda tutadi. Uni amalga oshirishda axborot xavfsizligidan manfaatdor taraflar oldiga qo'yiladigan vazifalarga alohida e'tibor berish zarur. Ushbu turli-tuman vazifalarni bir necha quyidagi asosiy guruhlarga ajratish mumkin:

1) *axborotdan foydalnishni ta'minlash*, ya'ni maqbul vaqt mobaynida axborot xizmatini olish hamda axborotni olishda ruxsatsiz taqiqlashni bartaraf etish;

2) *axborot yaxlitliligini ta'minlash,* ya'ni axborotning ruxsatsiz modifikatsiyalanishini yoki buzilishini bartaraf etish;

3) *axborot konfidensialligini ta'minlash,* ya'ni axborotdan ruxsatsiz tanishishni bartaraf etish.

Odatda, bir-biridan axborot xavfsizligining huquqiy, texnik, moliyaviy, tashkiliy va boshqa resursli ta'minoti bilan farqlanuvchi axborot xavfsizligi subyektlarining quyidagi to'rtta kategoriyasi ajratiladi:

- butun bir davlat;
- davlat tashkilotlari;
- tijorat tuzilmalari;
- alohida fuqarolar.

Yuqorida keltirilgan axborot xavfsizligini ta'minlashdagi asosiy vazifalar qamrab olgan quyidagi keng spektrli masalalarni ko'rib chiqish joiz hisoblanadi:

- konfidensiallik;

- yaxlitlik;
- identifikatsiya;
- autentifikatsiya;
- vakolat berish;
- foydalanishni nazoratlash;
- mulklik huquqi;
- sertifikatsiya;
- imzo;
- voz kechmaslik;
- sanasini yozish;
- olganligiga tilxat berish;
- bekor qilish;
- anonimlik.

Axborotning konfidensialligi – himoyaning eng kerakli vazifalaridan biri. Har bir insonda yoki tashkilotda shunday hujjatlar borki, ularning jamoa mulkiga aylanmasligi ta'minlanishi shart. Bunday hujjatlarni saqlashda qog'oz, fotoplyonka ishlatilsa, konfidensiallik ma'muriy usullar yordamida amalga oshiriladi. Ammo axborot kompyuterda ishlanib, ochiq aloqa kanali orqali uzatilsa, ma'muriy usullar ojizlik qiladi va yordamga axborot xavfsizligini ta'minlash usullari keladi. Konfidensiallikni ta'minlash masalasiga binoan ma'lumotlar shunday ko'rinishda uzatiladiki, hatto niyati buzuq eltuvchidan yoki uzatish muhitidan foydalana olganida ham himoyalangan ma'lumotlarni ololmaydi.

Axborotning yaxlitligi. Ma'lumotlar, ishlanishi va aloqa kanali bo'yicha uzatilishi jarayonida, tasodifan yoki atayin buzilishi mumkin. Axborot eltuvchida saqlanadigan joyidayoq buzilishi mumkin. Yaxlitlikni ta'minlashga (yaxlitlikni nazoratlashga) binoan ma'lumotlar saqlanishi va uzatilishi jarayonida modifikatsiyalanmaganligini tasdiqlash yoki ma'lumotlar buzilganligini aniqlash talab etiladi. Boshqacha aytganda, ma'lumotlarning har qanday o'zgarishi sezilmasdan qolmasligi zarur.

Identifikatsiya foydalanuvchini qandaydir noyob identifikator bilan aynanligini tasdiqlash uchun kerak. Undan so'ng identifikatorga yuklangan barcha harakatlarga ushbu identifikator biriktirilgan foydalanuvchi javobgar hisoblanadi.

Autentifikatsiya identifikatsiyaga zaruriy qo'shimcha hisoblanadi va identifikatorni taqdim etgan foydalanuvchining haqiqiyligini (autentligini) tasdiqlashga mo'ljallangan. Anonim bo'lmagan foydalanuvchi autentifikatsiyadan muvaffaqiyatli o'tgandagina ishlash imkoniyatiga ega bo'lishi shart.

Vakolat berishga binoan birorta ham foydalanuvchi autentifikatsiyadan muvaffaqiyatli o'tmagunicha tizimdan foydalanmasligi va birorta ham foydalanuvchi, agar u maxsus ruxsatnoma bilan vakolatga ega bo'lmasa, rusurslardan foydalanmasligi shart.

Foydalanishni nazoratlash kompleks tushuncha hisoblanadi va resurslardan foydalanishni cheklashga mo'ljallangan usullar va vositalarni anglatadi.

Mulklik huquqi foydalanuvchiga qandaydir resurslardan foydalanishga qonuniy huquqni va u istasa, ushbu resursni boshqa foydalanuvchiga o'tkazish imkoniyatini taqdim etishga mo'ljallangan. Mulklik huquqi odatda foydalanishni nazoratlash tizimining tarkibiy qismi hisoblanadi.

Sertifikatsiya – foydalanuvchi ishonadigan taraf tomonidan qandaydir faktni tasdiqlash jarayoni. Ko'pincha sertifikatsiya ochiq kalitning muayyan foydalanuvchiga yoki shirkatga tegishli ekanligini tasdiqlashda ishlatiladi, chunki ochiq kalitlar infrastrukturasidan faqat sertifikatsiya tizimining mavjudligida samarali foydalanish mumkin. Sertifikatlar foydalanuvchilar so'rovi bo'yicha maxsus vakolatli tashkilot – sertifikatsiya markazi tomonidan, ma'lum shartlar bajarilganida beriladi.

Imzo hujjat qabul qiluvchiga ushbu hujjatning aynan uzatuvchi tomonidan imzolanganligini isbotlashga imkon beradi. Bunda imzoni boshqa hujjatga o'tkazish va uzatuvchi o'zining imzosidan voz kechishi mumkin emas. Hujjatning har qanday o'zgarishi imzoning buzilishiga sabab bo'ladi va har qanday foydalanuvchi mustaqil tarzda imzoning haqiqiyligini tekshirishi mumkin.

Voz kechmaslik axborot almashish sxemasining xususiyati hisoblanadi. Unga binoan xabar qabul qiluvchining uchinchi tarafning xabar uzatuvchining kimligini tekshirishga jalb qilishi qobiliyatiga ega ekanligining isboti mavjud. Boshqacha aytganda, xabarni uzatuvchi mualliflikdan voz kechish imkoniyatiga ega emas.

Sanasini yozish ko'pincha imzo bilan birgalikda ishlatiladi va hujjat imzolangan onni qaydlaydi. Bu bitta hujjat bir necha foydalanuvchilar tomonidan imzolanganda, birinchilikni isbot qilishda foydali hisoblanadi, chunki har bir foydalanuvchi hujjat muallifligiga da'vo qiladi. Undan tashqari, sanasini yozish muddatli sertifikatlarda keng qo'llaniladi.

Olganligiga tilxat berish qabul qiluvchidan uzatuvchiga uzatiladi va uzatuvchi tomonidan uzatilgan axborot qabul qiluvchiga tilxatda ko'rsatilgan ondan kechikmasdan yetkazganligini isbotlashda ishlatilishi mumkin.

Bekor qilish – sertifikatlar, vakolatlar va imzolar ta'sir kuchini bekor qilish. Agar axborot almashishda ishtirok etuvchi yoki unga tegishli kalitlar va sertifikatlar obro'sizlansa, ushbu foydalanuvchini resurslardan foydalanishga yo'l qo'ymaslik va mos sertifikatlarga ishonmaslik zarur, chunki bu sertifikatlardan niyati buzuq foydalanishi mumkin. Bekor qilish muolajasi sertifikatsiya markaziga nisbatan ham qo'llanishi mumkin.

Anonimlik kamdan-kam uchraydi. Hukumatlar va shirkatlar uchun foydalanuvchining axborot muhitida qandaydir harakatlarining anonim bo'lib qolishligi foyda bermaydi. Shu sababli anonimlikni ta'minlovchi loyihalar kamdan-kam uchraydi va odatda uzoq yashamaydi. Zero kommunikatsiya vositalari ko'pincha u yoki bu xabarning uzatilishi marshrutini va demak, uzatuvchini aniqlashga imkon beradi.

Yuqorida keltirilgan vazifalar mavjud axborot dunyosi ehtiyojiga asosan tavsiflangan. Vaqt o'tishi bilan ba'zi vazifalar o'z dolzarbligini yo'qotishi va aksincha, yechimini kutuvchi yangi vazifalar paydo bo'lishi mumkin.

Sivilizatsiya rivojining zamonaviy bosqichida axborot nafaqat jamiyat va davlat institutlari faoliyatida, balki har bir shaxs hayotida hal qiluvchi rolni o'ynaydi.

Shaxsning axborot muhitidagi manfaatlari inson va fuqaroning axborotdan foydalanishdagi konstitutsiyaviy huquqlarining amalga oshirilishini, qonun taqiqlamagan faoliyatni, fizik, ma'naviy va intellektual rivojini hamda shaxsiy xavfsizligini ta'minlashni ko'zda tutadi.

Jamiyatning axborot muhitidagi manfaatlari ushbu muhitda shaxs manfaatlarini ta'minlashni, demokratiyani mustahkamlashni, huquqiy ijtimoiy davlatni yaratishni, jamiyat inoqligiga erishish va uni madadlashni, mamlakatning ma'naviy yangilanishini ko'zda tutadi.

Davlatning axborot muhitidagi manfaatlari inson va fuqaroning axborot olishidagi konstitutsiyaviy huquq va erkinligini ta'minlashni, olingan axborotdan konstitutsiyaviy tuzumning mustahkamligini, davlat suvereniteti va hududiy yaxlitligini, siyosiy, iqtisodiy va ijtimoiy barqarorlikni hamda qonuniylikni va huquqiy tartibni, teng huquqli va o'zaro foydali xalqaro hamkorlikni ta'minlash maqsadida foydalanishdagi shart-sharoitlarni yaratish uchun axborot infrastrukturasining garmonik rivojini ko'zda tutadi.

Nazorat savollari:

1. Axborot xavfsizligini ta'minlash vazifalari nima va u qaysi asosiy guruhlarni o'z ichiga oladi?
2. Axborot xavfsizligi subyektlarining kategoriyalarini tushuntirib bering.
3. Axborot xavfsizligini ta'minlash asosiy vazifalari qamrab olgan konfidensiallik, yaxlitlik, identifikatsiya va autentifikatsiya kabi masalalarini yoritib bering.
4. Axborot xavfsizligini ta'minlash asosiy vazifalari qamrab olgan vakolat berish, foydalanishni nazoratlash, mulklik huquqi, sertifikatsiya kabi masalalarini yoritib bering.
5. Axborot xavfsizligini ta'minlash asosiy vazifalari qamrab olgan imzo, voz kechmaslik, sanasini yozish kabi masalalarini yoritib bering.
6. Axborot xavfsizligini ta'minlash asosiy vazifalari qamrab olgan olganligiga tilxat berish, bekor qilish, anonimlik kabi masalalarini yoritib bering.
7. Axborot xavfsizligini ta'minlash darajalarini tavsiflab bering.

1.3. Xavfsizlik siyosati

Axborot xavfsizligi siyosati (yoki xavfsizlik siyosati) – tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta'minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja. Siyosat xavfsizlikni umumlashgan atamalarda, spetsifik detallarsiz tavsiflaydi. U xavfsizlikni ta'minlashning barcha dasturlarini rejalashtiradi. Axborot xavfsizligi siyosati tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta'minlashi shart.

Apparat vositalar va dasturiy ta'minot ish jarayonini ta'minlovchi vositalar hisoblanadi va ular xavfsizlik siyosati tomonidan qamrab olinishi shart. Shu sababli asosiy vazifa sifatida tizimni (jumladan tarmoq xaritasini) to'liq inventarizatsiyalashni ko'zda tutish lozim. Tarmoq xaritasini tuzishda har bir tizimdagi axborot oqimini aniqlash lozim. Axborot oqimlari sxemasi axborot oqimlari biznes-jarayonlarni qanchalik ta'minlayotganini ko'rsatishi mumkin hamda axborotni himoyalash va yashovchanligini ta'minlash uchun qo'shimcha choralarni ko'rish muhim bo'lgan sohani ko'rsatishi mumkin. Undan tashqari bu sxema yordamida axborot ishlanadigan joyni, ushbu axborot qanday saqlanishi, qaydlanishi, joyini o'zgartirishi va nazoratlanishi lozimligini aniqlash mumkin.

Inventarizatsiya apparat va dasturiy vositalardan tashqari dasturiy hujjat, apparatura hujjatlari, texnologik hujjat va h. kabi kompyuterga taalluqli bo'lmagan resurslarni ham qamrab olishi shart. Ushbu hujjatlar tarkibida tijoratni tashkil etish xususiyatlari to'g'risidagi axborot bo'lishi mumkin va bu hujjatlar buzg'unchilar foydalanishi mumkin bo'lgan joylarni ko'rsatadi.

Axborot xavfsizligi siyosatini aniqlashda quyidagilar amalga oshirilishi lozim:

1. Axborot xavfsizligi sohasida amal qilinadigan hujjatlar va standartlarni hamda axborot xavfsizligi siyosatining asosiy nizomlarini aniqlash, ya'ni:

- kompyuter texnikasi vositalaridan, dasturlardan va ma'lumotlardan foydalanishni boshqarish;
- virusga qarshi himoya;
- rezervli nusxalash masalalari;
- ta'mirlash va tiklash ishlarini o'tkazish;

- axborot xavfsizligi sohasidagi mojarolar xususida xabardor qilish.

2. Xavf-xatarlarni boshqarishga yondashishlarni aniqlash, ya'ni himoyalanganlikning bazaviy sathi yetarli ekanligini yoki xavf-xatarlarni tahlillashning to'liq variantini o'tkazish talab etilishini aniqlash.

3. Axborot xavfsizligi rejimiga qo'yiladigan talablarni aniqlash.

4. Sathlar bo'yicha qarshi choralarni strukturizatsiyalash.

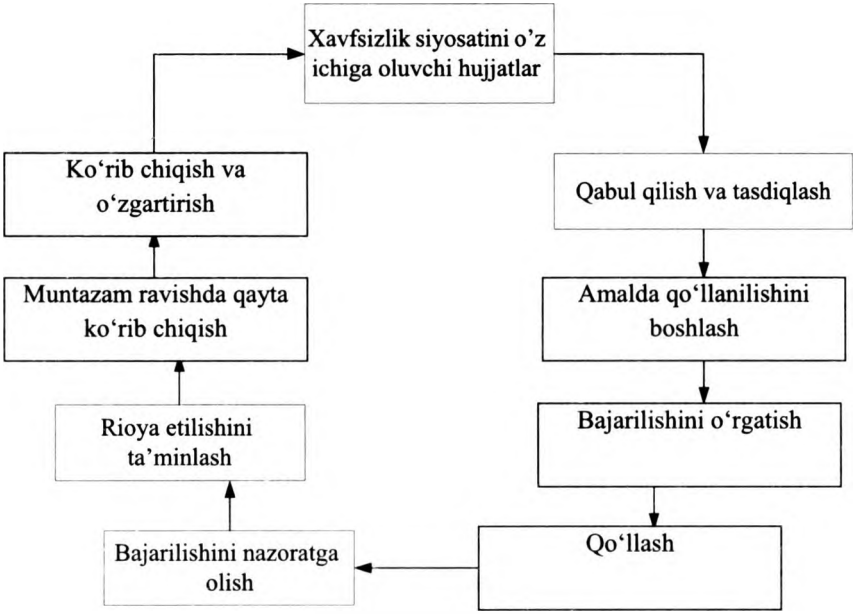
5. Axborot xavfsizligi sohasida sertifikatsiyalash tartibining standartlarga mosligini aniqlash.

6. Rahbariyatda axborot xavfsizligi mavzui bo'yicha kengashlar o'tkazish davriyligini, xususan, axborot xavfsizligi siyosatining nizomlarini qayta ko'rish hamda axborot tizimining barcha kategoriyali foydalanuvchilarini axborot xavfsizligi masalalari bo'yicha o'qitish tartibini aniqlash.

Tashkilotning real xavfsizlik siyosati quyidagi bo'limlarni o'z ichiga olishi mumkin:

- umumiy qoidalar;
- parollarni boshqarish siyosati;
- foydalanuvchilarni identifikatsiyalash;
- foydalanuvchilarning vakolatlari;
- tashkilot axborot resurslarini kompyuter viruslaridan himoyalash;
- tarmoq bog'lanishlarini o'rnatish va nazoratlash qoidalari;
- elektron pochta tizimi bilan ishlash bo'yicha xavfsizlik siyosati qoidalari;
- axborot resurslari xavfsizligini ta'minlash qoidalari;
- foydalanuvchilarning xavfsizlik siyosati qoidalarini bajarish bo'yicha majburiyatlari va h.

Qoidalar tashkilotning rivojlanishiga, yangi texnologiyalar, tizimlar va loyihalar paydo bo'lishiga muvofiq o'zgarishi lozim. Buning uchun qoidalarni davriy ravishda qayta ko'rib chiqish kerak. Xavfsizlik siyosatini qayta ko'rib chiqish usullaridan biri axborot kommunikatsiya tizimlari auditi hisoblanadi. Shu sababli tashkilot xavfsizlik siyosati va tabiiyki, axborot xavfsizligi siyosati o'zining hayotiy sikliga ega deyish mumkin (1.1-rasm).



1.1-rasm. Xavfsizlik siyosatining hayotiy sikli.

Xavfsizlik siyosati qoidalarini qayta ko'rib chiqish muddatlari xususida aniq bir ko'rsatma mavjud emas. Ammo ushbu muddat olti oydan bir yilgacha belgilanishi tavsiya etiladi.

Xavfsizlik qoidalari ishlab chiqilganidan va amalga kiritilganidan so'ng foydalanuchilar axborot xavfsizligi talablari bilan tanishib chiqishlari, xodimlar esa qoidalarni o'rganishlari lozim. Mojarolar paydo bo'lganda ishlab chiqilgan reja bo'yicha harakatlanish tavsiya etiladi.

Axborot xavfsizligini ta'minlash masalalari bo'yicha shug'ullanadigan yetakchi tashkilotlar xavfsizlik siyosati shablonlarini ishlab chiqdilar. Masalan, SANS (System Administration Networking and Security) instituti turli xavfsizlik siyosatining shablonlari seriyasini ishlab chiqdi (www.sans.org/resources/policies/).

Ushbu shablonlar tarkibiga quyidagi siyosatlar kiradi:

- *joiz shifrlash siyosati* – tashkilotda ishlatiluvchi kriptografik algoritmlarga qo'yiladigan talablarni aniqlaydi;

- *joiz foydalanish siyosati* – foydalanuvchilarni, tashkilot resurslarini va axborotning o'zini himoyalash uchun qurilmalardan va kompyuter xizmatlaridan foydalanishni aniqlaydi;

- *virusga qarshi himoya* – tashkilot tarmog'iga bo'ladigan kompyuter viruslari tahdidlarini samarali kamaytirishning asosiy prinsiplarini belgilaydi;

- *xarid imkoniyatlarini baholash siyosati* – tashkilot tomonidan himoya vositalarini xarid qilish imkoniyatlarini va axborot xavfsizligi guruhi tomonidan bajariladigan xarid qilinganlarni baholashga qo'yiladigan minimal talablarni aniqlaydi;

- *zaifliklarni skanerlash auditi siyosati* – axborot resurslarining yaxlitligiga ishonch hosil qilish, muvofiqlikni o'rnatish yoki foydalanish va tizim faolligining monitoringini o'tkazish maqsadida auditni kuzatish hamda xavf-xatarni baholash uchun talablarni aniqlaydi va mas'ul shaxsni tayinlaydi;

- *avtomatik tarzda uzatiladigan pochta siyosati* – menedjer yoki direktorning ruxsatisiz hech qanday pochta tashqi manbaga avtomatik tarzda yo'naltirilmasligi talablarini hujjatlashtiradi;

- *ma'lumotlar bazasidagi vakolatlarni kodlash siyosati* – ma'lumotlar bazasidagi foydalanuvchilar nomini va parollarni xavfsiz saqlash va olish uchun talablarni aniqlash;

- *telefon liniyasi orqali foydalanish siyosati* – tegishli foydalanishni va undan avtorizatsiyalangan xodimlar tomonidan foydalanishni aniqlaydi;

- *demilitarizatsiyalangan zona xavfsizligi siyosati* – demilitarizatsiyalangan zonada yoki tashqi tarmoq segmentlarida joylashgan laboratoriyalarda ishlatiladigan barcha tarmoq va qurilmalar uchun standartlarni belgilaydi;

- *jiddiy axborot siyosati* – konfidensiallikning mos darajalarini berish yo'li bilan tashkilot axborotini tasniflashga va xavfsizligiga qo'yiladigan talablarni belgilaydi;

- *parollarni himoyalash siyosati* – parollarni hosil qilish, himoyalash va almashtirish standartlarini aniqlaydi;

- *masofadan foydalanish siyosati* – tashkilot uchun tashqi hisoblanuvchi har qanday xostning yoki tarmoqning tashkilot tarmog'iga ulanish standartlarini aniqlaydi;

- *xavf-xatarni baholash siyosati* – tijorat hamkorligi bilan assotsiyatsiyalangan tashkilot axborot infratuzilmasida xavf-xatarni identifikatsiyalash, baholash va kamaytirish uchun talablarni aniqlaydi va mas'ul shaxslarni tayinlaydi;

- *marshrutizator xavfsizligi siyosati* – tashkilot ichki tarmog'i yoki faoliyat (mahsulotni tayyorlash) uchun ishlatiladigan marshrutizatorlar va kommutatorlar uchun xavfsizlikning minimal konfiguratsiyasi standartlarini aniqlaydi;

- *server xavfsizligi siyosati* – tashkilot ichki tarmog'i yoki mahsulot sifatida ishlatiladigan serverlar uchun xavfsizlikning minimal konfiguratsiyasi standartlarini aniqlaydi;

- *VPN xavfsizligi siyosati* – tashkilot tarmog'i bilan IPSec yoki L2TPVPN ulanishlardan masofadan foydalanish uchun talablarni aniqlaydi;

- *simsiz ulanishlar siyosati* – tashkilot tarmog'i bilan ulanish uchun ishlatiladigan simsiz tizim uchun standartlarni aniqlaydi.

Ta'kidlash lozimki, tashkilot qurilishining va faoliyat yuritishining o'ziga xos xususiyatlariga bog'liq holda tashkilotning xavfsizlik siyosati nabori shakllantiriladi.

Nazorat savollari:

1. Xavfsizlik siyosatini va uning ahamiyatini izohlab bering.
2. Xavfsizlik siyosatini aniqlashda qanday amallardan foydalaniladi?
3. Xavfsizlik siyosati qaysi bo'limlarni o'z ichiga olishi mumkinligini va ularni mohiyatini tushuntirib bering
4. Xavfsizlik siyosatining hayotiy sikli qanday ifodalanadi?
5. SANS instituti taqdim etgan xavfsizlik siyosati shablonlarini yoritib bering.

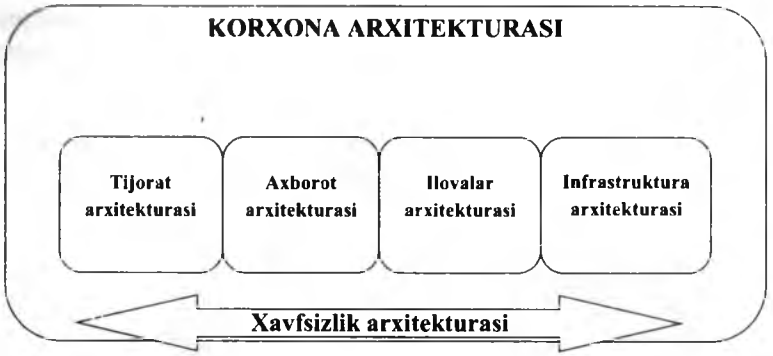
1.4. Axborot xavfsizligi arxitekturasi va strategiyasi

Zamonaviy tijorat oldida murakkab masalalar to'plami ko'ndalangki, beqaror iqtisodiy vaziyatda ularning dolzarbligi yanada oshadi. Bunday masalalarga quyidagilarni kiritish mumkin:

- daromadning oshishi;

- o‘zgaruvchi vaziyatlarga reaksiya tezligining oshishi;
- xarajat va chiqimlarning pasayishi;
- innovatsiyaning tezlashishi;
- bozorga mahsulot va xizmatlarni taqdim etish vaqtining qisqarishi;
- buyurtmachilar va sheriklar xolisligining oshishi;
- raqobatlik qobiliyatining oshishi;
- me’yoriy talablarga moslikni ta’minlash.

Yuqorida keltirilgan barcha masalalarni yechishda korxona arxitekturasidan foydalaniladi (1.2-rasm). Korxona arxitekturasi prinsiplar, yondashishlar va texnologiyalar naborini shakllantirishga imkon beradiki, ular tashkilotning joriy holatini hisobga olgan holda uning kelgusi transformatsiyasi, o‘sishi va rivojlanishi asosini belgilaydi.



1.2-rasm. Korxona arxitekturasi va uning boshqa arxitekturalar bilan bog‘liqligi.

Hozirda bunday arxitekturalarni yaratishda bir necha yondashishlar mavjud, masalan, TOGAF, Zachman Framework, FEAF, DoDAF va h.

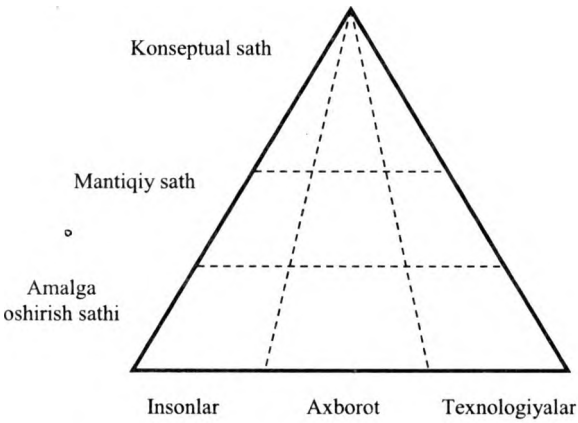
Ammo, qaysi bir yondashish tanlanmasin, hozirgi sharoitda axborotdan va axborot tizimidan foydalanmay rivojlanish mumkin emas. Axborot va axborot tizimlari nafaqat tijoratdagi har qanday o‘zgarishlarni madadlaydi, balki ularni oldindan sezadi, ularga oldindan tayyorlanadi, ba’zi hollarda esa yangi tijorat-imkoniyatlarining paydo bo‘lishiga yordam beradi. Biroq tijorat doimo

istalgancha rivojlanmaydi. Bunda ma'lumotlarning sirqib chiqishi, axborot texnologiyalari infrastrukturasi elementlarining ishdan chiqishi va h. bilan bog'liq axborot operatsion xavf-xatarlar anchagina rol o'ynaydi. Hozirgi va kelajak xavf-xatarga tayyor bo'lish uchun korxonaning boshqa arxitekturalari bilan uzviy bog'langan axborot xavfsizligi arxitekturasi zarur.

Axborot xavfsizligi arxitekturasi jarayonlarni, inson rolini, texnologiyalarni va turli xil axborotni tavsiflaydi hamda zamonaviy korxonaning murakkabligini va o'zgaruvchanligini hisobga oladi. Boshqacha aytganda, axborot xavfsizligining arxitekturasi tashkilotning va u bilan bog'liq boshqa komponentlar va interfeyslarning istalgan axborot xavfsizligi tizimi holatini tavsiflaydi. Bunda axborot xavfsiziligi arxitekturasi tijoratning joriy va eng muhimi, kelgusidagi ehtiyojini akslantiradi.

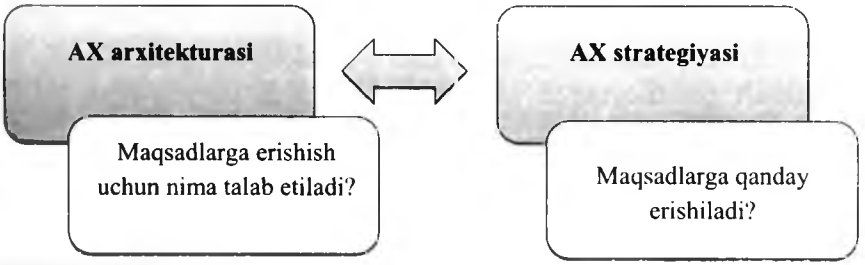
Odatda arxitekturaning 3 ta sathi ajratiladi – konseptual, mantiqiy va amalga oshirish (texnologik). 1.3-rasmda bunday arxitektura keltirilgan bo'lib, odatda texnologiyalar jihatidagi qismi xavfsizlik xizmati nazoratidan chetda qoladi.

Joriy holatdan qanday qilib yangi, mukammalroq va qo'yilgan maqsadlarga mos holatga o'tish mumkin? Buning uchun strategiya, ya'ni qo'yilgan maqsadlarga erishish uchun harakat yo'nalishi mavjud.



1.3-rasm. Axborot xavfsizligi arxitekturasi.

Strategiya – korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta'minlashga mo'ljallangan strukturalangan va o'zaro bog'langan harakatlar to'plami. 1.4-rasmda arxitektura bilan strategiyaning o'zaro bog'liqligi keltirilgan. Strategiya axborot xavfsizligi arxitekturasi ko'rinishidagi maqsadga ega bo'lgan holda unga erishishning optimal yo'lini belgilaydi.



1.4-rasm. Arxitektura bilan strategiyaning o'zaro bog'liqligi.

Ko'pincha strategiya va arxitektura tushunchalarini farqlamay, arxitektura tavsifini o'z ichiga olgan axborot xavfsizligi strategiyasi ishlab chiqiladi. Bu unchalik to'g'ri emas, chunki arxitektura, ya'ni maqsadlar vaqt o'tishi bilan o'zgarmasligi, bu maqsadlarga erishishdagi strategiya esa tashqi va ichki omillarga bog'liq holda jiddiy o'zgarishi mumkin. Strategiya va arxitektura bitta hujjatda tavsiflansa, strategiya o'zgarganida arxitekturani ham o'zgartirishga to'g'ri keladi.

Nazorat savollari:

1. Axborot xavfsizligi arxitekturasi va uning sathlari mohiyati.
2. Axborot xavfsizligi strategiyasi tushunchasi.
3. Korxona arxitekturasini tuzishda xavfsizlik strategiyasi va arxitekturasining o'rni.

II BOB. AXBOROT XAVFSIZLIGIGA BO‘LADIGAN TAHDIDLAR, HUJUMLAR VA ZAIFLIKLAR

2.1. Axborot xavfsizligiga tahdidlar va ularning tahlili

Axborot xavfsizligiga bo‘lishi mumkin bo‘lgan tahdidlarni tahlillash yaratilayotgan himoyalash tizimiga qo‘yiladigan talablarning to‘liq to‘plamini aniqlash maqsadida amalga oshiriladi. Odatda *tahdid* deganda (umumiy ma’noda) kimningdir manfaatlariga zarar yetkazuvchi hodisa (ta’sir, jarayon yoki voqea) tushuniladi. *Axborot tizimiga tahdid* deganda esa axborot tizimining xavfsizligiga bevosita yoki bilvosita zarar yetkazuvchi ta’sir imkoni tushuniladi.

Zamonaviy axborot tizimida saqlanuvchi va ishlanuvchi axborot juda ko‘p omillarning ta’siriga duchor bo‘lishi sababli tahdidlarning to‘liq to‘plamini tavsiflash masalasini formallashtirish mumkin emas. Shuning uchun tahdidlarning to‘liq ro‘yxatini emas, balki tahdidlar sinfining ro‘yxatini aniqlash maqsadga muvofiq hisoblanadi.

Axborot tizimiga bo‘lishi mumkin bo‘lgan tahdidlarni tasniflashni ularning quyidagi alomatlari bo‘yicha amalga oshirish mumkin:

1. *Paydo bo‘lish tabiati bo‘yicha* quyidagilar farqlanadi:

- axborot tizimiga obyektiv fizik jarayonlar yoki tabiiy hodisalar ta’sirida paydo bo‘luvchi *tabiiy tahdidlar*;
- inson faoliyati sabab bo‘luvchi axborot tizimiga *sun’iy tahdidlar.*

2. *Namoyon bo‘lishining atayinligi darajasi bo‘yicha* quyidagilar farqlanadi:

- *xodimning xatosi yoki loqaydligi tufayli paydo bo‘luvchi tahdidlar,* masalan, himoya vositasidan noto‘g‘ri foydalanish; xatoli ma’lumotlarni kiritish va h.;
- *atayin qilingan harakat natijasida paydo bo‘luvchi tahdidlar,* masalan, niyati buzuqlarning harakati.

3. *Tahdidlarning bevosita manbai bo'yicha* quyidagilar farqlanadi:

- *tabiiy muhit,* masalan tabiiy ofat, magnit bo'roni va h.;
- *inson,* masalan xodimning yollanishi, konfidensial ma'lumotlarning oshkor etilishi va h.;
- *ruxsat etilmagan dasturiy-apparat vositalar,* masalan, kompyuterning buzg'unchi funksiyali viruslar bilan zaharlanishi.

4. *Tahdidlar manbaining holati bo'yicha* quyidagilar farqlanadi:

- *nazoratlanuvchi axborot tizimi zonasidan tashqarisidagi manba,* masalan, aloqa kanali bo'yicha uzatiluvchi ma'lumotlarni, qurilmalarning elektromagnit, akustik va boshqa nurlanishlarini ushlab qolish;
- *nazoratlanuvchi axborot tizimi chegarasidagi manba,* masalan, yashirincha eshitish qurilmalaridan foydalanish, yozuvlarni, axborot eltuvchilarni o'g'rilash va h.
- *bevosita axborot tizimidagi manba,* masalan, axborot tizimi resurslaridan noto'g'ri foydalanish.

5. *Axborot tizimi faolligining darajasiga bog'liqligi bo'yicha* quyidagilar farqlanadi:

- *axborot tizimi faolligiga bog'liq bo'lmagan tahdidlar,* masalan axborot kriptohimoyasining fosh etilishi;
- *faqat ma'lumotlarni ishlash jarayonidagi tahdidlar,* masalan, dasturiy viruslarni yaratish va tarqatish tahdidi.

6. *Axborot tizimiga ta'sir darajasi bo'yicha* quyidagilar farqlanadi:

- *passiv tahdidlar,* ushbu tahdidlar amalga oshirilganida axborot tizimi strukturasi va mazmunida hech narsa o'zgarmaydi, masalan, maxfiy ma'lumotlarni nusxalash tahdidi;
- *aktiv tahdidlar,* ushbu tahdidlar amalga oshirilganida axborot tizimi va strukturasi va mazmuniga o'zgarishlar kiritiladi, masalan troyan oti va viruslarning kiritilishi.

7. *Foydalanuvchilarning yoki dasturlarning axborot tizimi resurslaridan foydalanish bosqichlari bo'yicha* quyidagilar farqlanadi:

- *axborot tizimi resurslaridan foydalanish bosqichida namoyon bo'luvchi tahdidlar,* masalan, axborot tizimidan ruxsatsiz foydalanish tahdidlari;

- *axborot tizimi resurslaridan foydalanishga ruxsat berilganidan keyingi tahdidlar,* masalan, axborot tizimi resurslaridan ruxsatsiz yoki noto'g'ri foydalanish tahdidlari.

8. *Axborot tizimi resurslaridan foydalanish usullari bo'yicha* quyidagilar farqlanadi:

- *axborot resurslaridan foydalanishning standart yo'lini ishlatadigan tahdidlar*, masalan, parollarga va foydalanishni chegaralashning boshqa rekvizitlariga noqonuniy ega bo'lib, ro'yxatga olingan foydalanuvchi sifatida niqoblanish tahdidi;

- *axborot resurslaridan foydalanishning yashirin nostandart yo'lini ishlatadigan tahdidlar*, masalan, operatsion tizimning hujjatlanmagan imkoniyatlarini ishlatib, axborot tizimi resurslaridan foydalanish tahdidi.

9. *Axborot tizimida saqlanadigan va ishlanadigan axborotning joriy joylanish joyi bo'yicha* quyidagilar farqlanadi:

- *tashqi xotira qurilmalaridagi axborotdan foydalanish tahdidi*, masalan, qattiq diskdan maxfiy axborotni ruxsatsiz nusxalash;

- *asosiy xotira axborotidan foydalanish tahdidi*, masalan, asosiy xotiraning qoldiq axborotini o'qish;

- *aloqa kanallarida aylanuvchi axborotdan foydalanish tahdidi,* masalan, aloqa kanaliga noqonuniy ulanib, yolg'on xabarlarni kiritish yoki uzatilayotgan xabarlarni modifikatsiyalash;

- *terminalda yoki printerda aks ettirilgan axborotdan foydalanish tahdidi*, masalan, aks ettirilgan axborotni yashirincha videokamera yordamida yozib olish.

Yuqorida qayd etilganidek, axborot tizimiga xavfli ta'sirlar tasodifiylariga yoki atayinlariga bo'linadi. Axborot tizimini loyihalash, yaratish va ekspluatatsiya qilish tajribasining tahlili ko'rsatadiki, axborot axborot tizimining barcha ishlash bosqichlarida turli tasodifiy ta'sirlar ostida bo'ladi.

Axborot tizimining ekspluatatsiyasida *tasodifiy ta'sir* sabablari quyidagilar bo'lishi mumkin:

- tabiiy ofat va elektr ta'minotining uzilishi sababli avariya holatlari;

- apparaturaning ishdan chiqishi;
- dasturiy ta'minotdagi xatoliklar;
- xizmatchi xodim va foydalanuvchilar faoliyatidagi xatoliklar;
- tashqi muhit ta'siri sababli aloqa kanalidagi xalallar.

Dasturiy ta'minotdagi xatoliklar eng ko'p uchraydi. Chunki, serverlar, ishchi stansiyalar, marshrutizatorlar va hokazolarning dasturiy ta'minoti inson tarafidan yoziladi va demak, ularda deyarli doimo xatoliklar mavjud. Dasturiy ta'minot qancha murakkab bo'lsa, undagi xatoliklarni va zaifliklarni aniqlash ehtimolligi shuncha katta bo'ladi. Ularning aksariyati hech qanday xavf tug'dirmaydi, ba'zilari esa niyati buzuqning serverni nazoratlashi, serverning ishdan chiqishi, resurslardan ruxsatsiz foydalanish kabi jiddiy oqibatlarga sabab bo'lishi mumkin. Odatda bunday xatoliklar dasturiy ta'minot ishlab chiqaruvchilar tomonidan muntazam taqdim etiluvchi yangilash paketi yordamida bartaraf etiladi. Bunday paketlarning o'z vaqtida o'rnatilishi axborot xavfsizligining zaruriy sharti hisoblanadi.

Atayin qilinadigan tahdidlar niyati buzuqning maqsadga yo'naltirilgan harakatlari bilan bog'liq. Niyati buzuq sifatida tashkilot xodimini, qatnovchini, yollangan kishini va h. ko'rsatish mumkin. Avvalo tashkilot, xodimining niyati buzuq bilan tushungan holda hamkorlik qilishiga e'tibor berishi lozim. Bunday hamkorlikka undovchi sabablar quyidagilar:

- tashkilot xodimining rahbariyatga qasdlik qilish maqsadida;
- niyati buzuq qarashlarning haqqoniyligiga ishongan holda;
- xodimning tashkilot rahbariyatining noqonuniy faoliyat yuritilayotganligiga ishongan holda;
- yolg'on harakatlar, ta'magirlik, shantaj, xarakterning salbiy jihatlaridan foydalanish, zo'rlash yo'li bilan hamkorlikka undash va h.

Nazorat savollari:

1. Axborot xavfsizligiga bo‘ladigan tahdidlar tushunchasi qanday ifodalanadi?
2. Tahdidlarni tasniflashda qanday alomatlari asos qilib olinadi?
3. Tabiiy va sun’iy tahdidlarni tushuntirib bering.
4. Bilmasdan va atayin qilinadigan tahdidlarni tushuntirib bering.

2.2. Axborot xavfsizligining zaifliklari

Zaifliklar tashkilot aktivlari bilan assotsiyatsiyalangan himoyaning kuchsizliklarini ifodalaydi. Ushbu kuchsizliklar nomaqbul mojarolarga sabab bo‘luvchi bitta yoki bir necha tahdidlar tomonidan foydalanishi mumkin. Zaiflikning o‘zi zarar yetkazmaydi, ammo aktivlarga zarar yetkazishga imkon beruvchi sharoit yoki sharoitlar to‘plami hisoblanadi. Boshqacha aytganda, zaifliklar – tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omillar. Shu sababli zaifliklarni baholash uchun mavjud xavfsizlik mexanizmlarini identifikatsiyalash va ularning samaradorligini baholash zarur.

Aktivlarga zarar yetkaza oluvchi mojarolarga sabab bo‘lish uchun tahdidlar va zaifliklar birlashishlari lozim. Shuning uchun tahdidlar bilan zaifliklar orasidagi bog‘liqlikni aniqlash zarur. Quyida xavfsizlikning turli jabhalaridagi zaifliklarga va ulardan foydalana oladigan tahdidlarga misollar keltirilgan.

1. Kadr resurslarining xavfsizligi (ISO/IEC 27002:2005, 8-bo‘lim)	
Zaiflik	***Zaiflikdan foydalanuvchi tahdid***
Xavfsizlikni yetarlicha o‘rgatilmasligi.	Texnik madadlash xodimining xatosi.
Xavfsizlik masalalaridan bexabarligi.	Foydalanuvchilar xatosi.
Monitoring mexanizmlarining mavjud emasligi.	Dasturiy ta’minotdan ruxsatsiz foydalanish.

Telekommunikatsiya va xabarlarni uzatish vositalaridan korrekt (to‘g‘ri) foydalanish bo‘yicha siyosatning mavjud emasligi.	Tarmoq uskunasidan ruxsatsiz foydalanish.
Ishdan bo‘shatilganda foydalanish huquqi bekor qilinmaydi.	Ruxsatsiz foydalanish.
Ishdan bo‘shatilganda resurslarni qaytarishni kafolatlovchi muolaja mavjud emas.	O‘g‘rilik.
Asossiz yoki norozi xodim.	Axborotni ishlovchi vositalarning suiiste’mol qilinishi.
Begona xodimning yoki ishdan keyin ishlovchi xodimning nazoratsiz ishlashi.	O‘g‘rilik.

2. Fizik xavfsizlik va atrof-muhit xavfsizligi (ISO/IEC 27002:2005, 9-bo‘lim)	
Zaiflik	***Zaiflikdan foydalanuvchi tahdid***
Binodan, xonalardan, ofislardan adekvat bo‘lmagan yoki e’tiborsiz fizik nazoratlash mexanizmlaridan foydalanish.	Atayin zarar yetkazish.
Binoni, eshiklarni va derazalarni fizik himoyalashning yo‘qligi.	O‘g‘rilik.
Suv toshishiga duchor zonada joylanishi.	Cho‘kish.
Himoyalanmagan saqlash.	O‘g‘rilik.
Axborotni saqlash vositalarining nomuvofiq o‘rnatilishi/nomunosib olib yurilishi.	Olib yurilishi jarayonida xatolik.
Uskunani davriy almashtirish sxemasining yo‘qligi.	Axborotni saqlash vositalarining eskirishi.
Uskunaning namlikka, changlikka va ifloslanishga duchor bo‘lishi.	Chang bosishi.
Uskunaning harorat o‘zgarishiga	Harorat rejimining buzilishi.

duchor bo'lishi.	
Uskunaning kuchlanish o'zgarishiga duchor bo'lishi.	Elektr manbaining fluktuatsiyasi.
Beqaror elektr manbai.	Elektr manbaining fluktuatsiyasi.

3. Kommunikasiyalarni va amallarni boshqarish (ISO/IEC 27002:2005, 10-bo'lim)	
Zaiflik	***Zaiflikdan foydalanuvchi tahdid***
Murakkab foydalanuvchi interfeysi.	Xodim xatosi.
Axborotni saqlash vositalarini tegishlicha tozalamasdan o'tkazish yoki ulardan takroran foydalanish.	Axborotdan ruxsatsiz foydalanish.
O'zgarishlarning adekvat bo'lmagan nazorati.	Xavfsizlik tizimining to'xtab qolishi.
Tarmoqni adekvat bo'lmagan boshqarish.	Trafikning ortiqcha yuklanishi.
Zaxirali nusxalash muolajalarining yo'qligi.	Axborotning yo'qolishi.
Xabarning jo'natilganligi yoki olinganligi xususidagi isbotning yo'qligi.	Javobgarlikdan bosh tortish.
Zarar keltiruvchi koddan himoyalashda ishlatiluvchi dasturiy ta'minotning yangilanmasligi.	Virus infeksiyasi.
Vazifalarning taqsimlanmaganligi.	Tizimni suiiste'mol qilish (tasodifiy yoki atayin).
Test va ishchi uskunaning ajratilmaganligi.	Harakatdagi tizimni ruxsatsiz modifikatsiyalash.
Nazoratsiz nusxalash.	O'g'rilik.
Umumfoydalanuvchi tarmoqlarga himoyalanmagan ulanishlar.	Dasturiy ta'minotdan avtorizatsiyalanmagan foydalanuvchilarning foydalanishi.

4. Foydalanish nazorati (ISO/IEC 27002:2005, 11-bo‘lim)	
Zaiflik	***Zaiflikdan foydalanuvchi tahdid***
Tarmoqdarda foydalanishni noto‘g‘ri cheklash.	Tarmoqqa ruxsatsiz ulanish.
Toza stollar va toza ekranlar siyosatining yo‘qligi.	Axborotning yo‘qolishi yoki shikastlanishi.
Foydalanuvchilarning autentifikatsiyasi kabi identifikatsiya va autentifikatsiya mexanizmlarining yo‘qligi.	Begona foydalanish identifikatorini o‘zlashtirish.
Mobil kompyuter uskuna himoyasining yo‘qligi.	Axborotdan ruxsatsiz foydalanish.
Ishchi stansiya aloqani uzganida tizimdan chiqaolmasligi.	Avtorizatsiyalanmagan foydalanuvchilar tomonidan dasturiy ta’minotning ishlatilishi.
Dasturiy ta’minotni testlashning nomuvofiq xajmda o‘tkazilishi yoki yo‘qligi.	Avtorizatsiyalanmagan foydalanuvchilar tomonidan dasturiy ta’minotning ishlatilishi.
Foydalanuvchilarning foydalanish huquqlari nazoratining va tahlilining yo‘qligi.	Tashkilotni tark etgan yoki ish joyini o‘zgartirgan foydalanuvchilar tomonidan foydalanish.
Parollarni yomon boshqarish (osongina aniqlanadigan parollar, tez-tez almashtirmaslik va h.).	Begona foydalanish identifikatorini o‘zlashtirish.
Tizim utilitalaridan nazoratsiz foydalanish.	Tizim yoki ilovani nazoratlash mexanizmlariga rioya qilmaslik.

5. Axborot tizimlariga erishish (xarid qilish), ishlab chiqish va kuzatish (ISO/IEC 27002:2005, 12-bo‘lim)	
Zaiflik	***Zaiflikdan foydalanuvchi tahdid***
Kritpografik kalitlarni nomuvofiq himoyalash.	Axborotning oshkor etilishi.
Kriptografiyadan foydalanish sohasidagi mukammal bo‘lmagan siyosat.	Qonunlarning yoki me’yoriy asoslarning buzilishi.

Kiruvchi yoki chiquvchi ma'lumotlar nazoratining yo'qligi.	Xatolik.
Ishlanadigan ma'lumotlarning tekshirilmasligi.	Axborotning buzilishi.
Dasturiy ta'minotni testlashning yo'qligi yoki yetarlicha hajmda bajarilmasligi.	Avtorizatsiyalanmagan foydalanuvchilarning dasturiy ta'minotdan foydalanishi.
Yomon hujjatlangan dasturiy ta'minot.	Texnik madadlovchi xodimning xatosi.
Ishlab chiqaruvchilar uchun tushunarsiz yoki to'liq bo'lmagan spetsifikatsiyalar.	Dasturiy ta'minotning adashishi.
Dasturiy ta'minotning nazoratsiz yuklanishi va ishlatilishi.	Zarar yetkazuvchi dasturiy ta'minot.
Korporativ ilovalarda shartli tekin yoki tekin dasturiy ta'minotdan nazoratsiz foydalanish.	Huquqiy javobgarlik.
Dasturiy ta'minotdagi ma'lum nuqsonlar.	Dasturiy ta'minotdan avtorizatsiyalanmagan foydalanuvchilarning foydalanishi.
Test ma'lumotlarini noto'g'ri tanlash.	Shaxsiy ma'lumotlardan ruxsatsiz foydalanish.

Nazorat savollari:

1. Axborot xavfsizligida zaiflik tushunchasi.
2. Kadr resurslarining xavfsizligi jihatidan kelib chiqadigan zaifliklarni tavsiflab bering.
3. Fizik xavfsizlik va atrof-muhit xavfsizligi jihatidan kelib chiqadigan zaifliklarni tavsiflab bering.
4. Kommunikatsiyalarni va amallarni boshqarish jihatidan kelib chiqadigan zaifliklarni tavsiflab bering.
5. Foydalanishlarni nazoratlash jihatidan kelib chiqadigan zaifliklarni tavsiflab bering.
6. Axborot kommunikatsiya tizimlarini xarid qilish, ishlab chiqish va kuzatish jihatidan kelib chiqadigan zaifliklarni tavsiflab bering.

2.3. Axborotning mahfiyligini, yaxlitligini va foydalanuvchanligini buzish usullari

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 sababli tarmoqdagi axborotga masofadan bo'ladigan asosiy namunaviy hujumlar quyidagilar:

- tarmoq trafigini 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 (Fayllarni uzatish protokoli) va TELNET (Virtual terminal protokoli) bo'yicha foydalanish uchun foydalanuvchi *identifikatsiya* va *autentifikatsiya* muolajalarini o'tishi lozim. Foydalanuvchini identifikatsiyalashda axborot sifatida uning identifikatori (ismi) ishlatilsa, autentifikatsiyalash uchun *parol* ishlatiladi. FTP va TELNET protokollarining xususiyati shundaki, foydaluvchilarning paroli va identifikatori tarmoq orqali ochiq, shifrlanmagan ko'rinishda uzatiladi. Demak, Internet xostlaridan foydalanish uchun foydalanuvchining ismi va parolini bilish kifoya.

Axborot almashinuvida Internetning masofadagi ikkita uzeli almashinuv axborotini *paketlarga* ajratadi. 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. Shu sababli, hozirda ommaviy tus olgan ICQ (Bir lahzali almashish xizmati) dasturi ham ishonchli emas. ICQning protokollari va axbo-

rotlarni 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 shundan 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 (Kanal sathi protokoli) 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 segment-

lariga murojaatga imkon beruvchi marshrutizatorga murojaat qilinadi. Agar foydalanuvchi 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:

- DNS-so'rovni kutish;
- 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;
- 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);
- 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).

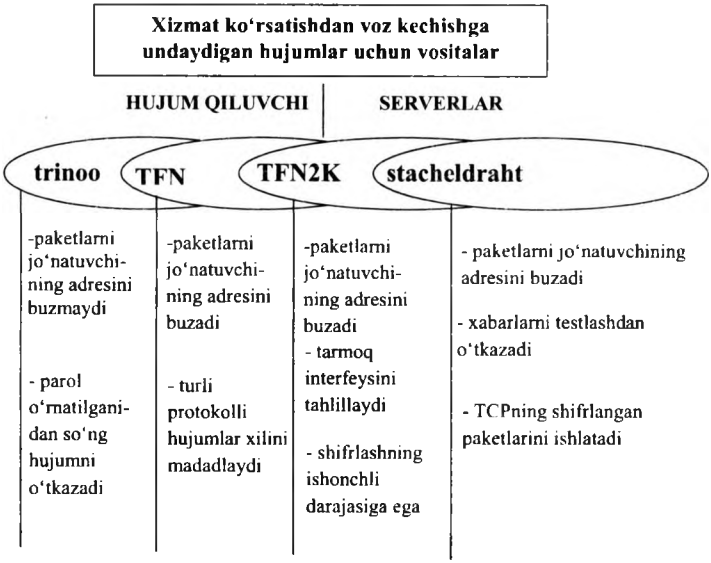
Yolg'on marshrutni kiritish. Ma'lumki, zamonaviy global tarmoqlari bir-biri bilan *tarmoq uzellari* yordamida ulangan tarmoq segmentlarining majmuidir. Bunda *marshrut* deganda ma'lumotlarni manbadan qabul qiluvchiga uzatishga xizmat qiluvchi tarmoq uzellarining ketma-ketligi tushuniladi. Marshrutlar xususidagi axborotni almashishni unifikatsiyalash uchun marshrutlarni boshqaruvchi maxsus protokollar mavjud. Internetdagi bunday protokollarga yangi marshrutlar xususida xabarlar almashish protokoli – ICMP (Tarmoqlararo boshqaruvchi xabarlar protokoli) va marshrutizatorlarni masofadan boshqarish protokoli SNMP (Tarmoqni boshqarishning oddiy protokoli) misol bo'la oladi. Marshrutni o'zgartirish hujum qiluvchi yolg'on xostni kiritishidan 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 oqimidan 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 (Xizmat qilishdan taqsimlangan voz kechish) kompyuter jinoyatchiligining nisbatan yangi xili bo'lsa-da, qo'rqinchli tezlik bilan tarqalmoqda. Bu hujumlarning o'zi anchagina yoqimsiz bo'lgani yetmaganidek, ular bir vaqtning o'zida masofadan boshqariluvchi yuzlab hujum qiluvchi serverlar tomonidan boshlanishi mumkin. Xakerlar tomonidan tashkil etilgan uzellarda DDoS hujumlar uchun uchta instrumental vositani topish mumkin: trinoo, TribeFloodNet (TFN) va TFN2K. Yaqinda TFN va trinooning eng yoqimsiz sifatlarini uyg'unlashtirgan yana bittasi stacheldraht ("tikon simlar") paydo bo'ldi.

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



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

Nazorat savollari:

1. Tarmoq trafigini tahlillashga asoslangan buzish usullarini tushuntirib bering.
2. Tarmoqning yolg‘on obyektini kiritishga asoslangan buzish usulini ishlash prinsipini tushuntirib bering.
3. Yolg‘on marshrutni kiritish qanday amalga oshiriladi?
4. Xizmat qilishdan voz kechishga undaydigan buzish usuli turlarini tavsiflab bering.

III BOB. AXBOROT XAVFSIZLIGI SOHASIGA OID XALQARO VA MILLIY ME'YORIY-HUQUQIY BAZA

3.1. Axborot xavfsizligi sohasiga oid xalqaro standartlar

Xavfsizlik standartlarining asosiy maqsadi axborot texnologiyalari mahsulotlarini ishlab chiqaruvchilar, iste'molchilar va kvalifikatsiyalash bo'yicha ekspertlar orasida o'zaro aloqani yaratish hisoblanadi.

Ishlab chiqaruvchilar uchun standartlar, axborot mahsulotlarining imkoniyatlarini taqqoslash uchun zarur. Undan tashqari standartlar axborot mahsulotlari xususiyatlarini obyektiv baholash mexanizmi hisoblanuvchi, sertifikatsiyalash muolajalari uchun zarur.

Iste'molchilar ehtiyojlariga muvofiq axborot mahsulotini asosli tanlashga imkon beruvchi usulga manfaatdordurlar. Buning uchun ularga xavfsizlikni baholash shkalasi zarur.

Axborot texnologiyalari mahsulotlarini kvalifikatsiyalash bo'yicha ekspertlar standartlarni ularga axborot texnologiyalari mahsulotlari tomonidan ta'minlanuvchi xavfsizlik darajasini baholashga imkon beruvchi instrument sifatida qabul qiladilar.

ISO/IEC 27001:2005 – "Axborot texnologiyalari. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar". Ushbu standart axborot xavfsizligini boshqarish tizimini (AXBT) ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat ko'rsatish va uni takomillashtirish modeli va talablaridan iborat. AXBT joriy etilishi tashkilotning strategik qarori bo'lib qolishi kerak. AXBTni ishlab chiqish va joriy etishda xavfsizlikning ehtiyojlari, maqsadlari, foydalaniladigan jarayonlari, tashkilotning ko'lami va strukturasi hisobga olinishi kerak. AXBT va uning yordamchi tizimlari vaqt o'tishi bilan o'zgaradi degan taxmin bor. Shuningdek, AXBTni kengaytirish masshtablari tashkilotning ehtiyojlariga bog'liq bo'ladi, masalan, oddiy vaziyat AXBT uchun oddiy yechimni talab qiladi.

Muvofiqlikni baholash uchun ushbu standartdan ichki va tashqi tomonlar foydalanishi mumkin.

Jarayonli yondashuv. Ushbu standart tashkilot AXBTni ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat ko'rsatish va uni takomillashtirishda jarayonli yondashuvning qo'llanishiga yo'naltirilgan.

Tashkilot muvaffaqiyatli ishlashi uchun faoliyatning ko'p sonli o'zaro bog'liq turlarini aniqlashi va ularni boshqarishni amalga oshirishi kerak. Aktivlardan foydalanuvchi va kirishlarni chiqishlarga o'zgartirish maqsadida boshqariladigan faoliyatning barcha turlariga jarayonlar sifatida qarash mumkin. Ko'pincha bir jarayonning chiqishi keyingi jarayonning bevosita kirishini hosil qiladi.

Tashkilotda jarayonlar tizimini identifikatsiyalash va ularning o'zaro harakati bilan bir qatorda jarayonlar tizimidan foydalanish, shuningdek, jarayonlarni boshqarish *jarayonli yondashuv* deb hisoblanishi mumkin.

Bunday yondashuv axborot xavfsizligida qo'llanganda quyidagilarning muhimligini ta'kidlaydi:

- tashkilotning axborot xavfsizligi talablarini va axborot xavfsizligi siyosati va maqsadlarini belgilash zarurligini tushunish;
- tashkilot barcha biznes-tavakkalchiliklarning umumiy kontekstida tashkilot axborot xavfsizligi xatarlarini boshqarish choralarini joriy etish va qo'llash;
- AXBT unumdorligi va samaradorligining doimiy monitoringi va tahlili;
- obyektiv o'lchashlar natijalariga asoslangan uzluksiz takomillashtirish.

Ushbu standartda AXBT har bir jarayonini ishlab chiqishda qo'llanishi mumkin bo'lgan *rejalashtirish – amalga oshirish – tekshirish - harakat* [«Plan-Do-Check-Act» (PDCA)] modeli keltirilgan.

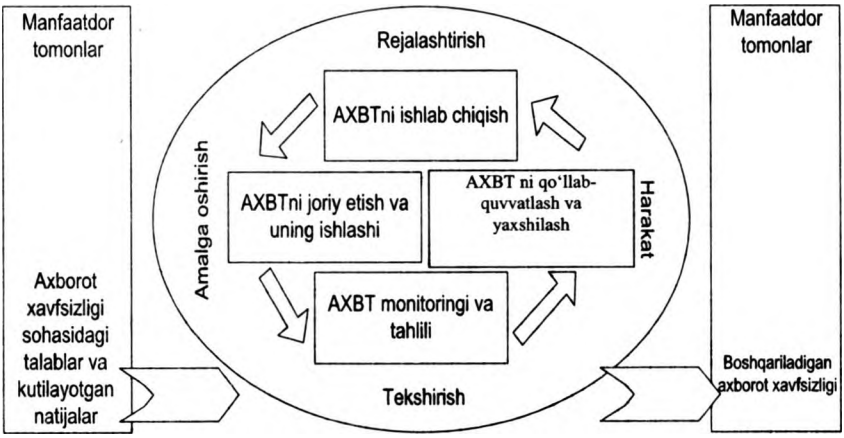
Ushbu model AXBT axborot xavfsizligi talablari va manfaatdor tomonlarning kutilayotgan natijalaridan kiruvchi ma'lumotlar sifatida qanday foydalanishini va zarur xatti-harakatlar va jarayonlarni amalga oshirish natijasida e'lon qilingan talablar va

kutilayotgan natijalarni qanoatlantirishidan dalolat beradigan ma'lumotlarni olishini ko'rsatadi.

Bundan tashqari, PDCA modeli «Axborot tizimlari va tarmoqlari xavfsizligi bo'yicha iqtisodiy hamkorlik va rivojlanish tashkiloti»ning amaldagi ko'rsatmalariga mos keladi. Ushbu standart xatarlarni boshqarish, xavfsizlik choralarini rejalashtirish va amalga oshirish, xavfsizlikni boshqarish va qayta baholashda ushbu prinsiplarni qo'llashning amaliy modelini taqdim etadi.

1-misol. Axborot xavfsizligining buzilishi tashkilot uchun jiddiy moliyaviy yo'qotishlarning va/yoki qandaydir qiyinchiliklarning sababi bo'la olmaydi degan talab qo'yilishi mumkin.

2-misol. Qandaydir jiddiy mojaro, masalan, sayt yordamida elektron savdoni amalga oshirayotgan tashkilot saytining buzilishi natijasida yuzaga keladigan holat uchun – tashkilot buzilish oqibatlarini minimumga keltirish uchun yetarli bilim va tajribaga ega bo'lgan mutaxassislarga ega bo'lishi kerak. 3.1-rasmda AXBT jarayonlariga PDCA modelini qo'llash ko'rsatilgan.



3.1-rasm. AXBT jarayonlariga PDCA modelini qo'llash.

Ushbu standart tashkilotga amaldagi AXBTni boshqa boshqaruv tizimlarining tegishli talablari bilan moslashtirish yoki integratsiya qilish imkonini beradi.

Boshqa boshqarish tizimlari bilan moslashuv. Ushbu standart boshqa boshqaruv standartlari bilan moslashuvini yaxshilash va integratsiya qilish uchun ISO 9001:2000 [2] va ISO 14001:2004 [3] standartlari bilan muvofiqlashtirilgan. Kerakli tarzda loyihalashtirilgan bitta boshqaruv tizimi barcha ushbu standartlarning talablariga javob berishga qodir. 3.1-jadvalda ushbu standartning ISO 9001:2000 va ISO 14001:2004 standartlari bilan o'zaro bog'liqligi ko'rsatilgan.

3.1-jadval.

Rejalashtirish (AXBTni ishlab chiqish)	Tashkilotning umumiy siyosati va maqsadlarida e'lon qilingan natijalarga erishish maqsadida siyosat va maqsadlarni belgilash, xatarlarni boshqarish va axborot xavfsizligini takomillashtirish bilan bog'liq bo'lgan jarayonlar va protseduralarni aniqlash.
Amalga oshirish (AXBTni joriy etish va uning ishlashi)	AXBT siyosati, metodlari, jarayonlari va protseduralarini joriy etish va uning ishlashi.
Tekshirish (AXBT monitoringi va tahlili)	Jarayonlarning AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo'lganida samaradorligini o'lchash. Natijalarning yuqori rahbariyat tomonidan tahlil qilinishi.
Harakat (AXBTni qo'llab quvvatlash va takomillashtirish)	AXBT ichki auditlari natijalariga rahbariyat tomonidan qilingan tahlil yoki uzluksiz takomillashtirish maqsadida boshqa manbalardan olingan ma'lumotlarga asoslangan tuzatuvchi va ogohlantiruvchi harakatlarni bajarish.

ISO/IEC 27002:2005 – "Axborot texnologiyasi. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

Axborot - biznesning boshqa muhim aktivlari kabi qiymatga ega bo'lgan aktiv va shunday ekan, u tegishli ravishda muhofaza qilingan bo'lishi kerak. Bu o'zaro aloqalar bilan doimo rivojlanayotgan amaliy ish muhitida ayniqsa muhim. Hozirgi vaqtda ushbu o'zaro aloqalar natijasida axborot tahdidlar va zaifliklarning o'sib borayotgan soni va turli xiliga duchor bo'lmoqda.

Axborot turli shakllarda mavjud bo'lishi mumkin. U qog'oz eltuvchida joylashtirilgan bo'lishi, elektron ko'rinishda saqlanishi, pochta orqali yoki telekommunikatsiyaning elektron vositalaridan foydalanib uzatilishi, plyonkadan namoyish qilinishi yoki og'zaki ifodalanishi mumkin. Axborot mavjudligining shaklidan, uni tarqatish yoki saqlash usulidan qat'iy nazar u doim adekvat muhofazalangan bo'lishi kerak.

Axborot xavfsizligi - axborotni biznesning uzluksizligini ta'minlash, biznes xavflarini minimumga keltirish va investitsiyalarni qaytarishni hamda biznes imkoniyatlarini maksimal oshirish maqsadida tahdidlarning keng spektridan muhofaza qilish demakdir.

Axborot xavfsizligiga dasturiy ta'minotning siyosatlari, metodlari, muolajalari, tashkiliy tuzilmalari va dasturiy ta'minot funksiyalari tomonidan taqdim etilishi mumkin bo'lgan axborot xavfsizligini boshqarish bo'yicha tadbirlarning tegishli kompleksini amalga oshirish yo'li bilan erishiladi. Ko'rsatilgan tadbirlar tashkilotning axborot xavfsizligi maqsadlariga erishishini ta'minlashi kerak.

Axborot xavfsizligining zarurati. Axborot va uni saqlab turuvchi jarayonlar, axborot tizimlari va tarmoq infratuzilmasi biznesning bebaho aktivlari bo'lib hisoblanadi. Axborot xavfsiligini aniqlash, ta'minlash, saqlab turish va yaxshilash tashkilotning raqobatbardoshliligi, qadrliligi, daromadliligi, qonun hujjatlariga muvofiqligini va ishbilarmonlik obro'sini ta'minlashda katta ahamiyatga ega.

Tashkilotlar, ularning axborot tizimlari va tarmoqlar xavfsizlikning turli kompyuter firibgarligi, ayg'oqchilik, zararkunandalik, vandalizm, yong'inlar yoki suv toshqinlari kabi tahdidlar bilan ko'proq to'qnashmoqdalar. Zararning bunday kompyuter viruslari, kompyuterni buzib ochish va «xizmat ko'rsatishdan bosh tortish»

kabi hujumlar manbalari keng tarqalmoqda, tajovuzkor bo‘lib bormoqda va ko‘proq mahorat bilan shakllanmoqda.

Axborot xavfsizligi biznesning jamoat va xususiy sektorida, shuningdek, kritik infratuzilmalarni muhofaza qilishda muhim. Axborot xavfsizligi ikkala sektorda ham yordam berishi kerak, masalan, elektron hukumatni yoki elektron biznesni joriy qilishda tegishli xavflardan mustasno bo‘lish yoki ularni kamaytirish uchun. Umumiy foydalanishdagi tarmoqlarning va xususiy tarmoqlarning birgalikda ishlashi, shuningdek, axborot resurslaridan birgalikda foydalanishi axborotdan foydalanishni boshqarishni qiyinlashtiradi. Ma’lumotlarga taqsimlab ishlov berishdan foydalanish tendensiyasi markazlashtirilgan nazorat samaradorligini susaytiradi.

Ko‘pgina axborot tizimlarini loyihalashda xavfsizlik masalalari e’tiborga olinmas edi. Texnik vositalar bilan erishilishi mumkin bo‘lgan xavfsizlik darajasi bir qator cheklashlarga ega, binobarin, tegishli boshqaruv vositalari va protseduralar bilan ta’minlanishi kerak. Axborot xavfsizligini boshqarish bo‘yicha zarur tadbirlarni tanlash puxtalik bilan rejalashtirish va detallashtirishni talab qiladi.

Axborot xavfsizligini boshqarish, kamida tashkilot barcha xodimlarining ishtirok etishiga muhtoj. Shuningdek, yetkazib beruvchilar, mijozlar yoki aksiyadorlarning ishtirok etishi ham talab qilinishi mumkin. Bundan tashqari, begona tashkilot muta-xassislarining maslahatlari kerak bo‘lib qolishi mumkin.

Agar axborot xavfsizligi sohasini boshqarish bo‘yicha tadbirlar axborot tizimini loyihalashtirish bosqichida texnik topshiriqqa kiritilsa, ancha arzonga tushadi va samaraliroq bo‘ladi.

Axborot xavfsizligi talablarini aniqlash. Tashkilot o‘zining axborot xavfsizligiga bo‘lgan talablarini quyidagi uchta muhim omilni hisobga olib, aniqlashi muhim:

- biznesning global strategiyasi va tashkilotning maqsadlarini e’tiborga olib, tashkilotda olingan xavflarni baholash yordamida tashkilot aktivlariga tahdidlar aniqlanadi, tegishli aktivlarning zaifligi va tahdidlar paydo bo‘lish ehtimoli, shuningdek, kelib chiqishi mumkin bo‘lgan oqibatlar baholanadi;

- tashkilot, uning savdo sheriklari, pudratchilar va xizmatlarni yetkazib beruvchilar, qoniqtirilishi kerak bo‘lgan yuridik talablar, qonun hujjatlarining talablari, tartibga soluvchi va shartnomaviy

talablar, shuningdek, ushbu tomonlarning ijtimoiy madaniy muhiti boshqa omil bo‘lib hisoblanadi;

- o‘zining ishlashini ta’minlash uchun tashkilot tomonidan ishlab chiqilgan prinsiplar, maqsadlar va talablarning maxsus to‘plami yana bir omil bo‘lib hisoblanadi.

Axborot xavfsizligi xavflarini baholash. Axborot xavfsizligiga qo‘yiladigan talablar xavflarni muntazam baholash yordamida aniqlanadi. Axborot xavfsizligini boshqarish bo‘yicha tadbirlarga ketgan sarf-xarajatlar axborot xavfsizligining buzilishi natijasida tashkilotga yetkazilishi mumkin bo‘lgan zarar miqdoriga mutanosib bo‘lishi lozim.

Ushbu baholashning natijalari axborot xavfsizligi bilan bog‘liq xavflarni boshqarish sohasida aniq choralar va ustuvorliklarni belgilashga, shuningdek, ushbu xavflarni minimumga keltirish maqsadida axborot xavfsizligini boshqarish bo‘yicha tadbirlarni joriy qilishga yordam beradi. Mavjud tadbirlarning samaradorliligiga ta’sir ko‘rsatishi mumkin bo‘lgan har qanday o‘zgarishlarni hisobga olish uchun xavflar tahlilini vaqti-vaqti bilan takrorlab turish kerak.

Axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlash. Axborot xavfsizligiga qo‘yiladigan talablar belgilanganidan va xavflar aniqlanganidan so‘ng xavflarni qabul qilsa bo‘ladigan darajagacha pasayishini ta’minlaydigan, axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlash va joriy etish kerak. Ushbu tadbirlar ushbu standartdan, boshqa manbalardan tanlab olinishi, shuningdek, axborot xavfsizligini boshqarish bo‘yicha tashkilotning o‘ziga xos ehtiyojlarini qondiradigan tadbirlar ishlab chiqilishi mumkin. Axborot xavfsizligini boshqarish bo‘yicha tadbirlarni tanlash xavflarni qabul qilish mezonlariga, xavflarga baho berish variantlariga asoslangan tashkiliy qarorlarga va xavflarni tashkilotda qabul qilingan boshqarishga umumiy yondashishga bog‘liq. Ushbu tanlovni tegishli milliy va xalqaro qonun hujjatlari va normalar bilan muvofiqlashtirish kerak.

Ushbu standartda keltirilgan axborot xavfsizligini boshqarish bo‘yicha ba’zi tadbirlar axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va ko‘pgina tashkilotlar uchun qo‘llanishi mumkin. Bunday tadbirlar quyiroqda

«Axborot xavfsizligini joriy qilish uchun tayanch nuqta» sarlavhasi ostida batafsilroq ko'rib chiqiladi.

Axborot xavfsizligini joriy qilish uchun tayanch nuqta. Axborot xavfsizligini boshqarish bo'yicha alohida tadbirlar axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va uni joriy qilish uchun tayanch nuqta bo'lib xizmat qilishi mumkin. Bunday tadbirlar qonun hujjatlarining asosiy talablariga asoslanadi yoki axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida qabul qilinishi mumkin.

Qonunchilik nuqtayi nazaridan axborot xavfsizligini boshqarish bo'yicha asosiy choralar quyidagilar hisoblanadi:

- ma'lumotlarni muhofaza qilish va shaxsiy axborotning konfidensialligi;
- tashkilot hujjatlarini muhofaza qilish;
- intellektual mulkka egalik qilish huquqi.

Axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida hisoblangan axborot xavfsizligini boshqarish bo'yicha tadbirlar quyidagilarni o'z ichiga oladi:

- axborot xavfsizligi siyosatini hujjatlashtirish;
- axborot xavfsizligini ta'minlash bo'yicha majburiyatlarni taqsimlash;
- axborot xavfsizligi qoidalariga o'qitish;
- ilovalardagi axborotga to'g'ri ishlov berish;
- texnik zaifliklarni boshqarish strategiyasi;
- tashkilotning uzluksiz ishini boshqarish;
- axborot xavfsizligi mojarolarini va takomillashtirishlarini boshqarish.

Sanab o'tilgan tadbirlarni ko'pgina tashkilotlar va axborot muhiti uchun qo'llasa bo'ladi. Ushbu standartda keltirilgan barcha tadbirlar muhim hisoblansa ham, qandaydir choraning o'rinli bo'lishi tashkilot to'qnash keladigan muayyan xavflar nuqtayi nazaridan belgilanishi kerak. Demak, yuqorida ta'riflangan yondashish axborot xavfsizligini ta'minlash bo'yicha tadbirlarni joriy qilish uchun tayanch nuqta bo'lib hisoblanishiga qaramay, u xavflarni baholashga asoslangan axborot xavfsizligini boshqarish bo'yicha tadbirlarni tanlashning o'rnini bosmaydi.

Muvaffaqiyatning eng muhim omillari. Tajriba shuni ko'rsatadiki, tashkilotda axborot xavfsizligini ta'minlash bo'yicha tadbirlarni muvaffaqiyatli joriy qilish uchun quyidagi omillar hal qiluvchi hisoblanadi:

- axborot xavfsizligi maqsadlari, siyosatlari va muolajalarining biznes maqsadlariga muvofiqligi;
- xavfsizlik tizimini joriy qilish, madadlash, monitoringini o'tkazish va modernizatsiya qilishga yondashishning korporativ madaniyat bilan muvofiqligi;
- rahbariyat tomonidan real qo'llab-quvvatlash va manfaatdorlik;
- xavfsizlik talablarini, xavflarni baholash va xavflarni boshqarishni aniq tushunish.

Tashkilotga tegishli qo'llanmalarni ishlab chiqish. Ushbu standart tashkilotning muayyan ehtiyojlariga kerakli qo'llanmalar ishlab chiqish uchun tayanch nuqta sifatida baholanishi kerak. Ushbu standartda keltirilgan yo'riqnomalar va tadbirlarning hammasi ham qo'llashga yaroqli bo'lavermaydi.

Bundan tashqari, ushbu standartga kiritilmagan qo'shimcha choralar kerak bo'lib qolishi mumkin. Bu holda auditorlar va biznes bo'yicha sheriklar tomonidan o'tkaziladigan muvofiqlik tekshiruvini yengillashtiradigan, bir vaqtda bir necha tomondan qilingan havolalarning saqlanishi foydali bo'lishi mumkin.

O'zDStISO/IEC 27005:2013 – "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligi risklarini boshqarish".

Ushbu standart tashkilotda axborot xavfsizligi risklarini boshqarish bo'yicha tavsiyalarni o'z ichiga oladi.

Ushbu standart O'z DSt ISO/IEC 27001 da belgilangan umumiy konsepsiyalarni qo'llab-quvvatlaydi va risklarni boshqarish bilan bog'liq yondashuv asosida axborot xavfsizligini aynan bir xil ta'minlashni amalga oshirish uchun mo'ljallangan.

Ushbu standartni to'la tushunib etish uchun O'z DSt ISO/IEC 27001 va O'z DSt ISO/IEC 27002da bayon qilingan konsepsiyalarni, modellarni, jarayonlarni va terminologiyani bilish zarur.

Ushbu standart tashkilotning axborot xavfsizligini obro'sizlantirishi mumkin bo'lgan risklarni boshqarishni amalga oshirishni

rejalashtiradigan barcha turdagi tashkilotlar (masalan, tijorat korxonalari, davlat muassasalari, notijorat tashkilotlar) uchun qo'llaniladi.

Ushbu standartda quyidagi standartlarga bo'lgan havolalardan foydalanilgan:

O'z DSt ISO/IEC 27001:2009 Axborot texnologiyalari. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar.

O'z DSt ISO/IEC 27002:2008 Axborot texnologiyasi. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

Ushbu standartdan foydalanilganda havola qilingan standartlarning O'zbekiston hududida amal qilishini joriy yilning 1-yanvarigacha bo'lgan holati bo'yicha tuzilgan standartlarning tegishli ko'rsatkichi va joriy yilda e'lon qilingan tegishli axborot ko'rsatkichlari bo'yicha tekshirish maqsadga muvofiqdir. Agar havola qilingan hujjat almashtirilgan (o'zgartirilgan) bo'lsa, u holda ushbu standartdan foydalanilganda almashtirilgan (o'zgartirilgan) standartga amal qilish lozim. Agar havola qilingan hujjat almashtirilmasdan bekor qilingan bo'lsa, u holda unga havola qilingan qoida ushbu havolaga taalluqli bo'lmagan qismida qo'llaniladi.

O'zDStISO/IEC 27006:2013 – "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini boshqarish tizimlarining auditi va ularni sertifikatlashtirish organlariga qo'yiladigan talablar".

O'z DSt ISO/IEC 17021 – bu tashkilotlarni boshqarish tizimlarining auditini va sertifikatlashtirilishini amalga oshiradigan organlar uchun mezonlarni o'rnatadigan standartdir. Agar bu organlar O'z DSt ISO/IEC 27001 ga muvofiq, axborot xavfsizligini boshqarish tizimlari (AXBT)ning sertifikatlashtirilishini va auditini o'tkazish maqsadida, O'z DSt ISO/IEC 17021 muvofiq keladigan organlar sifatida akkreditlanadigan bo'lsa, u holda O'z DSt ISO/IEC 17021 ga qo'llanma va qo'shimcha talablar zarur. Ular ushbu standartda taqdim etilgan.

Ushbu standartning matni O'z DSt ISO/IEC 17021 strukturasini takrorlaydi, AXBT uchun spetsifik bo'lgan qo'shimcha talablar va AXBTni sertifikatlashtirish uchun O'z DSt ISO/IEC 17021 ni

qo‘llash bo‘yicha qo‘llanma esa, «AX» abbreviaturasi bilan belgilanadi.

«Kerak» atamasidan ushbu standartda O‘z DSt ISO/IEC 17021 va O‘z DSt ISO/IEC 27001 talablarini aks ettirgan holda majburiy bo‘lgan shartlarni ko‘rsatish uchun foydalaniladi. «Zarur» atamasidan, garchi bu talablarni qo‘llash bo‘yicha qo‘llanma bo‘lsa ham, sertifikatlashtirish organi tomonidan qabul qilinishi ko‘zda tutiladigan shartlarni belgilash uchun foydalaniladi.

Ushbu standartning maqsadi - akkreditlash organlariga sertifikatlashtirish organlarini baholashlari shart bo‘lgan standartlarni yanada samarali qo‘llash imkoniyatini berishdir. Bu kontekstda sertifikatlashtirish organining qo‘llanmadan har qanday chetga chiqishi istisno hisoblanadi. Bunday chetga chiqishlarga har bir holat alohida ko‘rib chiqilishi asosidagina ruxsat berilishi mumkin, bunda sertifikatlashtirish organi akkreditlash organiga bu istisno qandaydir ekvivalent tarzda O‘z DSt ISO/IEC 17021, O‘z DSt ISO/IEC 27001 talablarining tegishli bandini va ushbu standart talablarini qanoatlantirishini isbotlab berishi kerak.

Izoh - ushbu standartda «boshqarish tizimi» va «tizim» atamalaridan bir-birini almashtirib foydalaniladi. Boshqarish tizimlari ta’rifini O‘z DSt ISO 9000 da topish mumkin. Bu xalqaro standartda foydalanilayotgan boshqarish tizimini axborot texnologiyalari tizimlari kabi tizimlarning boshqa turlari bilan adashtirmaslik zarur.

ISO/IEC 15408-1-2005 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari va vositalari. Axborot texnologiyalari xavfsizligini baholash mezonlari”.

ISO/IEC 15408-2005 xalqaro standarti ISO/IEC JTC 1 «Axborot texnologiyalari» birgalikdagi texnik qo‘mita, SC 27 «AT xavfsizligini ta’minlash metodlari va vositalari» kichik qo‘mita tomonidan tayyorlangan. ISO/IEC 15408-2005 ga o‘xshash matn «Axborot texnologiyalari xavfsizligini baholashning umumiy mezonlari» 2.3-versiya (2.3 UM deb nomlanadi) sifatida «Umumiy mezonlar» loyihasining homiy tashkilotlari tomonidan e’lon qilingan.

Standartning ikkinchi tahriri texnik jihatdan qayta ishlashga to‘g‘ri kelgan birinchi tahrir (ISO/IEC 15408:1999)ni bekor qiladi va uni almashtiradi.

ISO/IEC 15408-2005 ga o'xshash bo'lgan O'z DSt ISO/IEC 15408 «Axborot texnologiyalari - Xavfsizlikni ta'minlash metodlari va vositalari - Axborot texnologiyalari xavfsizligini baholash mezonlari» umumiy sarlavha ostidagi quyidagi qismlardan tashkil topgan:

1-qism: Kirish va umumiy model;

2-qism: Xavfsizlikka qo'yiladigan funksional talablar;

3-qism: Xavfsizlikka qo'yiladigan ishonch talablari.

O'z DSt ISO/IEC 15408 xavfsizlikni mustaqil baholash natijalarini qiyoslash imkoniyatini beradi. Bunga AT mahsulotlari va tizimlarining xavfsizlik funksiyalariga va xavfsizlikni baholashda ularga qo'llaniladigan ishonch choralariga qo'yiladigan talablar umumiy to'plamining taqdim etilishi bilan erishiladi.

Bunday mahsulotlar yoki tizimlarning xavfsizlik funksiyalari, shuningdek, oldindan qo'llaniladigan ishonch choralari qo'yiladigan talablarga javob berishi bois, baholash jarayonida belgilangan ishonch darajasiga erishiladi. Baholash natijalari iste'molchilarga AT mahsulotlari yoki tizimlari ularning taxmin qilinayotgan qo'llanilishi uchun yetarli darajada xavfsiz ekanligiga va ulardan foydalanishda bashorat qilinayotgan xavf-xatarlarning maqbulligiga ishonch hosil qilishlariga yordam berishi mumkin.

O'z DSt ISO/IEC 15408 AT mahsulotlari va tizimlarining xavfsizlik funksiyalari bilan ishlab chiqilishidagi kabi, shunday funksiyali tijorat mahsulotlari va tizimlarining sotib olinishida ham qo'llanma sifatida foydali. ATning bunday mahsuloti yoki tizimining baholanishi baholash obyekti (BO) deb ataladi. Bunday BOga, masalan, operatsion tizimlar, hisoblash tarmoqlari, taqsimlangan tizimlar va ilovalar kiradi.

O'zDStISO/IEC 15408 axborotni ruxsat etilmagan tarzda ochish, modifikatsiya qilish yoki undan foydalanish imkoniyatini yo'qotishdan muhofaza qilinishiga yo'naltirilgan. Xavfsizlik buzilishining ushbu uchta turiga taalluqli bo'lgan muhofaza toifalari, odatda, mos ravishda, konfidensiallik, butunlik va foydalana olishlik deb ataladi. Shuningdek, O'zDStISO/IEC 15408 AT xavfsizligining ushbu uchta tushuncha doirasidan tashqaridagi jihatlariga qo'llanilishi mumkin. O'z DSt ISO/IEC 15408 insonning g'araz niyatli harakatlari kabi, boshqa harakatlar natijasida yuzaga kela-

digan axborot tahdidlariga qaratilgan, shuningdek, O‘z DSt ISO/IEC 15408 inson omili bilan bog‘liq bo‘lmagan ba’zi bir tahdidlar uchun ham qo‘llanilishi mumkin. Bundan tashqari, O‘z DSt ISO/IEC 15408 ATning boshqa sohalarida qo‘llanilishi mumkin, biroq ularning vakolati qat’iy chegaralangan AT xavfsizligi sohasidan tashqarida deklaratsiya qilinmaydi.

O‘zDStISO/IEC 15408 apparat, dasturiy-apparat va dasturiy vositalar tomonidan amalga oshiriladigan AT xavfsizligi choralariga qo‘llaniladi. Agar ayrim baholash jihatlari faqat amalga oshirishning ba’zi bir usullari uchun qo‘llanilishi taxmin qilinsa, bu tegishli mezonlarni bayon qilishda ko‘rsatib o‘tiladi.

Nazorat savollari:

1. Axborot xavfsizligi sohasida standartlar va me’yoriy hujjatlarning tutgan o‘rni.
2. ISO/IEC 27001:2005 xalqaro standartining mohiyatini tushuntirib bering.
3. ISO/IEC 27002:2005 xalqaro sandartining vazifalarini tavsiflab bering.
4. O‘zDStISO/IEC 27005:2013 xalqaro standartini amalga kiritilishi mohiyati nimada?
5. O‘zDStISO/IEC 27006:2013 xalqaro standarti axborot xavfsizligi sohasidagi qanday muammolarni yechishga yordam beradi?
6. O‘z DSt ISO/IEC 15408:2008 xalqaro standarti nechta qismdan iborat va ularda yoritilgan masalalar nimalardan iborat?

3.2. Axborot xavfsizligi sohasiga oid milliy standartlar

Ushbu bo‘limda keltirilgan standartlar zamon talablari tomonidan kelib chiqqan holda amalga oshirilgan bo‘lib, asos sifatida O‘zbekiston Respublikasining "Elektron raqamli imzo xususida"gi va "Elektron hujjat almashinuvi xususida"gi qonunlarini keltirishimiz mumkin.

Ushbu standartlar EHM tarmoqlarida, telekommunikatsiyada, alohida hisoblash komplekslari va EHMda axborotni ishlash tizim-

lari uchun axborotni shifrlashning umumiy algoritmini va ma'lumotlarni shifrlash qoidasini belgilaydi.

O'z DSt 1092:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari".

Ushbu standart umumiy foydalanishdagi muhofazalanmagan telekommunikatsiya kanallari orqali uzatiladigan, berilgan xabar (elektron hujjat) ostiga qo'yilgan elektron raqamli imzo (ERI)ni shakllantirish va uning haqiqiyligini tasdiqlash uchun elektron raqamli imzo algoritmi (ERIA)ni belgilaydi.

Standart elektron raqamli imzoni shakllantirish va uning haqiqiyligini tasdiqlashda turli maqsadlar uchun kerakli axborotlarni qayta ishlash tizimlarida qo'llash uchun mo'ljallangan.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O'z DSt 1047:2003 Axborot texnologiyalari. Atamalar va ta'riflar.

O'z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta'riflar.

O'z DSt 1105:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi".

Ushbu « Ma'lumotlarni shifrlash algoritmi» (MShA) standarti elektron ma'lumotlarni muhofaza qilish uchun mo'ljallangan kriptografik algoritmni ifodalaydi. MShA - simmetrik blokli shifr bo'lib, axborotni shifrmatnga va dastlabki matnga o'girish uchun foydalaniladi. MShA 256 bit uzunlikdagi ma'lumotlar blokini shifrmatnga o'girish va shifrmatnni dastlabki matnga o'girish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitdan foydalanishi mumkin.

Standart, elektron hisoblash mashinalari (EHM) tarmoqlarida, alohida hisoblash komplekslari va EHMda axborotga ishlov berish tizimlarida axborotni shifrlashning yagona algoritmini o'rnatib, ma'lumotlarni shifrlash qoidalarini belgilaydi.

Ma'lumotlarni shifrlash algoritmi dasturiy, apparat yoki apparat-dasturiy kriptografik modullarda amalga oshirish uchun mo'ljallangan.

Tashkilotlar, korxonalar va muassasalar EHM tarmoqlarida, alohida hisoblash komplekslarida yoki EHMda saqlanuvchi va uzatiluvchi ma'lumotlarning kriptografik muhofazasini amalga oshirishda mazkur standartdan foydalanishlari mumkin.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O'z DSt 1047:2003 Axborot texnologiyalari. Atamalar va ta'riflar.

O'z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta'riflar.

O'z DSt 1106:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi".

Ushbu standart axborotni qayta ishlash va muhofaza qilishning kriptografik metodlarida, shu jumladan, avtomatlashtirilgan tizimlarda axborot uzatish, qayta ishlash va saqlashda elektron raqamli imzo (bundan keyin - ERI) protseduralarini amalga oshirish uchun qo'llaniladigan ikkilik simvollarining istalgan ketma-ketligi uchun xeshlash funksiyasining (bundan keyin - XF) algoritmini va hisoblash protsedurasini belgilaydi.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O'z DSt 1047:2003 Axborot texnologiyalari. Atamalar va ta'riflar.

O'z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta'riflar.

O'z DSt 1204:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik modullarga xavfsizlik talablari".

Ushbu standart ochiq va simmetrik kalitli kriptografik modullarga qo'yiladigan yagona xavfsizlik talablarini belgilaydi hamda axborotning kriptografik muhofaza qilish vositalarini loyihalash, ishlab chiqish, sotish (eltib berish) va undan foydalanish uchun mo'ljallangan. Standart EHM, telekommunikatsiya tarmoqlari, ayrim hisoblash komplekslari yoki EHMda saqlanadigan va uzatiladigan konfidensial axborotni muhofaza qiladigan kriptografik modullarga qo'yiladigan xavfsizlik talablarini belgilaydi.

Ushbu standartda quyidagi standartlarga havolalardan foydalanilgan:

O‘z DSt 1092:2005 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.

O‘z DSt 1105:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.

O‘z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.

Nazorat savollari:

1. O‘zbekiston Respublikasining O‘z DSt 1092:2009, O‘z DSt 1105:2009 va O‘z DSt 1106:2009 milliy standartlarining mohiyatini tushuntirib bering.
2. O‘z DSt 1204:2009 milliy standartida qanday masalalar yoritib berilgan?

3.3. Axborot xavfsizligi sohasiga oid me’yoriy hujjatlar

RH 45-215:2009 - Rahbariy hujjat. Ma’lumotlar uzatish tarmog‘ida axborot xavfsizligini ta’minlash to‘g‘risida Nizom. Ushbu hujjat N 100:2002 «Ma’lumotlar uzatish milliy tarmog‘ida axborot xavfsizligini ta’minlash to‘g‘risida nizom» o‘rniga amalga kiritilgan bo‘lib, ma’lumotlar uzatish tarmog‘ida (MUT) axborot xavfsizligini ta’minlash bo‘yicha asosiy maqsadlar, vazifalar, funksiyalar va tashkiliy-texnik tadbirlarni belgilaydi.

Nizom xonaning muhofaza qilinishini tashkil qilish, tarmoq komponentlarining saqlanganligi va fizik yaxlitligini ta’minlash, tabiiy ofatlar, energiya ta’minoti tizimida ishlamay qolishlardan muhofaza qilish masalalari, xodimlar va MUT mijozlarining shaxsiy xavfsizligini ta’minlash bo‘yicha choralari, shuningdek, Tezkor-qidiruv tadbirlar tizimini (TQTT) tashkil qilish masalalari va uning ishlashini tartibga solmaydi.

Ushbu hujjat talablari MUT normal ishlashini kuzatish, xizmat ko‘rsatish va ta’minlash ishlarini amalga oshiruvchi mutasaddi qo‘mita va vazirliklarning barcha korxonalariga taalluqlidir.

Ushbu Nizomga axborot muhofazasi bo‘yicha xizmatlar ro‘yxati o‘zgarganda yoki MUTni modernizatsiya qilish va rivojlantirishda o‘zgartirish hamda qo‘shimchalar kiritilgan bo‘lishi mumkin.

Ushbu Nizom axborotni muhofaza qilishning huquqiy, tashkiliy, rejimli, texnik, dasturiy va boshqa metodlari hamda vositalaridan foydalanish, shuningdek, axborot xavfsizligini ta’minlash qismida amalga oshirilgan choralarning samaradorligi uchun har tomonlama uzluksiz nazorat qilishni amalga oshirish asosida MUTda axborot xavfsizligini ta’minlash ko‘zda tutiladi.

MUTda axborot xavfsizligini ta’minlash AXTTni yaratish yo‘li bilan kompleksli va MUT hayotiy siklining barcha bosqichlarida tashkiliy-texnik tadbirlarni doimo o‘tkazish bilan hal etiladi.

MUT AXTT samarali ishlashini ta’minlash funksiyalari korxona rahbariga bevosita bo‘ysunadigan korxonaning MUT axborot xavfsizligini ta’minlash xizmati (bo‘limi)ga yuklatiladi.

Korxonaning MUT axborot xavfsizligini ta’minlash xizmati (bo‘limi) o‘z faoliyatida O‘zbekiston Respublikasining qonun hujjatlari va normativ hujjatlari, Prezident farmonlari, O‘zbekiston Respublikasi Vazirlar Mahkamasining qarorlari, Agentlikning normativ-huquqiy hujjatlari, korxona rahbarlarining buyruqlari va farmoyishlari hamda ushbu Nizomga amal qiladi.

Axborot xavfsizligini ta’minlash xizmati (bo‘limi) MUT serverlarida saqlanadigan va MUT telekommunikatsiya kanallari va vositalari bo‘ylab uzatiladigan, agar bu shartnomada ko‘zda tutilgan bo‘lsa, abonentlar axborotining konfidensialligi, yaxlitligi va undan erkin foydalanish uchun javobgar bo‘ladi.

Axborot xavfsizligini ta’minlash xizmati (bo‘limi) abonent terminallarida saqlanadigan abonent axborotining konfidensialligi, yaxlitligi va undan erkin foydalanish uchun javobgar bo‘lmaydi.

Axborot xavfsizligini ta’minlash xizmati (bo‘limi) viruslar bilan zararlangan hamda zararli dasturlarni o‘z ichiga olgan foydalanuvchi va abonentlarning axborot resurslari (MUT serverlarida joylashadigan va saqlanadigan, MUT telekommunikatsiya kanallari va vositalari bo‘ylab uzatiladigan), shuningdek, O‘zbekiston Respublikasining amaldagi qonun hujjatlari bilan taqiqlangan axborot

resurslari tarqalishining oldini olish bo'yicha choralarni qabul qilish huquqiga ega.

Abonentlarga axborotni muhofaza qilish bo'yicha qo'shimcha xizmatlarni taqdim etish shartnomada bayon etiladi.

MUT foydalnuvchilari va abonentlari o'z darajasida axborotni muhofaza qilish tizimlari yoki vositalarini qo'llash (ulardan foydalanish) huquqiga ega.

RH 45-185:2011 - Rahbariy hujjat. Davlat hokimiyati va boshqaruv organlarining axborqt xavfsizligini ta'minlash dasturini ishlab chiqish tartibi. Ushbu hujjat RH 45-185:2006 hujjati o'rniga amalga kiritilgan bo'lib, davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta'minlash dasturlarini ishlab chiqish tartibini belgilaydi.

Hujjat axborot xavfsizligini ta'minlash dasturlari doirasida ishlab chiqiladigan chora-tadbirlarning maqsadlari, vazifalari, tuzilmasi va ro'yxatiga qo'yiladigan namunaviy talablarni belgilaydi.

Ushbu hujjat talablari O'zbekiston Respublikasining davlat hokimiyati va boshqaruv organlariga taalluqli, shuningdek, ushbu organlarning axborot xavfsizligini ta'minlash dasturlarini yaratish uchun asos bo'lib hisoblanadi.

Ushbu hujjatni ishlab chiqish va joriy etishdan maqsad:

- axborot xavfsizligini tahdidlardan muhofaza qilish bo'yicha choralarning adekvatligiga erishish;
- davlat hokimiyati va boshqaruv organlarining ishlaridagi barqarorlik darajasini oshirish;
- xavfsizlik mojarolaridan yuzaga kelgan ziyon darajasini pasaytirish;
- axborot xavfsizligi infratuzilmasini yaratish;
- boshqa tashkilotlarning foydalanish xavfsizligini ta'minlash;
- boshqa tashkilotlarning ulanishi bilan bog'liq bo'lgan ehtimoliy xavflarni identifikatsiya qilish;
- axborot resurslariga mas'ul shaxslarni belgilash;
- davlat hokimiyati va organlari faoliyatida davlat axborot resurslarining ochiqligi va ommabopligini ta'minlash, axborot va kommunikatsiya texnologiyalaridan foydalanish asosida davlat hokimiyati va organlari bilan fuqarolar o'rtasidagi samarali o'zaro

hamkorlik uchun, ularning axborot xavfsizligini ta'minlagan holda, sharoitlar yaratish;

- muhofaza qilingan axborot va kommunikatsiya texnologiyalaridan foydalanish asosida davlat organlari faoliyatini takomillashtirish;

- davlat organlarida AX bo'yicha mutaxassislarni tayyorlash tizimini rivojlantirishdir.

Ushbu rahbariy hujjatning asosiy maqsadi - davlat hokimiyati va boshqaruv organlarini AX tahdidlaridan, ularga mumkin bo'lgan zarar yetkazilishidan muhofaza qilinishini ta'minlashdir.

Rahbariy hujjatning asosiy vazifasi davlat organlarining axborot xavfsizligini ta'minlash dasturini belgilash hisoblanadi.

RH 45-193:2007 - Rahbariy hujjat. Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta'minlash darajasini aniqlash tartibi. Ushbu hujjat davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta'minlash darajasini aniqlashning namunaviy tartibini belgilaydi.

Ushbu hujjat talablari davlat organlarining saytlari uchun xosting xizmatlarini taqdim etuvchi barcha xo'jalik yurituvchi subyektlar tomonidan qo'llanilishi majburiydir.

Hujjatda davlat organlarining saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini (AX) ta'minlash darajasini belgilash, axborot resurslarini yaratish va foydalanishning barcha aspektlarini hisobga olgan holda ushbu vazifaga kompleks yondoshilishiga asoslanadi. Buning uchun tashkiliy, texnik va dasturiy muhofaza qilish choralarini, xavf-xatarlar va axborotning muhofazalanganlik darajasini baholash va prognoz qilish bo'yicha tadbirlarni doimo rivojlanib borayotgan yagona tizimga umumlashtirish talab etiladi.

Axborotni muhofaza qilish o'z ichiga AXni ta'minlashga qaratilgan chora-tadbirlar kompleksini oladi: ma'lumotlarni kiritish, saqlash, qayta ishlash va uzatish uchun foydalaniladigan axborot va resurslarning butunligi, ulardan foydalana olishlik, zarur holda, konfidensialligini qo'llab-quvvatlash.

Axborotni muhofaza qilish maqsadi quyidagilar hisoblanadi:

- axborotning chiqib ketishi, o‘g‘irlanishi, yo‘qolishi, buzilishi, qalbakilashtirilishini oldini olish;

- axborotni yo‘q qilish, modifikatsiya qilish, buzish, nusxa ko‘chirish, blokirovka qilish bo‘yicha ruxsat etilmagan harakatlarning oldini olish;

- axborot resurslari va axborot tizimlariga (AT) noqonuniy aralashishning boshqa shakllarini oldini olish.

TSt 45-010:2010 – Tarmoq standarti. Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar. Ushbu tarmoq standarti O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi davlat standartlashtirish, metrologiya va sertifikatlashtirish markazi («O‘zdavstandart») tomonidan 2002-yil 6-avgustda 112/066-son bilan ro‘yxatga olingan TSt 45.010: «Отраслевой стандарт. Информационная безопасность в сфере связи и информатизации. Термины и определения» o‘rniga amalga kiritilgan bo‘lib, aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflarni belgilaydi.

Belgilangan atamalar barcha turdagi hujjatlarda qo‘llanilishi uchun majburiydir. Standartda ma’lumotnoma sifatida standartlashtirilgan atamalarning xorijiy ekvivalenti rus (R) va ingliz (E) tillarida keltirilgan.

Standartdan foydalanish qulayligi uchun atama moddalarining tegishli raqamlarini ko‘rsatgan holda o‘zbek, rus va ingliz tillaridagi atamalarni o‘z ichiga olgan alifbo ko‘rsatkichi keltirilgan.

Nazorat savollari:

1. RH 45-215:2009 – Rahbariy hujjat o‘z ichiga olgan masalalar nimalardan iborat?
2. RH 45-185:2011 – Rahbariy hujjat o‘z ichiga olgan masalalar nimalardan iborat?
3. RH 45-193:2011 – Rahbariy hujjat o‘z ichiga olgan masalalar nimalardan iborat?
4. TSt 45-010:2010 – Tarmoq standarti o‘z ichiga olgan masalalar nimalardan iborat?

IV BOB. XAVFSIZLIK MODELLARI

4.1. Xarrison-Ruzzo-Ulmanning diskretsion modeli

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

Himoyalangan axborot tizimlarini ishlab chiqaruvchilar xavfsizlik modelidan quyidagi hollarda foydalanishadi:

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

Iste'molchilar xavfsizlikning formal modellarini tuzish yo'li bilan ishlab chiqaruvchilarga o'zlarining talablarini aniq va ziddiyatli bo'lmagan shaklda yetkazish hamda himoyalangan tizimlarning o'zlarining ehtiyojlariga mosligini baholash imkoniyatiga ega bo'ladilar.

Kvalifikatsiya (malaka) bo'yicha ekspertlar himoyalangan tizimlarda xavfsizlik siyosatining amalga oshirilish adekvatligini tahlillash mobaynida xavfsizlik modelidan etalon sifatida foydalanadilar.

Xavfsizlik modeli quyidagi bazaviy tasavvurlarga asoslangan.

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

mumkin. Tizimni bunday tasavvur etishda axborotni ishlash xavfsizligi, xavfsizlik siyosatini shakllantiruvchi qoidalar va cheklashlar to'plamiga mos holda subyektlarning obyektlardan foydalanishni boshqarish masalasini yechish orqali ta'minlanadi. Agar subyektlar xavfsizlik siyosati qoidalarini buzish imkoniyatiga ega bo'lmasa, tizim xavfsiz hisoblanadi. Ta'kidlash lozimki, "obyekt" va "subyekt" tushunchalarining tavsifi turli modellarda jiddiy farqlanishi mumkin.

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

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

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

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

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

Xarrison-Ruzzo-Ulmanning diskretsion modeli klassik (mumtoz) diskretsion model hisoblanib, subyektlarning obyektlardan foydalanishni ixtiyoriy boshqarishni va foydalanish huquqlarining tarqalishi nazoratini amalga oshiradi.

Ushbu model doirasida axborotni ishlash sistemasi axborotdan foydalanuvchi subyektlar (S to'plam), himoyalanuvchi axborotga ega bo'lgan obyektlar (O to'plam) va mos harakatlarni (masalan o'qish (R), yozish (W), dasturni bajarish (E)) vakolatini anglatuvchi foydalanish huquqlarining chekli to'plami $R = \{r_1, r_2, ..., r_n\}$ majmui ko'rinishida ifodalanadi.

Shu bilan birga model ta'siri doirasiga subyektlar orasidagi munosabatlarni kiritish uchun barcha subyektlar bir vaqtning o'zida obyektlar hisoblanadi - $S \subset O$. Tizim ahvoli holat tushunchasi yordamida modellashtiriladi. Tizim holati makoni uni tashkil etuvchi obyektlar, subyektlar va huquqlar to'plamlarining dekart ko'paytmasi sifatida shakllantiriladi - $O \times S \times R$. Bu makonda tizimning joriy holati uchlik orqali aniqlanadi. Bu uchlikka subyektlar to'plami, obyektlar to'plami va subyektlarning obyektlardan foydalanish huquqlarini tavsiflovchi foydalanish matritsasi kiradi - $Q = (S, O, M)$. Matritsa qatorlari subyektlarga, ustunlari esa obyektlarga mos keladi. Obyektlar to'plami o'z ichiga subyektlar to'plamini olganligi sababli matritsa to'g'ri to'rtburchak ko'rinishida bo'ladi. Matritsaning ixtiyoriy yacheykasi $M[S, O]$ subyekt "S"ning obyekt "O"dan, foydalanish huquqlari to'plami R ga tegishli foydalanish huquqlari naboriga (to'plamiga) ega. Tizimning vaqt bo'yicha ahvoli turli holatlar orasidagi o'tishlar yordamida modellashtiriladi. O'tish matritsa M ga quyidagi ko'rinishlardagi komandalar yordamida o'zgartirish kiritish yo'li bilan amalga oshiriladi:

$$command^{\alpha}(x_1, \ldots, x_k)$$
$$\text{if } r_1 \text{ in } {}^{M}[x_{s_1}, \ldots, x_{o_1}] \text{ and}$$
$$r_2 \text{ in } {}^{M}[x_{s_2}, \ldots, x_{o_2}] \text{ and}$$
$$\ldots$$
$$r_m \text{ in } {}^{M}[x_{s_m}, \ldots, x_{o_m}] \text{ and}$$
$$\text{then}$$
$$op_1, op_2, \ldots, op_n$$

Bu yerda α – komanda nomi; x_i – komanda parametrlari bo'lib, subyektlar va obyektlarning identifikatorlari hisoblanadi; s_i va o_i – "1"dan "k"gacha diapazonda subyektlar va obyektlarning indekslari; op_i – elementar amallar. Komanda tarkibidagi elementar amallar M matritsa yacheykalarida ko'rsatilgan foydalanish huquqlarining mavjudligini anglatuvchi barcha shartlar haqiqiy bo'lganidagina bajariladi.

Klassik (mumtoz) modelda faqat quyidagi elementar amallar joiz hisoblanadi:

enter "r" into $M[s, o]$ ("s" subyektga "o" obyekt uchun "r" huquqni qo'shish (kiritish))

delete "r" from $M[s,o]$ ("s" subyektdan "o" obyekt uchun "r" xuquqni yo'q qilish)

create subject "s" (yangi "s" subyektni yaratish)

create subject "o" (yangi "o" obyektni yaratish)

destroy subject "s" (mavjud "s" subyektni yo'q qilish)

destroy subject "o" (mavjud "o" obyektni yo'q qilish)

$Q = (S, O, M)$ holatda bo'lgan tizimda ixtiyoriy elementar amal "op"ning ishlatilishi tizimning boshqa $Q'(S', O', M')$ holatga o'tishiga sabab bo'ladiki, bu holat oldingi holatdan bo'lmaganida bitta komponenti bilan farqlanadi. Bazaviy amallarning ishlatilishi tizim holatida quyidagi o'zgarishlarga olib keladi:

enter "r" into $M[s,o]$ (bu erda $s \in S, o \in O$)

$$O' = O$$

$$S' = S$$

$$M'[x_s, x_o] = M[x_s, x_o] \text{ agar } [(x]_s, x_o) \neq (s,o) \text{ bo'lsa,}$$

$$M'[s,o] = M[s,o] \cup \{r\}.$$

"enter" amali foydalanish matritsasining mavjud yacheykasiga "r" huquqini kiritadi. Har bir yacheykaning tarkibi foydalanish huquqi to'plami sifatida ko'riladi, ya'ni agar kiritilayotgan huquq bu to'plamda bo'lsa, yacheyka o'zgarmaydi. "enter" amali foydalanish matritsasiga faqat huquq qo'shadi va hech narsani yo'q qilmaydi. Shu sababli bu amalni "monoton" amal deb atashadi.

delete "r" from (bu yerda $s \in S, o \in O$)

$$O' = O$$

$$S' = S$$

$$M'[x_s, x_o] = M[x_s, x_o] \text{ agar } [(x]_s, x_o) \neq (s,o),$$

$$M'[s,o] = M[s,o] \setminus \{r\}.$$

"delete" amalining ta'siri "enter" amalining ta'siriga teskari. Bu amal foydalanish matritsasining yacheykasidagi huquqni yo'q qiladi, agar bu huquq ushbu yacheykada bo'lsa, har bir yacheykaning tarkibi foydalanish huquqi to'plami sifatida ko'rilganligi sababli, yo'q qilinadigan huquq ushbu yacheykada bo'lmasa, "delete" amali hech narsa qilmaydi. "delete" amali foydalanish matritsasidan axborotni yo'q qilishi sababli, bu amal "monoton bo'lmagan" amal deb ataladi.

create subject "s\" "(bu erda $s \notin S$)

$O' = O \cup \{s\}$

$S' = S \cup \{s\}$

$M'[x_g, x_o] = M[x_g, x_o]$ *barcha* $[(x]_g, x_o) \in S \times O$ *uchun*

$M'[s, x_o] = \emptyset$ *barcha* $x_o \in O'$ *uchun*

$M'[s, x_g] = \emptyset$ *barcha* $x_g \in S'$ *uchun*

destroy subject s (bu erda $(s \in S)$)

$O'' = O\{s\}$

$S'' = S\{s\}$

$M[x_g, x_o]' = M[(x]_g, x_o)$ *barcha* $[(x]_g, x_o) \in S' \times O'$

create object "o" (bu erda $o \notin O$)

$O' = O \cup \{o\}$

$S' = S$

$M'[x_g, x_o] = M[x_g, x_o]$ *barcha* $[(x]_g, x_o) \in S \times O$

$M'[x_g, o] = \emptyset$ *barcha* $x_g \in S'$ *uchun*

destory object o (bu yerda $(o \in O \backslash S)$)

$O'' = O\{o\}$

$S' = S$

$M'[x_g, x_o] = M[[x]_g, x_o]$ *barcha* $[(x]_g, x_o) \in S' \times O'$

create subject va *destory subject* amallari monoton va monoton bo‘lmagan amallarning o‘xshash juftlarini ifodalaydi.

Ta’kidlash lozimki, har bir amal uchun uni bajarishga yana oldindan qo‘yiladigan shart mavjud: *enter* yoki *delete* amallari yordamida foydalanish matritsasining yacheykasini o‘zgartirish uchun ushbu yacheyka mavjud bo‘lishi, ya’ni mos subyekt va obyektning mavjud bo‘lishi shart. Shunga o‘xshash $create\frac{subject}{object}$ yaratish amallari uchun yaratiluvchi subyekt/obyektning mavjud bo‘lmasligi, $destory\frac{subject}{object}$ yo‘q qilish amali uchun yo‘qotiluvchi subyekt/obyektning mavjudligi shart. Ixtiyoriy amalga oldindan qo‘yiladigan shart bajarilmasa, u amalning bajarilishi natija bermaydi.

Rasman $\sum(Q, R, C)$ tizim tavsifi quyidagi elementlardan tashkil topgan:

- foydalanish huquqlarining chekli to‘plami $R = \{r_1, \ldots, r_n\}$;

- dastlabki subyektlar $S_0 = \{s_1, \ldots, s_n\}$ va obyektlar $O_0 = \{o_1, \ldots, o_m\}$-ning chekli to'plamlari, bu yerda $S_0 \subseteq O_0$;

- tarkibida subyektlarning obyektlardan foydalanish huquqlari bo'lgan dastlabki foydalanish matritsasi - M_0;

- har biri yuqorida sanab o'tilgan elementar amallar terminallarida bajarish va sharxlash shartlaridan tashkil topgan – buyruqlarning chekli to'plami - $C = \{\alpha_i(x_1, \ldots, x_k)\}$.

Tizimning vaqt bo'yicha ahvoli holatlar (Q_i) ketma-ketligi yordamida modellashtiriladi. Har bir keyingi holat C to'plamdagi qandaydir komandaning oldingi holatga qo'llash natijasi hisoblanadi - $Q_{n+1} = C_n(Q_n)$. Shunday qilib, tizimning u yoki bu holatga tushishi yoki tushmasligi C dagi komandalar va ular tarkibidagi amallarga bog'liq. Har bir holat subyektlar, obyektlar to'plamlari va huquqlar matritsasi orasidagi mavjud foydalanish munosabatlarini belgilaydi. Xavfsizlikni ta'minlash uchun ba'zi foydalanish munosabatlarini taqiqlab qo'yish lozimligi sababli, tizimning berilgan dastlabki holati uchun u tushishi mumkin bo'lmagan holatlar to'plamini aniqlash imkoniyati mavjud bo'lishi shart. Bu shunday dastlabki shartlarni (C komandalar O_0 obyektlar to'plamining, S_0 subyektlar to'plamining M_0 foydalanish matritsaning shartini) berishga imkon beradiki, bu shartlarda tizim xavfsizlik nuqtayi nazaridan nomaqbul holatga tusha olmaydi. Demak, ahvoli oldindan bashorat qilinuvchi tizimni qurish uchun quyidagi savolga javob berish lozim: qandaydir subyekt s qachondir qandaydir obyekt $o$dan foydalanish huquqiga ega bo'lishi mumkinmi?

Shu sababli Xarrison-Ruzzo-Ulman modelining xavfsizlik mezoni quyidagicha ta'riflanadi:

Berilgan tizim uchun dastlabki holat $Q_0 = (S_0, O_0, M_0)$ r huquqqa nisbatan xavfsiz hisoblanadi, agar qo'llanilishi natijasida r huquq M matritsa yacheykasiga kiritiladigan Q_0 komandalar ketma-ketligi mavjud bo'lmasa (Q_0 holatda M matritsada ushbu xuquq bo'lmagan).

Ushbu mezonning mohiyati quyidagicha: agar subyekt oldindan obyektdan foydalanish xuquqi $r$ga ega bo'lmasa, tizimning xavfsiz konfiguratsiyasi uchun u hech qachon obyektdan foydalanish huquqi r ga ega bo'lmaydi. Birinchi qarashda bunday ta'rif juda g'ayrioddiy tuyuladi, chunki r huquqiga ega bo'la olmaslik, tarkibi-

da enter "*r*" into $M[s,o]$ amali bo'lgan komandalardan foydalanishdan voz kechishga olib keladigandek, aslida esa bunday emas. Masala shundaki, subyekt yoki obyektning yo'q qilinishi matritsaning mos qator yoki ustunidagi barcha huquqlarning yo'q qilinishiga olib keladi, ammo qator yoki ustunning o'zini yo'q qilinishiga va matritsa o'lchamlarining qisqarishiga olib kelmaydi. Demak, dastlabki holatda qandaydir yacheykada "*r*" huquq mavjud bo'lgan bo'lsa, bu huquqqa taalluqli bo'lgan subyekt yoki obyekt yo'q qilinganidan so'ng yacheyka tozalanadi, ammo subyekt yoki obyekt yaratilishi natijasida mos *enter* komandasi yordamida ushbu yacheykaga yana "*r*" huquq kiritiladi. Bu xavfsizlikning buzilishini anglatmaydi.

Xavfsizlik mezonidan kelib chiqadiki, ushbu model uchun foydalanish huquqlar qiymatini tanlash va ulardan komandalar shartida foydalanish muhim ahamiyatga ega. Model huquqlar ma'nosiga hech qanday cheklashlar qo'ymay va ularni teng qiymatli hisoblasa-da, komandalar bajarilishi shartida qatnashuvchi huquqlar aslida obyektlardan foydalanish huquqlari (masalan, o'qish va yozish) emas, balki foydalanishni boshqarish huquqlari, yoki foydalanish matritsasi yacheykalarini modifikatsiyalash huquqlari hisoblanadi. Shunday qilib, ushbu model mohiyatan nafaqat subyektlarning obyektlardan foydalanishni, balki subyektdan obyektga foydalanish huquqlarini tarqalishini tavsiflaydi. Chunki, aynan foydalanish matritsasi yacheykalari mazmunining o'zgarishi, komandalar, jumladan, xavfsizlik mezonining buzilishiga olib keluvchi, foydalanish matritsasining o'zini modifikatsiyalovchi komandalar bajarilishi imkonini belgilaydi.

Ta'kidlash lozimki, muhofazalangan tizimni qurish amaliyoti nuqtayi nazaridan Xarrison-Ruzzo-Ulman modeli amalga oshirishda eng oddiy va boshqarishda samarali hisoblanadi, chunki hech qanday murakkab algoritmlarni talab qilmaydi, shuningdek, foydalanuvchilar vakolatlarini obyektlar ustida amal bajarilishigacha aniqlikda boshqarishga imkon beradi. Shu sababli, ushbu model zamonaviy tizimlar orasida keng tarqalgan. Undan tashqari ushbu modelda taklif etilgan xavfsizlik mezoni amaliy jihatdan juda kuchli hisoblanadi, chunki oldindan tegishli vakolatlar berilmagan foydalanuvchilarning ba'zi axborotdan foydalana olmasliklarini kafolatlaydi.

Barcha diskretsion modellar "troyan oti" yordamidagi hujumga nisbatan zaif, chunki ularda faqat subyektlarning obyektlardan foydalanish amallari nazoratlanadi (ular orasidagi axborot oqimi emas). Shu sababli, buzg'unchi qandaydir foydalanuvchiga unga bildirmay "troyan" dasturini qistirsa, bu dastur ushbu foydalanuvchi foydalana oladigan obyektdan buzg'unchi foydalana oladigan obyektga axborotni o'tkazadi. Natijada xavfsizlikning diskretsion siyosatining hech qanday qoidasi buzilmaydi, ammo axborotning sirqib chiqishi sodir bo'ladi.

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

Nazorat savollari:

1. Xavfsizlik modellari va ulardan foydalanish holatlarini tavsiflab bering.
2. Xarrison-Ruzzo-Ulmanning diskretsion modelida bajariladigan amallarni tushuntirib bering.
3. Xarrison-Ruzzo-Ulmanning diskretsion modelida xavfsizlik mezonini ta'riflab bering.
4. Xarrison-Ruzzo-Ulmanning diskretsion modelining afzalliklari va kamchiliklarini tushuntirib bering.

4.2. Bella-LaPadulaning mandatli modeli

Foydalanishni boshqarishning mandatli modeli ko'pgina mamlakatlarning davlat va hukumat muassasalarida qabul qilingan maxfiy hujjat almashish qoidalariga asoslangan. Bella-LaPadula siyosatining asosiy mazmuni amaliy hayotdan olingan bo'lib, himoyalanuvchi axborotni ishlashda qatnashuvchilarga va bu axborot mavjud bo'lgan hujjatlarga xavfsizlik sathi nomini olgan maxsus belgi, masalan, "maxfiy", "mutlaqo maxfiy" va h. kabilarni tayinlashdan iborat. Xavfsizlikning barcha sathlari o'rnatilgan ustunlik

munosabati asosida tartiblanadi, masalan, "mutlaqo maxfiy" sathi "maxfiy" sathidan yuqori yoki undan ustun turadi. Foydalanishni nazoratlash o'zaro harakatdagi tomonlarning xavfsizlik sathlariga bog'liq holda quyidagi ikkita oddiy qoida asosida amalga oshiriladi:

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

2. Vakolatli shaxs (subyekt) xavfsizlik sathi o'zining xavfsizlik sathidan past bo'lmagan hujjatlarga axborot kiritishga haqli.

Birinchi qoida yuqori sath shaxslari tomonidan ishlanadigan axborotdan past sath shaxslari tomonidan foydalanishdan himoyalashni ta'minlaydi. Ikkinchi qoida (juda muhim qoida) axborotni ishlash jarayonida yuqori sath ishtirokchilariga axborotning sirqib chiqishini (bilib yoki bilmasdan) bartaraf etadi.

Shunday qilib, diskretsion modellarda foydalanishni boshqarish foydalanuvchilarga ma'lum obyektlar ustida ma'lum amallarni bajarish vakolatini berish yo'li bilan amalga oshirilsa, mandatli modellar foydalanishni xufiya holda – tizimning barcha subyekt va obyektlariga xavfsizlik sathlarini belgilash yordamida boshqaradi. Ushbu xavfsizlik sathlari subyektlar va obyektlar orasidagi joiz o'zaro harakatlarni aniqlaydi. Demak, foydalanishni mandatli boshqarish bir xil xavfsizlik sathi berilgan subyektlar va obyektlarni farqlamaydi va ularning o'zaro harakatiga cheklashlar mavjud emas. Shu sababli, foydalanishni boshqarish moslanuvchanlikni talab qilganida, mandatli model qandaydir diskretsion model bilan birgalikda qo'llaniladi. Bunda diskretsion model bir sathdagi subyekt va obyektlar orasidagi o'zaro harakatni nazoratlashda va mandatli modelni kuchaytiruvchi qo'shimcha cheklashlarni o'rnatishda ishlatiladi.

Xavfsizlikning Bella-LaPadula modelida tizim Xarrison-Ruzzo-Ulman modeliga o'xshash subyektlar S, obyektlar O va foydalanish huquqlari to'plami ko'rinishida ifodalanadi. Obyektlar to'plami subyektlar to'plamini o'z ichiga oladi $S \subset O$ va foydalanishning faqat ikkita xili *read (o'qish), write (yozish)* ko'riladi. Ammo ushbu model qo'shimcha huquqlarni (masalan, axborotni qo'shish, dasturni bajarish va h.) kiritish bilan kengaytirilishi mumkin bo'lsa-da, ular bazaviy (o'qish va yozish) huquqlar orqali akslantiriladi. Foydala-

nishni moslanuvchan boshqarishni ta'minlashga imkon bermaydigan bunday qat'iy yondashishning ishlatilishi mandatli modelda subyektning obyekt ustida bajariladigan amal nazoratlanmasligi, balki axborot oqimi nazoratlanishi bilan izohlanadi. Axborot oqimi faqat ikki xil bo'lishi mumkin: subyektdan obyektga (yozish) va obyektdan subyektga (o'qish).

Nazorat savollari:

1. Bella-LaPadulaning mandatli modelini tushuntirib bering.
2. Xarrison-Ruzzo-Ulmanning diskretsion modeli va Bella-LaPadulaning mandatli modellarining o'zaro farqi.
3. Mandatli model asosida foydalanishni nazoratlashda qo'llaniladigan asosiy qoidalarni tushuntirib bering.

4.3. Xavfsizlikning rolli modeli

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

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

Rol siyosati keng tarqalgan, chunki bu siyosat boshqa qat'iy va rasmiy siyosatlardan farqli o'laroq real hayotga juda yaqin. Haqiqatan, tizimda ishlovchi foydalanuvchilar shaxsiy ismidan harakat qilmay, ma'lum xizmat vazifalarini amalga oshiradi, ya'ni o'zlarining shaxsi bilan bog'liq bo'lmagan qandaydir rollarni bajaradi.

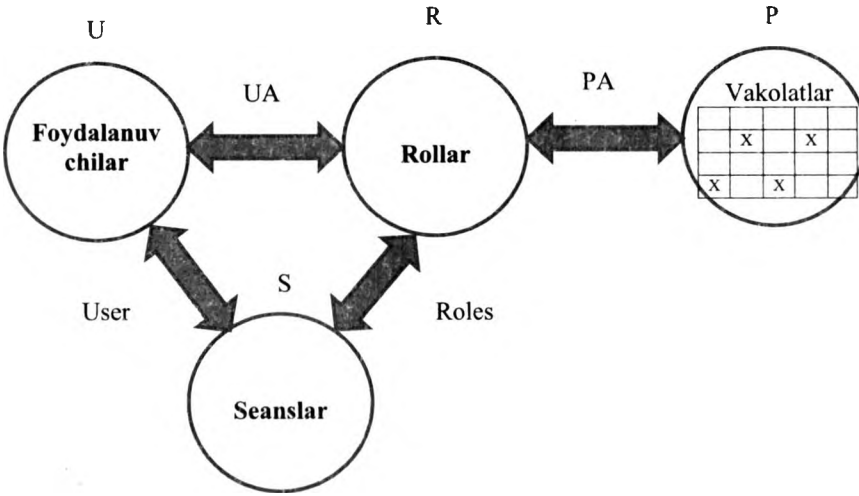
Shu sababli foydalanishni boshqarish va vakolatlarni berish real foydalanuvchilarga emas, balki axborot ishlashning ma'lum jarayonlari qatnashchilarini ifodalovchi abstrakt rollarga berish mantiqqa to'g'ri keladi. Xavfsizlik siyosatiga bunday yondashish

tatbiqiy axborot jarayon qatnashchilari orasida vazifa va vakolatlarining bo'linishini hisobga olishga imkon beradi, chunki rolli siyosat nuqtayi nazaridan axborotdan foydalanishni amalga oshiruvchi foydalanuvchining shaxsi emas, balki unga xizmat vazifasini o'tashga qanday vakolatlar zarurligi ahamiyatlidir. Masalan, axborotni ishlovchi real tizimda tizim ma'muri, ma'lumotlar bazasi menedjeri va oddiy foydalanuvchilar ishlashi mumkin.

Bunday vaziyatda rolli siyosat vakolatlarni ularning xizmat vazifalarga mos holda taqsimlashga imkon beradi: ma'mur roliga unga tizim ishini nazoratlashga va tizim konfiguratsiyasini boshqarishga imkon beruvchi maxsus vakolatlar beriladi, ma'lumotlar bazasining menedjeri ma'lumotlar bazasi serverini boshqarishni amalga oshirishga imkon beradi, oddiy foydalanuvchilarning huquqi esa tatbiqiy dasturlarni ishga tushirish imkonini beruvchi minimum orqali chegaralanadi. Undan tashqari, tizimda rollar soni real foydalanuvchilar soniga mos kelmasligi mumkin – bitta foydalanuvchi, agar unga turli vakolatlarni talab qiluvchi turli vazifalar yuklangan bo'lsa, bir nechta rolni (ketma-ket yoki parallel) bajarishi mumkin, bir nechta foydalanuvchilar bir xil ishni bajarsa, ular bir xil roldan foydalanishlari mumkin.

Rolli siyosat ishlatilganida foydalanishni boshqarish ikki bosqichda amalga oshiriladi: birinchi bosqichda har bir rol uchun obyektdan foydalanish huquqlari to'plamidan iborat vakolatlar to'plami ko'rsatiladi, ikkinchi bosqichda har bir foydalanuvchiga uning qo'lidan keladigan rollar ro'yxati tayinlanadi. Rollarga vakolatlar eng kichik imtiyoz prinsipida tayinlanadi, ya'ni har bir foydalanuvchi o'zining ishini bajarish uchun faqat minimal zarur vakolatlar to'plamiga ega bo'lishi shart.

Rolli model tizimni quyidagi to'plamlar ko'rinishida tavsiflaydi (4.1-rasmga qaralsin):



4.1-rasm. Foydalanishni boshqarishning rolli modeli.

U – foydalanuvchilar to‘plami;

R – rollar to‘plami;

P – obyektdan foydalanish vakolatlari to‘plami (masalan, foydalanish huquqlari matritsasi ko‘rinishida);

S – foydalanuvchilarni tizim bilan ishlash seanslari to‘plami.

Yuqorida sanab o‘tilgan to‘plamlar uchun quyidagi munosabatlar belgilanadi:

$PA \subseteq P \times R$ - har bir rolga unga berilgan vakolatlarni tayinlab, vakolatlar to‘plamini rollar to‘plamiga akslantiriladi;

$UA \subseteq U \times R$ - har bir foydalanuvchi uchun uning qo‘lidan keladigan rollar naborini aniqlab, foydalanuvchilar to‘plamini rollar to‘plamiga akslantiradi.

Xavfsizlikning rolli siyosatida foydalanishni boshqarish qoidalari quyidagi funksiyalar orqali aniqlanadi:

$user: S \to U$ - har bir seans S uchun ushbu funksiya foydalanuvchini aniqlaydi, bu foydalanuvchi tizim bilan ushbu seansni amalga oshiradi: $user(s) = u$;

$roles: S \to P(R)$ – har bir seans S uchun ushbu funksiya R to‘plamdan rollar to‘plamini aniqlaydi, bu rollardan foydalanuvchi bir vaqtda foydalanishi mumkin: $roles(s) = \{r_i \mid (user(s_i), r_i) \in UA\}$.

$permissions: S \to P$ – har bir seans S uchun ushbu funksiya ushbu seansga joiz vakolatlar to'plamini beradi, bu to'plam ushbu seansda joriy etilgan barcha rollar vakolatlarining majmui sifatida aniqlanadi: $permissions(S) \to U_{r \in roles(S)}\{p_i | (p_i, r) \in PA\}$.

Rolli modelning xavfsizlik mezoni sifatida quyidagi qoida ishlatiladi: tizim xavfsiz hisoblanadi, agar seans S da ishlovchi ixtiyoriy foydalanuvchi vakolat p ni talab qiluvchi harakatlarni faqat $p \in permissions(s)$ bo'lganida amalga oshira olsa.

Rolli modelning xavfsizlik mezoni ta'rifidan kelib chiqadiki, foydalanishni boshqarish, asosan rollarga vakolatlarni berish bilan emas, balki foydalanuvchilarga rollarni tayinlovchi UA munosabatni va seansdagi joiz rollar to'plamini aniqlovchi $roles$ funksiyasini berish orqali amalga oshiriladi. Shu sababli, rolli modelning ko'p sonli talqini $user, roles$ va $permission$ funksiyalar xili hamda PA va UA munosabatlarga qo'yiladigan cheklashlar orqali farqlanadi.

Xulosa sifatida ta'kidlash lozimki, foydalanishni boshqarishning rolli siyosati boshqa siyosatlardan farqli o'laroq rasmiy isbot yordamida xavfsizlikni amalda kafolatlamay, faqat cheklashlar xarakterini aniqlaydi. Cheklashlar xarakteriga rioya qilish esa tizim xavfsizligining mezoni xizmatini o'taydi. Bunday yondashish foydalanishni nazoratlashning amalda osongina qo'llash mumkin bo'lgan oddiy va tushunarli qoidalarini olishga imkon beradi, ammo tizimni nazariy isbotiy bazadan mahrum etadi. Ba'zi vaziyatlarda bu hol rolli siyosatdan foydalanishni qiyinlashtiradi, ammo har qanday holda rollardan foydalanish subyektlardan foydalanishga qaraganda qulayroq, chunki bu foydalanuvchilar orasida vazifalarni va javobgarlik doirasini taqsimlashni ko'zda tutuvchi axborot ishlashning keng tarqalgan texnologiyalariga juda mos keladi. Undan tashqari, rolli siyosat foydalanuvchilarga tayinlangan rollar vakolatlari diskretsion yoki mandatli siyosat tomonidan nazoratlanganida, boshqa xavfsizlik siyosatlari bilan birgalikda ishlatilishi mumkin. Bu esa foydalanishni nazoratlashni ko'p sathli sxemasini qurishga imkon beradi.

Xavfsizlik siyosati modellari bo'yicha xulosalar.

Xavfsizlikning diskretsion va mandatli siyosatlari mavjud avtomatlashtirilgan axborot tizimlarida qabul qilingan an'anaviy mexanizmlarga mos keladi. Diskretsion modellar uchun obyektlarga

(fayllarga) huquqlar ular tegishli bo'lgan foydalanuvchilar tomonidan tayinlanadi, jarayon vakolatlari esa uni foydalanuvchi nomidan bajarilayotgan foydalanuvchi identifikatori orqali aniqlanadi. Mandatli model uchun obyektlarning xavfsizlik darajasi ularda saqlanayotgan hujjatlarning maxfiylik grifiga mos keladi, subyektlarning xavfsizlik darajasi esa foydalanuvchilarning "ruxsat (dopusk)" kategoriyasiga asosan aniqlanadi. Aksincha, rolli siyosat xavfsizlikning tatbiqiy siyosatini akslantiradi. Shu sababli bu siyosatda aniq moslik mavjud emas. Ushbu siyosatni amalga oshirish mexanizmini tatbiqiy masala shartlari hamda rollar va vakolatlarni tayinlash metodikasiga asosan ishlab chiqish zarur.

Modellarning turli-tumanligi va ularni amalga oshirishdagi yondashishlarning ko'pligi, qaysi modellar boshqalaridan yaxshi va qaysilarini u yoki bu holda ishlatish afzal hisoblanadi, mazmunidagi savol tug'ilishiga sabab bo'ladi. Bu savolga javob quyidagicha. Xavfsizlik – tahdidlarga muvaffaqiyatli qarshilik ko'rsatish. Shu sababli xavfsizlik modelining o'zi himoyani ta'minlamaydi, faqat tizim arxitekturasining asos bo'ladigan prinsipini taqdim etadi. Bu prinsipning amalga oshirilishi modeldagi mavjud xavfsizlik xususiyatini ta'minlaydi. Demak, tizimning xavfsizligi bir xilda uchta omil orqali aniqlanadi: modelning xususiyati, uning tizimga ta'sir etuvchi tahdidlarga adekvatligi va tizim qanchalik korrekt amalga oshirilganligi. Axborot xavfsizligi nazariyasi sohasidagi turli-tuman nazariy ishlanmalarning mavjudligi ma'lum tahdidlarga adekvat modelni tanlash muammo emas, oxirgi hal etuvchi so'z tanlangan modelni himoyalangan tizimda amalga oshirishda qolgan.

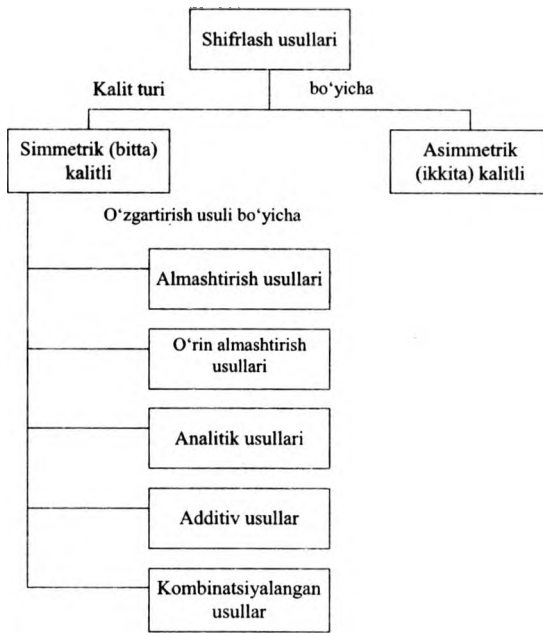
Nazorat savollari:

1. Rolli modelning xavfsiz axborot kommunikatsiya tizimlarini loyihalashdagi o'rni.
2. Xavfsizlikning rolli modeli tizimni qanday to'plamlar ko'rinishida tavsiflaydi?
3. Rolli modelning xavfsizlik mezonini tushuntirib bering.
4. Rolli modelning diskretsion va mandatli modellardan farqi nimada?

V BOB. AXBOROTNI KRIPTOGRAFIK HIMOYALASH

5.1. Shifrlash usullari

Shifrlash usullari turli alomatlari bo'yicha turkumlanishi mumkin. Turkumlanish variantlaridan biri 5.1-rasmda keltirilgan.



5.1-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 qo'yiladi.

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 simvollarining raqamli ekvivalentlarini o'zgartirish orqali amalga oshiriladi.

Monoalfavitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko'rinishida 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 $h_{0i}(s_{0i})$ songa 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 koeffitsent; k_2-siljitish koeffitsenti. Tanlangan k_1,k_2 koeffitsentlar 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=<ABDEFGHIKLMNOPQRSTUVXYZO'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_{0h}=<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:

$$k_1 h_{01} + k_2 = nR + h_{1i}$$

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 kriptotahlillovchi ushlab qolingan axborotni 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 (5.2-rasm).

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.

ABDEF.....	.....	.....ShChNg_
BDEF.....	.....	.....ShChNg_A
DEFG.....	.....	.....ChNg_AB
.....	.....	.....
_ABD.....	.....	.....G‘ShChNg

5.2-rasm. Vijiner matritsasi.

Agar kalit sifatida <G‘O‘ZA> so‘zi tanlangan bo‘lsa, shifrlash matritsasi beshta qatordan iborat bo‘ladi (5.3-rasm).

T_{Sh}

ABDEFGHIJKLMNOPRQSTUVXYZO‘G‘ShChNg_
G‘ShChNg_ABDEFGHIJKLMNOPRQSTUVXYZO‘
O‘G‘ShChNg_ABDEFGHIJKLMNOPRQSTUVXYZ
ZO‘G‘ShChNg_ABDEFGHIJKLMNOPRQSTUVXY
ABDEFGHIJKLMNOPRQSTUVXYZO‘G‘ShChNg_

5.3-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 matritsasi $T_{sh}=(b_{ij})$ ni qurish.

3-qadam. Dastlabki matnning har bir simvoli s_{0r} tagiga kalit simvoli k_m joylashtiriladi. Kalit keragicha 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 $k_m= b_{jl}$ shart bajariluvchi i qator topiladi;

3) $s_{or}= b_{il}$ 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 matnda 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 5.4-rasmda keltirilgan.

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 PAXTA G'ARAMI
Dastlabki matn PAXTA G'ARAMI

5.4-rasm. Vijiner matritsasi yordamida shifrlash misoli.

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.

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 $1{,}6 \cdot 10^9$ kombinatsiyasi 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 (5.5-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.

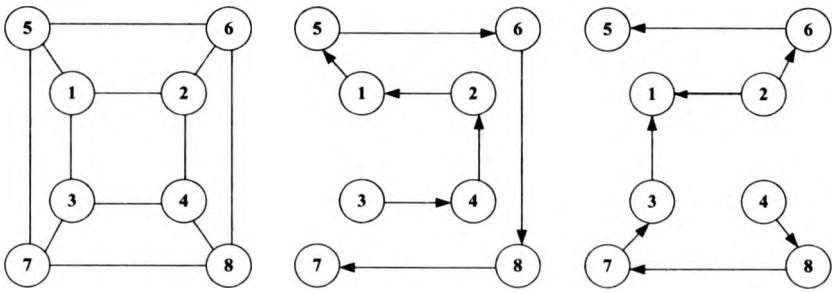
4-qadam. Simvollarning shifrlangan ketma-ketligi belgilangan L uzunlikdagi bloklarga ajratiladi. L kattalik 1-qadamda dastlabki axborot bo'linadigan bloklar uzunligidan farqlanishi mumkin.

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

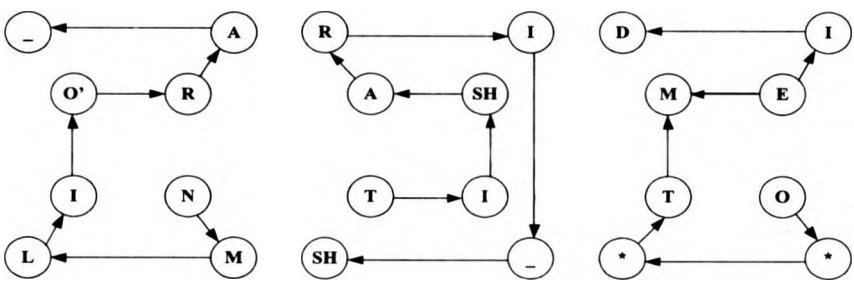
Jadvaldan simvollar element nomerlari kelishi tartibida o'qiladi.

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 5.5-

rasmda keltirilgan jadval va ikkita marshrutdan foydalaniladi. Berilgan shartlar uchun matritsalari to'ldirilgan marshrutlar 5.6-rasmda keltirilgan ko'rinishga ega.



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



5.6-rasm. Gamilton marshruti yordamida shifrlash misoli.

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;

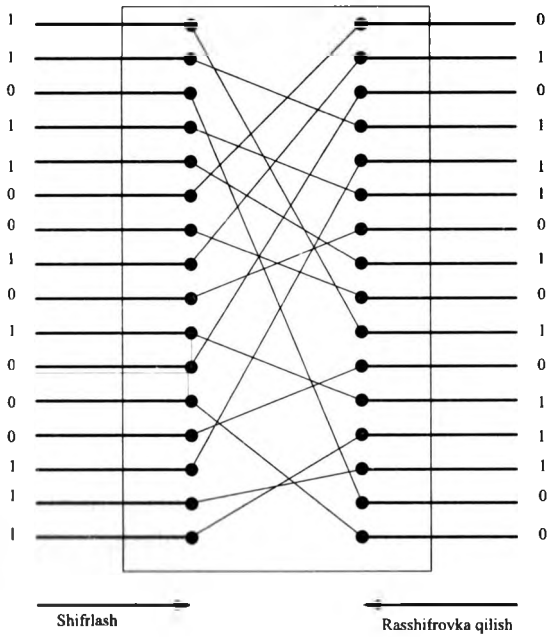
3-qadam. Marshrutlarga binoan simvollarni joy-joyiga qo'yish orqali shifrmatnni hosil qilish.

T_1=<NMLIO'RA_TISHARI_SHTOEMDI**>

4-qadam. Shifrmatnni bloklarga ajratish.

T_1=<NMLI O'RA_ TISHA RI_SH TOEMDI**>

Amaliyotda o'rin almashtirish usulini amalga oshiruvchi maxsus apparat vositalar katta ahamiyatga ega (5.7-rasm).



5.7-rasm. O‘rin almashtirish sxemasi.

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

O‘rin almashtirish usullarining amalga oshirilishi sodda bo‘lsada, 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.

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.

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix} = \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix}$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix} = \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix}$$

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:

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

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:

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

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix} = \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix} = \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix}$$

6-qadam. Rasshifrovka qilingan so'zning son ekvivalenti T_e=<1,10,12,1,14,1> 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, shifrlashinng 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 kriptotahlillovchi tomonidan statistik usullar yordamida rasshifrovka qilinishi mumkin. Kalit va dastlabki axborot uzunliklari qanchalik farqlansa, shifrmatnga 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 usullaridagidek 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-kompyuterdagi so‘zning bitlardagi uzunligi. Shakllantiruvchi son ketma-ketliklarining takrorlanish davri s-toq son va a (mod4)=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 vektorini 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 etish 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‘gri 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’lumotlarning bir necha yuz Kbaytini shifrlash imkoniyati mavjud. Ras-

shifrovka 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_y ga ko'paytiriladi va shifrlangan vektorlar shakllantiriladi:

$$f_i^* = f_i \cdot M_y$$

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 $\left(M_y^{-1}\right)$ga ko'paytiriladi.

$$f_i = f_i^* \cdot M_y^{-1}$$

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 usullarni apparat-dasturiy usulda, ya'ni usulning bir bosqichi apparat usulda, ikkinchi bosqichi dasturiy usulda amalga oshirilishi maqsadga muvofiq hisoblanadi.

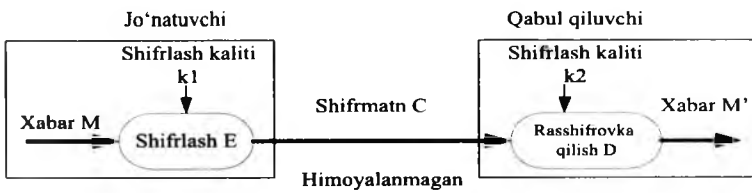
Nazorat savollari:

1. Shifrlashning monoalfavitli almashtirish usulini tushuntirib bering.
2. Polialfavitli almashtirish usulining ishlash prinsipi.
3. O'rin almashtirish usullari qanday amalga oshiriladi?

4. Shifrlashning analitik usulini tushuntirib bering.
5. Shifrlashning additiv usuli qanday amalga oshiriladi?
6. Shifrlashning kombinatsiyalangan usulini yoritib bering.

5.2. Simmetrik shifrlash tizimlari

Axborotni 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 5.8-rasmda keltirilgan.



5.8-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'ri-

nishidagi 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.

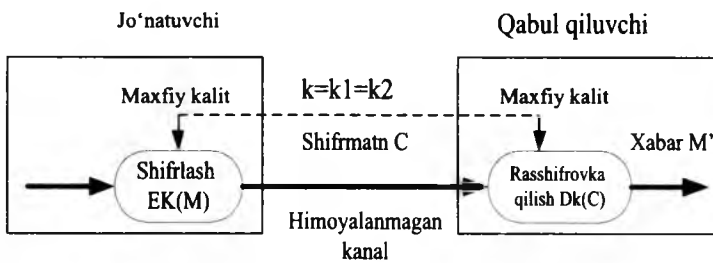
Kriptotizimlarning ikkita sinfi farqlanadi:

- 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 5.9-rasmda keltirilgan.

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 eltuvchisidan masalan, disketda yoki smart-kartada saqlanadi. Shaxsiy kalit eltuvchisi egasidan boshqa odamlarning 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.



5.9-rasm. Simmetrik shifrlash kriptotizimining sxemasi.

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 nuqtayi nazaridan nojoizdir. Haqiqatan, kalit obro'sizlantirilganda (yo'qotilganida, o'g'irlanganda) barcha abonentlarning hujjat almashishi xavf ostida qoladi. Bu holda kalitlarning matritsasi (5.10-rasm) ishlatilishi mumkin.

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

5.10-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 naboridan iborat. Kalitlar nabori (tarmoq naborlari) kriptografik tarmoqning barcha abonentlari o'rtasida taqsimlanadi. Taqsimlash aloqaning

himoyalangan kanallari orqali yoki qo'ldan-qo'lga tarzda amalga oshiriladi.

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 ketma-ketlikning o'rnini almashtirish ko'zda tutilgan.

DES algoritmidagi shifrlash jarayonining blok-sxemasi 5.11–rasmda keltirilgan. Rasshifrovka jarayoni shifrlash jarayoniga invers bo'lib, shifrlashda ishlatiladigan kalit yordamida amalga oshiriladi.

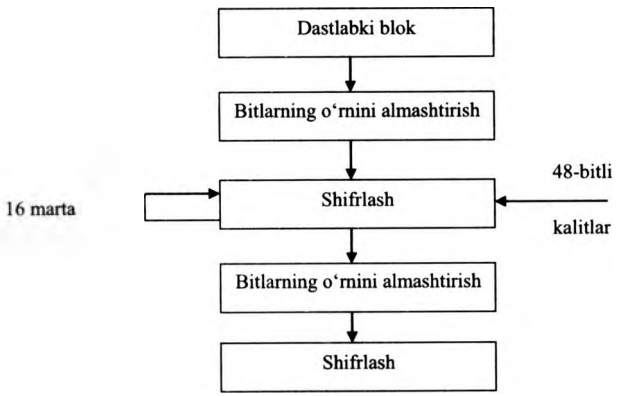
Hozirda bu standart quyidagi ikkita sababga ko'ra foydalanishga butunlay yaroqsiz hisoblanadi:

- kalitning uzunligi 56 bitni tashkil etadi, bu kompyuterlarning 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).

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.



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

Undan tashqari tanlovda ishtirok etuvchilar uchun quyidagi tavsiyalar berilgan edi:

• ham apparat usulda, ham programm usulda osongina amalga oshiriluvchi amallardan foydalanish;

• 32 xonali protsessorlardan foydalanish;

• iloji boricha shifr strukturasini 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-oktyabrda 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.

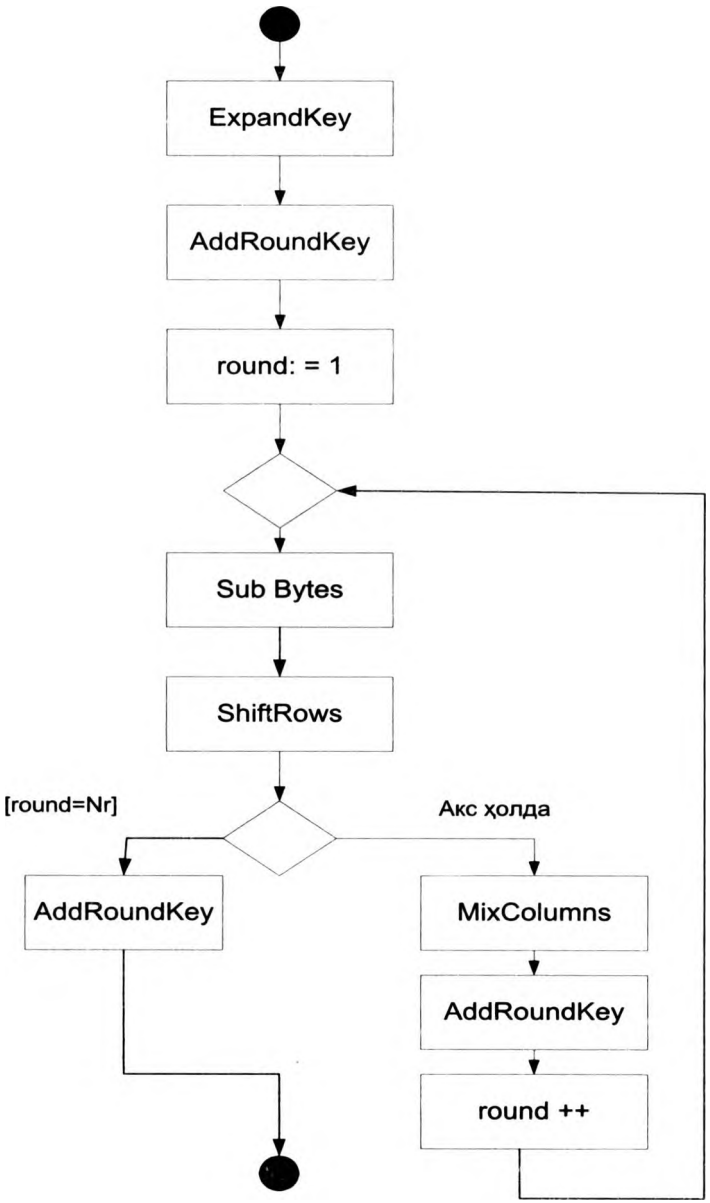
Shifrdagi barcha o‘zgartirishlar qat’iy matematik asosga ega. Amallarning strukturasi va ketma-ketligi algoritmning ham 8-bitli, ham 32-bitli mikroprotsessorlarda samarali bajarilishiga imkon beradi. Algoritm strukturasida ba’zi amallarning parallel ishlanishi, ishchi stansiyalarida shifrlash tezligining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

Ushbu algoritmning shifrlash jarayoni quyidagi blok sxema orqali ifodalangan (5.12-rasm).

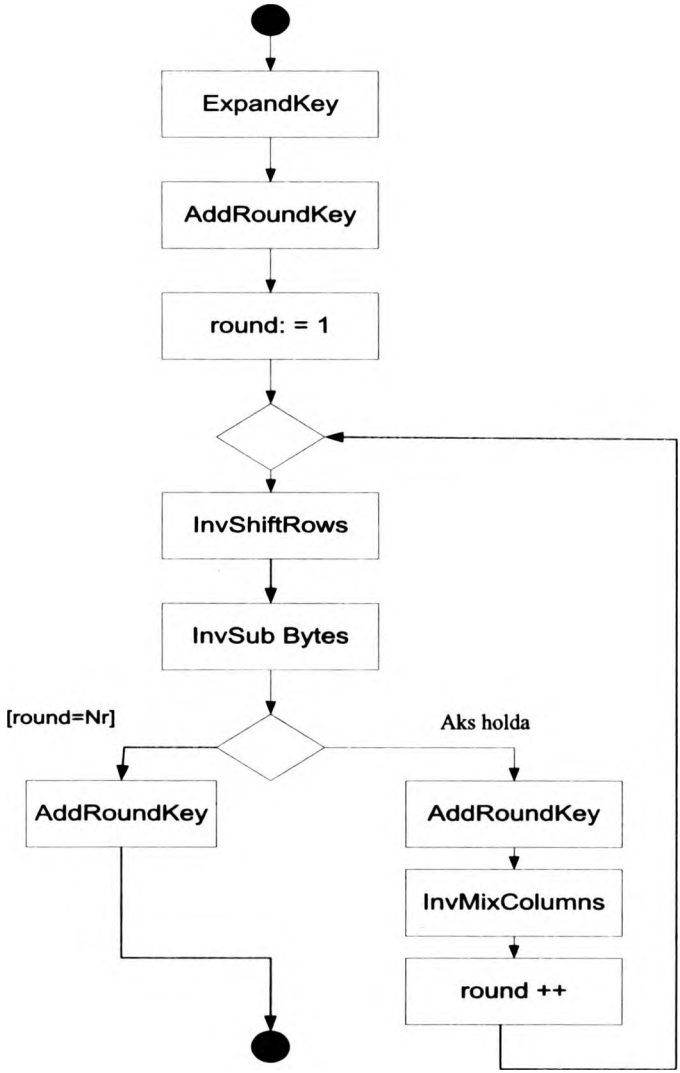
Shifrlash jarayonining har bir raund shifrlash jarayonlari quyida keltirilgan to‘rtta akslantirishlardan foydalanilgan holda amalga oshiriladi:

- *Sub Bytes* – algoritmda jadval asosida baytlarni almashtiradi, ya’ni S-blok akslantirishlarini amalga oshiradi;
- *ShiftRows* – algoritmda berilgan jadvalga ko‘ra holat baytlarini siklik surish;
- *MixColumns* – ustun elementlarini aralashtiradi, ya’ni algoritmda berilgan matritsa bo‘yicha akslantirishni amalga oshiradi;
- *AddRoundKey* – raund kalitlarini qo‘shish, ya’ni bloklar mos bitlarini *XOR* amali bilan qo‘shish.

Deshifrlash jarayonida shifrlash jarayonidagi *Sub Bytes, ShiftRows, MixColumns* va *AddRoundKey* funksiyalari o‘rniga mos ravishda *invSub Bytes, invShiftRows, invMixColumns* va *AddRoundKey* teskari almashtirish funksiyalari qo‘llaniladi (5.13-rasm).



5.12-rasm. Shifrlash jarayoni.



5.13-rasm. Deshifrlash jarayoni.

Rossiyaning axborotni shifrlash standarti. Rosssiya 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 almashtirish algoritmining mohiyati quyidagicha (5.14-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 mod2^{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.

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.

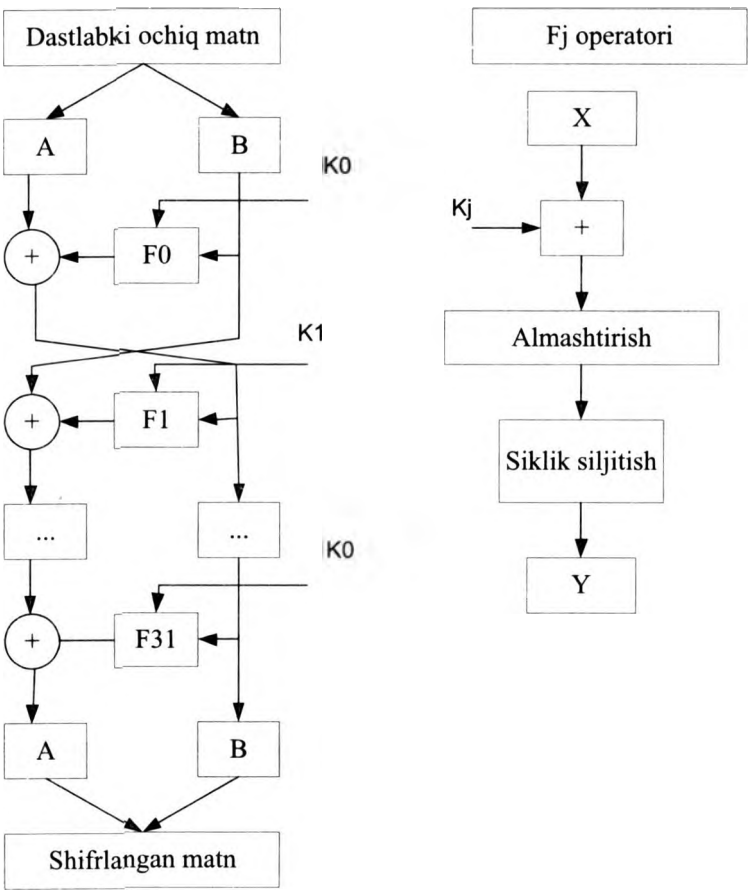
Har bir i-iteratsiyada K_j kalitning (kalitlar 8 ta) 32 xonali so'zi quyidagi qoidaga binoan tanlanadi:

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

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.



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

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 kompyuter 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 asosida bog'langan.

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

Imitovstavkani shakllantirish algoritmi quyidagi harakatlarning 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 iteratsiyalariga 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 mod 2 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 blok $T(m\text{-}1)$ 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.

O'zbekistonning ma'lumotlarni shifrlash standarti. O'z DSt 1105-2009 ma'lumotlarni shifrlash algoritmi diamatritsaviy funksiyalarni qo'llagan holda 256 bit uzunlikdagi ma'lumotlar blokini shifrmatnga o'girish va shifrmatnni dastlabki matnga o'girish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitlardan foydalanishga mo'ljallangan.

Ushbu standartda O'z DSt 1109 bo'yicha atamalar hamda quyidagi atamalar mos ta'riflari bilan qo'llanilgan:

- *initsializatsiyalash vektori:* Kriptografik algoritm doirasida kriptografik jarayonning tayanch nuqtasini aniqlash uchun ishlatiladigan vektor;

- *seans kaliti:* Shifrlash kaliti va funksional kalit asosida shakllanadigan maxfiy kalitlarning ikki o'lchamli massivi;

- *shifrlash vositalari:* Axborot almashtirishning kriptografik algoritmlarini amalga oshiruvchi va ularni qayta ishlashda, saqlashda va telekommunikatsiya kanallari bo'ylab uzatishda axborotni ruxsat etilmagan foydalana olishdan muhofaza qilish uchun mo'ljallangan apparat, dasturiy va apparat-dasturiy vositalar;

- *shifrmatn bloklarini ilaktirish rejimi:* Har bir shifrlangan (dastlabki matnga o'girilgan) kriptografik blok oldingi shifrlangan (dastlabki matnga o'girilgan) blokka bog'liq bo'lgan shifrlash rejimi. Birinchi blok uchun shifrmatnning oldingi bloki sifatida initsializatsiyalash vektoridan foydalaniladi. Ochiq matnning oxirgi bloki to'liq bo'lmagan holatda, u zarur uzunlikkacha to'ldiriladi;

- *elektron kod kitobi rejimi:* Ochiq matnning barcha bloklari ma'lumotlarini shifrlash algoritmlariga muvofiq bir-biridan mustaqil, bitta kalit bilan shifrlanadigan shifrlash rejimi.

Ma'lumotlarni shifrlash algoritmi quyidagi funksiyalardan foydalanadi [9]:

- ***Aralash()*** – oddiy shifr almashtirish bo'lib, dastlabki matnni shifrmatnga va teskari yo'nalishda almashtirish uchun diamatritsaviy qismlar ustida amalga oshiriladi; mazkur shifralmashtirish kirishi Holat massivining diamatritsaviy qismlari hamda K1 va K2 massivlari bo'lib, chiqishi Holat massividir;
- ***BaytAlmash()*** – oddiy shifralmashtirish bo'lib, dastlabki matnni shifrmatnga va teskari yo'nalishda Holat massivi elementlarini almashtirish massivi elementlari bilan bayt sathida almashtirish uchun foydalaniladi; mazkur shifralmashtirish kirishi bayt sathida Holat massivi, almashtirish massivi chiziqli massiv BsA [256] yoki BsAD [256] bo'lib, chiqishi bayt sathida Holat massividir;
- ***Sur()*** – Holat massivi elementlarini yanada yaxshiroq aralashtirish uchun, dastlabki matnni shifrmatnga va teskari yo'nalishda almashtirishda foydalaniladi; mazkur almashtirish kirishi bayt sathida Holat massivi, chiqishi ustun bo'ylab shifrlashda pastga va satr bo'ylab o'ngga yoki shifrni ochishda ustun bo'ylab yuqoriga va satr bo'ylab chapga surilgan bayt sathida Holat massividir;
- ***ShaklSeansKalitBayt()*** – seans uchun kalit shakllantirish bo'lib, dastlabki matnni shifrmatnga va teskari yo'nalishda almashtirishda BaytAlmash() shifralmashtirishini bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi shifrlash kaliti k va funksional kalit kf bo'lib, chiqishi bayt sathida chiziqli massivlar B_{sA} [256] va B_{sAD} [256];
- ***ShaklSeansKalit()*** – seans uchun kalit shakllantirish bo'lib, dastlabki matnni shifrmatnga va teskari yo'nalishda almashtirishda Aralash() shifralmashtirishini bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi baytli elementlardan tarkib topgan chiziqli massiv Kst=[32] bo'lib, chiqishi maxsus tuzilmali diamatritsalardan tashkil topgan (K1t , K2) yoki (K1 , K2t) massivlar juftliklaridir;
- ***ShaklBosqichKalit()*** – seans davomida seans-bosqich kalitidan bosqich kalitini shakllantirish bo'lib, dastlabki matnni shifr-

matnga va teskari yo'nalishda almashtirishda Qo'shBosqichKalit() almashtirishini bajarish uchun foydalaniladi; mazkur almashtirish kirishi chiziqli seans-bosqich kaliti massivi kse, chiqishi bayt sathida berilgan ikki o'lchamli Ke[8,4] massividir;

- ***Qo'shBosqichKalit()*** – oddiy shifralmashtirish bo'lib, dastlabki matnni shifrmatnga va teskari yo'nalishda Holat va bosqich kaliti massivi Ke elementlari ustida istisnoli YoKI (2 moduli bo'yicha bitlab qo'shish) amalini bajarishdan iborat; mazkur shifralmashtirish kirishi bayt sathida Holat massivi, Ke massivi bo'lib, chiqishi bayt sathida Holat massividir;
- ***Qo'shHolat()*** – oddiy shifralmashtirish bo'lib, shifrlash bloklari ustida amalga oshiriladigan elektron kod kitobi rejimidan boshqa rejimlarda dastlabki matnni shifrmatnga va teskari yo'nalishda XOR amali ishtirokida foydalaniladigan almashtirish.

Shifrlash kriptografik modulini ishga tushirishda avvalo, modulga shifrlash kaliti k va funksional kalit k_f, o'rnatilgan bosqichlar soni e hamda rejim *m=ShBil* uchun initsializasiyalash vektori IV yuklanadi. Shuningdek, dastlabki matnni shifrmatnga almashtirish rejimida dastlabki matn, shifrmatnni dastlabki matnga almashtirish rejimida esa shifrmatn kriptografik modulning *Holat* massiviga yuklanadi. Shifrlash jarayonining boshlanishida ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit(K_{st}) va ShaklBosqichKalit(k_{se}) ishga tushiriladi. ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit(K_{st}) shifralmashtirishlari chiqishida bayt sathida almashtirish massivlari va diamatritsaviy qismlardan tarkib topgan seans kaliti massivlari shakllantiriladi. Bu massivlar toki k, k_f lar o'zgarmas bo'lib qolar ekan, keyingi seanslarda ham foydalanilaveradi. ShaklBosqichKalit(k_{se}) shifralmashtirishi chiqishida boshlangich va har bir bosqich uchun shakllantirilgan bosqich kalitlari to'plami shakllantiriladi.

Elektron kod kitobi (Elektron kod kitobi) m=Ekk va shifr bloklarni ilaktirish (ShifrBloklarni ilaktirish) m=ShBil rejimlariga tegishli psevdokod keltirilgan.

Aralash (Holat,Ks), BaytAlmash (Holat,Ba), Qo'shBosqichKalit (Holat,Ke), Sur (Holat) oddiy shifralmashtirishlari va ShaklSeansKalitBayt(k,kf), ShaklSeansKalit(Kst), ShaklBosqichKalit (kse) va Qo'shHolat (Holatt, Holat) almashtirishlari keyingi bandda keltirilgan.

Shifrlash modulining dasturiy-apparatli shaklida funksional kalit yangilash jarayonini ShaklSeansKalitBayt(k,k_f), ShaklSeans-Kalit (K_{st}), ShaklBosqichKalit(k_{se}) almashtirish jarayonlari bilan qo'shib olib borish maqsadga muvofiqdir. Unda shifr protsedurasiga ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit (K_{st}), ShaklBosqichKalit(k_{se}) natijalarini kiritish nazarda tutilishi lozim.

Shifrlash protsedurasining psevdokodi quyida keltirilgan:

Shifr (int blok soni, byte IV[32], byte kirish [blok soni] [32], byte chiqish [blok soni] [32], byte k[32], byte k_f[32], byte e)

```
begin
   byte k_e [8, 4], K_s [8, 4], K_e [8, 4]
   Holat [8, 4], Holatn [8, 4]
if (m=Sh)
   ShaklSeansKalitBayt (k, k_f)
   ShaklSeansKalit (K_st)
   ShaklBosqichKalit (k_se)
   for blok=1 step 1 to blok_soni
   Holat=kirish[blok]
   if (m=ShBil)
     if (blok=1)
          Holatn=IV
     else
          Holatn=chiqish[blok-1]
     end if
     Qo'shHolat (Holat, Holatn)
   end if
   for    bosqich=1 step 1 to e
     Qo'shBosqichKalit (Holat, K_e)
     Aralash (Holat, K_s)
     Sur (Holat)
     BaytAlmash (Holat, B_a)
   end for
   Qo'shBosqichKalit (Holat, K_e)
   Aralash (Holat, K_s)
   Chiqish [blok]=Holat
   end for
else
```

```
        ShaklSeansKalitBayt (k, kf)
        ShaklSeansKalit (Kst)
        ShaklBosqichKalit (kse)
        for blok=1 step 1 to blok_soni
          Holat=kirish [blok]
          Aralash (Holat, Ks)
          Qo'shBosqichKalit (Holat, Ke)
          for bosqich=1 step 1 to e
                BaytAlmash (Holat, Ba)
                Sur (Holat)
                Aralash (Holat, Ks)
                Qo'shBosqichKalit (Holat, Ke)
          end for
          if (m=ShBil)
                if (blok=1)
                      Holatn=IV
                else
                      Holatn=kirish[blok-1]
                end if
                Qo'shHolat (Holat, Holatn)
          end if
          chiqish[blok]=Holat
        end for
    end if
    end
```

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 qo'yiladigan 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, foydalanuvchilari yuz milliondan oshib ketgan «Internet»

tarmog'ida simmetrik shifrlash tizimini qo'shimcha usul va vositalarsiz qo'llashning iloji yo'q.

Nazorat savollari:

1. Simmetrik shifrlash tizimlarining ishlash sxemasini tushuntirib bering.
2. AQShning axborotni shifrlash standarti DES algoritmini tushuntirib bering.
3. AQShning axborotni shifrlash standarti AES algoritmini tushuntirib bering.
4. Rossiyaning axborotni shifrlash standarti GOST 2814-89 algoritmini ishlash sxemasini tushuntirib bering.
5. O'zbekiston Respublikasining ma'lumotlarni shifrlash standarti O'z DSt 1105-2009 algoritmini ishlash sxemasini tushuntirib bering.
6. Simmetrik shifrlash tizimlarining afzalliklari va kamchiliklari.

5.3. Asimmetrik shifrlash tizimlari

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 5.15-rasmda keltirilgan. 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 qila olmaydi, chunki abonent Vning maxfiy kaliti unda yo'q.

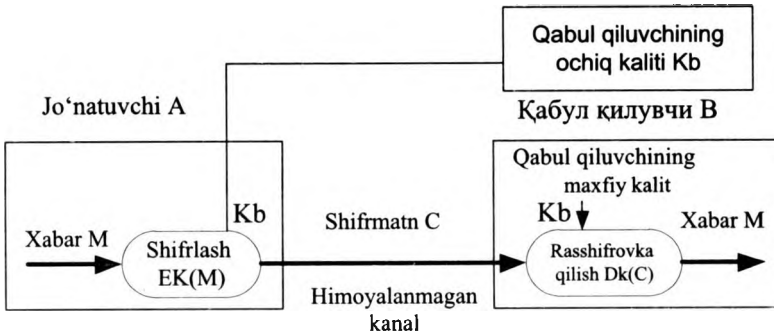
Asimmetrik kriptotizimda axborotni himoyalash axborot qabul qiluvchi kaliti $k_V$ning maxfiyligiga asoslangan.

Asimmetrik kriptotizimlarning asosiy xususiyatlari quyidagilar:

1. Ochiq kalitni va shifrmatnni 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.

Asimmetrik shifrlashning birinchi va keng tarqalgan kriptoalgoritmi RSA 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, demak, RSA bardoshliligini oshishiga imkon yaratadi.



5.15-rasm. Asimmetrik shifrlashning umumlashtirilgan sxemasi.

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 holi 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 apparat amalga oshirilishi, simmetrik algoritmlardagiga nisbatan anchagina murakkab;
- ochiq kalitlarni almashtirib qo'yilishidan himoyalash zarur. Faraz qilaylik, "A" abonentning kompyuterida "V" abonentning ochiq kaliti "K_V" saqlanadi. "n" niyati buzuq odam "A" abonentda saqlanayotgan 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" kalitini 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.

Asimmetrik shifrlash tizimlari ochiq kalitli shifrlash tizimlari 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 soddalashtiradi.

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 200dan 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:

$$e*d=1(modf(p,q)).$$

Bu shartga binoan $e*d$ 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'iy 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 $X(i)$, $i=\overline{1,l}$ 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:

$$Y(i) = (X(i))^e \pmod{n}.$$

Axborotni rasshifrovka qilishda quyidagi munosabatdan foydalaniladi:

$$X(i) = (Y(i))^d \pmod{n}.$$

Misol. <GA3> 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. $(e \cdot 3) \cdot (\text{mod}\, 20) = 1$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, anchagina 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 kriptotizmsida 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 masalasini) 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.

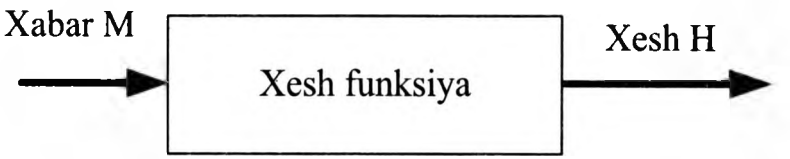
Ayrim muhim qo‘llanishlarda nafaqat kalit, balki shifrlash algoritmi ham maxfiy bo‘ladi. Shifrlarning kriptobardoshligini oshirish uchun bir necha kalit (odatda uchta) ishlatilishi mumkin. Birinchi kalit yordamida shifrlangan axborot ikkinchi kalit yordamida shifrlanadi va h.

Nazorat uchun savollar:

1. Asimmetrik shifrlash tizimlarini ishlash prinsipini tushuntirib bering.
2. RSA asimmetrik algoritmining shirflash qadamlarini yoritib bering.
3. El Gamal asimmetrik shifrlash algoritmi qanday matematik muammolarga asoslangan?
4. Asimmterik shirflash algoritmlari turiga kiruvchi qanday algoritmlarni bilasiz?
5. Asimmterik shirflash algoritmlarining afzalliklari va kamchiliklari.

5.4. 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 (5.16-rasm).



5.16-rasm. Xeshni shakllantirish sxemasi.

Xesh-qiymat h(M) – xabar M ning daydjesti, ya'ni ixtiyoriy uzunlikdagi asosiy xabar *M*ning zichlantirilgan ikkilik ifodasi. Xeshlash funksiyasi o'lchami megabayt va undan katta bo'lgan imzo chekiluvchi hujjat *M*ni 128 va undan katta bitga (xususan, 128 yoki 256 bit) zichlashga imkon beradi. Ta'kidlash lozimki, xesh-funksiya *h(M)* qiymatining hujjat *M*ga bog'liqligi murakkab va hujjat *M* ning 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 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 nuqtayi nazaridan $h(x')=h(x)$ bo'ladigan $x' \neq x$ ni topish mumkin emas.

Ikkita turli xabarning bitta tugunchaga (svertka) zichlash nazariy jihatdan mumkin. Bu kolliziya yoki to'qnashish deb ataladi. Shuning uchun xeshlash funksiyasining bardoshliligini 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 bitta 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 shakllantarishda va tekshirishda ishlatiladi.

Xesh-funksiya foydalanuvchini autentifkatsiyalashda 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 –MD4, MD5,SHA1, SHA2.

MD4 va MD5 – P. Rayvest tomonidan ishlab chiqilgan axborot daydjestini hisoblovchi algoritm. Ularning har biri 128 bitli xesh-kodni tuzadi. MD2 algoritmi eng sekin ishlasa, MD4 algoritmi tezkor ishlaydi. MD5 algoritmi MD4 algoritmining modifikatsiyasi bo'lib, MD4 algoritmida 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.

SHA-1 xeshlash funksiyasi algoritmi. Kafolatlangan bardoshlilikka ega bo'lgan xeshlash algoritmi SHA (SecureHash-Algorithm) AQShning standartlar va texnologiyalar Milliy instituti (NIST) tomonidan ishlab chiqilgan bo'lib, 1992-yilda axborotni qayta ishlash federal standarti (PUBFIPS 180) ko'rinishida nashr qilindi. 1995-yilda bu standart qaytadan ko'rib chiqildi va SHA-1 deb nomlandi (PUB FIPS 180). SHA algoritmi MD4 algoritmiga asoslanadi va uning tuzilishi MD4 algoritmining tuzilishiga juda yaqin. Bu algoritm elektron raqamli imzoni shakllantirish bo'yicha DSS standartida qo'llash uchun mo'ljallangan. Bu algoritmda kiruvchi ma'lumot uzunligi 2^{64} bitdan kichik, xesh qiymat uzunligi 160 bit bo'ladi. Kiritilayotgan ma'lumot 512 bitlik bloklarga ajratilib, qayta ishlanadi.

Xesh qiymatni hisoblash jarayoni quyidagicha bosqichlardan iborat:

1-bosqich: To'ldirish bitlarini qo'shish.

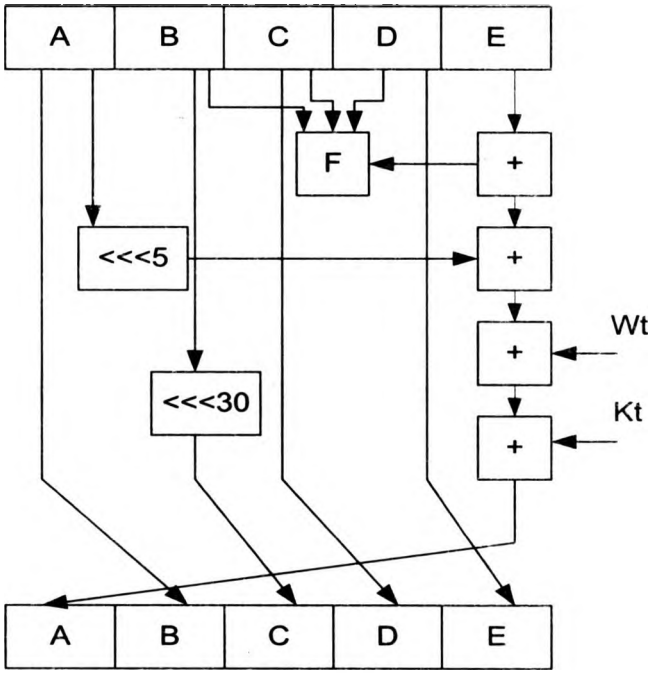
2-bosqich: Ma'lumotning uzunligini qo'shish.

3-bosqich: Xesh qiymat uchun bufer initsializatsiya qilish.

4-bosqich: Ma'lumotni 512 bitlik bloklarga ajratib, qayta ishlash.

5-bosqich: Natija.

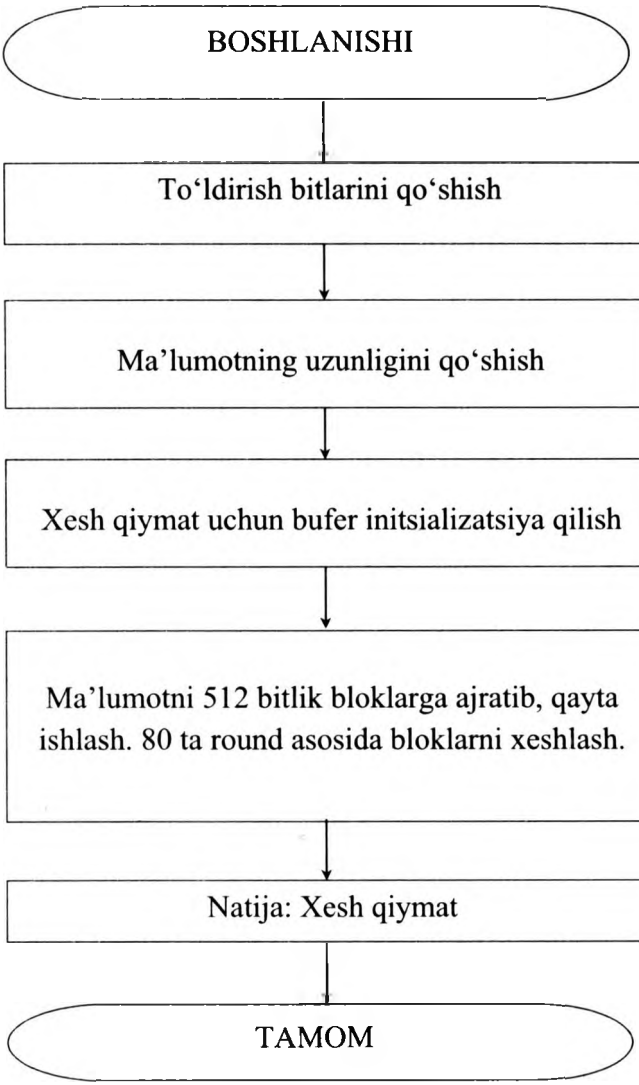
SHA-1 algoritmidagi bir iteratsiya sxemasi 5.17-rasmda keltirilgan.



5.17-rasm. SHA-1 algoritmida bir iteratsiyasining sxemasi.

SHA1 xeshlash funksiyasi algoritmining ishlash blok sxemasi 5.18-rasmda keltirilgan.

GOST R34.11-94 xeshlash funksiyasi algoritmi. Rossiyaning GOST R 34.11-94 xesh funksiya standarti axborotni kriptografik usulda muhofaza qilish uchun, xususan, GOST R 34.11-94 va GOST R 34.10-2001 elektron raqamli imzo algoritmlarida ishlatish uchun mo'ljallangan. Xesh funksiyaning qiymatini hisoblash jarayonida GOST 28147-89 shifrlash standartidan foydalaniladi.



5.18-rasm. SHA1 algoritmi ishlash blok sxemasi.

GOST R 34.11-94 xesh funksiya standartida chiqish uzunligi belgilangan qadamli xeshlash funksiyasidan foydalanuvchi ketma-ket xeshlash usulidan foydalaniladi. Xesh-funksiya argumentining

uzunligi 256 bit bo‘lgan funksiya bo‘lib, xesh qiymat uzunligi 256 bit bo‘ladi.

Xeshlanadigan ma’lumot uzunligi ixtiyoriy bo‘lib, ma’lumot uzunligi 256 bit bo‘lgan bloklarga ajratiladi. Oxirgi blok uzunligi 256 bitdan kichik bo‘lsa, 256 bitgacha nol bilan to‘ldiriladi. Undan tashqari, bu bloklarning oxiriga ma’lumot uzunligining kodini bildiruvchi va nazorat yig‘indisini bildiruvchi yana ikkita 256 bitlik bloklarga qo‘shiladi. Ma’lumot uzunligining kodini blok xeshlanadigan ma’lumotning bit uzunligi $\mathrm{mod}2^{256}$ bo‘yicha hisoblanib (bu protsedura MD kuchaytirish deyiladi) hosil qilinadi. Nazorat yig‘indisining kodini bildiruvchi blok esa, oxirgi to‘liqmas blok nol bilan to‘ldirilgandan keyin barcha bloklarning yig‘indisi $\mathrm{mod}2^{256}$ bo‘yicha hisoblanib, hosil qilinadi.

GOST R 34.11-94 xeshlash funksiyasini hisoblashda quyidagi belgilashlardan foydalaniladi:

M – xeshlanishi kerak bo‘lgan ma’lumot;

h – M ma’lumotni $h(M) \in V_{256}(2)$ga akslantiruvchi xesh-funksiya, bu yerda $V_{256}(2)$ – uzunligi 256 bit bo‘lgan barcha ikkilik so‘zlar to‘plami,

$E_K(A)$ – A ni GOST 28147-89 shifrlash algoritmidan foydalanib, K kalitda shifrlash natijasi,

$H \in V_{256}(2)$ – berilgan boshlang‘ich vektor.

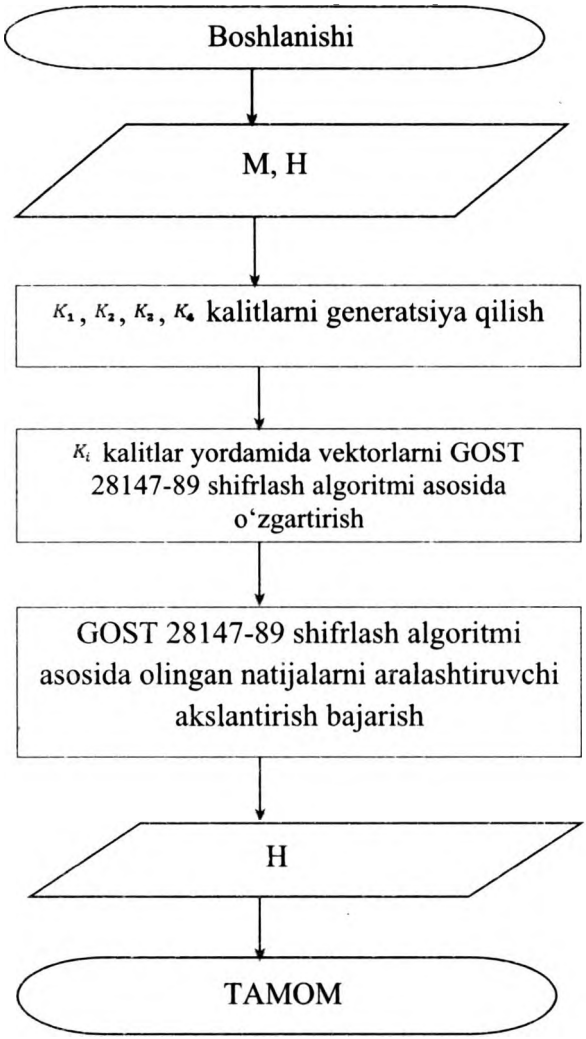
GOST R 34.11-94 xeshlash funksiyasini hisoblash uchun quyidagilar zarur:

- qadamli xeshlash funksiyasi $\chi: V_{256}(2) \times V_{256}(2) \to V_{256}(2)$ni hisoblash algoritmi;

- xesh qiymatni iterativ hisoblash jarayoni.

Qadamli xeshlash funksiyasi uch bosqichda hisoblanadi. Birinchi bosqichda uzunliklari 256 bit bo‘lgan to‘rtta K_1, K_2, K_3, K_4 kalit generatsiya qilinadi. Ikkinchi bosqichda boshlang‘ich N vektor har birining uzunligi 64 bit bo‘lgan to‘rtta blokka ajratiladi va bu bloklar mos K_1, K_2, K_3, K_4 kalitlar bilan GOST 28147-89 algoritmi yordamida shifrlanadi. Uchinchi bosqichda shifrlash natijasini aralashtiruvchi akslantirish bajariladi.

Qadamli xeshlash funksiyasini hisoblash algoritmining blok-sxemasi 5.19-rasmda keltirilgan.



5.19-rasm. Xesh qiymatni hisoblash algoritmining blok-sxemasi.

"O'z DSt 1106:2009" O'zbekiston davlat standarti hisoblanadi. Ushbu standartda xesh-funksiyani hisoblashning ikki xil algoritmi keltirilgan.

1-algoritmda modul arifmetikasining bir tomonlama funksiyasi qo'llaniladi, u bo'yicha hisoblashlar darajaga ko'tarish amallaridagi

kabi aynan o'sha mehnat sarfi darajasida oson amalga oshiriladi, funksiyani invertirlash (teskarilash) esa, ***(A, B)*** noma'lum parametrda diskret logarifm muammosini yechish jarayoniga nisbatan ko'proq hisoblashlar sarfi va vaqtni talab qiladi. Ko'paytirish, darajaga ko'tarish va teskarilash kabi asosiy amallar yangi bir tomonlama funksiyada parametr bilan ko'paytirish, darajaga ko'tarish va teskarilash deb nomlangan. Darajaga ko'tarishning bir tomonlama funksiyasi ushbu bir tomonlama funksiyaning xususiy holidir. Xeshlash funksiyasida parametr (koeffitsient) sifatida natural sonlar uchligidan ***(A, B, R)*** foydalaniladi.

Ushbu algoritmda kirish blokining uzunligi ***128*** yoki ***256*** bitga karrali hamda chiqish bloki va xeshlash kalitining uzunligi ***128*** yoki ***256*** bit. Har bir blok uchun kriptografik almashtirishlar ***10*** ta bosqichda amalga oshiriladi. Xesh-funksiyasi algoritmining ma'lumotlarini xeshlash protsedurasida xeshlash kaliti ***k*** va xeshlashning oraliq natijasi asosida shakllangan bosqich kalitlari k_e dan foydalaniladi.

Xesh qiymatni hisoblash ***holat*** massivi ustida kriptografik o'zgartirishlarni bajarish bilan amalga oshiriladi. ***Holat*** massivi to'rtta satr (qator) va sakkizta ustunda joylashgan yarim baytlardan (baytlardan) iborat, bunda har bir satr *32 (64)* bitdan iborat.

Xesh qiymatni hisoblashda dastlab kiruvchi ma'lumot ***128*** yoki ***256*** bit uzunlikdagi ***b*** ta bloklarga bo'linadi, to'lmay qolgan blok ***0*** lar bilan to'ldiriladi. ***Holat*** massivi dastlabki blok bilan; asosiy qismning umumiy uzunligi 2^{256} modul bo'yicha bitlarda aniqlanadi, bu qism **256** bit uzunlikdagi ***uzunlik*** blokidan iborat; keyin 2^{256} modul bo'yicha asosiy qism bloklari qiymatlarining summasi hisoblanadi, u ***256*** bit uzunlikdagi *nazorat summasining* blokidan ***(NY)*** iborat; asosiy qism, ***uzunlik*** bloki va ***b+2*** bloklardagi yarim bayt (bayt) darajasidagi ikki o'lchamli elementlar shaklidagi ***NY*** blok xeshlash funksiyasi kirish ma'lumotlaridan iborat. Dastlabki bosqich ***128 (256)*** bit uzunlikdagi ***k*** xeshlash kalitining nusxasini ikki o'lchamli k_e massivga ko'chirish bilan tugallanadi.

Kirish ma'lumotlarining har bir bloklariga nisbatan xeshlash jarayonlari ikkita blok: ***holat*** hamda ***holatn*** ustida ***Qo'sh (holat, holatn)***, ***BaytZichlash(holat, holatn)*** o'zgartirishlar juftining zanjirini bajarishdan boshlanadi va 10 ta bosqich davomida ***holat*** joriy

xesh-qiymatini shakllantirish bilan tugallanadi. Xeshlash jarayonlarining eng avvalida dastlabki xesh-qiymat sifatida 1-blokdan ***holat*** bloki sifatida, 2-blokdan esa - ***holatn*** bloki sifatida foydalaniladi; agar kirish ma'lumotlari faqat bitta blokdan iborat bo'lsa, 2-blok sifatida ***uzunlik*** blokidan foydalaniladi[10].

So'ngra ***holatn*** massiviga navbatdagi blokdan nusxa ko'chiriladi va ***Qo'sh(holat, holatn)***, ***BaytZichlash(holat, holatn)*** o'zgartirishlar juftligi natijasi, joriy xesh-qiymat ***holat*** va ***holatn*** ustida xeshlash protsedurasining 10 bosqichi amalga oshiriladi va h.k. ***holatn*** massiviga nusxa olinadigan oxirgi blok sifatida ***NY*** bloki hisoblanadi. Shunday qilib, xeshlash bosqichlarining umumiy soni ***(b+2)10*** ga teng bo'ladi.

Xeshlash protsedurasining har bir bosqichi (raundi) dastlabki ***Qo'sh (holat, holatn)***, ***BaytZichlash (holat, holatn)*** o'zgartirishlar juftligi bilan birga bloklarga nisbatan siklik tartibda amalga oshiriluvchi ***Aralash(holat,k_e), Qo'sh(holat,holatn), SurHolat (holat)), SurKalit(k_e), TuzilmaKalit(k_e, k)*** o'zgartirishlardan iborat.

2-algoritm GOST R 34.11-94 kabi amalga oshiriladi[10].

Nazorat savollari:

1. Xeshlash funksiyasining ishlash sxemasini tushuntirib bering.
2. SHA-1 xeshlash funksiyasi algoritmini tushuntirib bering.
3. GOST R 34.11 Rossiyaning xeshlash funksiyasi algoritmi ishlash sxemasini tavsiflab bering.
4. "O'z DSt 1106:2009" O'zbekiston Respublikasi davlat standarti o'z ichiga oladigan xeshlash funksiyasining ikkita algoritmini yoritib bering.

5.5. 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'lsada, yubormaganman deydi;

- *almashtirish* – abonent *V* hujjatni o'zgartiradi, yoki yangisini shakllantiradi 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 strukturalariga, davlat korxona va tashkilotlariga, xususiy shaxslarga anchagina 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 ishlashi bo'yicha oddiy qo'lyozma imzoga o'xshash bo'lib, quyidagi afzalliklarga ega:

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

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

- imzo chekilgan matn yaxlitligini kafolatlaydi.

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

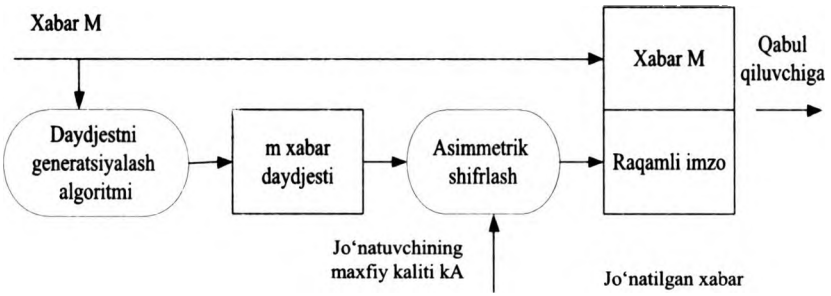
Imzoni shakllantirish muolajasida xabar jo'natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo'natuvchining ochiq kalitidan foydalaniladi.

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 kaliti 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 (5.20-rasm).

Xesh-funksiya imzo chekiluvchi dastlabki matn Mni daydjest $m$ga zichlashtirishga xizmat qiladi. Daydjest M–butun matn Mni 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.



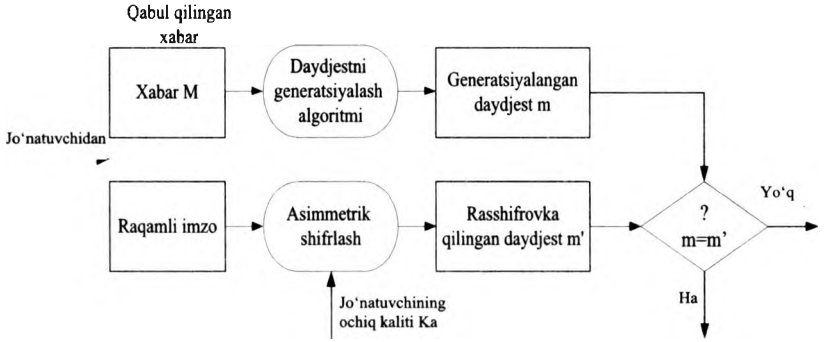
5.20-rasm. Elektron raqamli imzoni shakllantirish sxemasi.

Raqamli imzoni tekshirish muolajasi. Tarmoq abonentlari olingan xabar *M*ning raqamli imzosini ushbu xabarni jo'natuvchining ochiq kaliti K_A yordamida tekshirishlari mumkin (5.21-rasm).

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 – 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.



5.21-rasm. Elektron raqamli imzoni tekshirish sxemasi.

Imzo chekiluvchi faylga joylashtiriluvchi elektron raqamli imzo 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 tugashi 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 *V*da saqlanayotgan ochiq kalit $K_A$ni o'zining ochiq kaliti K_n bilan almashtirishi.

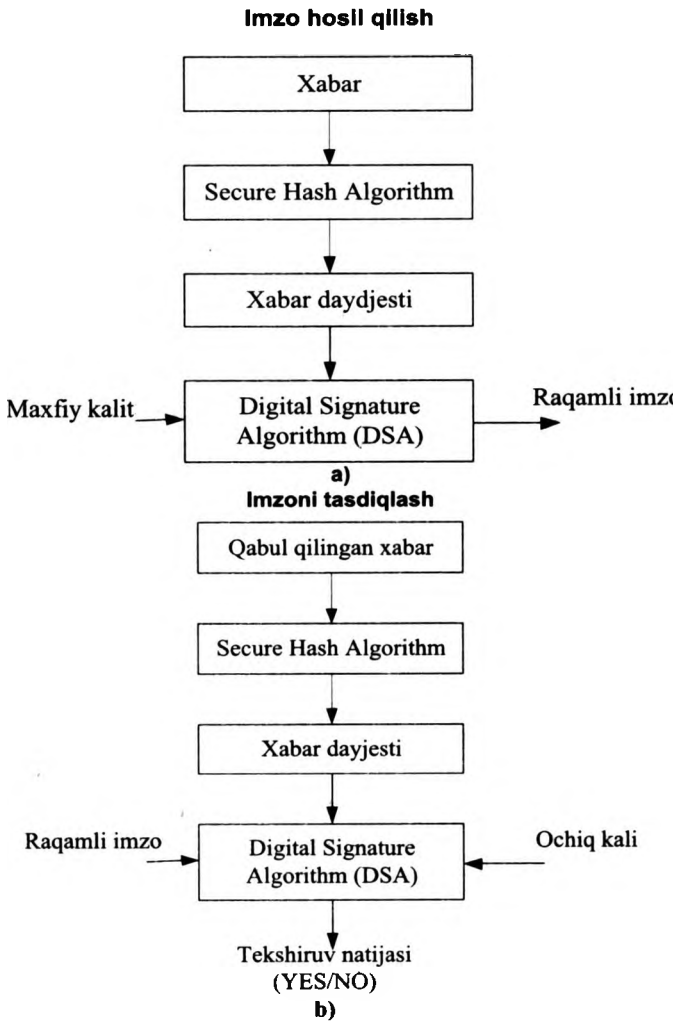
So‘ngra niyati buzuq odam n abonent V ga hujjatlarni o‘zining maxfiy kaliti k_n yordamida imzo chekib, jo‘natishi mumkin. Bu hujjatlar imzosini tekshirishda abonent V abonent A imzo chekkan hujjatlarni va ularning elektron raqamli imzolarini to‘g‘ri va xech kim tomonidan modifikatsiyalanmagan deb hisoblaydi. 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 algoritmi 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.

AQShning DSS standarti. 1991-yilda NIST (National Institute of Standard and Technology) tomonidan DSA (Digital Signature Algorithm) algoritmiga asoslangan DSS (Digital Signature Standard) ERI standartining loyihasi muhokamaga qo‘yildi. Ushbu algoritm bardoshliligi yetarli katta tub xarakteristikaga ega bo‘lgan chekli maydonda diskret logarifmlash masalasining murakkabligiga asoslangan.

Ushbu elektron raqamli imzoni shakllantirish va tekshirish standartida 512 yoki 1024 bit uzunlikdagi kalitlar qo‘llaniladi va elektron raqamli imzoning 160 bitli 2 ta sondan iborat. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari 5.22-rasmda keltirilgan.

Elliptik egri chiziqlarga asoslangan raqamli imzo algoritmi ECDSA (Elliptic Curve Digital Signature Algorithm) – DSA algoritmga tuzilish jihatidan analog hisoblanadi, lekin hisoblashlar butun sonlar maydonida emas, balki elliptik egri chiziqlar nuqtalari guruhida bajariladi va uning kriptobardoshliligi elliptik egri chiziqlar nuqtalari guruhida diskret logarifmlash muammolariga asoslanadi. ECDSA algoritmi 1999 yilda ANSI standarti sifatida, 2000-yilda esa IEEE va NIST standartlari sifatida qabul qilingan.



5.22-rasm. Elektron raqamli imzoni shakllantirish (a) va tekshirish (b) jarayonlari.

GOST R 34.10 elektron raqamli imzoni shakllantirish va tekshirish algoritmi GOST R 34.10-94 raqamli standart hisoblanib, DSA algoritmiga o'xshash ishlaydi. Lekin undan keyin GOST 34.10-2001 standarti ishlab chiqilib, amalda 2011-yilgacha qo'llani-

lib kelingan. 2012-yilda GOST 34.10-2012 standarti qabul qilingan va GOST 34.10-2001 bilan ikkalasi elliptik egri chiziqlar muammolariga asoslangan hisoblanadi.

Ushbu standartda elektron raqamli imzoni shakllantirish avvalgi algoritmlardagi kabi bo'lib, xeshlash funksiyasi sifatida GOST R 34.11-2012 algoritmi qo'llaniladi. Ushbu algoritmda elektron raqamli imzoni shakllantirish jarayoni va uni tekshirish jarayoni quyidagi rasmlarda keltirilgan (5.23 va 5.24-rasm).

Elektron raqamli imzoni shakllantirish. M xabar ostiga qo'yiladigan elektron raqamli imzoni olish uchun algoritm bo'yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: xabarning xesh-funksiyasi hisoblanadi: m=H(M);

2-qadam: $e \equiv m \pmod t$ ni hisoblanadi. Agar $e=0$ bo'lsa, u holda $e=1$ ni aniqlanadi;

3-qadam: ushbu $0<k<t$ tengsizlikni qanoatlantiruvchi tasodifiy (psevdotasodifiy) k butun soni generatsiya qilinadi;

4-qadam: elliptik egri chiziqning $C=[k]N$ nuqtasi hisoblanadi va $r = x_c \pmod t$ ni aniqlanadi, bu yerda $x_c - C$ nuqtaning x koordinatasi. Agar $r = 0$ bo'lsa, u holda 3-qadamga qaytiladi;

5-qadam: $s \equiv (rd+ke) \pmod t$ ifodaning qiymati hisoblanadi. Agar $s=0$ bo'lsa, 3-qadamga qaytiladi;

6-qadam: r va s larni ERI sifatida chiqishga beriladi.

Ushbu jarayon uchun dastlabki (kirishdagi) ma'lumotlar M xabar va ERIning yopiq kaliti d, chiqish natijasi bo'lib esa, (r, s) elektron raqamli imzo hisoblanadi.

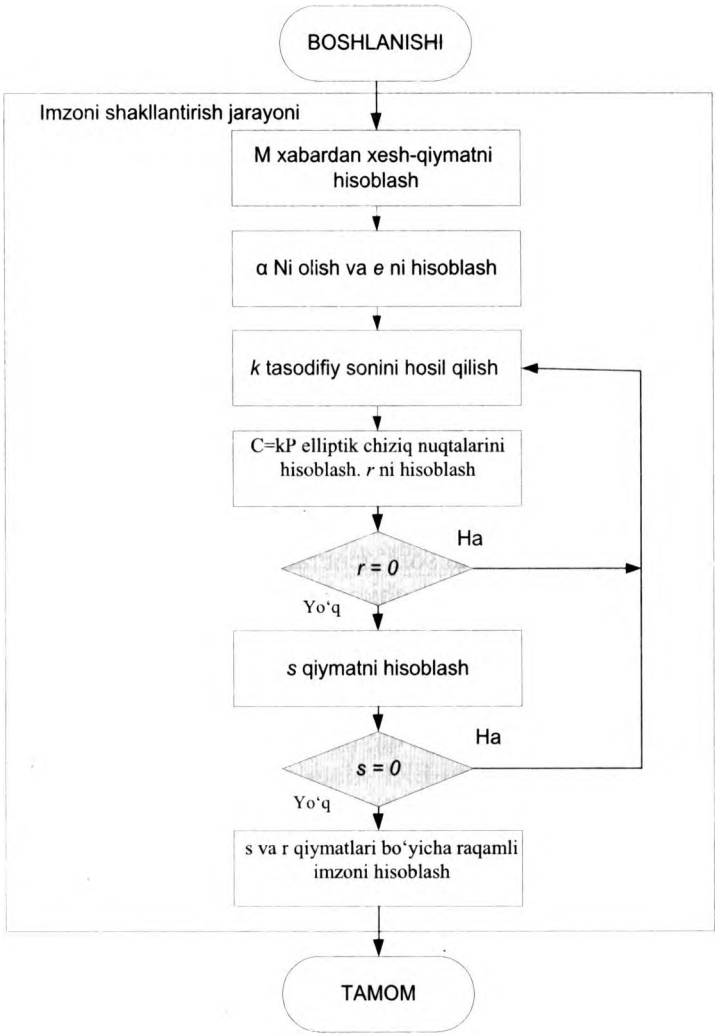
Elektron raqamli imzoning haqiqiyligini tasdiqlash. Olingan M xabar ostiga qo'yilgan ERI haqiqiyligini tasdiqlash uchun algoritm bo'yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: agar $0 < r < t$, $0<s<t$ tengsizliklar bajarilsa, navbatdagi qadamga o'tiladi, aks holda, "imzo haqiqiy emas" deb qabul qilinadi;

2-qadam: M xabar bo'yicha xesh-funksiyani hisoblanadi: m=H(M);

3-qadam: $e \equiv m \pmod t$ ni hisoblang. Agar $e=0$ bo'lsa, u holda $e=1$ ni aniqlanadi;

4-qadam: $v \equiv e^{-1} \pmod t$ ifodaning qiymati hisoblanadi;

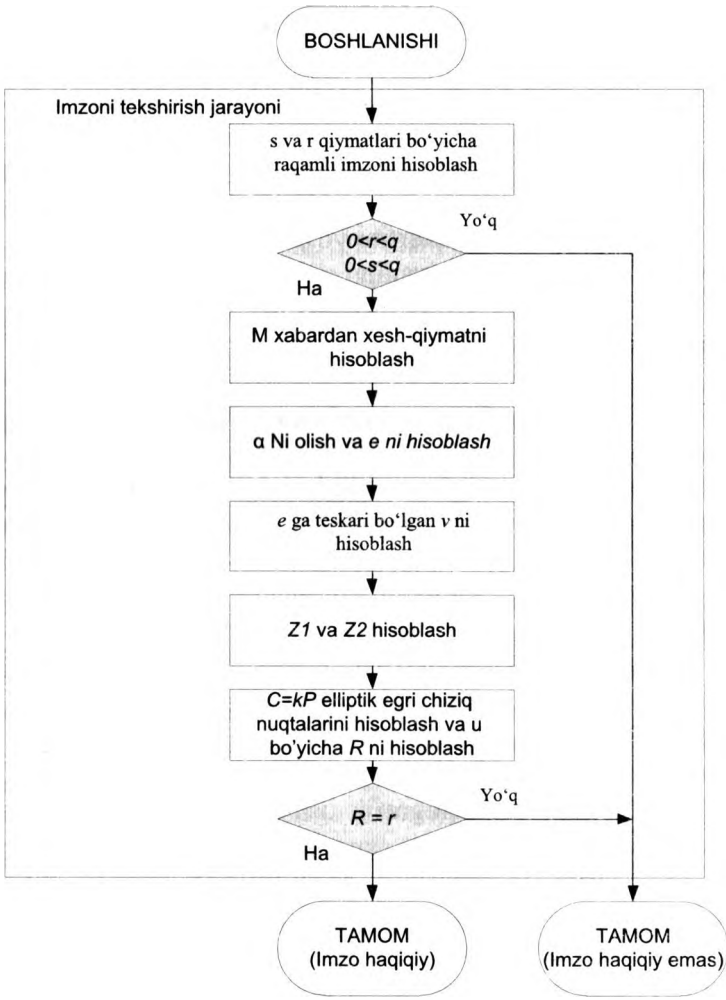


5.23-rasm. Elektron raqamli imzoni shakllantirish jarayoni.

5-qadam: ushbu $z_1 \equiv sv(mod\ t)$, $z_2 \equiv -rv(mod\ t)$ ifodalar qiymatlari hisoblanadi;

6-qadam: elliptik egri chiziqning $C = [z_1]N + [z_2]T$ nuqtasi hisoblanadi va $R \equiv x_c(mod\ t)$ni aniqlang, bu yerda $x_c - C$ nuqtaning x koordinatasi.

7-qadam: agar $R=r$ tenglik bajarilsa, u holda “imzo haqiqiy”, aks holda “imzo haqiqiy emas” deb qabul qilinadi.



5.24-rasm. Elektron raqamli imzoni tekshirish jarayoni.

Ushbu jarayon uchun dastlabki (kirishdagi) ma’lumotlar bo‘lib, imzolangan M xabar, (r, s) elektron raqamli imzo va ERI ochiq

kaliti, chiqish natijasi bo‘lib esa, mazkur ERI haqiqiyligi yoki haqiqiy emasligi haqidagi axborot hisoblanadi.

Nazorat savollari:

1. Elektron raqamli imzoni shakllantirish sxemasini tavsiflab bering.
2. Elektron raqamli imzoni tekshirish jarayonining sxemasini tushuntirib bering.
3. AQShning DSS standartini yoritib bering.
4. GOST R 34.10 Rossiyaning standartini tavsiflab bering.
5. O‘z DSt 1092-2009 algoritmi asoslangan matematik muammolarni tushuntirib bering.

5.6. Steganografiya usullari

Steganografiya so‘zi yunon tilida maxfiy belgilar bilan yozilgan (steganos - sir, graphy - yozuv) ma’nosini bildiradi, tarixi esa ming yillarni o‘z ichiga oladi. Axborotni steganografik himoyalashni turli texnikaviy, kimyoviy, fizikaviy va psixologik usullar yordamida amalga oshirish mumkin.

Steganografiya kriptografiya o‘rnini bosmaydi, balki uni to‘ldiradi. Steganografiya usullari yordamida xabarni bekitish xabar uzatilishi faktini aniqlash ehtimolligini anchagina pasaytiradi. Agar ushbu xabar shifrlangan bo‘lsa, u yana bir qo‘shimcha himoyalanish sathiga ega bo‘ladi. Steganografik usullaridan axborotni ruxsatsiz foydalanishdan himoyalashda, tarmoqlarni monitoringlashga va tarmoq resurslarini boshqarishga qarshilik ko‘rsatishda, ro‘yxatda ko‘rsatilmagan foydalanuvchilardan dasturiy ta’minotni niqoblashda, ba’zi intellektual mulkka egalik huquqini himoyalashda hamda raqamli obyektlarni autentifikatsiyalashda foydalaniladi.

Ma’lum steganografik usullarini quyidagi ikkita guruhga ajratish mumkin:

- moddiy steganografik usullar;
- axborot steganografik usullari.

Moddiy steganografik usullar steganografik konteynerning (maxfiy axborot o‘rnatiladigan obyektning) fizikaviy yoki kimyoviy

xususiyatlari asosida axborotni bekitish uchun ishlatiladi. Bunday xususiyatlarga misol tariqasida gabarit o'lchamlarini, konteyner rangini yoki ma'lum ta'sir natijasida o'rnatilgan axborotning namoyon bo'lish qobiliyatini ko'rsatish mumkin.

Bunday steganografik usullarning tadqiqi va yaratilishi axborotning turli moddiy eltuvchilari xususiyatlarini va axborotni o'rnatishning norasmiy usullarini o'rganish bilan bog'liq.

Moddiy steganografik usullarga ko'rinmaydigan siyohlar, mikronuqtalar va h. taalluqli. Hozirda audiotexnika, videotexnika va hisoblash texnikasi axborotni eltuvchi standart vositalar hisoblanadi.

Axborot steganografik usullar ma'lumotlarni konteynerning axborot bilan to'ldirilishi xususiyati asosida bekitish uchun ishlatiladi. Ushbu usullar lingvistik va raqamlilarga ajratiladi.

Lingvistik steganografik usullarda til yoki harflarni, raqamlarni o'z ichiga olmaydigan (rasmlar, obyektlarning o'zaro joylashishi va h.) boshqa muhit ortiqchaligi ishlatiladi. Ushbu sinfga maxfiy xabarni bekitish uchun zarur matnni generatsiyalash usulini hamda sahifadagi qator holatini yoki gapdagi so'z holatini o'zgarishiga va h. asoslanuvchi usullarni kiritish mumkin.

Raqamli steganografik usullar bir tomondan absolyut aniqlikka muhtoj bo'lmagan fayllarning vazifasini yo'qotmagan holda shaklini bir muncha o'zgartirish mumkinligiga, ikkinchi tomondan bunday fayllardagi bir muncha o'zgarishlarni farqlovchi maxsus asboblarni yo'qligiga yoki inson sezgi organlarining qobiliyatsizligiga asoslangan.

Raqamli steganografik usullar quyidagi turlarni o'z ichiga oladi:

1. Konteynerni tanlash usuli bo'yicha.
2. Axborotdan foydalanish usuli bo'yicha.
3. Konteynerni tashkil etish usuli bo'yicha.
4. Xabarni qayta tiklash usuli bo'yicha.
5. Konteynerni ishlash usuli bo'yicha.
6. Vazifasi bo'yicha.
7. Konteyner turiga ko'ra.
8. Konteynerga axborotni o'rnatish usuli bo'yicha.

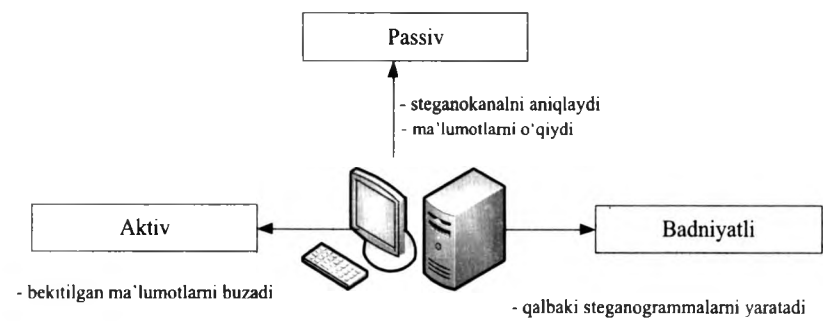
Raqamli steganografik usullarga misol tariqasida LSB-usulni (Least Significant Bits – eng kichik qiymatli bit) ko'rsatish mumkin.

Ushbu usulga binoan fayl-konteynerdagi ma'lumotlar baytining bir necha kichik bitlari bekitiluvchi xabar bitlari bilan almashtiriladi. Ushbu usul amalga oshirilishining soddaligi, demak, ushbu usulga asoslangan dasturiy mahsulotning tezkorligi hamda yaratilgan steganokanalning yuqori o'tkazish qobiliyati bilan bog'liq qator afzalliklarga ega. Ammo ushbu usuldan yuqori steganobardoshlik talab qilinmaydigan masalalarni yechishda foydalanish mumkin. Chunki LSB – usul niyati buzuqning aktiv hujumlariga bardosh bera olmaydi.

Xabarni fayl - konteynerning *spektral sohasida bekituvchi usullar* steganobardosh usullar hisoblanadi. Raqamli steganografiyaning spektral usullari xilma-xil, ba'zilari esa LSB-usul bilan kombinatsiyalab ishlatiladi.

Fayl - konteynerdagi ma'lumotlarni chastotali ifodalashda kosinusni diskret o'zgartirish, Fureni diskret o'zgartirish, veyvlet-o'zgartirish, Karunen-Loev, Adamar va Xaar o'zgartirishlar kabi diskret ortogonal o'zgartirishlardan foydalaniladi.

Steganografik tizimlarda axborotni himoyalash prinsiplari. Steganografik tizimlarni buzuvchi passiv, aktiv va badniyatli bo'lishi mumkin (5.25-rasm).



5.25-rasm. Steganografik tizimlarni buzuvchilar turi.

Passiv buzuvchi faqat stegokanal mavjudligi faktini aniqlashi va o'rnatilgan ma'lumotlarni o'qishi mumkin. Aktiv buzuvchi nafaqat bekitilgan ma'lumotlarni aniqlashi va o'qishi, balki ularni to'laligicha yoki qisman buzishi mumkin. Badniyatli buzuvchi eng

xavfli hisoblanadi, chunki u nafaqat steganogrammani buzadi, balki qalbaki steganogrammani yaratadi.

Buzuvchi (tahlilchi) u yoki bu tahdidni amalga oshirish uchun quyidagi hujumlardan foydalanadi:

- *ma'lum to'ldirilgan konteyner asosidagi hujum.* Buzuvchi bir yoki bir necha steganogrammaga ega va steganokanal mavjudligi faktini aniqlash hamda boshqa steganogrammalarni tahlillash imkoniyati uchun ochiq matnni tiklash yoki kalitni aniqlash topshirig'ini bajaradi;

- *ma'lum o'rnatilgan ochiq matn asosidagi hujum.* Buzuvchi bir necha bekitilgan ochiq matnlar va mos steganogramma namunalari asosida kalitni olish maqsadida mos tahlilni amalga oshiradi. Bunday hujumlar ko'pincha intellektual mulkni himoyalash tizimlariga taalluqli hisoblanadi;

- *tanlangan bekitilgan ochiq matn asosidagi hujum.* Bunda tahlilchi (steganotahlilchi) shaxsiy ochiq matnlarini taklif qilish va steganogrammalarni tahlillash imkoniyatiga ega bo'ladi;

- *tanlangan bekitilgan ochiq matn asosidagi adaptiv hujum.* Ushbu hujum oldingi hujumning xususiy holi hisoblanadi va tahlilchining avvalgi steganogrammalarni tahlillash natijalariga bog'liq holda tiqishtirish uchun xabarni adaptiv tanlash imkoniyati bilan xarakterlanadi;

- *tanlangan to'ldirilgan konteyner asosidagi hujum.* Steganoanalitik steganogramma namunalarini aniqlash maqsadida o'zi tanlagan ochiq matn uchun steganogrammani yaratish imkoniyatiga ega;

- *ma'lum bo'sh konteyner asosidagi hujum.* Bunday steganotahlilchi ma'lum bo'sh konteyner bilan nazarda tutilgan steganogrammani taqqoslash asnosida steganokanal mavjudligini har doim aniqlashi mumkin;

- *tanlangan bo'sh konteyner asosidagi hujum.* Bunda steganotahlilchining xabar jo'natuvchisini tavsiya etilgan konteynerdan foydalanishga majbur etish imkoniyatiga ega bo'lishi shart;

- *konteynerning yoki uning qismining ma'lum matematik modeli asosidagi hujum.* Bunda hujumchi o'rnatilgan shubhali ochiq matnning unga ma'lum modeldan farqini aniqlashga urinadi. Xabar

jo'natuvchisi va hujumchi turli modellarga ega bo'lishi mumkin. U holda yaxshi model egasi yutib chiqadi.

Nazorat savollari:

1. Steganografiyaning axborotni kriptografik himoyalash sohasidagi o'rni.
2. Moddiy steganografik usullarni tushuntirib bering.
3. Axborot steganografik usullarning turlarini tavsiflab bering.
4. Steganografik tizimlarda axborotni himoyalash prinsipini tushuntirib bering.

5.7. Kriptotahlil usullari

Kriptotahlil – shifrlangan matndan maxfiy kalitni (tiklash algoritmini yoki matematik funksiyani) bilmay turib, ochiq matnni (foydali xabarni) olish va tiklash usullari majmui.

Kriptotahlilning muvaffaqiyatli o'tkazilishi natijasida ochiq matn olinishi hamda kriptotizimning zaif joylari aniqlanishi mumkin.

Kriptotahlilni amalga oshirishga urinish *fosh etish* deb yuritiladi. Ochiq matnni kriptotahlil fosh etishning quyidagi xillari mavjud bo'lib, har biriga nisbatan kriptotahlilchining ishlatilgan shifrlash algoritmi xususida to'liq xabardorligi nazarda tutiladi.

1. *Faqat shifrmatn yordamida fosh etish.* Kriptotahlilchi ixtiyorida bir necha xabarning bitta shifrlash algoritmi yordamida shifrlangan shifrmatnlari mavjud. Kriptotahlilchining vazifasi iloji boricha xabarlar katta sonining ochiq matnini fosh etish yoki, yaxshisi, xabarlarni shifrlashda ishlatilgan kalitga (kalitlarga) ega bo'lish.

2. *Ochiq matn yordamida fosh etish.* Kriptotahlilchining ixtiyorida nafaqat bir necha xabarning shifrmatnlari, balki ushbu xabarlarning ochiq matnlari mavjud. Uning vazifasi xabarlarni shifrlashda ishlatilgan kalitga (kalitlarga) ega bo'lish.

3. *Tanlangan ochiq matn yordamida fosh etish.* Kriptotahlilchi ixtiyorida nafaqat shifrmatnlar va bir necha xabarning ochiq matnlari, balki shifrlash uchun ochiq matnni tanlash imkoniyati

mavjud. Uning vazifasi xabarlarni shifrlashda ishlatilgan kalitga (kalitlarga) yoki shu kalit (kalitlar) yordamida shifrlangan yangi xabarlarni deshifratsiyalash imkonini beruvchi algoritmga ega bo'lish.

4. *Tanlangan ochiq matn yordamida adaptiv fosh etish.* Bu tanlangan ochiq matn yordamida fosh etishning xususiy holi. Kriptotahlilchi nafaqat shifrlangan matnni tanlashi, balki shifrlash natijasi asosida o'zining keyingi tanlov rejasini tuzishi mumkin. Tanlangan ochiq matn yordamida fosh etishda kriptotahlilchi shifrlash uchun ochiq matnning faqat bitta katta blokini tanlashi mumkin bo'lsa, tanlangan ochiq matn yordamida adaptiv fosh etishda u ochiq matnning kichik blokini, so'ngra birinchi tanlash natijasidan foydalanib, keyingi blokni va h. tanlashi mumkin.

5. *Tanlangan shifrmatn yordamida fosh etish.* Kriptotahlilchi deshifratsiyalash uchun turli shifrmatnlarni tanlashi mumkin va deshifrlangan ochiq matnlardan foydalana oladi. Masalan, kriptotahlilchi avtomatik tarzda deshifrlashni bajaruvchi "qora quti"dan foydalana oladi. Kriptotahlilchining vazifasi kalitga ega bo'lish.

6. *Tanlangan kalit yordamida fosh etish.* Bu xil fosh etish kriptotahlilchi kalitni tanlashi mumkinligini bildirmaydi, balki unda turli kalitlar orasidagi bog'lanish xususida qandaydir axborot borligini bildiradi.

7. *Jinoiy kriptotahlil.* Kriptotahlilchi kalitga ega bo'lish maqsadida kimnidir qo'rqitadi, shantaj qiladi, qiynaydi. Poraxo'rlik ba'zida kalitni xarid etish yordamida fosh etish deb ataladi. Bu kabi qudratli fosh etish usullari algoritmni sindirishning eng yaxshi yo'li hisoblanadi.

Turli algoritmlarga, ularni sindirishning qanchalik qiyinligiga bog'liq holda, xavfsizlikning turli sathlari taqdim etiladi. Algoritmni quyidagi hollarda xavfsiz deb hisoblash mumkin:

- algoritmni sindirish qiymati shifrlangan ma'lumotlar qiymatidan katta bo'lsa;
- algoritmni sindirish vaqti shifrlangan ma'lumotlarning sir saqlanishi shart bo'lgan vaqtidan katta bo'lsa;
- bitta kalit yordamida shifrlangan ma'lumotlar hajmi algoritmni sindirish uchun zarur ma'lumotlar hajmidan kam bo'lsa.

Fosh etish murakkabligini quyidagi koeffitsientlar yordamida o'lchash mumkin:

- ma'lumotlar murakkabligi. Fosh etish amalining kirish yo'lida foydalaniladigan ma'lumotlar hajmi;
- ishlash murakkabligi. Fosh etish uchun kerakli vaqt. Ko'pincha ish koeffitsienti deb yuritiladi;
- xotiraga talablar. Fosh etishga kerakli xotira sig'imi.

Fosh etishning ba'zi amallari uchun koeffitsientlarning o'zaro aloqasi joiz hisoblanadi: tezroq fosh etishga xotiraga talablarni kuchaytirish evaziga erishish mumkin.

Murakkablik talaygina kattalik orqali ifodalanadi. Muayyan algoritm uchun ishlash murakkabligi 2128 ni tashkil etsa, algoritmni fosh etish uchun 2128 ta amal kerak bo'ladi (ushbu amallar murakkab va davomli bo'lishi mumkin). Masalan, agar hisoblash quvvati sekundiga million amal bajarsa va masalani yechish uchun million parallel protsessor ishlatilsa, kalitga ega bo'lish uchun 1019 yildan ko'proq vaqt talab etiladi. Bu koinot mavjud bo'lgan vaqtdan million marta ko'pdir.

Fosh etish murakkabligi o'zgarmay qolganida kompyuter quvvati oshib boradi. Oxirgi 50 yil mobaynida hisoblash quvvati nihoyatda oshib ketdi va ushbu tendensiya davom etishiga shubha yo'q. Aksariyat kriptografik usullar parallel kompyuterlar uchun yaroqli hisoblanadi: masalan, milliard kichik fragmentlarga ajratiladiki, ularni yechish uchun protsessorlararo ta'sirning keragi bo'lmaydi. Kriptotizimlarni sindirishga bardoshli loyihalashda hisoblash vositalari kelajagini hisobga olish zarur.

Nazorat savollari:

1. Kriptotahlil tushunchasi.
2. Kripotahlil usullarini sanab bering.
3. Tahlillash murakkabligini qanday koeffitsientlar yordamida o'lchash mumkin.

VI BOB. IDENTIFIKASIYA VA AUTENTIFIKATSIYA

6.1. Identifikasiya va autentifikatsiya tushunchasi

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 *indentifikatori* deb yuritiladi. Agar foydalanuvchi tarmoqda ro'yxatga olingan indentifikatorga 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 qilishiga 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'z 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) – subektga 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 nuqtayi 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 birbiriga 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 haqiqiyligini tasdiqlash uchun subyekt tizimga turli axborotni taqdim etadi. Bunday axborot turi "Autentifikatsiya faktori" deb yuritiladi. Autentifikatsiyalashning quyidagi uchta faktori farqlanadi:

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

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

- *qandaydir daxlsiz xarakteristikalar asosida.* Ushbu faktor o'z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko'zining rangdor pardasi va to'r pardasi, barmoq izlari,

kaft geometriyasi va h.) asoslangan usullarni oladi. Bu faktorda kriptografik usullar va vositalar ishlatilmaydi. Beometrik xarakteristikalar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

Subyektning haqiqiyligini tasdiqlash autentifikatsiyaning uchta faktoridan biri yordamida amalga oshirilishi mumkin. Masalan, foydalanuvchini autentifikatsiyalash jarayonida undan parol yoki barmoq izlari so'ralishi mumkin. Autentifikatsiya jarayonida faqat bitta faktor ishlatilsa, bunday autentifikatsiya *bir faktorli* deb yuritiladi.

Autentifikatsiya jarayonida bir necha faktor ishlatilsa, bunday autentifikatsiya *ko'p faktorli* deb yuritiladi. Masalan, autentifikatsiya jarayonida foydalanuvchi smart-kartadan va qo'shimcha paroldan (yoki PIN-koddan) foydalanishi lozim. Ikki faktorli va uch faktorli autentifikatsiya tushunchalari ham ishlatiladi.

NCSC-TG-017 hujjatda ko'p faktorli autentifikatsiya turlari uchun 1,2 xilli, 2,3 xilli va 1,2,3 xilli autentifikatsiya atamalari kiritilgan. 1,2 xilli autentifikatsiya (*bir ikki xilli autentifikatsiya* deb yuritiladi), masalan, autentifikatsiyaning ikki faktorini ishlatadi: birinchi (bir narsani bilish asosida) va ikkinchi (bir narsaga egaligi asosida).

1,2,3 xilli autentifikatsiya (*bir ikki uch xilli autentifikatsiya* deb yuritiladi), autentifikatsiyaning uchta faktorining kombinasiyasini ishlatadi (bir narsa bilish asosida, bir narsaga egaligi asosida va qandaydir daxlsiz xarakteristikalar asosida).

Agar autentifikatsiyalashda bir omilli autentifikatsiya ishlatilsa bunday autentifikatsiya zaif hisoblanadi. Shu sababli, xavfsizlikning yuqori darajasini ta'minlash uchun ko'p faktorli autentifikatsiyadan foydalanish maqsadga muvofiq hisoblanadi.

Bankomatdan foydalanuvchini haqiqiyligini tasdiqlashda ikki faktorli autentifikatsiya keng tarqalgan. Bu bir vaqtda magnit hoshiyali karta va PIN-kod 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 iboraga asoslanuvchi muntazam o'zgarib turuvchi qiymat ishlatiladi.

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

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

Autentifikatsiya jarayonlarini xavfsizlikning ta'minlanish 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 qat'iy autentifikatsiya;
- nullik bilim bilan isbotlash xususiyatiga ega bo'lgan autentifikatsiya jarayonlari (protokollari);
- foydalanuvchilarni biometrik autentifikatsiyasi.

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

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 autenfikatsion almashinish jarayonida trafikni modifikatsiyalash niyatida qatnashadi. Almashtirib qo'yishning quyidagi xili mavjud: ikkita foydalanuvchi o'rtasidagi autentifikatsiya muvaffaqiyatli o'tib, ulanish o'rnatilganidan so'ng buzg'unchi foydalanuvchilardan birini chiqarib tashlab, uning nomidan ishni davom ettiradi;

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

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

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

- *matn tanlashli hujum* (chosen text attack). Niyati buzuq 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 yondashishga 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 nullik bilim bilan isbotlash xususiyatiga ega bo'lgan protokollarni ko'rsatish mumkin;
- *sirni saqlash.* Jiddiy kalitli axborotni saqlash usuli ko'zda tutiladi.

Nazorat savollari:

1. Identifikatsiya va autentifikatsiya tushunchasi.
2. Autentifikatsiya texnologiyasining turlarini tushuntirib bering.
3. Autentifikatsiya protokollariga bo'ladigan hujumlarni tavsiflab bering.
4. Autentifikatsiya protokollarini tanlashda qo'llaniladigan mezonlarni yoritib bering.

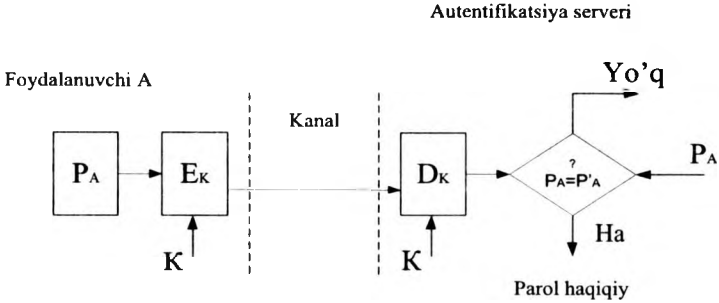
6.2. Parollar asosida autentifikatsiyalash

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 6.1-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.



6.1-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 buzuqning tizimda ma'mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan, parol fayllaridan foydalanish imkoniyatidir.

Xavfsizlik nuqtayi 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 bardoshliligi 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 orqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to'lov plastik kartochkalariga o'xshash mikroprotsessor o'rnatilgan miniatyur qurilmalar ko'rinishda amalga oshiradi. Odatda, kalitlar deb ataluvchi bunday kartalar, klaviaturaga va katta bo'lmagan displey darchasiga ega.

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

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, CiscoSystems 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 vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi, 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, 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 foydalanib 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 hamda 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 nabori 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 autentifikatsiyalash 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 generatoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

- o'zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;
- bir tomonlama funksiyaga asoslangan parollar ketma-ketligi. Ushbu usulning mohiyatini bir tomonlama funksiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik

nuqtayi nazaridan bu usul ketma-ket o'zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

Keng tarqalgan 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.

Nazorat savollari:

1. Ko'p martali parollarga asoslangan autentifikatsiya texnologiyasi.
2. Bir martali parollarga asoslangan autentifikatsiya texnologiyasi.
3. Bir martali parollarni hosil qilishda psevdotasodifiy sonlar generatoridan foydalanish.

6.3. Sertifikatlar asosida autentifikatsiyalash

Tarmoqdan foydalanuvchilar soni millionlab o'lchanganida parollarning 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 alternativa 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 tekshirish va ochiq kalit adresi hamda 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 Communications 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.

Nazorat savollari:

1. Elektron sertifikatlar tarkibiga qanday axborotlarni oladi?
2. Elektron sertifikatlarni afzalliklari va kamchiliklari.
3. Elektron sertifikatlar qaysi asosiy xalqaro standart talablariga javob berishi lozim.

6.4. Qat'iy autentifikatsiyalash

Kriptografik protokollarda 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 uning 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 ishontirish 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 nabori 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 hujumlashni 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 algoritmlari;

- elektron raqamli imzo asosidagi qat’iy autentifikatsiyalash algoritmlari.

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 autentifikatsiyalash protokollaridan foydalaniladi. Bu server bilan har bir taraf kalitni bilishligini o‘rtoqlashishadi.

Ushbu yondashish sodda bo‘lib tuyulsa-da, aslida bunday autentifikatsiyalash protokolini ishlab chiqish murakkab va xavfsizlik nuqtayi nazaridan *shubhasiz emas*.

Quyida shifrlashning simmetrik algoritmlariga asoslangan, ISO/IEC9798-2da spetsifikatsiyalangan autentifikatsiyalash protokollarining 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:

g_A- qatnashuvchi A generatsiyalagan tasodifiy son;

g_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:

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

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 autentifikatsiyalash:

$$A \leftarrow B: r_B$$

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

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:

$$A \leftarrow B : r_B$$
$$A \rightarrow B : E_K(r_A, r_B, B)$$
$$A \leftarrow B : E_K(r_A, r_B)$$

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" va lokal hamda 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 autentifikatsiyalashning asosiy protokoli sifatida o'rnatilganligi alohida qiziqish o'yg'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 bartaraflanishini 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 rasshifrovka 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.

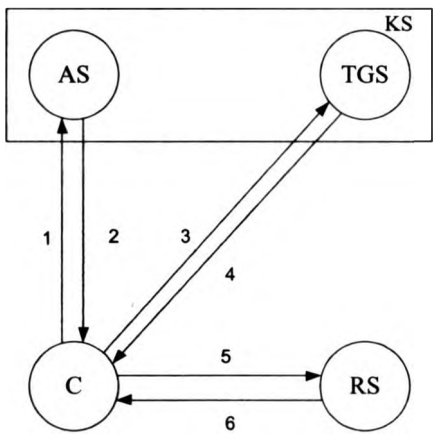
Xaqiqiylikni o'zaro tasdiqlash maqsadida V taraf vaqt belgisi T plyus 1 dan iborat xabar yaratadi, uni K kalit yordamida shifrlaydi va A tarafga jo'natadi:

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

Agar bu xabar rasshifrovka qilingandan 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 (6.2-rasm).



Belgilashlar:
KS – Kerberos tizimi serveri
AS – Autentifikatsiya serveri
TGS – Mandatlarni ajratish tizimi serveri
RS – Axborot resurslari serveri
C – Kerberos tizimi mijozi

6.2-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 (6.2-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 yubora olmaydi va tarmoq xizmatidan foydalanishga ruxsat ololmaydi.

Axborotning ushlab qolinishi va ruxsatsiz foydalanishi imkoniyatlarini bartaraf etish maqsadida, Kerberos tarmoqda har qanday boshqarish axboroti uzatilganida, maxfiy kalitlar kompleksini (mijozning maxfiy kaliti, serverning maxfiy kaliti, mijoz-server juftining maxfiy seans kalitlari) ko'p marta shifrlashni ishlatadi. Kerberos shifrlashning turli algoritmlaridan va xesh-funksiyalardan foydalanishi mumkin, ammo madadlash uchun Triple DES va MD5 algoritmlari o'rnatilgan.

Kerberos tizimida ishonch hujjatlarining ikki turidan foydalaniladi: mandat (tricket) va autentifikator (authentificator).

Mandat serverga mandat berilgan mijozning identifikatsion ma'lumotlarini xavfsiz uzatish uchun ishlatiladi. Uning tarkibida axborot 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 qilolmaydi (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:

$A_{C,S} = \{C, t, калит\}K_{C,S}$

Mijoz maqsadli serverdan foydalanishni xohlaganida autentifikatorni yaratadi. Uning tarkibida mijoz ismi, vaqt belgisi, mijoz va server uchun umumiy bo'lgan, seans kaliti $K_{C,S}$da shifrlangan 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 autentfikatsiyalash muolajasini o'tishda ishlatishiga imkon bermaydi.

Kerberos xabarlari.

Kerberosning 5-versiyasida xabarlarning quyidagi turlari ishlatiladi (6.2-rasmga qaralsin).

1. Mijoz – Kerberos: *C, tgs.*
2. Kerberos – mijoz : $\{K_{c,tgs}\}K_c\{T_{c,tgs}\}K_{tgs}$.
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.

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

Mijoz Kerberosning autentifikatsiya serveriga o'zining ismi, *TGS* serverining (bir nechta server *TGS* bo'lishi mumkin) xabarini 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, demak, u autentifikatsiyalash serverining javobini rasshifrovka qila olmaydi. Shu sababli niyati buzuq odam mandatni yoki seans kalitini ololmaydi. 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* autentifikatorni rasshifrovka qilishda *TGT*dagi seans kalitidan foydalanadi. Nihoyasida autentifikatordagi axborot mandat axboroti bilan taqqoslanadi. Aniqrog'i, chiptadagi mijozning tarmoq adresi so'rovda ko'rsatilgan tarmoq adresi bilan, shuningdek 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 daqiqa 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 xizmatlar bitta mandat, ammo turli autentifikatorlar yordamida ketma-ket bir necha marta so'ralishi mumkin. O'sha mandat va autentifikatorning ishlatilgan vaqt belgisi bilan qilingan so'rov rad qilinadi.

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.

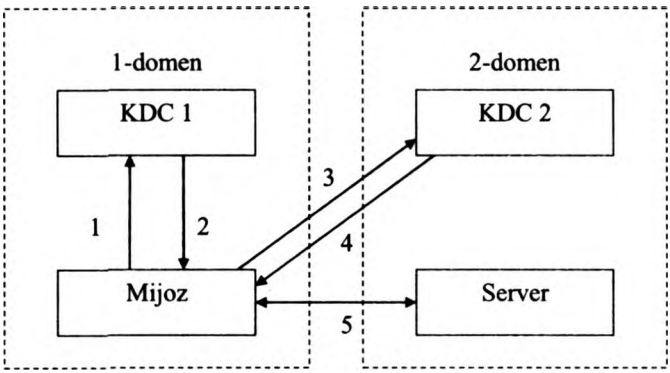
Endi mijoz o'zining haqiqiyligini maqsad serveriga isbotlashi mumkin. Maqsad serverida autentifikatsiyadan muvaffaqiyatli o'tish uchun mijoz tarkibida o'zining ismi, tarmoq adresi, vaqt belgisi bo'lgan va seans kaliti "mijoz-server"da shifrlangan autentifikatorni yaratadi va uni TGS xizmatidan olib berilgan 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 bilan 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* (referalticket) taqdim etadi (6.3-rasm).



6.3-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 sonining domenlar soniga mutanosib ravishda oshishi sababli, so'rovlarni muayyan KDClarga bir ma'noda qayta adreslovchi qandaydir markaziy domen qurishga 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 sirqib chiqishiga olib kelishi mumkin. Hatto kalitlar, foydalanuvchi ishlash seansida faqat operativ 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 hujumlashdan 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

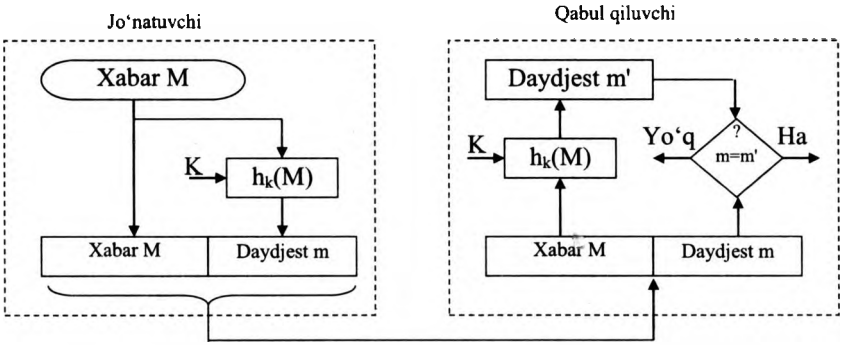
shifrlashning o'ziga xos xususiyati shundaki, u mohiyati bo'yicha bir tomonlamadir, ya'ni teskari o'zgartirish-qabul qiluvchi tarafda rasshifrovka qilish bilan birga olib borilmaydi. Ikkala taraf (jo'natuvchi va qabul qiluvchi) bir tomonlama shifrlash muolajasidan foydalanadi.

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 (6.4-rasm).

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 qaytadan 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.

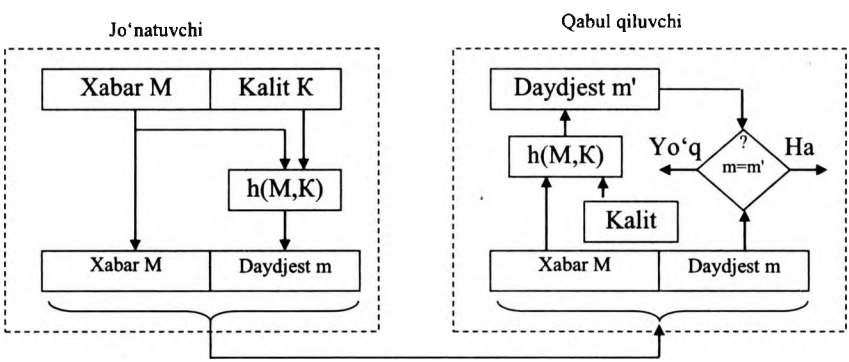
Daydjestni hisoblashda, oddiy nazorat yig'indisidan farqli ravishda, maxfiy kalitlar ishlatiladi. Agar daydjest olinishida faqat jo'natuvchi va qabul qiluvchiga ma'lum bo'lgan parametr-kalitli bir tomonlama xesh-funksiya ishlatilsa, dastlabki xabarning har qanday modifikatsiyasi darhol ma'lum bo'ladi.



6.4-rasm. Ma'lumotlar yaxlitligini tekshirishda bir tomonlama xesh-funksiyaning ishlatilishi (I-variant).

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.

6.5-rasmda ma'lumotlar yaxlitligini tekshirishda bir tomonlama xesh-funksiya ishlatilishining boshqa varianti keltirilgan.



6.5-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'lla-

niladi, 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 bilishni quyidagi usullarning biri yordamida namoyish etishi mumkin:

- ochiq kalitda shifrlangan so'rovni rasshifrovka qilish;
- so'rov so'zining 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, uning nomidan harakat qilganida ham, bardosh berishi lozimligi haqida foydalanuvchilarni ogohlantirishi 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 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. Unday keyin $x=x'$ ekanligini va B' identifikator haqiqatan qatnashuvchi Vga ko'rsatayotganini tasdiqlovchi qator taqqoslashlar bajariladi. Taqqoslash muvaffaqiyatli o'tsa, qatnashuvchi A "r"ni qatnashuvchi V ga uzatadi. Qatnashuvchi B "r"ni

olganidan so'ng, uni birinchi xabarda jo'natgan qiymati 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 Vning ochiq kaliti yordamida shifrlash algoritmi faraz qilinadi. Protokol quyidagi strukturaga 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;
- $cert_A$ – 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 to'g'riligini, olingan identifikator V ni 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.

Nazorat savollari:

1. Qat'iy autentifikatsiyalash muolajalarini tushuntirib bering.
2. Simmetrik algoritmlarga asoslangan qat'iy autentifikatsiyalash sxemasini tushuntirib bering.
3. Kerberos protokolida domenlararo autentifikatsiyalash xususiyatlari nimada?
4. Bir tomonlama kalitli xesh-funksiyalardan foydalanishga asoslangan qat'iy autentifikatsiyalash sxemasini tavsiflang.
5. Asimmetrik algoritmlarga asoslangan qat'iy autentifikatsiyalash protokollari ishlash sxemasini tushuntirib bering.
6. Raqamli imzoga asoslangan qat'iy autentifikatsiyalash protokolini yoritib bering.

6.5. 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 alomatlarning sog'lom shaxsdan ajratib bo'lmasligi;

- biometrik alomatlarni soxtalashtirishning qiyinligi.

Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik alomatlar 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 qismtizimi ishlashining namunaviy sxemasi quyidagicha. Tizimda ro'yxatga olinishida foydalanuvchidan o'zining xarakterli alomatlarini bir yoki bir necha marta namoyish qilinishi talab etiladi. Bu alomatlar 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 nuqtayi nazaridan biometrik autenfikatsiyalash tizimi quyidagi ikkita parametr orqali xarakterlanadi:

- xatolik inkorlar koeffitsienti FRR (false-rejectrate);
- xatolik tasdiqlar koeffitsienti FAR (false-alarmrate).

Xatolik inkor tizim qonuniy foydalanuvchi shaxsini tasdiqlamaganda paydo bo'ladi (odatda FRR qiymati, taxminan, 100 dan birni tashkil etadi). *Xatolik tasdiq* tizim noqonuniy foydalanuvchi shaxsini tasdiqlaganida paydo bo'ladi (odatda FAP qiymati, taxminan, 10000 dan birni tashkil etadi). Bu ikkala koeffitsient bir-biri bilan bog'liq: xatolik inkor koeffitsientining har biriga ma'lum xatolik tasdiq koeffitsienti mos keladi. Mukammal biometrik tizimda ikkala xatolikning ikkala parametri nolga teng bo'lishi shart. Afsuski, biometrik tizim ideal emas, shu sababli nimanidur qurbon qilishga to'g'ri keladi. Odatda tizimli parametrlar shunday sozlanadiki, mos xatolik inkorlar koeffitsientini aniqlovchi xatolik tasdiqlarning istalgan koeffitsientiga 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 qaydlovchi 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.

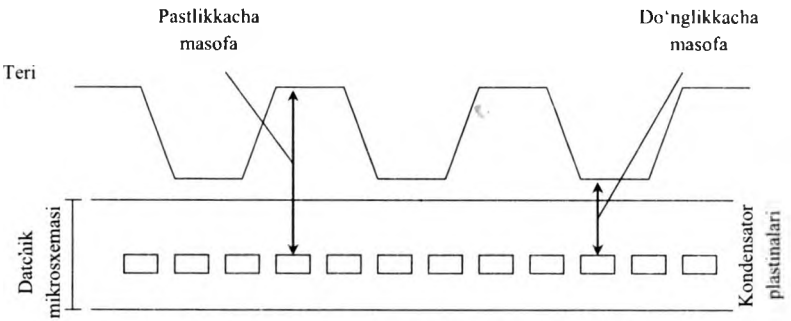
Bunday texnologiyalarni ishlab chiquvchi kompaniyalar barmoq izlarini olishda turli, xususan, elektrik, elektromagnit va boshqa usullarni amalga oshiruvchi vositalardan foydalanadilar.

Skanerlardan biri barmoq izi tasvirini shakllantirish maqsadida teri qismlarining sig'im qarshiligini o'lchaydi. Masalan, Veridicom kompaniyasining daktiloskopik qurilmasi yarim-o'tkazgichli datchik yordamida sig'im qarshiligini aniqlash orqali axborotni yig'adi. Sensor ishlashining prinsipi quyidagicha: ushbu asbobga qo'yilgan barmoq kondensator plastinalarining biri vazifasini o'taydi (6.6-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.

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.



6.6-rasm. Sensor ishlashining prinsipi.

Integral sxemalar asosidagi barmoq izlari datchiklarining kichik o‘lchamlari va yuqori bo‘lmagan narxi, ularni himoya tizimi uchun ideal interfeysga aylantiradi. Ularni kalitlar uchun breloklarga o‘rnatish mumkin. Natijada foydalanuvchi kompyuterdan boshlab to kirish yo‘li, avtomobillar va bankomatlar eshiklaridan himoyali foydalanishni ta’minlaydigan universal kalitga ega bo‘ladi.

Qo‘l panjasining geometrik shakli bo‘yicha autentifikatsiyalash tizimlari. Qo‘l panjasi shaklini o‘quvchi qurilmalar barmoqlar uzunligini, qo‘l panja qalinligi va yuzasini o‘lchash orqali qo‘l panjasining hajmiy tasvirini yaratadi. Masalan, Recognition Systems kompaniyasining mahsulotlari 90 dan ortiq o‘lchamlarni amalga oshiradi. Natijada keyingi taqqoslash uchun 9 xonali namuna shakllantiriladi. Bu natija qo‘l panjasini individual skanerida yoki markazlashtirilgan ma’lumotlar bazasida saqlanishi mumkin. Qo‘l panjasini skanerlovchi qurilmalar narxining yuqoriligi va o‘lchamlarining kattaligi sababli tarmoq muhitida kamdan-kam 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 koeffitsienti, 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 hisoblanali.

Ta'kidlash lozimki, yuz tuzilishini aniqlash texnologiyasi yanada takomillashtirilishni talab etadi. Yuz tuzilishini aniqlovchi aksariyat algoritmlar quyosh yorug'ligi jadalligining kun bo'yicha tebranishi natijasidagi yorug'lik o'zgarishiga ta'sirchan bo'ladilar. Yuz holatining o'zgarishi ham aniqlash natijasiga ta'sir etadi. Yuz holatining 45^0 ga o'zgarishi aniqlashni samarasiz bo'lishiga olib keladi.

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

ba'zi chegaralanishlarga ega. Turli odamlar o'xshash ovozlar bilan gapirishi mumkin, har qanday odamning ovozi vaqt mobaynida kayfiyati, hissiyotlik holati va yoshiga bog'liq holda o'zgarishi mumkin. Uning ustiga telefon apparatlarning turli-tumanligi va telefon orqali bog'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.

Nazorat savollari:

1. Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik alomatlar.
2. Biometrik autentifikatsiyalashning daktiloskopik tizimi ishlash sxemasini tushuntirib bering.
3. Qo'l panjasining geometrik shakli bo'yicha autentifikatsiyalash tizimlarini tushuntirib bering.
4. Yuz tuzilishi bo'yicha autentifikatsiyalash tizimlarining ishlash prinsipini tushuntirib bering.
5. Ovoz bo'yicha autentifikatsiyalash tizimlari xususiyatlari.
6. Ko'z yoyi to'r pardasining naqshi bo'yicha autentifikatsiyalash tizimini yoritib bering.

VII bob. KOMPYUTER VIRUSLARI VA ZARARKUNANDA DASTURLAR BILAN KURASHISH MEXANIZMLARI

7.1. 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'hshash.

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.

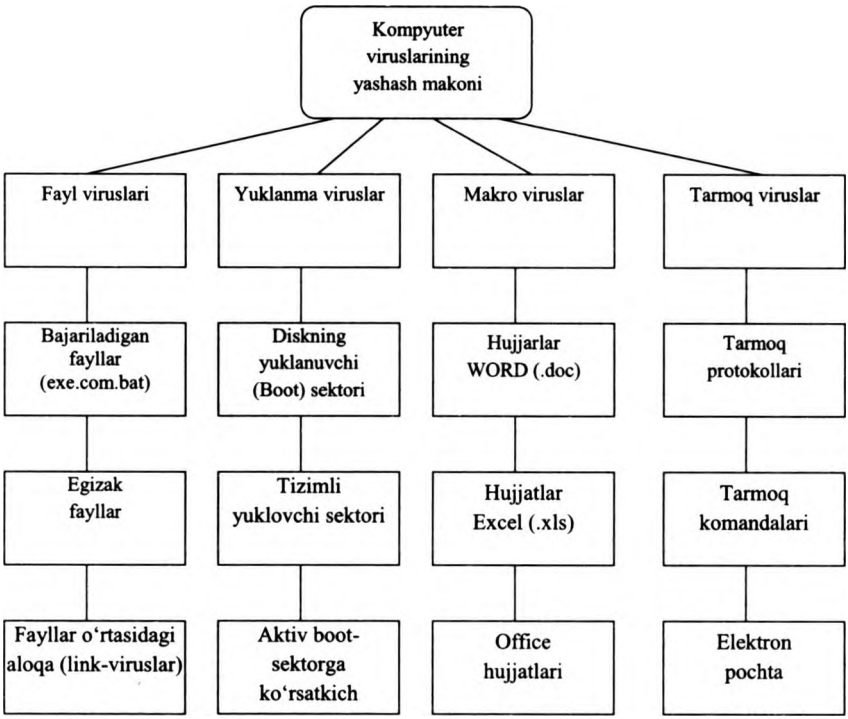
Ta'kidlash lozimki, bu xususiyatlar zaruriy, ammo yetarli emas. Ko'rsatilgan xususiyatlarni hisoblash muhitidagi zarar keltiruvchi dastur ta'sirining destruktivlik va sir boy bermaslik xususiyatlari bilan to'ldirish lozim.

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 (7.1-rasm).



7.1-rasm. Yashash makoni bo'yicha kompyuter viruslarining turkumlanishi.

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko'p tarqalgan viruslar xili), yoki fayl-yo'ldoshlarni (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 (MasterBootRecord) 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, InternetRelayChat) bo'linadi.

Kompyuter viruslarining ko'pgina kombinatsiyalangan xillari ham mavjud, masalan – tarmoqli makrovirus tahrirlanuvchi hujjatlarni zaxarlaydi 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 hayot 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 operativ xotiraga nusxalash bo'lib, so'ngra boshqarish virus badani 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 harakatlarni 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 qismini 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 kodni "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. Polimorf 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 bekitishlari 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 operativ xotiradan bo'shaladi. 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. Yuklanuchi 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 dasturining birinchi komandasi (*com*) yoki fayl sarlavhasini (*exe*) modifikatsiyalash orqali ta'minlanadi.

3. Fayl o'rtasiga kiritish. Odatda, bu usuldan viruslar strukturasi oldindan ma'lum fayllarga (masalan, *Command.com* fayli) yoki tarkibida bir xil qiymatli baytlar ketma-ketligi bo'lgan, uzunligi virus joylashishiga yetarli fayllarga tatbiqan foydalaniladi.

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 kamaytirsa-da, 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'tkazish 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'rilovchi 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'rilashda 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 kelganida, 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 qaerdan xavf tug'ilishini 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 kataloglaridan, 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 MicroSoftWord, 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 makroviruslarni tarqatish kanali vazifasini o'taydi, chunki axborot 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 nusxalari hisoblanadi. Disketlar va CD-disklardagi noqununiy nusxalarda ko'pincha turli-tuman viruslar bilan zaharlangan fayllar bo'ladi. Viruslarni tarqatish manbalariga elektron anjumanlar va FTP va BBS fayl-serverlar ham taalluqli.

O'quv yurtlarida va Internet-markazlarida o'rnatilgan va umumfoydalanish 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 tizimlariga 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.

Nazorat savollari:

1. Kompyuter virusi va zarar keltiruvchi dasturlar tushunchasi.
2. Kompyuter viruslarini qaysi asosiy alomatlariga ko'ra turkumlash mumkin?
3. Kompyuter virusini bajarilish davri qanday bosqichlarni o'z ichiga oladi?
4. Zarar keltiruvchi dastur turlarini va ularning ishlash prinsipini tushuntirib bering.
5. Kompyuter viruslari va zarar keltiruvchi dasturlarni tarqalish kanallarini tushuntirib bering.

7.2. 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 hamda 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 bajari-

luvchi shubhali harakatlarni monitoringlovchi virusga qarshi dastur doimo bo'ladi. Virusga qarshi monitoring barcha ishga tushiriluvchi dasturlarni, yaratiluvchi, ochiluvchi va saqlanuvchi hujjatlarni, Internet orqali olingan, disketdan yoki har qanday kompakt-diskdan nusxalangan dastur va hujjatlarning fayllarini tekshirishga imkon beradi. Agar qandaydir dastur xavfli harakat 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 dastur xillari. Virusga qarshi dasturlarning quyidagi 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 ancha-

gina 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 operativ xotira va fayllarni skanerlash yo'li bilan muayyan virusga xarakterli bo'lgan niqobni qidiradi. Dastur-faglar nafaqat viruslar bilan zaharlangan fayllarni topadi, balki ularni davolaydi ham, ya'ni fayldan dastur-virus badanini olib tashlab, faylni dastlabki holatiga qaytaradi. Dastur-faglar avval operativ 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 MSWORD va Excel muhitlarida hujjat almashinish tizimini himoyalashda eng qulay va ishonchli ychim 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. Monitoringlashning rezident vositalari tizimni ishonchliroq himoyalashni 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 tezda 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 modifykatsiyasi 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 yuklanishidan 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 har doim 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 no'malum 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 hatto eng yaxshi virusga qarshi dastur skanerlash jarayonini oxirigacha olib bora olmasa, u befoyda hisoblanadi;

- viruslarni barcha tarqalgan xillarini aniqlash fazilati, ichki fayl-hujjatlar/jadvallarni (MSOffice), joylashtirilgan va arxivlangan fayllarni skanerlash, virusga qarshi dasturning asosiy vazifasi-100% viruslarni aniqlash va ularni davolash;

- barcha ommaviy platformalar (DOS, Windows 95/NT, NovellNetWare, 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 foydalanishi 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 mutloq 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 oldin bu disketda virus borligini o'zining kompyuteridagi virusga qarshi dastur yordamida doimo tekshirish;

- axborotni ikkilash. Avvalo dasturiy ta'minotning distributiv eltuvchilarini saqlashga va ishchi axborotning 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:

- OfficeGuard – blokirovka qiluvchi, makrovirusdan 100% himoyalanishni 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;
- 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 Spider Guard, Internet orqali virus bazalarini yangilashning avtomatik tizimi va avtomatik tekshirish jadvalini rejalashtiruvchi mavjud. Pochta fayllarini tekshirish amalga oshirilgan. Dr.Webda ishlatiluvchi algoritmlar haqida ma'lum bo'lgan barcha virus xillarini aniqlashga imkon beradi. Dr.Web dasturining muhim xususiyati – oddiy signaturali qidirish natija bermaydigan murakkab shifrlangan va polimorf viruslarni aniqlash imkoniyatidir;
- Symantec Antivirus – Symantec kompaniyasining korporativ foydalanuvchilarga taklif etgan virusga qarshi mahsuloti nabori. Symantec mahsulotidan ishchi joylarining umumiy soni 100 va undan ortiq bo'lganida, shuningdek, 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 qo'riqchi;
- boshqarish dasturi;
- rejalashtiruvchi.

Dastur Internet dan yuklanuvchi fayllarni skanerlaydi. Internet orqali yangilanishlarni avtomatik tarzda tekshirish va yuklash funksiyasi ham mavjud. Dastur xotirani, yuklanish sektorini tekshirishda ishlatiladi va unda viruslar bo'yicha keng ko'lamdagi ma'lumotnoma mavjud.

Nazorat savollari:

1. Kompyuter viruslarini aniqlashning asosiy usullari nimalardan iborat?
2. Virusga qarshi dastur turlari va ularning ishlash prinsipi.
3. Virusga qarshi dasturlarning sifatini baholovchi mezonlarni sanab bering.
4. Virusga qarshi himoyaning profilaktika choralarini tushuntirib bering.

7.3. Virusga qarshi himoya tizimini qurish

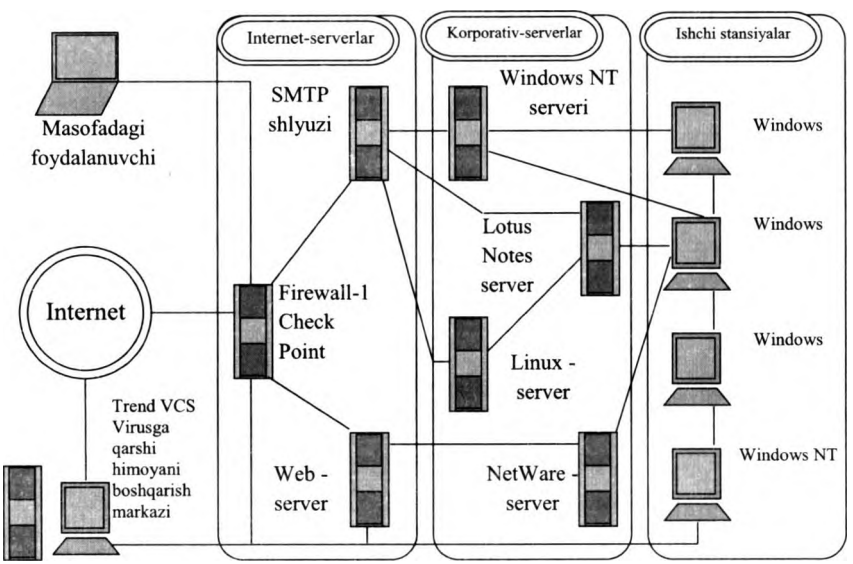
Hozirda o'rtacha kompaniyaning korporativ kompyuter tarmog'i tarkibida o'nlab va yuzlab ishchi stansiyalari, o'nlab serverlar, telekommunikatsiyaning turli faol va passiv asbob-uskunalari mavjud bo'lgan yetarlicha murakkab strukturaga ega (7.2-rasm).

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, muammoni 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.

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 moslanuvchan tizimdir. Bunday tizim korporativ tarmoqning ichki strukturasi doirasida viruslarni va boshqa g'anim dasturlarning tarqalishiga yo'l qo'ymaydi. Virusga qarshi himoyaning samarali korporativ tizimi turli virus hujumlarini-ma'lum va noma'lumlarini, ular namoyon bo'lishining dastlabki bosqichida aniqlaydi va betaraflashtiradi.



7.2–rasm. Korporativ tarmoqning namunaviy arxitekturasi.

Albatta, turli vaziyatlar bo'lishi mumkin, masalan, masofadan foydalanuvchining zaharlangan kompyuterining korporativ serverga ulanishida 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 kamdan-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 oshib boradi. Korporativ tarmoqni viruslardan himoyalash xarajatlari korxona umumiy xarajatlari ro'yxatida oxirgi bandini 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;
- Internetdan Web yoki FTP 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 hamda 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.

Nazorat savollari:

1. Virusga qarshi himoyaga ega korporativ tarmoqning namunaviy arxitekturasini tushuntirib bering.
2. Virus va zarar keltiruvchi dasturlardan himoyalovchi korporativ tizimni qurishda bajariladigan himoyalash variantlarini tanlashning mohiyatini tushuntirib bering.
3. Virus va zarar keltiruvchi dasturlardan himoyalovchi korporativ tizimni qurishda bajariladigan virusga qarshi siyosatni ishlab chiqish afzalligi.
4. Virus va zarar keltiruvchi dasturlardan himoyalovchi korporativ tizimni qurishda bajariladigan axborot kommunikatsiya resurslarini inventarizatsiyalash va monitoringlash jarayonini yoritib bering.
5. Virus va zarar keltiruvchi dasturlardan himoyalovchi korporativ tizimni qurishda bajariladigan xavfizlik rejasini amalga oshirish jarayonini tushuntirib bering.

VIII BOB. AXBOROTNI HIMOYALASHDA TARMOQLARARO EKRANLARNING O'RNI

8.1. Tarmoqlararo ekranlarning ishlash xususiyatlari

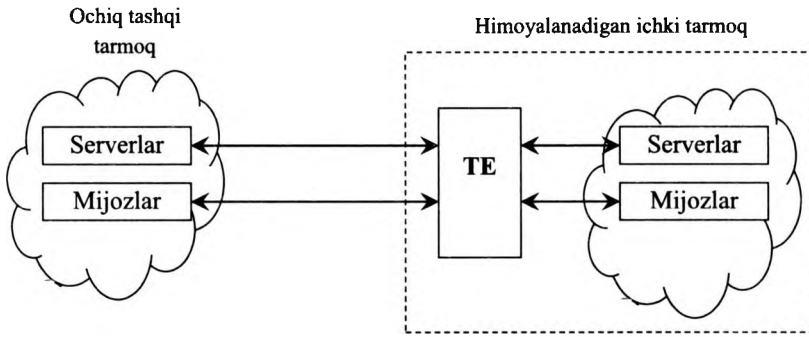
Tarmoqlararo ekran (TE) - *brandmauer* yoki *firewall sistemasi* deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko'p qismlarga ajratish va ma'lumot paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o'tish 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 ishlatilishi 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 (8.1-rasm). Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtayi nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi.

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.



8.1-rasm. Tarmoqlararo ekranni ulash sxemasi.

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 sath shlyuzi (application gateway);
- ekspert sathi shlyuzi (stateful inspection firewall).

Ishlatiladigan texnologiya bo'yicha:

- protokol holatini nazoratlash (Stateful inspection);
- vositachilar modullari asosida (proxy);

Bajarilishi bo'yicha:

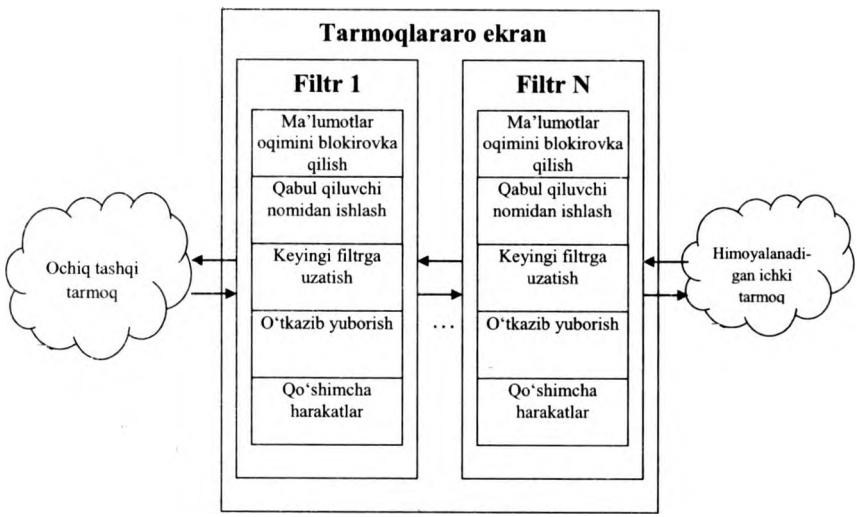
- apparat-dasturiy;
- dasturiy;

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 (8.2-rasm).



8.2-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 qilish:

- 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 hamda 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 kesh xotiraga saqlash;
- xabarlar oqimini filtrlash va o'zgartirish, masalan, viruslarni dinamik tarzda qidirish va axborotni shaffof shifrlash;
- foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;
- ichki tarmoq adreslarini translyatsiyalash;
- 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, ActiveXControls) autentifkatsiyalash 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 hamda 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 vositachi-dasturlarning 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.

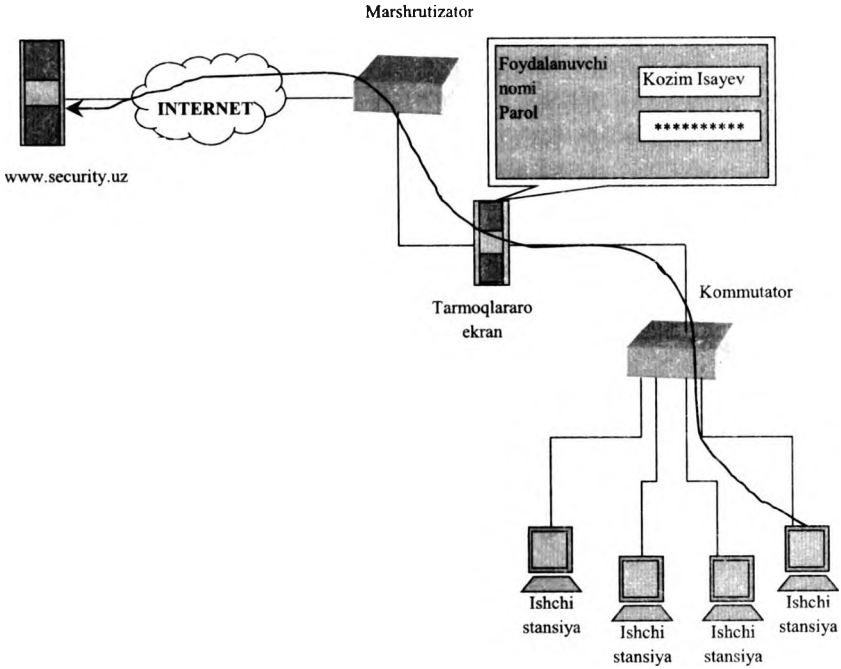
Foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash ba'zida oddiy identifikatorni (ism) va parolni taqdim etish bilan amalga oshiriladi (8.3-rasm). Ammo bu sxema xavfsizlik nuqtayi nazaridan zaif hisoblanadi, chunki parolni begona shaxs ushlab qolib, ishlatishi mumkin. Internet tarmog'idagi 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.

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 autentifikatsiyalanadi. Bundan keyin ma'mur belgilagan 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 autentifikatsiyalanmagan 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.



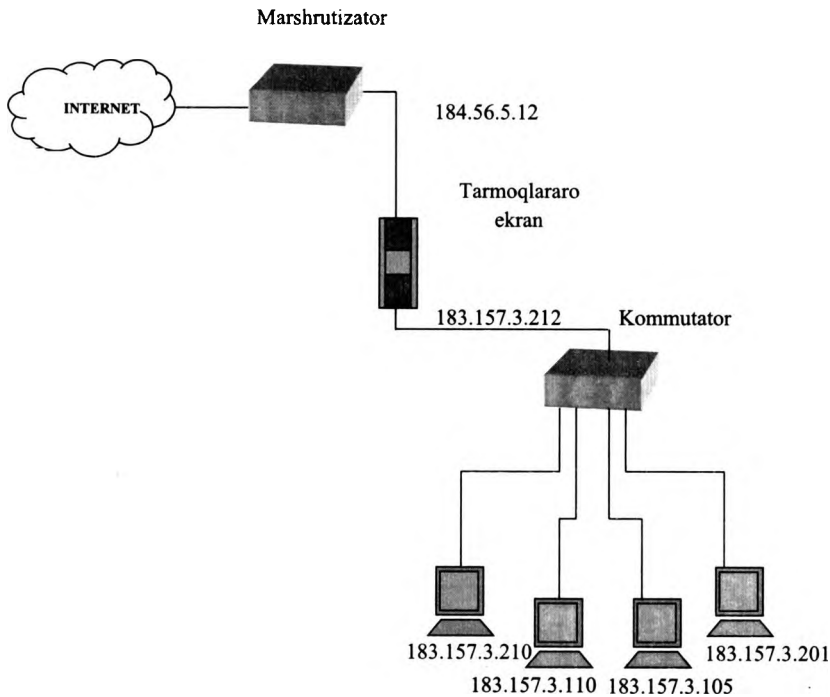
8.3-rasm. Parol bo‘yicha foydalanuvchini autentifikatsiyalash sxemasi.

Ichki tarmoq adreslarini translyatsiyalash. Ko‘pgina hujumlarni amalga oshirishda niyati buzuq odamga qurbonining adresini bilish kerak bo‘ladi. Bu adreslarni hamda butun tarmoq topologiyasini bekitish uchun tarmoqlararo ekranlar eng muhim vazifani – ichki tarmoq adreslarini translyatsiyalashni bajaradi (8.4-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 translyatsiyalash 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.



8.4-rasm. Tarmoq adreslarini translatsiyalash.

Bunday yondashishda ichki tarmoq topologiyasi tashqi foydalanuvchilardan yashiringan, demak, ruxsatsiz foydalanish masalasi qiyinlashadi. Adreslarni translyatsiyalash tarmoq ichida tashqi tarmoq, masalan, Internetdagi adreslash bilan kelishilmagan adreslashning xususiy tizimiga ega bo'lishiga imkon beradi. Bu ichki tarmoq-

ning adres makonini kengaytirish va tashqi adres tanqisligi muammosini samarali yechadi.

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 foydalanish qoidasini o'zgartirish va h. ham taalluqli. Bunday ro'yxatga olish zaruriyat tug'ilganda (xavfsizlik mojarosi paydo bo'lganida, 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 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 bardoshliligini aniq bilish va tarmoqlararo ekranni himoyalash tadbirlarining adekvatligini aniqlash lozim. Undan tashqari, tarmoqdan foydalanish statistikasi tarmoq asbob-uskunalari dasturlariga talablarni ifodalash maqsadida xavf-xatarni tadqiqlash 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'lma-

gan tarmoqlararo ekranni tarmoqlararo himoyaning samarali vositasi deb bo'lmaydi.

Nazorat savollari:

1. Tarmoqlararo ekran vositalari tushunchasi va uning vazifalari.
2. Tarmoqlararo ekranlarning OSI modeli sathlari bo'yicha turkumlanishi.
3. Trafiklarni filtrlash funksiyasining ishlashini tushuntirib bering.
4. Tarmoq adreslarini translyatsiyalash qanday amalga oshiriladi?
5. Tarmoqlararo ekranlarning vositachilik funksiyalarining mohiyati nimadan iborat?

8.2. 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.

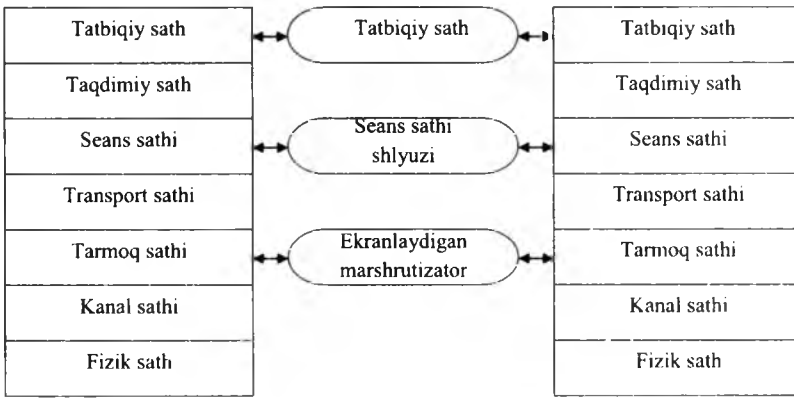
Ekranlar kompleksi ko'pincha etalon modelning tarmoq, seans, tatbiqiy sathlarida ishlaydi. Mos holda, quyidagi bo'linmaydigan brandmauerlar farqlanadi (8.5-rasm).

- 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 bekitilgan ma'lumotlarni avtomatik tarzda rasshifrovka qilishni amalga

oshirishi mumkin. Bu holda, bunday ekran OSI modelining nafaqat tatbiqiy sathida, balki taqdimiy sathida ham ishlaydi.

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.



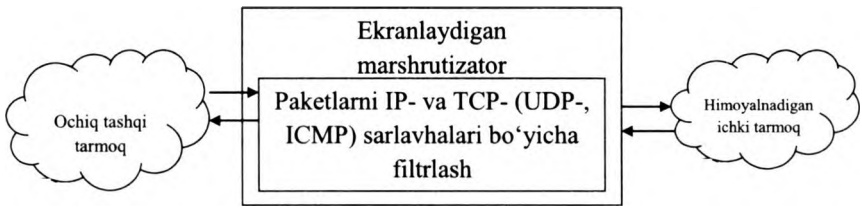
8.5-rasm. OSI modelining alohida sathlarida ishlaydigan tarmoqlararo ekranlar turi.

Yuqorida keltirilgan tarmoqlararo ekranlarning 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 (screeningrouter) (paketli filtr (packetfilter) 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 brakka 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 (8.6-rasm).



8.6-rasm. Paketli filtrning ishlash sxemasi.

Har bir paketning IP- va TCP/UDP – sarlavhalarining tahlil-lanuvchi hoshiyalari sifatida quyidagilar ishlatilishi mumkin:

- jo'natuvchi adresi;
- qabul qiluvchi adresi;
- paket xili;
- paketni fragmentlash bayrog'i;
- manba porti nomeri;
- qabul qiluvchi port nomeri.

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 fragment-langan IP-paketning qismpaketi 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. Portlar 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 nuqtayi nazaridan, uni yaroqsiz holga chiqaradi.

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 hamda chiqishda paketlarni filtrlashi mumkin.

Paketli filtrlarning kamchiligi sifatida quyidagilarni ko'rsatish mumkin. Ular xavfsizlikning yuqori darajasini ta'minlamaydi, chunki faqat paket sarlavhalarini tekshiradi va ko'pgina kerakli funksiyalarni madadlamaydi. Bu funksiyalarga, masalan, oxirgi uzellarni autentifikatsiyalash, xabarlar paketlarini kriptografik bekitish 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 sarlavhalarini 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 translyatsiyalashga atalgan. U OSI modelining seans sathida ishlaydi va ishlashi jarayonida etalon modelning transport va tarmoq sathlarini ham qamrab oladi. Seans sathi shlyuzining himoyalash funksiyalari vositachilik funksiyalariga taalluqli.

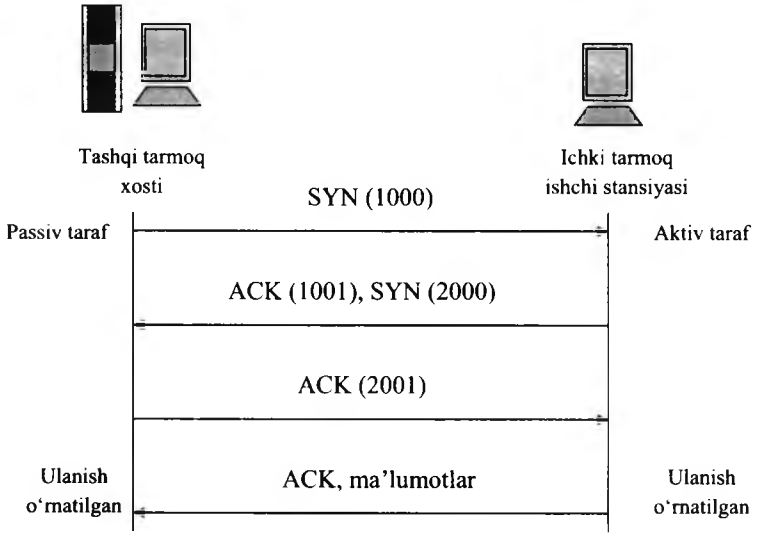
Virtual ulanishlarning nazorati aloqani kvitirlashni kuzatishdan hamda o'rnatilgan virtual kanallar bo'yicha axborot uzatilishini nazoratlashdan iborat. Aloqani kvitirlashning nazoratida seans sathida shlyuz ichki tarmoq ishchi stansiyasi va tashqi tarmoq kompyuteri orasida virtual ulanishni kuzatib, 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 kvirtirlash 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.

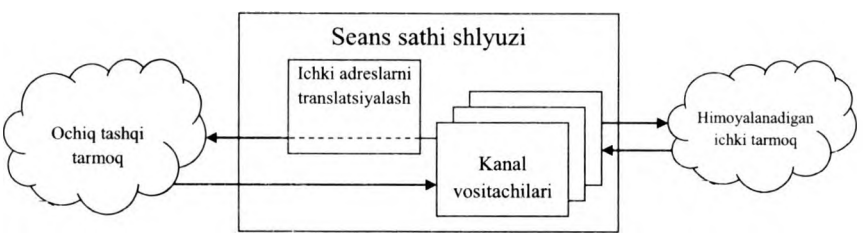
Bu muolaja SYN (Sinxronlash) va ACK (Tasdiqlash) bayroqlari orqali belgilanuvchi TCP-paketlarni almashishdan iborat (8.7-rasm).

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 kvirtirlash jarayoni tugallanadi.



8.7-rasm. TCP protokoli bo'yicha aloqani kvitirlash sxemasi.

Seans sathi shlyuzi (8.8-rasm) uchun so'ralgan seans joiz hisoblanadi, qachonki aloqani kvirtirlash jarayoni bajarilishida SYN va ACK bayroqlar hamda TCP-paketlari sarlavhalaridagi sonlar o'zaro mantiqiy bog'langan bo'lsa.



8.8-rasm. Seans sathi shlyuzining 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 ulanishlarining 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 axboroti to'planishi ham mumkin.

Seans sathi shlyuzlarida virtual ulanishlarni nazoratlashda *kanal vositachilari* (pipeproxy) deb yuritiluvchi maxsus dasturlardan foydalaniladi. Bu vositachilar ichki va tashqi tarmoqlar orasida virtual kanallarni o'rnatadi, so'ngra TCP/IP ilovalari generatsiyalagan 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) translyatsiyalashni ham ta'minlaydi. Ichki adreslarni translyatsiyalash ichki tarmoqdan tashqi tarmoqqa jo'natiluvchi barcha paketlarga nisbatan bajariladi.

Amalga oshirilishi nuqtayi nazaridan seans sathi shlyuzi yetarlicha oddiy va nisbatan ishonchli dastur hisoblanadi. U ekranlovchi marshrutizatorni virtual ulanishlarni nazoratlash va ichki IP-adreslarni translyatsiyalash 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 (TCPhijacking) ushlab

qolinishida niyati buzuq odam hujumlarini hatto ruxsat berilgan sessiya doirasida amalga oshirishi mumkin.

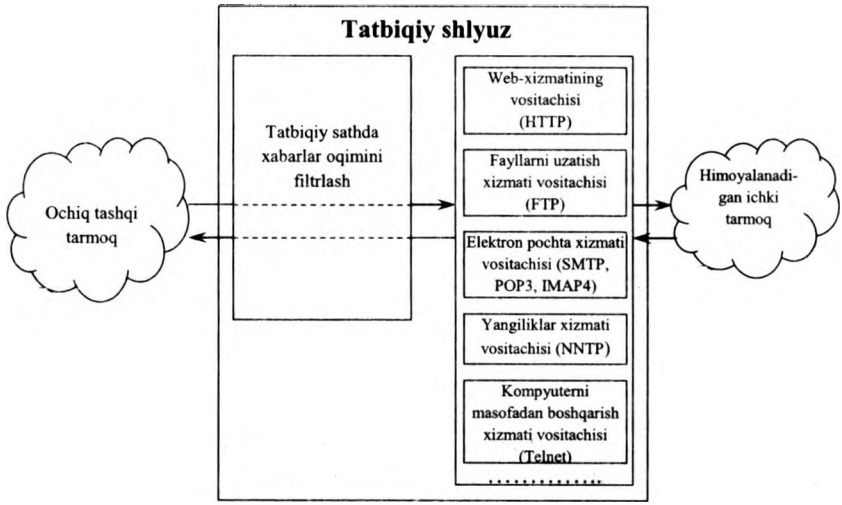
Amalda aksariyat seans sath shlyuzlari mustaqil mahsulot bo'lmay, tatbiqiy sath shlyuzlari bilan komplektda taqdim etiladi.

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 cheklash;
- axborot 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 (applicationproxy) 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 (8.9-rasm).



8.9-rasm. Tatbiqiy shlyuzning ishlash sxemasi.

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.

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 translyatori 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 cheklashlar, 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 qo'yiladigan 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 vosi-

tachi 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 harajat sarflanadi.

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* (statefulinspection) 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 afzallik: 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 FireWall-1 va ON Guardlarni ko'rsatish mumkin.

Nazorat savollari:

1. Ekranlovchi marshrutizatorlarning ishlash prinsipini tushuntirib berin.
2. Seans sathi shlyuzining funksiyalarini yoritib bering.
3. Tatbiqiy sath shlyuzi qanday tartibda ishlashini tushuntirib bering.
4. Ekranlovchi marshrutizatorlar, seans sathi shlyuzi va tatbiqiy sath shlyuzi qo'llaydigan funksiyalarning bir-biridan farqi nimada?

8.3. 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 tarmog'ining 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 cheklashlar ham beriladi. Bu cheklashlar foydalanuvchilarning Internetning 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, har qanday 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 nuqtayi nazaridan yaxshiroq hisoblanadi. Mohiyati bo'yicha "oshkora ruxsat etilmagani man qilingan" prinsipi 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 tarmoqlararo 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 cheklovchi 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 cheklash, shuningdek, 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 bekitishga manfaatdor. Masofadagi foydalanuvchilar bilan ishlash himoyalanuvchi tarmoq resurslaridan foydalanishning qat'iy cheklanishini 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 qismtarmoqli 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 (8.10-rasm).

Ekranlovchi marshrutizator (paketli filtr) kiruvchi va chiquvchi paketlarni ularning adreslari va portlari asosida blokirovka qilish va filtrlash uchun konfiguratsiyalangan.

8.10-rasm. Tarmoqlararo ekran – ekranlovchi marshrutizator.

Himoyalanuvchi tarmoqdagi kompyuterlar Internetdan to'g'ridan-to'g'ri foydalana oladi, 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, kirish va chiqish yo'li portlari nomeri bo'yicha filtrlamasa, "oshkora ruxsat etilmagani man qilingan" siyosatini amalga oshirish qiyinlashadi.

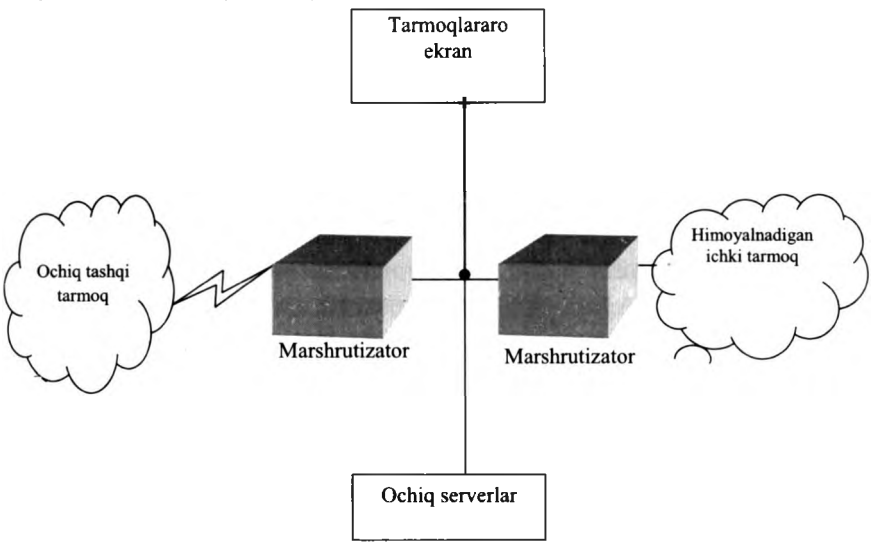
Paketlarni filtrlashga asoslangan tarmoqlararo ekranning kamchiliklari quyidagilar:

- 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.

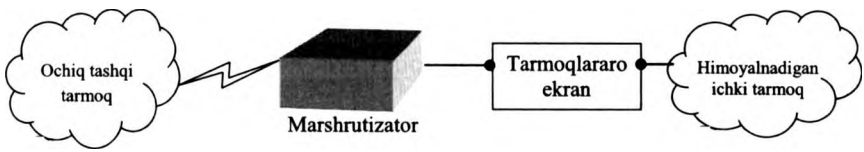
Lokal tarmoqni umumiy himoyalash sxemalari. Bitta tarmoq interfeysli brandmauerlardan foydalanilgan himoyalash sxemalari (8.11-rasm) xavfsizlik va konfiguratsiyalashning qulayligi nuqtayi nazaridan samarasiz hisoblanadi. Ular ichki va tashqi tarmoqlarni fizik ajratmaydilar, demak, tarmoqlararo aloqaning ishonchli himoyasini ta'minlay olmaydilar.



8.11- rasm. Bitta tarmoq interfeysli firewall yordamida lokal tarmoqni himoyalash.

Lokal tarmoqni umumiy himoyalash sxemasi eng oddiy yechim bo'lib, unda brandmauer lokal tarmoqni tashqi g'anim tarmoqdan butunlay ekranlaydi (8.12-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.

Lokal tarmoq tarkibidagi ochiq serverlar ham tarmoqlararo ekranlar tomonidan himoyalanadi. Ammo, tashqi tarmoq foydalana oladigan serverlarni himoyalanuvchi lokal tarmoqlarning boshqa resurslari bilan birlashtirish, tarmoqlararo aloqa xavfsizligini jiddiy pasaytiradi.



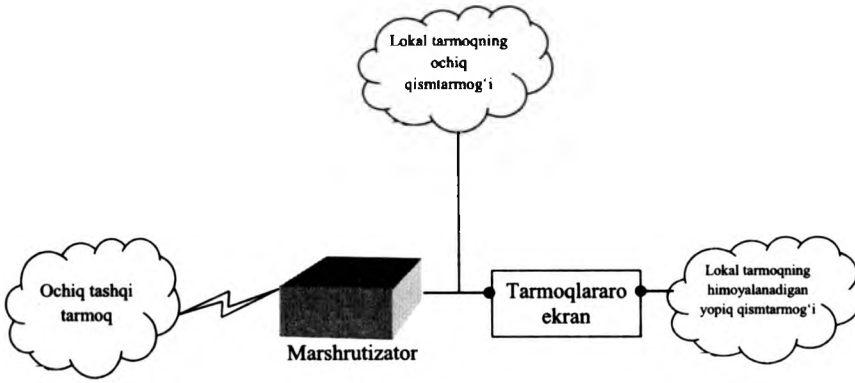
8.12-rasm. Lokal tarmoqni umumiy himoyalash sxemasi.

Tarmoqlararo ekran foydalanadigan xostga foydalanuvchilarni kuchaytirilgan autentifikatsiyalash uchun dastur o'rnatilishi mumkin.

Himoyalanuvchi yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemalar. Agar lokal tarmoq tarkibida umumfoydalanuvchi ochiq serverlar bo'lsa, ularni tarmoqlararo ekrandan oldin ochiq qismtarmoq sifatida chiqarish maqsadga muvofiq hisoblanadi (8.13-rasm).

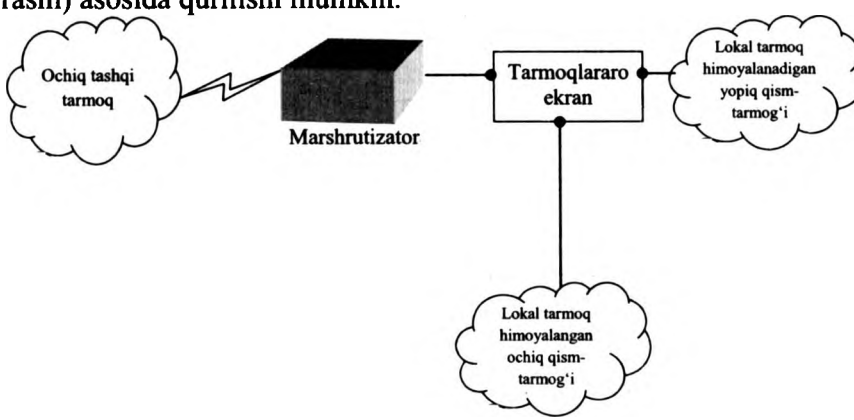
Ushbu usul lokal tarmoq yopiq qismining kuchli himoyalanishini, ammo tarmoqlararo ekrangacha joylashgan ochiq serverlarning pasaygan himoyalanishini ta'minlaydi.

Ba'zi brandmauerlar bu serverlarni o'zida joylashtiradi. Ammo bu brandmauerning xavfsizligi va kompyuterning yuklanishi nuqtai nazaridan yaxshi yechim hisoblanmaydi. Himoyalanuvchi yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemani ochiq qismtarmoq xavfsizligiga qo'yiladigan talablarning yuqori bo'lmagan hollarida ishlatilishi maqsadga muvofiq hisoblanadi. Agar ochiq server xavfsizligiga yuqori talablar qo'yilsa, yopiq va ochiq qismtarmoqlarni alohida himoyalash sxemalaridan foydalanish zarur.



8.13-rasm. Himoyalanadigan yopiq va himoyalanmaydigan ochiq qismtarmoqli sxema.

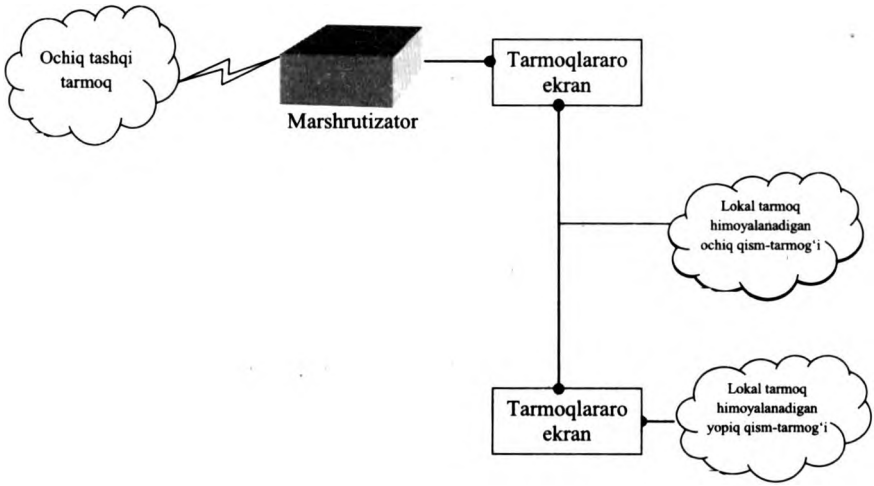
Yopiq va ochiq qism tarmoqlarni alohida himoyalovchi sxemalar. Bunday sxemalar uchta tarmoq interfeysli bitta brandmauer (8.14-rasm) yoki ikkita tarmoq interfeysli ikkita brandmauer (8.15-rasm) asosida qurilishi mumkin.



8.14 -rasm. Uchta tarmoq inte... bir brandmauer asosida yopiq va ochiq qimstarmoqlarni alohida himoyalash sxemasi.

Ikkala holda ham ochiq va yopiq qismtarmoqlardan faqat tarmoqlararo ekran orqali foydalanish mumkin. Bunda ochiq qismtar-

moqdan foydalanish yopiq qismtarmoqdan foydalanishga imkon bermaydi.



8.15-rasm. Ikkita tarmoq interfeysli ikkita brandmauer asosida yopiq va ochiq qismtarmoqlarni alohida himoyalash sxemasi.

Ikkita brandmauerli sxema tarmoqlararo aloqa xavfsizligining yuqori darajasini ta'minlaydi. Bunda har bir brandmauer yopiq tarmoqni himoyalashning alohida eshelonini hosil qiladi, himoyalanuvchi ochiq qismtarmoq esa ekranlovchi qismtarmoq sifatida ishtirok etadi. Odatda ekranlovchi qismtarmoq shunday konfiguratsiyalanadiki, qismtarmoq kompyuteridan g'anim tashqi tarmoq va lokal tarmoqning yopiq qismtarmog'i foydalana olsin. Ammo tashqi tarmoq va yopiq qismtarmoq orasida to'g'ridan-to'g'ri axborot paketlarini almashish mumkin emas. Ekranlovchi qismtarmoqli tizimga 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 ulashni shunday amalga oshirish lozimki, uning ishi faqat tarmoqlararo ekran orqali bajarilsin. Bu masofadagi foydalanuvchilarning tashkilot axborot resurslari bilan ishlash xavfsizligining kerakli darajasini ta'minlashga imkon beradi.

Terminal serverni ochiq qismtarmoq 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 serverning o'zini xavfsizligini ta'minlash va mijozlarning 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. Yaqin vaqtgacha bunday chegara barcha marshrutizatorlar yoki boshqa qurilmalar (masalan, modemlar) orqali o'tar va ular yordamida tashqi tarmoqlarga chiqilar edi. Ammo hozirda tarmoqlararo ekran orqali himoya-

lanuvchi tarmoqning to'la huquqli egasi – himoyalanuvchi perimetr tashqarisidagi xodim hisoblanadi. Bunday xodimlar sirasiga uydagi yoki mehnat safaridagi xodimlar kiradi. Shubxasiz, 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:

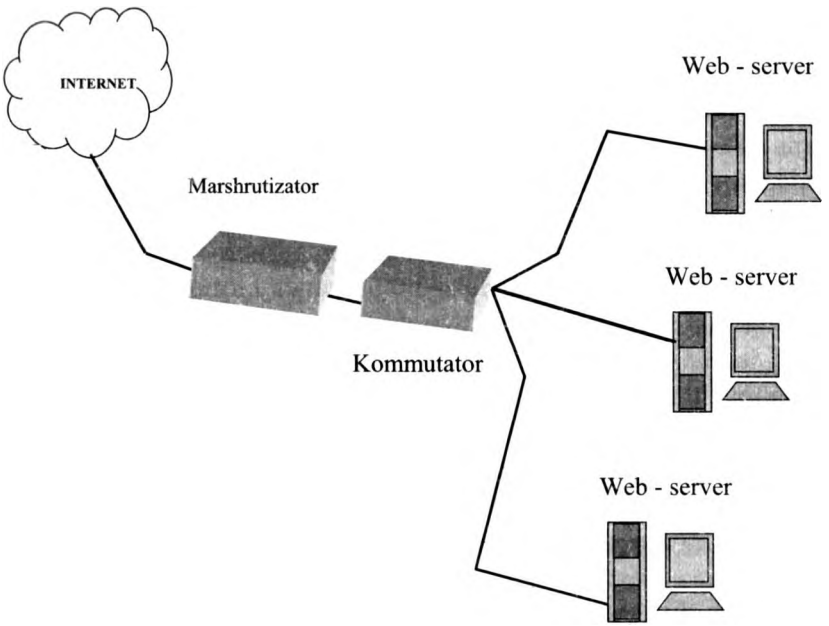
- taqsimlangan tarmoqlararo ekranlardan (distributed firewall) foydalanish;
- virtual xususiy tarmoq VPNlar imkoniyatidan foydalanish.

Taqsimlangan tarmoqlararo ekran tarmoqning alohida kompyuterini himoyalovchi markazdan boshqariluvchi tarmoq mini-ekranlar 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 avval himoyalash vositalarini, sinchiklab, 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.



8.16-rasm. Taqsimlangan tarmoqlararo ekranlar yordamida korporativ serverlarni himoyalash.

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. 8.16-rasmda korporativ

serverlarni taqsimlangan tarmoqlararo ekranlar yordamida himoyalash sxemasi keltirilgan.

An'anaviy va taqsimlangan tarmoqlararo ekranlar quyidagi ko'rsatkichlari bo'yicha taqqoslanadi.

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 har qanday hujumga bardosh bera olmaydi. Taqsimlangan brandmauer operatsion tizimning yadro sathida ishlaydi hamda barcha kiruvchi va chiquvchi paketlarni tekshirib, korporativ serverlarni ishonchli himoyalaydi.

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, unumdorligi paket/daqiqa bo'yicha belgilangan cheklashga 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.

Nazorat savollari:

1. Tarmoqlarni ekranlovchi marshrutizatorlar yordamida himoyalash sxemasini tushuntirib bering.
2. Tarmoqlararo ekran yordamida lokal tarmoqni himoyalash sxemasini yoritib bering.
3. Himoyalanadigan yopiq va himoyalanmaydigan ochiq qismtarmoqli sxemani tushuntirib bering.
4. Yopiq va ochiq qismtarmoqlarni tarmoqlararo ekranlar yordamida alohida himoyalash sxemasining mohiyati.
5. Ikkita tarmoqlararo ekran orqali ochiq va yopiq qismtarmoqlarni alohida himoyalash sxemasini tavsiflab bering.
6. Shaxsiy va taqsimlangan tarmoqlararo ekranlar, ularning kamchilik va afzalliklari.

IX BOB. OPERATSION TIZIM HIMOYASI

9.1. Operatsion tizim xavfsizligini ta'minlash muammolari

Himoyalangan operatsion tizim tushunchasi. Axborotni himoyalashning aksariyat dasturiy vositalari tatbiqiy dasturlardir. Ularni bajarish uchun operatsion tizim (OT) tomonidan madadlash talab etiladi. Operatsion tizim ishlaydigan muhit *ishonchli hisoblash bazasi* deb yuritiladi. Ishonchli hisoblash bazasi operatsion tizimning, dasturlarning, tarmoq resurslarining, fizik himoyalash vositalarining, hatto tashkiliy muolajalarning axborot himoyasini ta'minlovchi elementlarning to'liq to'plamini o'z ichiga oladi. Bularning ichida eng asosiysi himoyalangan operatsion tizim hisoblanadi.

Agar u operatsion tizim tahdidlarning asosiy sinfidan himoyalanish vositalariga ega bo'lsa, *himoyalangan* hisoblanadi. Himoyalangan operatsion tizim tarkibida foydalanuvchilarning OT resurslaridan foydalanishlarini cheklovchi vositalar hamda operatsion tizim bilan ishlashni boshlagan foydalanuvchilarning haqiqiyligini tekshirish vositalari bo'lishi shart. Undan tashqari, himoyalangan OT operatsion tizimni tasodifan yoki atayin ishdan chiqarishga qarshi ta'sir vositalariga ega bo'lishi shart.

Agar operatsion tizim barcha tahdidlardan emas, balki bir qancha tahdidlardangina himoyalanishni ko'zda tutsa, bunday OT *qisman himoyalangan* deb yuritiladi.

Himoyalangan operatsion tizimni yaratishdagi yondashishlar.

Himoyalangan operatsion tizimni yaratishda ikkita asosiy yondashish mavjud – fragmentli va kompleks. *Fragmentli yondashishda* avvalo bitta tahdiddan so'ngra boshqa tahdiddan va h. himoyalanish tashkil etiladi.

Fragmentli yondashish qo'llanilganda, OT himoyasi qismtizimi, odatda, turli ishlab chiqaruvchilar taqdim etgan boshqa-boshqa dasturlar to'plamidan iborat bo'ladi. Ushbu dasturiy vositalar bir-biriga bog'liq bo'lmagan tarzda ishlaydi, ya'ni ularning o'zaro uzviy

bog'lanishini tashkil etishi mumkin emas. Undan tashqari bunday qismtizimning ba'zi elementlari noto'g'ri ishlashi mumkin. Natijada tizim ishonchliligi keskin pasayadi.

Kompleks yondashishda himoya funksiyalari operatsion tizimga uning arxitekturasini loyihalash bosqichida kiritiladi va uning ajralmas qismi hisoblanadi. Kompleks yondashish asosida yaratilgan himoya qismtizimning alohida elmentlari axborotni himoyalashni tashkil etish bilan bog'liq turli masalalar yechilganida bir-biri bilan uzviy bog'langan bo'ladi. Shu sababli himoya qismtizimining alohida komponentlari orasida ixtilof bo'lmaydi. Kompleks yondashish asosida himoya qismtizimini shunday qurish mumkinki, hatto OT ishdan chiqqanda ham niyati buzuq shaxs tizimning himoya funksiyalarini o'chira olmaydi. Fragmentli yondashishda himoya qismtizimini bunday tashkil etish mumkin emas. Odatda, kompleks yondashish asosida yaratiluvchi operatsion tizimni himoyalash qismtizimi shunday loyihalanadiki, uning ba'zi elementlarini almashtirish mumkin bo'ladi.

Himoyalashning ma'muriy choralari.

Operatsion tizimni himoyalashning dasturiy-apparat vositalari himoyaning ma'muriy choralari bilan to'ldirilishi shart. Ma'mur tomonidan doimiy malakali madadsiz hatto ishonchli dasturiy-apparat himoya ham buzilishi mumkin.

Himoyaning asosiy ma'muriy choralari quyidagilar:

1. *Operatsion tizimning, ayniqsa uning himoyalash qismtizimining to'g'ri ishlashini doimiy nazoratlash.* Agar operatsion tizim eng muhim hodisalarning maxsus jurnalda avtomatik tarzda qayd etilishini madadlasa, bunday nazoratni tashkil etish qulay hisoblanadi.

2. *Xavfsizlikning adekvat siyosatini tashkil etish va madadlash.* Operatsion tizimda qabul qilingan xavfsizlik siyosatining adekvat bo'lmasligi, niyati buzuq shaxsning tizim resurslaridan ruxsatsiz foydalanishiga va operatsion tizimning ishonchli ishlashini pasayishiga sabab bo'lishi mumkin. Operatsion tizim xavfsizligi siyosati niyati buzuqning operatsion tizim xavfsizligini yengishga urinishiga hamda OT konfiguratsiyasining o'zgarishiga, tatbiqiy dasturlarining o'rnatilishiga va yo'qotilishiga operativ tarzda reaksiya bildirib, operatsion tizimga doimo tuzatish kiritishi lozim.

3. Foydalanuvchilarni operatsion tizim bilan ishlaganda *xavfsizlik choralariga rioya qilishlari lozimligini uqtirish* va ushbu choralarga rioya qilinishini nazoratlash.

4. Operatsion tizim dasturlari va ma'lumotlarining *rezerv nusxalarini muntazam tarzda yaratish va yangilash.*

5. Operatsion tizimning konfiguratsion ma'lumotlaridagi va xavfsizlik siyosatidagi o'zgarishlarni doimo nazoratlash. Ushbu o'zgarishlar xususidagi axborotni operatsion tizim xavfsizligini yenggan niyati buzuq shaxsga o'zining ruxsatsiz harakatlarini niqoblashga qiyinchilik tug'dirish uchun noelektron axborot eltuvchilarida saqlash maqsadga muvofiq hisoblanadi.

Ta'kidlash lozimki, muayyan operatsion tizimda axborotni himoyalashning yana boshqa ma'muriy choralari talab etilishi mumkin.

Nazorat savollari:

1. Himoyalangan operatsion tizim tushunchasi.
2. Himoyalangan operatsion tizimni yaratishdagi yondashishlarni tushuntirib bering.
3. Himoyalashning ma'muriy choralari nimalarni o'z ichiga oladi?

9.2. Operatsion tizimni himoyalash qismtizimining arxitekturasi

Operatsion tizimni himoyalash qismtizimining asosiy funksiyalari. Operatsion tizimni himoyalash qismtizimi quyidagi asosiy funksiyalarni bajaradi:

Identifikatsiya, autentifikatsiya va avtorizatsiya. Himoyalangan operatsion tizimda har qanday foydalanuvchi (foydalanuvchi subyekt) tizim bilan ishlashdan oldin identifikatsiyani, autentifikatsiyani va avtorizatsiyani o'tishi lozim. Foydalanuvchi subyektning identifikatsiyasiga binoan subyekt operatsion tizimga o'zi xususidagi identifikatsiyalovchi axborotni (ismi, hisob raqami va h.) bildiradi va shu tariqa o'zini identifikatsiyalaydi. Foydalanuvchi subyektning autentifikatsiyasiga binoan, subyekt operatsion tizimga identifikatsiyalovchi axborotdan tashqari uning haqiqatdan ham foydalanuvchi

subyekt ekanligini tasdiqlovchi *autentifikatsiyalovchi axborotni* taqdim etadi. Foydalanuvchi subyektning avtorizatsiyasi muvaffaqiyatli identifikatsiyalash va autentifikatsiyalash muolajalaridan so'ng amalga oshirilada. Subyektni avtorizatsiyalashda operatsion tizim subyektning tizimda ishlashini boshlanishiga zarur harakatlarni bajaradi. Subyektni avtorizatsiyalash muolajasi operatsion tizimni himoyalash qismtizimiga to'g'ridan-to'g'ri taalluqli emas. Avtorizatsiya jarayonida identifikatsiyalangan va autentifikatsiyalangan foydalanuvchi subyektning tizimda ishlashini tashkil etish bilan bog'liq texnik masalalar yechiladi.

Foydalanishni cheklash. Har bir foydalanuvchi xavfsizlikning joriy siyosatiga binoan ruxsat etilgan operatsion tizim obyektlaridan foydalanishi mumkin. Operatsion tizim obyektlaridan foydalanishni cheklash jarayonining asosiy tushunchalari – foydalanish obyekti, obyektdan foydalanish usuli va foydalanuvchi subyekt. Foydalanish obyekti deganda, uskuna resurslari (protsessor, xotira segmentlari, printer, disklar va h.) hamda dasturiy resurslar (fayllar, dasturlar va h.) tushuniladi. Obyektdan foydalanish usuli deganda, obyekt uchun belgilangan amal tushuniladi. Masalan, protsessor faqat komandalarni bajaradi, xotira segmentlari yozilishi va o'qilishi mumkin, magnit kartalaridan axborot faqat o'qilishi mumkin, fayllar uchun esa "o'qish", "yozish" va "qo'shib qo'yish" (fayl oxiriga axborotni qo'shib qo'yish) kabi amallar belgilanishi mumkin. Foydalanish subyekti deganda, obyekt ustida amallar bajarilishini (qandaydir foydalanish usuli bo'yicha murojaatni) boshlab beruvchi tushuniladi. Ba'zida foydalanish subyektiga tizimda bajariluvchi jarayonlarni kiritishadi. Ammo mantiqan, nomidan jarayon bajariluvchi foydalanuvchini foydalanish subyekti deb hisoblash kerak. Operatsion tizimda harakatdagi foydalanishni cheklash qoidalari, xavfsizlikning joriy siyosati aniqlanganida, tizim ma'muri tomonidan o'rnatiladi.

Audit. Operatsion tizimga nisbatan auditni qo'llashda *xavfsizlik jurnali* yoki *audit jurnali* deb yuritiluvchi maxsus jurnalda OTga xavf tug'diruvchi hodisalar qayd etiladi. Audit jurnalini o'qish huquqiga ega foydalanuvchilar *auditorlar* deb ataladi. Operatsion tizimga xavf tug'diruvchi hodisalarga odatda quyidagilar kiritiladi:

- tizimga kirish yoki undan chiqish;

- fayllar ustida amallar bajarish (ochish, bekitish, nomini o'zgartirish, yo'q qilish);

- masofadagi tizimga murojaat;

- imtiyozlarni yoki xavfsizlikning boshqa atributlarini almashtirish (foydalanish rejimini, foydalanuvchining ishonchlilik darajasini va h.).

Agar audit jurnalida barcha hodisalar qayd etilsa, axborot hajmi tezda o'sib boradi. Bu esa qayd etilgan hodisalarni samarali tahlillashga imkon bermaydi. Shu sababli, foydalanuvchilar va hodisalarga nisbatan tanlov asosidagi qaydlashni ko'zda tutish lozim. Qanday hodisalarni qaydlash, qanday hodisalarni qaydlamaslik masalasini yechish auditorlarga yuklanadi. Ba'zi operatsion tizimlarda audit qismtizimi qaydlangan hodisalar xususidagi axborotni yozish bilan bir qatorda ushbu hodisalar xususida auditorlarga interaktiv xabar berish imkoniyati ko'zda tutilgan.

Xavfsizlik siyosatini boshqarish. Axborot xavfsizligi siyosati doimo adekvat holatda ushlab turilishi shart, ya'ni u OT ishlashi sharoitining o'zgarishiga tezda reaksiya ko'rsatishi lozim. Axborot siyosatini boshqarish ma'mur tomonidan OTga o'rnatilgan tegishli vositalardan foydalanilgan holda amalga oshiriladi.

Kriptografik funksiyalar. Axborotni himoyalashni kriptografik vositalardan foydalanmasdan amalga oshirishni tasavvur qilib bo'lmaydi. Operatsion tizimda shifrlash foydalanuvchilar parolini hamda tizim xavfsizligi uchun jiddiy bo'lgan boshqa ma'lumotlarni saqlash va aloqa kanali orqali uzatishda ishlatiladi.

Tarmoq funksiyalar. Zamonaviy operatsion tizimlar, odatda, alohida emas, balki lokal va/yoki global kompyuter tarmoqlari tarkibida ishlaydi. Bitta tarmoq tarkibidagi kompyuterlarning operatsion tizimlari turli masalalarni, xususan, axborotni himoyalashga bevosita daxldor masalalarni yechishda o'zaro aloqada bo'ladi.

Himoyalanish standartini qanoatlantiruvchi har qanday operatsion tizim yuqorida keltirilgan barcha funksiyalarni bajaruvchi himoya qismtizimiga ega bo'lishi shart.

Nazorat savollari:

1. Operatsion tizimni himoyalash qismtizimining asosiy funksiyalarini ahamiyati nimada?
2. Operatsion tizimda identifikatsiya, autentifikatsiya, avtorizatsiya va foydalanishlarni cheklash funksiyalarini tushuntirib bering.
3. Operatsion tizimda audit va xavfsizlik siyosatini boshqarish funksiyalarini yoritib bering.
4. Operatsion tizimda kriptografik funksiyalar va tarmoq funksiyalarining ahamiyatini tavsiflab bering.

9.3. Axborotni himoyalashda dasturiy ilovalarning qo'llanilishi

Niyati buzuqning kompyuterdan ruxsatsiz foydalanishi nafaqat ishlanadigan elektron hujjatlarning o'qilishi va/yoki modifikatsiyalanishi, balki niyati buzuq tomonidan boshqariluvchi dasturiy zakladkani kiritilishi imkoniyati bilan xavfli. Ushbu dasturiy zakladka quyidagi harakatlarni amalga oshirishga imkon beradi:

- keyinchalik kompyuterda saqlanadigan yoki tahrirlanadigan elektron hujjatlarni o'qish va/yoki modifikatsiyalash;
- elektron hujjatlarni himoyalashda ishlatiluvchi turli muhim axborotni tutib olish;
- istilo qilingan kompyuterdan lokal tarmoqning boshqa kompyuterlarini istilo qilishda asos (plasdarm) sifatida foydalanish;
- kompyuterda saqlanadigan axborotni yo'q qilish yoki zarar keltiruvchi dasturiy ta'minotni ishga tushirish yo'li bilan kompyuterni ishdan chiqarish.

Kompyuterni ruxsatsiz foydalanishdan himoyalash axborotni himoyalashning asosiy muammolaridan biri hisoblanadi. Shu sababli, aksariyat operatsion tizimlarga va ommabop dasturiy paketlarga ruxsatsiz foydalanishdan himoyalashning turli qismtizimlari o'rnatilgan. Masalan, Windows oilasidagi operatsion tizimga kirishda foydalanuvchilarni autentifikatsiyalashni bajarish. Ammo, ruxsatsiz foydalanishdan jiddiy himoyalanish uchun o'rnatiladigan vositalarning yetishmasligi shubha tug'dirmaydi. Shu sababli, himoyalashning standart vositalariga qo'shimcha tarzda foydalanishni chek-

lashning maxsus vositalaridan foydalanish zarur. Bunday maxsus vositalarni shartli ravishda quyidagi guruhlarga ajratish mumkin:

- axborotni kriptografik himoyalashning dasturiy vositalari;
- tarmoqni himoyalashning dasturiy vositalari;
- VPN tarmoqni qurishning dasturiy vositalari;
- himoyalanganlikni tahlillovchi dasturiy vositalar;
- antiviruslar.

Axborotni kriptografik himoyalashning dasturiy vositalari – mustaqil yoki boshqa tizimlar tarkibida ishlovchi va axborot xavfsizligini ta'minlash uchun uni kriptografik o'zgartirilishini ta'minlovchi ma'lumotlarni ishlash tizimining dasturiy va texnik elementlari majmui. Quyida ushbu dasturiy vositalarga taalluqli xorijiy va mamlakatimiz kompaniyalarining mahsulotlari keltirilgan.

M-506A-XP – MS Windows 2000/XP/2003/7 operatsion tizim boshqaruvida ishlovchi lokal hisoblash tarmoqlarida axborotni himoyalashga mo'ljallangan dasturiy-apparat kompleks. M-506A-XP ikkita asosiy masalani hal etadi: axborotni ruxsatsiz foydalanishdan himoyalaydi va Rossiya standarti GOST28147-89ga muvofiq, amalga oshirilgan ma'lumotlarni kriptografik himoyalashni bajaradi.

Kriptoprovayder KriptoPro CSP 3.6 – axborotni kriptografik himoyalashning sertifikatsiyalangan vositasi bo'lib, ikkita asosiy masalani hal etadi: standart va hamma joyda ishlatiluvchi Microsoft firmasining ishonchli Rossiya kriptografiyasili ilovalardan foydalanish imkoniyati (korporativ foydalanuvchilar uchun) va Microsoft firmasi mahsulotlaridan foydalangan holda yangi, ishonchli himoyalangan ilovalarni yaratish imkoniyati (tizimli integratorlar uchun).

Axborotni himoyalash tizimining Secret Disk oilasi shaxsiy kompyuterdan muayyan foydalanuvchilar uchun himoyalangan axborot eltuvchilarini virtual mantiqiy disklarini tashkil etish yo'li bilan axborotni himoyalashga imkon beradi. Foydalanuvchilar uchun ma'lumotlarni shifrlash "shaffof" rejimida amalga oshiriladi, ya'ni axborot yozilishida avtomatik tarzda shifrlanadi, o'qishda deshifrovka qilinadi.

Blok xost – ERI – sertifikatsiyalangan kriptoProCSPdan foydalangan holda MS Windows platformasidagi shifrlash va elektron raqamli imzoni yaratish tizimi. MS Windows operatsion tizimiga

o‘rnatilgan boshqa kriptoprovayderlar bilan ham ishlash madadlanadi.

KriptoARM – kriptografik vositalar bilan ishlashning qulayligini ta’minlovchi universal dasturiy ta’minot. KriptoARM axborotni ishonchli himoyalashga va Internet tarmog‘i bo‘yicha uzatiladigan va turli xil eltuvchilardagi (disketlardagi, flesh kartalardagi, tokenlardagi) elektron ma’lumotlarning muallifligini kafolatlashga mo‘ljallangan.

HIMFAYL – fayllarni himoyalangan saqlash tizimi shaxsiy kompyuterda yoki axborotni tashqi disk eltuvchilarida saqlanuvchi papkalar va fayllarning maxfiyligini (konfidensialligini), yaxlitligini ta’minlash va ularni ruxsatsiz foydalanishdan himoyalash uchun mo‘ljallangan.

E-XAT – himoyalangan elektron pochta tizimi foydalanuvchilari orasida elektron xabarlarni himoyalangan almashishini tashkil etishga mo‘ljallangan. Ushbu tizim axborotni kriptografik himoyalash vositalaridan va axborotni kriptografik himoyalash sohasidagi davlat standarti asosidagi elektron raqamli imzo (milliy kriptoprovayder) vositalaridan foydalanadi. E-XAT tizimi uyda ishlash uchun uchta tilni madadlaydi: o‘zbek (lotin va kirillitsa), rus (kirillitsa) va ingliz (lotin).

Tarmoqni himoyalashning dasturiy vositalari. Aksariyat hujumga urinishlar tashqaridan bo‘lishi sababli, tarmoq xavfsizligiga alohida e’tibor berish zarur. Tarmoqlararo ekran – ma’lum protokollarga muvofiq kiruvchi va chiquvchi ma’lumotlar paketini filtrlash vazifasini bajaruvchi apparat yoki dasturiy vositalar kompleksi. Quyida muayyan tashkilotlar uchun tarmoqlararo ekran ishlashini sozlash va tayyor variantlarini tanlash imkonini beruvchi dasturiy mahsulotlar keltirilgan.

Trust Access – taqsimlangan tarmoqlararo ekran Rossiyaning “Hisoblash texnikasi vositalari. Tarmoqlararo ekranlar. Ruxsatsiz foydalanishdan himoyalash. Axborotni ruxsatsiz foydalanishdan himoyalash ko‘rsatkichi” talablariga muvofiq sertifikatlangan.

Security Studio Endpoint Protection – o‘zida tarmoqlararo ekranni, hujumlarni aniqlash va virusga qarshi vositalarni birlashtiradi. Tarmoq resurslaridan xavfsiz foydalanishni ta’minlaydi, spam va turli xil tashqi tahdidlardan himoyalaydi.

UserGateProxy&Firewall – foydalanuvchilarning Internetdan foydalanishlarini, trafikni qayd etishni va filtrlashni, resurslarni tashqi hujumlardan himoyalashni tashkil etishga mo'ljallangan.

CISCO IDS/IPS – hujumlarni qaytarish bo'yicha yechim. Unda an'anaviy mexanizmlar bilan bir qatorda tarmoq trafigidagi nonormalliklarni va tarmoq ilovalarining normal harakatidan chetlanishlarini kuzatuvchi noyob algoritmlar ishlatiladi.

DallasLock 8.0 – K – axborotni himoyalash markazi "Konfident" tomonidan ishlab chiqilgan avtomatlashtirilgan ishchi stansiyalarni va serverlarni ruxsatsiz foydalanishdan himoyalash tizimi.

Secret Net 6.5 (K - varianti) – axborotni ruxsatsiz foydadanishdan himoyalash tizimi.

PAK "Sobol" – ruxsatsiz foydalanishdan himoyalashni ta'minlovchi ishonchli yuklashning dasturiy-apparat moduli. Lokal tarmoq tarkibidagi alohida kompyuterni hamda ishchi stansiya/serverlarni himoyalashni ta'minlashi mumkin.

SZI "Blokxost-set" – axborot resurslarini ruxsatsiz foydalanishdan ko'p funksiyali himoyalashga mo'ljallangan. Windows oilasidagi operatsion tizim boshqaruvidagi tizimlarda ishlaydi.

PAK "Blokxost-MDZ" – kompyuterni yuklash bosqichida axborot resurslarini ruxsatsiz foydalanishdan himoyalaydi. Qattiq diskdagi axborotning saqlanishini ta'minlaydi.

VPN tarmoqni qurishning dasturiy vositalari. Ushbu dasturiy komplekslar virtual xususiy tarmoqlarni qurishga, ularni kuzatishga, shifrlangan kanal bo'yicha ma'lumotlarni xavfsiz uzatish uchun tunnellarni yaratishga hamda talablar va shartlarga muvofiq virtual tarmoqni o'zgartirish imkoniyatiga xizmat qiladi. Quyida virtual xususiy tarmoqni qurish uchun dasturiy mahsulotlar keltirilgan.

Shifrlashning apparat-dasturiy kompleksi "Kontinent"-3.5 – TCP/IP protokollarini ishlatuvchi umumfoydalanuvchi global tarmoqlar asosida virtual xususiy tarmoqlarni qurish vositasi hisoblanadi. Kompleks VPNning tarkibiy qismlari orasida ochiq aloqa kanali bo'yicha uzatiluvchi axborotni kriptografik himoyalashni ta'minlaydi. Kompleks uzatiladigan va qabul qilinadigan paketlarni turli mezonlar (adreslash, o'lchash, kengaytirish va h.) bo'yicha filtrlashni amalga oshiradi. Bu esa tarmoqni ishonchli himoyalashni ta'minlaydi.

VipNeTCustom – dasturiy va dasturiy - apparat mahsulotlar qatori hisoblanib, yirik tarmoqlarda axborotni himoyalashni tashkil etish imkoniyatiga ega va axborotni himoyalashning quyidagi ikkita masalasiga mo'ljallangan:

- boshqarish markazlariga ega virtual xususiy tarmoqni tashkil etish yo'li bilan aloqaning umumfoydalanuvchi va ajratilgan kanallari bo'yicha foydalanish, cheklangan axborotni uzatuvchi himoyalangan muhitni yaratish;
- elektron raqamli imzo mexanizmlaridan foydalanish maqsadida ochiq kalitlar infrastrukturasini tashkil etish.

Himoyalanganlikni tahlillovchi dasturlar. Himoya samaradorligini nazoratlash, axborotdan ruxsatsiz foydalanish hamda axborotni yoki axborotni ishlash va uzatish vositalarining normal ishlashining buzilishi evaziga, axborotning texnik kanallar bo'yicha sirqib chiqishini o'z vaqtida aniqlash va bartaraf etish maqsadida amalga oshiriladi. Ushbu vazifani "xavfsizlik skanerlari" deb ataluvchi "himoyalanganlikni tahlillash vositalari" bajaradi. Quyida himoyalanganlikni tahlillash vositalarining dasturiy mahsulotlari keltirilgan.

XSpider 7.8 – zaifliklarni tatbiqiy hamda tizimli sathlarda tezdan samarali qidirishni amalga oshiruvchi tarmoq xavfsizligi skaneri. Ushbu skaner har qanday ko'lamli tarmoqlarda xavfsizlik maqomini nazoratlashning samarali tizimini barpo etadi.

Tarmoq revizori – ruxsatsiz foydalanishga urinishlarni bartaraf etishga mo'ljallangan tarmoq skaneri. Tarmoq revizori TCP/IP steki protokollaridan foydalanuvchi o'rnatilgan tarmoq dasturiy va apparat ta'minoti zaifliklarini aniqlash uchun ishlatiladi.

Skaner BC - himoyalanganlikni kompleks tahlillash tizimi. Ushbu skaner operatsion tizimli va oldindan o'rnatilgan dasturiy ta'minotli yuklovchi DVD yoki USB – to'plagich. O'rnatilgan dasturiy ta'minot axborot tizimi himoyalanganligini kompleks tahlillashni va testlashni amalga oshiradi.

Antiviruslar. Hozirda kichik kompaniyalar hamda korporatsiyalar tomonidan ishlab chiqiladigan va madadlanadigan virusga qarshi dasturiy mahsulotlarning yetarlicha katta soni mavjud. Ularning orasida virusga qarshi kompleks dasturlarni alohida ajratish mumkinki, bu dasturlar kompyuterda o'rnatilgan dasturiy ta'minotni to'-

liq nazoratlaydi. Quyida bunday dasturiy mahsulotlarning ba'zilari keltirilgan.

Dr.Web – Rossiyaning virusga qarshi ommaviy dasturi. Dastur tarkibida rezident qo'riqchi SpIDerGuard, Internet orqali virus bazalarini yangilashning avtomatik tizimi va avtomatik tekshirish jadvalini rejalashtiruvchi mavjud. Pochta fayllarini tekshirish amalga oshirilgan. Dr. Web dasturining muhim xususiyati – oddiy signaturali qidirish natija bermaydigan murakkab shifrlangan va polimorf viruslarni aniqlash imkoniyatidir.

Kasperskiy laboratoriyasi – axborot xavfsizligi sohasidagi ildam qadamlar bilan rivojlanayotgan kompaniyalardan biri. Kompaniya virusga qarshi tadqiqotlar, xavfli ilovalarga qarshi ta'sirlar, trafikni filtrlash va hokazolarni o'z ichiga oluvchi, juda jiddiy IT-tahdidlar bilan uzluksiz kurashish yillarida to'plangan boy tajribaga ega. Kasperskiy laboratoriyasi barcha kategoriyali klientlarning ehtiyojlarini hisobga oluvchi virusdan, spamdan, xaker hujumidan ishonchli himoyalashni ta'minlovchi keng ko'lamli yechimlarni taqdim etadi.

"Eset" kompaniyasi – virusga qarshi dastur ta'minotini xalqaro ishlab chiqaruvchisi, kiberjinoyatchilikdan va kompyuter tahdidlaridan himoyalash sohasidagi ekspert. Kompaniya dunyoning 180 ta mamlakatida vakillariga ega. Ushbu kompaniya ma'lum va noma'lum zarar keltiruvchi dasturlarni detektirlash va xavfsizlantirishga imkon beruvchi tahdidlarni aniqlashning evristik usullarini yaratish sohasining tashabbuskori hisoblanadi. Eset Nod 32 – Rossiyada virusga qarshi yechimlar ommabopligi bo'yicha ikkinchi o'rinda turadi, har bir uchinchi kompyuter uning himoyasida.

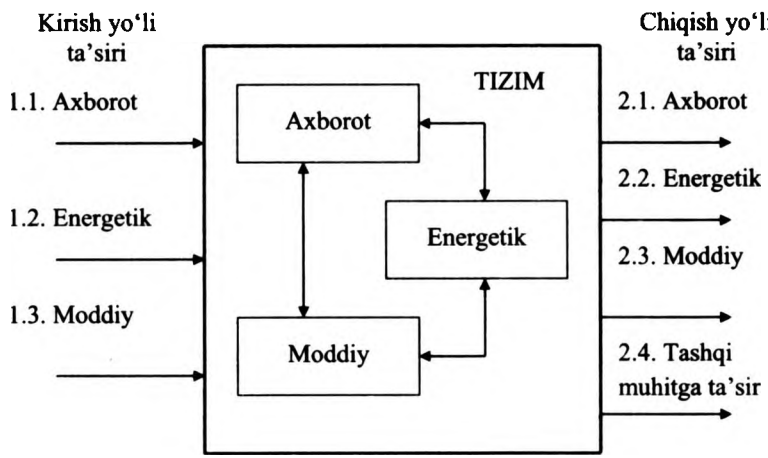
Nazorat savollari:

1. Axborotni himoyalashda qo‘llaniladigan dasturiy vositalarning shartli ravishda qanday guruhlarga ajratish mumkin?
2. Axborotni kriptografik himoyalashning dasturiy vositalarini ishlash prinsipini tushuntiring.
3. Tarmoqni himoyalashning dasturiy vositalarini tavsiflab bering.
4. VPN tarmoqlarni qurish dasturiy vositalarini ishlash prinsipini tushuntirib bering.
5. Himoyalanganlikni tahlillovchi dasturiy ilovalarning ahamiyati.
6. Antivirus vositalarining operatsion tizimlarni himoyalashda tutgan o‘rni.

X BOB. AXBOROT SIRQIB CHIQISH KANALLARI

10.1. Axborot sirqib chiqadigan texnik kanallar va ularning turkumlanishi

Axborotning texnik kanal bo'yicha sirqib chiqishi nuqtayi nazaridan obyekt modeli o'zaro va tashqi muhit bilan bog'langan axborot, energetik, moddiy tizimlarni o'z ichiga oladi (10.1-rasm).

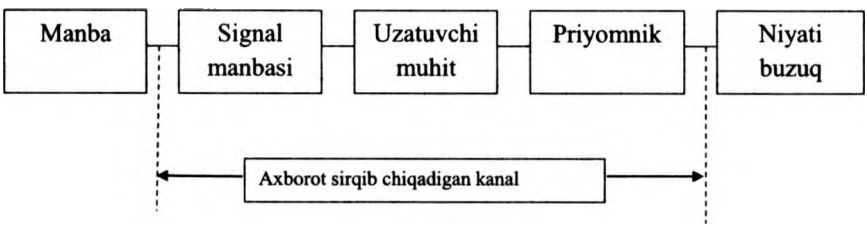


10.1-rasm. Obyekt modeli.

Axborot tizimi energetik tizim bilan va u orqali tashqi muhit bilan o'zaro ta'sirda bo'ladi. Energetik tizim orqali axborot sirqib chiqadigan kanal shakllanishi mumkin. Obyektning energetik tizimining tashqi muhitga ta'siri natijasida niqobni ochuvchi akustik maydon yaratiladi. Energetik tizim moddiy tizim bilan ham o'zaro ta'sirda bo'ladi va natijada, tebranma (mexanik) maydon shakllanadi. Tebranma maydon axborot tizimi signalini modulyatsiya qilishi mumkin. Har bir tizim o'zining elementlariga, bog'lanishlarining ichki strukturasiga, o'zgaruvchi parametrlari soniga hamda

tashqi muhit orqali o‘zaro ta’siriga bog‘liq cheklashlarga ega. Obyektlarning ishlashi ularning haqiqiy maqsad va vazifalarini kuzatishdan bekitadi. Har bir tizimda axborot sirqib chiqadigan texnik kanallar mavjud.

Axborot sirqib chiqadigan texnik kanallar deganda, texnik vositalarning ishlash jarayonida paydo bo‘luvchi turli tabiatli qo‘shimcha nurlanish hisobiga, axborotning bexosdan uzatilishi tushuniladi. Axborot sirqib chiqadigan texnik kanalning strukturasi 10.2 – rasmda keltirilgan.



10.2-rasm. Axborot sirqib chiqadigan texnik kanal strukturasi.

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

Dastlabki signal – axborot manbaidan olinadigan axborot eltuvchisidir. Quyidagi *signal manbalarini* ko‘rsatish mumkin:

- elektromagnit va akustik to‘lqinlarini qaytaruvchi kuzatuv obyekti;
- o‘zidan optik va radio diapazonlaridagi elektromagnit to‘lqinlarini tarqatuvchi kuzatuv obyekti;
- funksional aloqa kanalining uzatuvchi qurilmasi;
- yashirincha o‘rnatilgan qurilma;
- xavfli signal manbai;
- axborot bilan modulyatsiyalangan akustik to‘lqinlar manbai.

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

Uzatish muhiti - eltuvchi ko'chib yuruvchi fazoning qismi. U eltuvchining ko'chib yurishi shartlarini belgilovchi fizik parametrlar nabori orqali xarakterlanadi. Tarqalish muhitini tavsiflashda quyidagi asosiy parametrlarni hisobga olish zarur:

- subyektlar va moddiy jismlar uchun fizik to'siqlar;
- masofa birligidagi signalning susayish o'lchovi;
- chastota xarakteristikalari;
- signal uchun xalallar ko'rinishi va quvvati.

Qabul qiluvchi qurilma quyidagi vazifalarni bajaradi:

- qabul qiluvchiga kerakli axborot eltuvchisini tanlash;
- qabul qilingan signalni axborotni olishni ta'minlovchi qiymatigacha kuchaytirish;
- eltuvchidan axborotni olish;
- axborotni qabul qiluvchiga (insonga, texnik qurilmaga) tushunarli signal shakliga o'zgartirish va signalni xatosiz o'zlashtirilishiga yetarli qiymatgacha kuchaytirish.

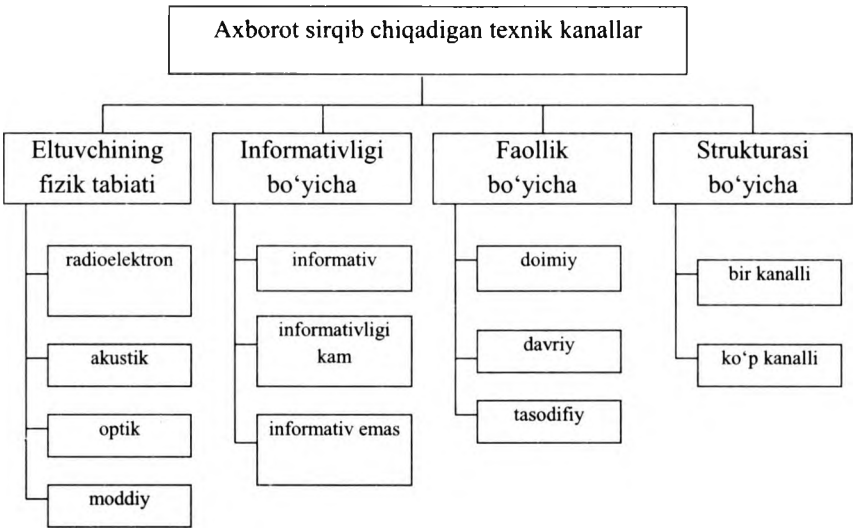
Axborot sirqib chiqadigan texnik kanallarning turkumlanishi 10.3-rasmda keltirilgan.

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

- radioelektron;
- akustik;
- optik;
- moddiy.

Axborot sirqib chiqadigan radioelektron kanalda eltuvchi sifatida radiodiapazondagi elektrik, magnit va elektromagnit maydonlar hamda metall o'tkazuvchilar bo'yicha tarqaluvchi elektr toki (elektronlar oqimi) ishlatiladi. Radioelektron kanalning chastotalar diapazoni quyidagicha:

- past chastotali 10-1 km (30-300 KGs);
- o'rta chastotali 1 km-100 m (300 KGs-3MGs);
- yuqori chastotali 100-10 m (3-30 MGs);
- ultra yuqori chastotali 10-1m (30-300 MGs);
- o'ta yuqori chastotali 10-1sm (3-30 GGs).



10.3-rasm. Axborot sirqib chiqadigan texnik kanallarning turkumlanishi.

Akustik kanalda axborot eltuvchisi sifatida muhitda tarqaluvchi akustik to'lqinlar ishlatiladi. Akustik kanalning chastotalar diapazoni quyidagicha:

- infratovush 1500-75 m (1-20Gs);
- pastki tovush 150-5m (1-300Gs);
- tovush 5-0,2m (300-16000Gs);
- ultratovush -16000 Gsdan 4 MGs gacha.

Optik kanaldagi axborot eltuvchisi – elektromagnit maydon (fotonlar). Optik diapazon quyidagilarga bo'linadi:

- uzoq infraqizil qism. Diapazon 100-10mkm (3-300TGs);
- o'rta va yaqin infraqizil qism. Diapazon 10-0,76 mkm (30-400 TGs);
- ko'rinadigan diapazon (ko'k-yashil-qizil). Diapazon 0,76-0,4 mkm (400-750 TGs).

Moddiy kanalda axborotning sirqib chiqishi himoyalanuvchi axborotli eltuvchilarning nazoratlanuvchi zona tashqarisiga ruxsat-

siz tarqalishi hisobiga ro'y beradi. Eltuvchi sifatida ko'pincha hujjatlar qo'l yozmasi va ishlatilgan nusxalash qog'ozlari ishlatiladi.

Informativligi bo'yicha axborot sirqib chiqadigan kanallar informativ, informativligi kam va informativ emaslarga bo'linadi. Kanal informativligi kanal bo'yicha uzatiluvchi axborot qiymati orqali baholanadi.

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

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

- akustik axborotning sirqib chiqishi xavfi;
- tasviriy axborotning sirqib chiqishi xavfi;
- axborotning qo'shimcha elektromagnit nurlanishlar va navodkalar bo'yicha sirqib chiqishi xavfi.

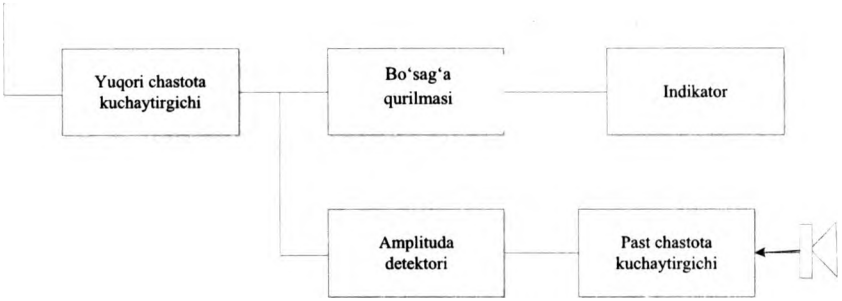
Strukturalari bo'yicha axborot sirqib chiqadigan kanallar bir kanalli va ko'p kanalli bo'lishi mumkin. Ko'p kanallilarda axborot sirqib chiqishi bir qancha ketma-ket yoki parallel kanallar bo'yicha bo'ladi.

Nazorat savollari:

1. Axborot sirqib chiqadigan texnik kanallar tushunchasi.
2. Axborot sirqib chiqadigan texnik kanal strukturasini tushuntirib bering.
3. Axborot sirqib chiqadigan texnik kanallarning turkumlanishi.

10.2. Axborot sirqib chiqadigan texnik kanallarni aniqlash usullari va vositalari

Elektromagnit nurlanish indikatorlari qo'shimcha elektromagnit nurlanishlarni aniqlash va nazoratlash uchun ishlatiladi. Indikatorning soddalashtirilgan sxemasi 10.4-rasmda keltirilgan.



10.4-rasm. Elektromagnit nurlanish indikatorining sxemasi.

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

Indikatorning ishlash prinsipi quyidagicha. Indikator sxemasida tashqi signallar fonida test akustik signalini ajratishga imkon beruvchi past chastota kuchaytirgichi va radiokarnay mavjud. Test akustik signal bilan modulyatsiyalangan nurlanishni indikator antennasi qabul qiladi va kuchaytirilgandan so'ng radiokarnayga uzatiladi. Radiozakladka mikrofoni bilan indikator radiokarnayi orasida xushtakni eslatuvchi tovush signali ko'rinishida namoyon bo'luvchi musbat teskari bog'lanish o'rnatiladi. Bu akustik teskari bog'lanish yoki "akustik bog'lanish" rejimi deb ataladi.

Elektromagnit maydon indikatorlari quyidagi ko'rsatkichlari bilan xarakterlanadi:

- chastotaning ishchi diapazoni;
- sezuvchanlik;
- zakladkani topish radiusi;
- ta'minot manbai xili;
- zakladkani qidirish rejimida avtonom ishlash vaqti;
- indikatsiya xili.

Zamonaviy indikator D-008 ning ko'rinishi 10.5-rasmda keltirilgan. Asbob ishlashining ikkita rejimi mavjud:

• radionurlantiruvchi zakladkani qidirishga mo‘ljallangan maydonni aniqlash;

• yashirincha tinglovchi qurilmalarni qidirishga mo‘ljallangan simli liniyalarni tahlillash.

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

10.5-rasm. D-008 indikatori.

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

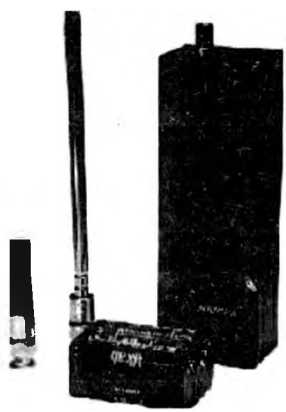
Radiochastotomerlar elektromagnit nurlanishning chastota bo‘yicha bo‘sag‘aning oshib ketishini qaydlaydi. Zakladkani qidirish xonani reja asosida radiochastotomer bilan aylanish yo‘li orqali amalga oshiriladi va zakladka bo‘lishi mumkin bo‘lgan joy tekshirilayotgan xonaning ma’lum nuqtasidagi signalning maksimal sathi bo‘yicha aniqlanadi. Nurlanish aniqlanganda, displeyda olingan signal chastotasi ko‘rsatiladi, tovush yoki yorug‘lik orqali xabar beriladi.

Radiochastotomerlarning ba'zi xillari axborotni yuqori chastotada liniya orqali uzatuvchi zakladkalarni aniqlashda qo'llaniladi. Niyati buzuqning texnik vositasining uzatish chastotasi 40-600 KGs (ba'zida 7 MGs gacha) diapazonda bo'ladi.

RICh-3 chastotomerning (10.6-rasm) ishlash prinsipi radiosignallarni keng polosali detektirlashga asoslangan. Bu esa ixtiyoriy modulyatsiyali radiouzatuvchi qurilmalarni aniqlash imkoniyatini beradi.

Asbob ikkita rejimda ishlaydi: qidirish va qo'riqlash.

Qidirish rejimi radiomikrofonlar, telefon radiotranslyatorlar, radiostetoskoplar, yashirin videokameralar o'rnatilgan joylarni aniqlashda ishlatiladi. Undan tashqari radiostansiyalar va radiotelefonlarni ruxsatsiz ishga tushirilganligini aniqlaydi.



10.6-rasm. RICh-3 chastotomeri.

Qo'riqlash rejimi begona radionurlanish manbasini paydo bo'lish onini qaydlashga va trevoga signalini uzatishga imkon beradi.

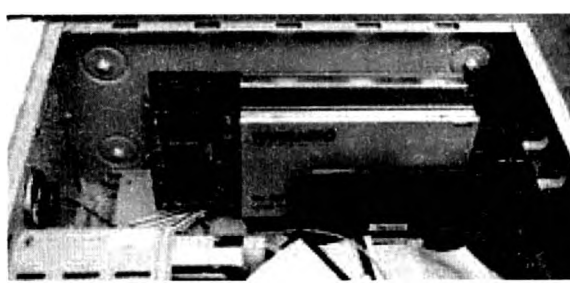
RICh-3 asbobi chastota o'lchanishining yuqori aniqligida (0,002%), chastotaning 100-3000 MGs diapazonida ishlaydi.

Skanerlovchi priyomniklar transportda tashiladigan va qo'lda olib yuriladiganlarga bo'linadi. Maydon indikatori va radiochastotomerlarga o'xshab, skanerlovchi priyomniklar axborot sirqib chiquvchi kanallarni aniqlashda qo'llanilishi mumkin.

10.7-rasmda Winradio skanerlovchi priyomnikning tashqi ko‘rinishi keltirilgan. Ushbu priyomnik kompyuterning 16-bitli slotiga o‘rnatiladigan karta ko‘rinishida yasalgan (10.8-rasm), bu esa uning ketma-ket portlar orqali ulanadiganlariga nisbatan imkoniyatlarini orttiradi.

Winradio 1000 modeli 500 kGs dan 1300 mGs gacha chastotalarda ishlaydi va turli modulyatsiyali signalni qabul qilishi mumkin. Dasturiy boshqarish sichqoncha va klaviatura yordamida qurilma resurslarini operativ boshqarishga imkon beradi. Boshqarish paneli monitor ekranida akslantiriladi. Tezligi – 50 kanal/s, chastota bo‘yicha o‘zgartirish qadami 1 kGs dan to 1 mGs gacha.

10.7-rasm. Winradio skanerlaydigan qabul qiluvchi qurilma.



10.8-rasm. Winradio skanerlovchi priyomnikni kompyuterga o‘rnatish.

Winradio Communication firmasi radiopriyomniklari komplekti tarkibiga boshqarishning quyidagi dasturiy vositalari kiradi:

- bazaviy dasturiy ta’minot;

• qo‘shimcha dasturiy ta’minot;

• skanerlash rejimini amalga oshirishiga imkon beruvchi dasturiy ta’minot.

Bazaviy dasturiy ta’minot priyomnik ishlashini boshqaruvchi asosiy boshqarish dasturi bo‘lib, quyidagi masalalarni hal etadi: priyomnikni ish chastotasiga va ishlash rejimiga o‘rnatish, skanerlash parametrlarini belgilash va natijalarini akslantirish, ish natijalari bo‘yicha ma’lumotlar bazasini shakllantirish.

Qo‘shimcha dasturiy ta’minot priyomnikning funksional imkoniyatlarini kengaytirishga imkon beradi:

• Digital Suite dasturi signalning vaqt va chastota xarakteristikalarini tahlillashga, turli standartlardagi signallarini ishlashga hamda audio - signallarini WAV – formatda qattiq diskka yozishga imkon beradi. Signallarni tahlillash va ishlash muolajalarini amalga oshirishda kompyuterning standart tovush kartasidan foydalaniladi.

• Datebase dasturi ixtisoslashtirilgan ma’lumotlar bazasining shakllanishini ta’minlaydi. Dastur tarkibiga butun dunyo bo‘yicha uch yuz mingdan ortiq qaydlangan chastotalarini, manzil mamlakati, geografik koordinatlari ko‘rsatilgan radiostansiyalar xususidagi axborotli ma’lumotlar bazasi kiradi.

Skanerlashning ko‘pgina algoritmlari mavjud. Ularning asosiy vazifalari quyidagilar:

• agar qabul qilinadigan signal sathi berilgan bo‘sag‘adan oshsa, skanerlash to‘xtatiladi. Operator tovush yoki nur orqali ogohlantiriladi.

• signal aniqlanganida skanerlash to‘xtatiladi va signal yo‘qolganida skanerlash qaytadan boshlanadi;

• signalni tahlillash vaqtida skanerlash to‘xtatib turiladi va skanerlash rejimi ishga tushirilganida davom ettiriladi;

• qo‘l yordamida skanerlash – priyomnikni sozlash operator yordamida amalga oshiriladi.

Qo‘shimcha dasturiy ta’minot chastotalari ma’lum radiozakladkalarni qidirishda ishlatiladi. Bunda ba’zi skanerlovchi priyomniklarda modulyatsiyaning berilgan xili va ustivor kanallar bo‘yicha skanerlash ko‘zda tutilgan.

Yuqorida aytib o'tilganidek, shaxsiy kompyuterlarning aniqlash qurilmalari bilan kompleksda ishlatilishi, signallarni aniqlash va tahlillash bo'yicha imkoniyatlarni jiddiy kengaytiradi. "Skanerlovchi priyomnik + shaxsiy kompyuter" komplekti avtomatlashtirilgan qidiruv kompleksining oddiy misoli hisoblanadi. Yanada murakkab tizimlar ham shaxsiy kompyuter va skanerlovchi priyomnik asosida quriladi, ammo ular kompleksning tezkorligini hamda funksional imkoniyatlarini kengaytiruvchi qo'shimcha bloklarga ega.

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

"KRONA" kompleksi (10.9-rasm) quyidagi muolajalarni bajarishga mo'ljallangan:

- hozirgi kunda ma'lum barcha niqoblash vositalaridan foydalanuvchi radiozakladkalarni aniqlash va lokalizatsiyalash. Z GGs gacha diapazonda ishlaydi (qo'shimcha konvertor bilan 18 GGs gacha). Ma'lumotlarni uzatuvchi raqamli kanallarni va axborotni radiokanal bo'yicha uzatuvchi yashirin videokameralarni avtomatik tarzda aniqlash imkoniyatiga ega. Mavjud dasturiy ta'minot radiozakladkalarni yuqori darajada ishonchlilikda aniqlashga imkon beradi;
- himoyalanuvchi obyektdagi elektromagnit ahvolni muttasil monitoringlash. Dasturiy ta'minot yangi yoki ma'lum signallar parametrlarini qidirish va baholash, chastota diapazonini nazoratlash, qayd etilgan chastotalarni nazoratlash va h. masalalarini yechishga imkon beradi.

"KRONA Pro" kompleksi ko'p kanalli kompleks bo'lib, radionurlanuvchi vositalarni aniqlashda va radiomonitoringni amalga oshirishda qo'llaniladi. Nazorat diapazoni 10..3000 MGs (qo'shimcha konvertor bilan 18000 MGs gacha). Ushbu kompleks yashirin radiouzatuvchi radiokameralarni, ma'lumotlarni uzatuvchi raqamli kanallarni avtomatik tarzda aniqlaydi. O'rnatilgan joyni topish aniqligi 10 sm gacha, avtonom ta'minot 2 soatgacha. Kompleks axborotni ruxsatsiz oluvchi vositalarni aniqlash imkoniyatiga ega.

10.9-rasm. "KRONA" rusumli avtomatlashtirilgan qidiruv kompleksi.

Yuqorida ko'rilgan avtomatlashtirilgan qidiruv komplekslari standart kompyuterlarda va oddiy ko'chmas skanerlovchi priyomniklar asosida qurilgan. Maxsus qidiruv dasturiy – apparat vositalar alohida guruhga ajratiladi. Masalan, RK855-S, ScanbockSelectPlus, OSCOROSC-5000 Deluxe (10.10-rasm).

10.10-rasm. OSCOR OSC-5000 DeLuxe rusumli maxsus avtomatlashtirilgan qidiruv kompleksi.

Ular radiozakladkalarni avtomatik tarzda qidirishga mo'ljallangan. Komplekslar tarkibida maxsus skanerlovchi priyomnik, mikroprotsessor va test akustik signal generatori yoki tovushsiz korrelya-

tor mavjud. Bunday komplekslarning asosiy xarakteristikasi – unumdorlik, ya'ni aniqlangan signalni radiozakladka signallari sinfiga taalluqli ekanligiga sarflangan vaqtni inobatga olgan holda radiodiapazonni tahlillash tezligi.

Nazorat savollari:

1. Elektromagnit nurlanish indikatorining ishlash sxemasini tushuntirib bering.
2. Radiochastotomerlarning ishlash rejimlarini tushuntirib bering.
3. Skanerlovchi qurilmalarning axborot sirqib chiqishidan himoyalashdagi ahamiyati.
4. Shaxsiy kompyuterlar asosida qurilgan avtomatlashtirilgan qidiruv kompleksi.

10.3. Obyektlarni injener himoyalash va texnik qo'riqlash

Axborot manbalarini fizik himoyalash tizimi niyati buzuqning himoyalanuvchi axborot manbalariga suqilib kirishini oldini oluvchi hamda tabiiy ofatdan, avvalo yong'indan, ogohlantiruvchi vositalarni o'z ichiga oladi.

Injener konstruksiyalar tahdid manbalarini axborot manbalari tomon harakati (tarqalishi) yo'lida ushlab qoluvchi to'siqlarni yaratadi. Ammo axborotni himoyalashni ta'minlash uchun tahdidlarni niyati buzuqning va tabiiy ofatning himoyalanuvchi axborotli manbaga ta'siridan oldin neytrallash zarur. Buning uchun tahdid *neytrallash vositalari* tomonidan aniqlanishi va oldi olinishi zarur. Bu masalalar *axborot manbalarini texnik qo'riqlash* vositalari tomonidan hal etiladi.

Axborotga tahdidlarning turlari va ro'y berishi vaqtining noaniqligi, axborotni himoyalovchi vositalarning ko'p sonliligi va turli – tumanligi, favqulot vaziyatlardagi vaqtning tanqisligi, *axborotni fizik himoyalash vositalarini boshqarishga* yuqori talablar qo'yadi.

Boshqarish quyidagilarni ta'minlashi lozim:

- axborotni himoyalashning umumiy prinsiplarini amalga oshirish;

• axborotni fizik himoyalash tizimini va uni sirqib chiqishidan himoyalash tizimini yagona doirada ishlashini muvofiqlashtirish;

• axborotni himoyalash bo'yicha operativ qaror qabul qilish;

• himoya choralarining samaradorligini nazoratlash.

Fizik himoyalash tizimini boshqarish bo'yicha me'yoriy hujjatlar axborotni himoyalash bo'yicha yo'riqnomalarda o'z aksini topgan. Ammo yo'riqnomalarda barcha vaziyatlarni hisobga olish mumkin emas. Fizik himoyalash tizimining vositalari vaqt tanqisligi sharoitida notipik vaziyatlar sodir bo'lganida to'g'ri xulosa qabul qilinishini ta'minlashi lozim.

Axborotni himoyalash uning samaradorligini nazoratlamasdan amalga oshirish mumkin bo'lmaganligi sababli, boshqarish tizimining muhim vazifasi – himoyalash bo'yicha choralarni turli xil nazoratlashni tashkil etish va amalga oshirishdir.

Fizik himoyalash tizimining tarkibi turli-tuman: oddiy qulfli yog'och eshikdan to qo'riqlashning avtomatlashtirilgan tizimigacha. Fizik himoyalash tizimning umumlashtirilgan sxemasi 10.11-rasmda keltirilgan.

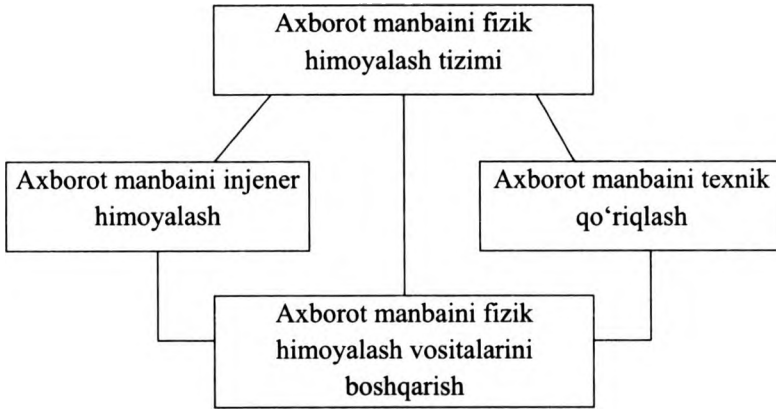
Obyektlarni injener himoyalash va texnik qo'riqlash zaruriyati statistika orqali tasdiqlanadi, ya'ni suqilib kirishlarning 50% dan ko'prog'i xodimlar va mijozlar tomonidan erkin foydalaniladigan obyektlarga amalga oshirilsa, faqat 5 % kuchli qo'riqlash rejimli obyektlarga amalga oshiriladi.

Niyati buzuqlarning suqilib kirishlari yashirincha, instrument yordamida yoki portlatish orqali injener konstruksiyalarini mexanik buzish bilan amalga oshirilishi mumkin. Ba'zi hollarda suqilib kirishlar qorovullarni neytrallash bilan harbiy hujum ko'rinishida amalga oshiriladi.

Axborotni injener himoyalashni quyidagilar ta'minlaydi:

• niyati buzuqning va tabiiy ofatning axborot manbalariga (yoki qimmatbaho narsalarga) qarab harakat qilishi mumkin bo'lgan yo'ldagi tabiiy va sun'iy to'siqlar;

• foydalanishni nazoratlovchi va boshqaruvchi tizimlarning to'suvchi qurilmalari.



10.11-rasm. Axborot manbaini fizik himoyalash tizimining strukturasi.

Tabiiy to'siqlarga tashkilot hududida yoki yonidagi yurish qiyin bo'lgan joylar (zovurlar, jarlar, qoyalar, daryolar, quyuq o'rmon va changalzor) taalluqli bo'lib, ulardan chegaralar mustahkamligini kuchaytirishda foydalanish maqsadga muvofiq hisoblanadi.

Sun'iy to'siqlar odamlar tomonidan yaratilib, tabiiy to'siqlardan konstruksiyasi va niyati buzuq ta'siriga barqarorligi bilan jiddiy farqlanadi. Ularga turli devorlar, qavatlararo pollar, shiplar, bino derazalari va h. taalluqli.

Barqarorligi eng past to'siqlarga binolarning eshiklari va derazalari, ayniqsa, binoning birinchi va oxirgi qavatlaridagi eshiklar va derazalar taalluqli. Eshiklar (darvozalar)ning mustahkamligi ularning qalinligiga, ishlatilgan material xiliga va konstruksiyasiga hamda qulflarning ishonchligiga bog'liq.

Derazalar mexanik ta'sirga bardosh oyna va metall panjaralar yordamida mustaxkamlanadi.

Himoyaning oxirgi chegaralarini metall shkaflar, seyflar tashkil etadi. Shu sababli ularning mexanik mustaxkamligiga yuqori talablar qo'yiladi.

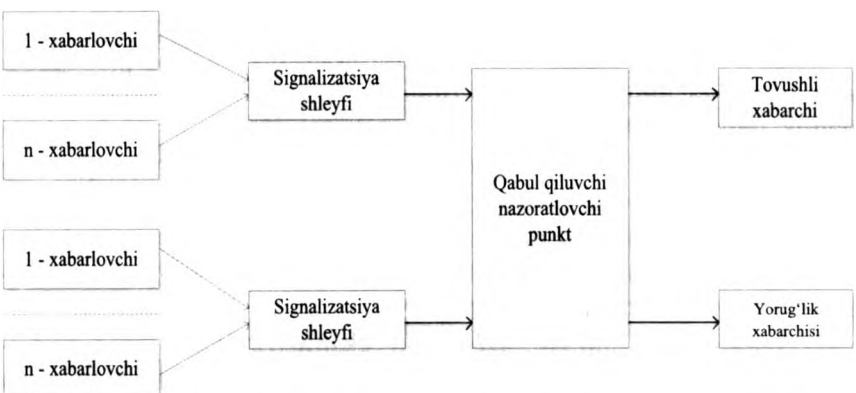
Metall shkaflar maxfiylik grifi yuqori bo'lmagan hujjatlarni, qimmatbaho narsalarni, katta bo'lmagan pul mablag'ini saqlashga

mo‘ljallangan. Shkaflarning ishonchliligi faqat metalning pishiqligiga va qulflarning maxfiyligiga bog‘liq.

Muhim hujjatlarni, narsalarni, katta pul mablag‘ini saqlash uchun *seyflar* ishlatiladi. Seyflarga devorlari orasidagi bo‘shliqqa turli materiallar, masalan, beton birikmalari bilan to‘ldirilgan ikki qavatli metall shkaflar taalluqli.

Niyati buzuqlarning g‘ovlarni va mexanik to‘siqlarni yengishga urinishlarini hamda yong‘inni aniqlash uchun turli fizik prinsiplarda qurilgan *obyektlarni qo‘riqlovchi texnik vositalardan* foydalaniladi.

10.12-rasmda obyektlarni qo‘riqlovchi texnik vositalar kompleksining namunaviy strukturasi keltirilgan. Qo‘riqlaydigan *xabarlovchi* (datchik) texnik qurilma bo‘lib, u unga niyati buzuq tomonidan mexanik kuch va maydon ta’sir qilganida, trevoga signalini shakllantiradi.



10.12-rasm. Obyektlarni qo‘riqlovchi texnik vositalar kompleksining namunaviy strukturasi.

Samarali universal datchiklarni yaratish mumkin bo‘lmaganligi sababli, niyati buzuqning alohida alomatlarini va yong‘inni sezuvchi datchik turlarining katta soni yaratilgan. Turli xil datchiklardan olingan ma’lumotlardan birgalikda foydalanish xatoliklarni kamaytirishga imkon beradi.

Signalizatsiya shleyfi elektr zanjirni hosil qilib, datchiklar va qabul qiluvchi - nazoratlovchi asboblarning elektr bog'lanishini ta'minlaydi. Ulovchi simlarni tejash maqsadida datchiklar guruhlarga birlashtiriladi, shleyflar esa qabul qiluvchi – nazoratlovchi asbob bilan ulanadi. Masalan, qo'riqlovchi va yong'in datchiklari trevoga signallarini bitta shleyf orqali uzatadi.

Shleyflar qancha ko'p bo'lsa, datchiklarning o'rnatilish joylarining lokalizatsiyalanganligi shunchalik aniq bo'ladi va niyati buzuqning suqilib kirish joyi aniqroq aniqlanadi. Undan tashqari qo'riqlash va yong'in signalizatsiyalari uchun alohida shleyflar bo'lishi maqsadga muvofiq hisoblanadi. Bu holda yong'indan qo'riqlashning signalizatsiya vositalarini ish vaqtida o'chirib qo'yish mumkin.

Qabul qiluvchi – nazoratlovchi punkt datchiklardan keladigan signallarni qabul qilish va ishlashga, qo'riqlash xodimlarini tovush va yorug'lik signali yordamida trevoga signallari kelganligi, datchiklar va shleyflar ishlashidagi nosozliklar xususida xabardor qilishga mo'ljallangan.

Hozirda *televizion kuzatuv tizimi* keng qo'llanilmoqda. Bu tizim tarkibiga tungi vaqtda qo'riqlanuvchi hududda kerakli yoritilganlik darajasini ta'minlovchi navbatchi yorituvchi vositalari ham kiradi. Kuzatish tizimi qo'riqlanuvchi hudud va niyati buzuqlarning harakatini masofadan vizual nazoratlashga imkon beradi. Undan tashqari zamonaviy kuzatuv vositalarining imkoniyatlari niyati buzuqning nazoratlanuvchi zonalarga suqilib kirishini aniqlash va qo'riqlash masalalarini hal eta oladi.

Avtonom qo'riqlash tizimining ekspluatatsiyasi katta sarf - xarajatlarni talab etadi. Shu sababli markazlashtirilgan qo'riqlash tizimlari keng qo'llaniladi. Ushbu tizimda niyati buzuqlarni neytrallashtirish masalasi bir necha tashkilotlar uchun umumiy hisoblanadi.

Markazlashtirilgan qo'riqlashga misol tariqasida omonat bank filiallarini, kichik firmalarni, xususiy uylarni, dala hovlilarni, xonadonlarni qo'riqlashni ko'rsatish mumkin. Hududiy yonma – yon, masalan, bitta binoda joylashgan firmalar qo'riqlashning umumiy bo'linmasiga ega bo'lishlari mumkin. Samarali markazlashtirilgan qo'riqlashni ichki ishlar vazirligining qo'riqlash xizmati bo'linmasi ta'minlaydi.

Trevoga signali kelishi bilan operator buyrug'i bo'yicha qo'riqlash obyektiga qurollangan xodimlar guruhi jo'natiladi. Qo'riqlash guruhining obyektga yetib kelish vaqti qat'iy belgilangan (5-7 daqiqa). Ammo markazlashtirilgan qo'riqlash tizimining reaksiya vaqti avtonom qo'riqlash tizimiga qaraganda katta, ayniqsa, agar qo'riqlanuvchi obyekt mobil qo'riqlash guruhining mashinasi turgan joydan uzoqda bo'lsa. Undan tashqari ushbu vaqt ba'zi hollarda nojoiz kattalashishi mumkin. Bunga misol tariqasida radioaloqaning buzilishini, yo'llardagi tirbandlikni, tasodifiy yo'l - transport hodisalarini va h. ko'rsatish mumkin. Ammo, markazlashtirilgan qo'riqlash tizimi tahdidlarni, ayniqsa, qurolli hujumlarni neytrallashda katta imkoniyatlarga ega.

Nazorat uchun savollar:

1. Axborot manbalarini fizik himoyalash tizimi tushunchasi.
2. Obyektlarni injener himoyalash va texnik qo'riqlash tizimi tarkibi.
3. Obyektlarni qo'riqlovchi texnik vositalar kompleksining namunaviy strukturalari.

FOYDALANILGAN VA TAVSIYA ETILADIGAN ADABIYOTLAR

1. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд. 4-е – М.: Ленанд, 2015.

2. Шаньгин В.Ф. Информационная безопасность. – М.: ДМК Пресс, 2014.

3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений выс. Образования/ – М.: Издательский центр «Академия», 2014.

4. Мельников Д.А. Информационная безопасность открытых систем: учебник / – М.: Флинта: Наука, 2013.

5. Stamp, Mark. Information security: principles and practice / Mark Stamp/ -2nd ed. ISBN 978-0-4-470-62639-9(hardback)/ QA76.9.A25S69, USA, 2011.

6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы 4-издание. – Питер, 2010, 944с.

7. Hacking exposed. Web Applications 3. Joel Scambray, Vincent Liu, Caleb Sima. 2010.

8. P.Y.A. Ryan, S.A. Schneider, M.H. Goldsmith, G. Lowe and A.W. Roscoe. The Modelling and Analysis of Security Protocols: the CSP Approach. The original version is in print December 2010 with Pearson Education.

9. Hacking exposed. Network Security Secret &solutions. Stuart McClure, Joel Scambray, Jeorge Kurtz. 2009.

10. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. Учебное пособие. Допущено УМО. – М.: Изд. центр «Академия», 2009, 272 с.

11. Панасенко Сергей Алгоритмы шифрования. Специальный справочник. –Санкт-Петебург, 2009, 576с.

12. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. – Т.: "Алоқачи", 2008.

13. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. – М.: Издательство ТРИУМФ, 2008 .

14. Варфоломеев А.А. Основы информационной безопасности. – Москва, 2008, 412с.

15. Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации. – Екатеринбург УГТУ–УПИ, 2008.

16. Андрончик А.Н., Богданов В.В., Домуховский Н.А., Коллеров А.С., Синадский Н.И., Хорьков Д.А., Щербаков М.Ю. Защита информации в компьютерных сетях. Практический курс. – Екатеринбург, УГТУ–УПИ, 2008, 248с.

17. Rafail Ostrovskiy, Roberto de Prisco, Ivan Visconti. Security and Cryptography for networks. Springer-Verlag Berlin Heidelberg 2008.

18. Johnny Long, Timothy Mullen, Ryan Russel, Scott Pinzon. Stealing the network. How to own a shadow. 2007.

19. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition. USA, 2006.

20. Романец Ю.В., Тимофеев П.А. Защита информации в компьютерных системах и сетях. – Санкт-Петербург, 2006.

21. Торокин А.А. Инженерно–техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А.Торокин – М.: Гелиос АРВ, 2005, 960с.

22. Бузов Г.А. и др. Защита от утечки информации по техническим каналам. – М.: Телеком, 2005.

23. Қосимов С.С. Ахборот технологиялари. Ўқув қўлланма. – Т.: "Алоқачи", 2006.

24. Низамутдинов М. Ф. Тактика защиты и нападения на Web-приложения. – Петербург, 2005, 432 с.

25. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. – М.: Горячая линия – Телеком, 2005, 229 с.

26. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защиты информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004.

27. Гамаюнов Д.Ю., Качалин А.И. Обнаружение атак на основе анализа переходов состояний распределённой системы. – Москва, 2004.

28. Горбатов В.С, Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия-Телеком, 2004, 248 с.

29. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров. – Москва, 2004.

30. G‘aniev S.K., Karimov M.M. Hisoblash sistemalari va tarmoqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qo‘llanma. – Toshkent Davlat texnika universiteti, 2003.

31. Астахов А.М. Аудит безопасности информационных систем. //Конфидент. 2003, -№1,2.

32. Соколов А., Степанюк О. Защита от компьютерного терроризма. Справочное пособие. БХВ – Петербург: Арлит, 2002.

33. ISO/IEC 27001:2005 – “Axborot texnologiyalari. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar”.

34. ISO/IEC 27002:2005 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

35. O‘zDStISO/IEC 27005:2013 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish”.

36. O‘zDStISO/IEC 27006:2013 – “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlarining auditi va ularni sertifikatlashtirish organlariga qo‘yiladigan talablar”.

37. ISO/IEC 15408-1-2005 – "Axborot texnologiyasi. Xavfsizlikni ta'minlash metodlari va vositalari. Axborot texnologiyalari xavfsizligini baholash mezonlari".

38. O'z DSt 1092:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari".

39. O'z DSt 1105:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi".

40. O'z DSt 1106:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi".

41. O'z DSt 1204:2009 – "Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik modullarga xavfsizlik talablari"

42. RH 45-215:2009 – Rahbariy hujjat. Ma'lumotlar uzatish tarmog'ida axborot xavfsizligini ta'minlash to'g'risida Nizom.

43. RH 45-185:2011 – Rahbariy hujjat. Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta'minlash dasturini ishlab chiqish tartibi.

44. RH 45-193:2007 – Rahbariy hujjat. Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta'minlash darajasini aniqlash tartibi.

45. TSt 45-010:2010 – Tarmoq standarti. Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta'riflar.

ILOVALAR

1 - ilova

RSA SHIFRLASH ALGORITMINING DASTURIY AMALGA OSHIRILISHI.

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

1-qadam. Ikkita 200dan 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:

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

Listing (S++ dasturlash tilida).

```
printf("Ikkitatubsonnikiriting\t: ");
scanf("%d%d",&p,&q);
n = p*q;
phi=(p-1)*(q-1);
printf("\n\tF(n)\t= %d",phi);
do
{
printf("\n\nKiritishe\t: ");
scanf("%d",&e);
```

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.

Listing (S++ dasturlash tilida).

```
while(FLAG==1);
d = 1;
do
{
s = (d*e)%phi;
d++;
}while(s!=1);
d = d-1;
```

6-qadam. Dastlabki axborotning fizik tabiatidan qat'iy nazar raqamli ikkili ko'rinishda ifodalanadi. Bitlar ketma-ketligi *L* bit uzunlikdagi bloklarga ajratiladi, bu herda $L–L \geq \log_2(n+1)$ shartini qanoatlantiruvchi eng kichik butun son. Har bir blok [0, *n*-1] oraliqqa taalluqli butun musbat son kabi ko'riladi. Shunday qilib, dastlabki axborot $X(i)$, $i=\overline{1,I}$ 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:

$$Y(i) = (X(i))^e \pmod n.$$

Listing (S++ dasturlash tilida).

```
    voidencrypt()
{
inti;
C = 1;
for(i=0;i<e;i++)
C=C*M%n;
C = C%n;
printf("\n\tShifrlanganso'z: %d",C);
}
```

Axborotni rasshifrovka qilishda quyidagi munosabatdan foydalaniladi:

$$X(i) = (Y(i))^d \pmod{n}.$$

Listing (S++ dasturlash tilida).

```
    voiddecrypt()
{
inti;
M = 1;
for(i=0;i<d;i++)
M=M*C%n;
M = M%n;
printf("\n\tDeshifrlanganso'z : %d",M);
}
```

DES shifrlash algoritmining dasturiy amalga oshirilishi.

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 ketma-ketlikning o'rnini almashtirish ko'zda tutilgan.

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

Hozirda bu standart quyidagi ikkita sabab ga ko‘ra foydalanishga butunlay yaroqsiz hisoblanadi:

- kalitning uzunligi 56 bitni tashkil etadi, bu shaxsiy kompyuterlarning 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).

DES algoritmining dasturiy kodi:

```
# include <stdio.h>
# include <fstream.h>
# include <string.h>
# include <iostream.h>
//Kalit kiritish jarayoni
int key[64]={
0,0,0,1,0,0,1,1,
0,0,1,1,0,1,0,0,
0,1,0,1,0,1,1,1,
0,1,1,1,1,0,0,1,
1,0,0,1,1,0,1,1,
1,0,1,1,1,1,0,0,
1,1,0,1,1,1,1,1,
1,1,1,1,0,0,0,1
};
//Bloklarga ajratish jarayoni
class Des
{
 public:
int keyi[16][48],
total[64],
left[32],
```

- right[32],
- ck[28],
- dk[28],
- expansion[48],
- z[48],
- xor1[48],
- sub[32],
- p[32],
- xor2[32],
- temp[64],
- pc1[56],
- ip[64],
- inv[8][8];
- char final[1000];
- void IP();
- void PermChoice1();
- void PermChoice2();
- void Expansion();
- void inverse();
- void xor_two();
- void xor_oneE(int);
- void xor_oneD(int);
- void substitution();
- void permutation();
- void keygen();
- char * Encrypt(char *);
- char * Decrypt(char *);
- };
- //Boshlang‘ich IP o‘zgartirish
- void Des::IP() //Initial Permutation
- {
- int k=58,i;
- for(i=0;i<32;i++)

```
{
ip[i]=total[k-1];
if(k-8>0) k=k-8;
else    k=k+58;
}
k=57;
for( i=32;i<64;i++)
{
ip[i]=total[k-1];
if(k-8>0)  k=k-8;
else       k=k+58;
}
}
void Des::PermChoice1() //Permutation Choice-1
{
int k=57,i;
for(i=0;i<28;i++)
{
pc1[i]=key[k-1];
if(k-8>0)  k=k-8;
else       k=k+57;
}
k=63;
for( i=28;i<52;i++)
{
pc1[i]=key[k-1];
if(k-8>0)  k=k-8;
else    k=k+55;
}
k=28;
for(i=52;i<56;i++)
{
pc1[i]=key[k-1];
```

- k=k-8;
- }
- }
- void Des::Expansion() //Expansion Function applied on `right' half
- {
- int exp[8][6],i,j,k;
- for(i=0;i<8;i++)
- {
- for(j=0;j<6;j++)
- {
- if((j!=0)||(j!=5))
- {
- k=4*i+j;
- exp[i][j]=right[k-1];
- }
- if(j==0)
- {
- k=4*i;
- exp[i][j]=right[k-1];
- }
- if(j==5)
- {
- k=4*i+j;
- exp[i][j]=right[k-1];
- }
- }
- }
- exp[0][0]=right[31];
- exp[7][5]=right[0];
- k=0;
- for(i=0;i<8;i++)
- for(j=0;j<6;j++)

- expansion[k++]=exp[i][j];
- }
- void Des::PermChoice2()
- {
- int per[56],i,k;
- for(i=0;i<28;i++) per[i]=ck[i];
- for(k=0,i=28;i<56;i++) per[i]=dk[k++];
- z[0]=per[13];z[1]=per[16];z[2]=per[10];z[3]=per[23];z[4]=p
er[0];z[5]=per[4];z[6]=per[2];z[7]=per[27];
- z[8]=per[14];z[9]=per[5];z[10]=per[20];z[11]=per[9];z[12]=
per[22];z[13]=per[18];z[14]=per[11];z[15]=per[3];
- z[16]=per[25];z[17]=per[7];z[18]=per[15];z[19]=per[6];z[2
0]=per[26];z[21]=per[19];z[22]=per[12];z[23]=per[1];
- z[24]=per[40];z[25]=per[51];z[26]=per[30];z[27]=per[36];z
[28]=per[46];z[29]=per[54];z[30]=per[29];z[31]=per[39];
- z[32]=per[50];z[33]=per[46];z[34]=per[32];z[35]=per[47];z
[36]=per[43];z[37]=per[48];z[38]=per[38];z[39]=per[55];
- z[40]=per[33];z[41]=per[52];z[42]=per[45];z[43]=per[41];z
[44]=per[49];z[45]=per[35];z[46]=per[28];z[47]=per[31];
- }
- void Des::xor_oneE(int round) //for Encrypt
- {
- int i;
- for(i=0;i<48;i++)
- xor1[i]=expansion[i]^keyi[round-1][i];
- }
- void Des::xor_oneD(int round) //for Decrypt
- {
- int i;
- for(i=0;i<48;i++)
- xor1[i]=expansion[i]^keyi[16-round][i];
- }
- void Des::substitution()

```
{
int s1[4][16]={
14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7,
0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8,
4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0,
15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13
};
int s2[4][16]={
15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10,
3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5,
0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15,
13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9
};
int s3[4][16]={
10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8,
13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1,
13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7,
1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12
};
int s4[4][16]={
7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15,
13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9,
10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4,
3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14
};
int s5[4][16]={
2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9,
14,11,2,12,4,7,13,1,5,0,15,10,3,9,8,6,
4,2,1,11,10,13,7,8,15,9,12,5,6,3,0,14,
11,8,12,7,1,14,2,13,6,15,0,9,10,4,5,3
};
int s6[4][16]={
12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11,
```

```
10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8,
9,14,15,5,2,8,12,3,7,0,4,10,1,13,11,6,
4,3,2,12,9,5,15,10,11,14,1,7,6,0,8,13
};
int s7[4][16]={
4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1,
13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6,
1,4,11,13,12,3,7,14,10,15,6,8,0,5,9,2,
6,11,13,8,1,4,10,7,9,5,0,15,14,2,3,12
};
int s8[4][16]={
13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7,
1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2,
7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8,
2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11
};
int a[8][6],k=0,i,j,p,q,count=0,g=0,v;
for(i=0;i<8;i++)
{
for(j=0;j<6;j++)
{
a[i][j]=xor1[k++];
}
}
for( i=0;i<8;i++)
{
p=1;q=0;
k=(a[i][0]*2)+(a[i][5]*1);
j=4;
while(j>0)
{
q=q+(a[i][j]*p);
p=p*2;
```

- j--;
- }
- count=i+1;
- switch(count)
- {
- case 1: v=s1[k][q]; break;
- case 2: v=s2[k][q]; break;
- case 3: v=s3[k][q]; break;
- case 4: v=s4[k][q]; break;
- case 5: v=s5[k][q]; break;
- case 6: v=s6[k][q]; break;
- case 7: v=s7[k][q]; break;
- case 8: v=s8[k][q]; break;
- }
- int d,i=3,a[4];
- while(v>0)
- {
- d=v%2;
- a[i--]=d;
- v=v/2;
- }
- while(i>=0)
- {
- a[i--]=0;
- }
- for(i=0;i<4;i++)
- sub[g++]=a[i];
- }
- }
- void Des::permutation()
- {
- p[0]=sub[15];p[1]=sub[6];p[2]=sub[19];p[3]=sub[20];p[4]=sub[28];p[5]=sub[11];p[6]=sub[27];p[7]=sub[16];

- p[8]=sub[0];p[9]=sub[14];p[10]=sub[22];p[11]=sub[25];p[12]=sub[4];p[13]=sub[17];p[14]=sub[30];p[15]=sub[9];
- p[16]=sub[1];p[17]=sub[7];p[18]=sub[23];p[19]=sub[13];p[20]=sub[31];p[21]=sub[26];p[22]=sub[2];p[23]=sub[8];
- p[24]=sub[18];p[25]=sub[12];p[26]=sub[29];p[27]=sub[5];p[28]=sub[21];p[29]=sub[10];p[30]=sub[3];p[31]=sub[24];
- }
- void Des::xor_two()
- {
- int i;
- for(i=0;i<32;i++)
- {
- xor2[i]=left[i]^p[i];
- }
- }
- void Des::inverse()
- {
- int p=40,q=8,k1,k2,i,j;
- for(i=0;i<8;i++)
- {
- k1=p;k2=q;
- for(j=0;j<8;j++)
- {
- if(j%2==0)
- {
- inv[i][j]=temp[k1-1];
- k1=k1+8;
- }
- else if(j%2!=0)
- {
- inv[i][j]=temp[k2-1];
- k2=k2+8;
- }

- }
- p=p-1;q=q-1;
- }
- }
- char * Des::Encrypt(char *Text1)
- {
- int i,a1,j,nB,m,iB,k,K,B[8],n,t,d,round;
- char *Text=new char[1000];
- strcpy(Text,Text1);
- i=strlen(Text);
- int mc=0;
- a1=i%8;
- if(a1!=0) for(j=0;j<8-a1;j++,i++) Text[i]=' '; Text[i]='\0';
- keygen();
- for(iB=0,nB=0,m=0;m<(strlen(Text)/8);m++) //Repeat for TextLenth/8 times.
- {
- for(iB=0,i=0;i<8;i++,nB++)
- {
- n=(int)Text[nB];
- for(K=7;n>=1;K--)
- {
- B[K]=n%2; //Converting 8-Bytes to 64-bit Binary Format
- n/=2;
- } for(;K>=0;K--) B[K]=0;
- for(K=0;K<8;K++,iB++) total[iB]=B[K]; //Now `total' contains the 64-Bit binary format of 8-Bytes
- }
- IP(); //Performing initial permutation on `total[64]'
- for(i=0;i<64;i++) total[i]=ip[i]; //Store values of ip[64] into total[64]
- for(i=0;i<32;i++) left[i]=total[i]; // +--> left[32]
- // total[64]--|

- for(;i<64;i++) right[i-32]=total[i];// +--> right[32]
- for(round=1;round<=16;round++)
- {
- Expansion(); //Performing expansion on `right[32]' to get `expansion[48]'
- xor_oneE(round); //Performing XOR operation on expansion[48],z[48] to get xor1[48]
- substitution();//Perform substitution on xor1[48] to get sub[32]
- permutation(); //Performing Permutation on sub[32] to get p[32]
- xor_two(); //Performing XOR operation on left[32],p[32] to get xor2[32]
- for(i=0;i<32;i++) left[i]=right[i]; //Dumping right[32] into left[32]
- for(i=0;i<32;i++) right[i]=xor2[i]; //Dumping xor2[32] into right[32]
- }
- for(i=0;i<32;i++) temp[i]=right[i]; // Dumping -->[swap32bit]
- for(;i<64;i++) temp[i]=left[i-32]; // left[32],right[32] into temp[64]
- inverse(); //Inversing the bits of temp[64] to get inv[8][8]
- /* Obtaining the Cypher-Text into final[1000]*/
- k=128; d=0;
- for(i=0;i<8;i++)
- {
- for(j=0;j<8;j++)
- {
- d=d+inv[i][j]*k;
- k=k/2;
- }
- final[mc++]=(char)d;

- k=128; d=0;
- }
- } //for loop ends here
- final[mc]='\0';
- return(final);
- }
- char * Des::Decrypt(char *Text1)
- {
- int i,a1,j,nB,m,iB,k,K,B[8],n,t,d,round;
- char *Text=new char[1000];
- unsigned char ch;
- strcpy(Text,Text1);
- i=strlen(Text);
- keygen();
- int mc=0;
- for(iB=0,nB=0,m=0;m<(strlen(Text)/8);m++) //Repeat for TextLenth/8 times.
- {
- for(iB=0,i=0;i<8;i++,nB++)
- {
- ch=Text[nB];
- n=(int)ch;//(int)Text[nB];
- for(K=7;n>=1;K--)
- {
- B[K]=n%2; //Converting 8-Bytes to 64-bit Binary Format
- n/=2;
- } for(;K>=0;K--) B[K]=0;
- for(K=0;K<8;K++,iB++) total[iB]=B[K]; //Now `total' contains the 64-Bit binary format of 8-Bytes
- }
- IP(); //Performing initial permutation on `total[64]'
- for(i=0;i<64;i++) total[i]=ip[i]; //Store values of ip[64] into total[64]

- for(i=0;i<32;i++) left[i]=total[i]; // +--> left[32]
- // total[64]--|
- for(;i<64;i++) right[i-32]=total[i];// +--> right[32]
- for(round=1;round<=16;round++)
- {
- Expansion(); //Performing expansion on `right[32]' to get `expansion[48]'
- xor_oneD(round);
- substitution();//Perform substitution on xor1[48] to get sub[32]
- permutation(); //Performing Permutation on sub[32] to get p[32]
- xor_two(); //Performing XOR operation on left[32],p[32] to get xor2[32]
- for(i=0;i<32;i++) left[i]=right[i]; //Dumping right[32] into left[32]
- for(i=0;i<32;i++) right[i]=xor2[i]; //Dumping xor2[32] into right[32]
- } //rounds end here
- for(i=0;i<32;i++) temp[i]=right[i]; // Dumping -->[swap32bit]
- for(;i<64;i++) temp[i]=left[i-32]; // left[32],right[32] into temp[64]
- inverse(); //Inversing the bits of temp[64] to get inv[8][8]
- /* Obtaining the Cypher-Text into final[1000]*/
- k=128; d=0;
- for(i=0;i<8;i++)
- {
- for(j=0;j<8;j++)
- {
- d=d+inv[i][j]*k;
- k=k/2;
- }

```
final[mc++]=(char)d;
k=128;  d=0;
}
} //for loop ends here
final[mc]='\0';
char *final1=new char[1000];
for(i=0,j=strlen(Text);i<strlen(Text);i++,j++)
final1[i]=final[j]; final1[i]='\0';
return(final);
}
int main()
{
Des d1,d2;
char *str=new char[1000];
char *str1=new char[1000];
 //strcpy(str,"PHOENIX it & ece solutions.");
cout<<"Enter a string : ";
gets(str);
str1=d1.Encrypt(str);
cout<<"\ni/p Text: "<<str<<endl;
cout<<"\nCypher : "<<str1<<endl;
//  ofstream fout("out2_fil.txt"); fout<<str1; fout.close();
cout<<"\no/p Text: "<<d2.Decrypt(str1)<<endl;
return 0;
}
// Kalit generatsiyasi jarayoni
void Des::keygen()
{
PermChoice1();
int i,j,k=0;
for(i=0;i<28;i++)
{
ck[i]=pc1[i];
```

```
}
for(i=28;i<56;i++)
{
dk[k]=pc1[i];
k++;
}
int noshift=0,round;
for(round=1;round<=16;round++)
{
if(round==1||round==2||round==9||round==16)
noshift=1;
else
noshift=2;
while(noshift>0)
{
int t;
t=ck[0];
for(i=0;i<28;i++)
ck[i]=ck[i+1];
ck[27]=t;
t=dk[0];
for(i=0;i<28;i++)
dk[i]=dk[i+1];
dk[27]=t;
noshift--;
}
PermChoice2();
for(i=0;i<48;i++)
keyi[round-1][i]=z[i];
}
}
```

Parolli autentifikatsiyalash algoritmining dasturiy amalga oshirilishi.

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.

Autentifikatsiyalash algoritmining dasturiy kodi(S++ dasturlash tilida).

Foydalanuvchini autentifikatsiyadan o'tkazish funksiyasi:

```
void Auth()
{
   cout<<"Authentification process";
   ifstream Passfile("password.txt", ios::in);
   Passfile>>inpass;
   ifstream Userfile("username.txt", ios::in);
   Userfile>>inuser;
   system("cls");
   cout<<"USERNAME: ";
   cin>>user;
   cout<<"PASSWORD: ";
   cin>>pass;
   Userfile.close();
   Passfile.close();
   if(user==inuser&&pass==inpass)
   {
```

```
        cout<<"\nHit enter to continue to members area";
              getch();
        //Nimadir sh qisin
        main();
    }
    else
    {
        cout<<"nope";
        getch();
        main();
    }
}
```

Foydalanuvchini ro‘yxatdan o‘tkazish funksiyasi:

```
void Registration()
{
    string tempuser, temppassword;
    cout<<"Enter Username: ";
    cin>>tempuser;
    cout<<"\nEnter password: ";
    cin>>temppassword;
    ofstream Userfile("username.txt", ios::out);
    Userfile<<tempuser;
    Userfile.close();
    ofstream Passfile("password.txt", ios::out);
    Passfile<<temppassword;
    Passfile.close();
    cout<<"Account hass been added";
    getch();
    main();
}
```

2-ilova

ATAMALARNING RUS, O‘ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG‘ATI

Авторизация – представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.

Avtorizasiya – tizimda foydalanuvchiga, uning ijobiy autenfikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.

Authorization – View user specific access rights on the basis of a positive result in its authentication system.

Авторское право – совокупность правовых норм, которые регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства.

Mualliflik huquqi – fan, adabiyot va san’at asarlarini yaratish, foydalanish va huquqiy himoyalashda vujudga keladigan munosabatlarni tartibga soluvchi huquqiy normalar majmui.

Copyright – the body of law, which regulate the relations arising in connection with the creation and use of scientific, literary and artistic works (copyright).

Администратор защиты – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Himoya ma’muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Security administrator – access entity responsible for the protection of the automated system from unauthorized access to information.

Акустическая защищенность выделенного помещения – уровень акустической защищенности выделенного помещения, достигнутый в результате проведения акустической защиты.

Ajratilgan xonaning akustik himoyalanganligi – akustik himoyaning o'tkazilishi natijasida erishilgan ajratilgan xonaning akustik himoyalanganligi darajasi.

Acoustic protection dedicated premises – level of acoustic protection dedicated space made as a result of acoustic protection.

Акустическая информация – информация, носителем которой являются акустические сигналы.

Akustik axborot – eltuvchisi akustik signallar bo'lgan axborot.

Acoustic information – information that is held by acoustic signals.

Алгоритм – упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Algoritm – amallarning cheklangan soni yordamida masala yechimini belgilovchi buyruqlarning cheklangan to'plami.

Algorithm – an ordered finite set of clearly defined rules for solving a finite number of steps.

Алгоритм блочного шифрования – алгоритм зашифрования, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков открытого текста, имеющих фиксированную длину. Представляет со-

бой алгоритм простой замены блоков текста фиксированной длины.

Shifrlashning blokli algoritmi – shifrlash algoritmi bo'lib, kalitning har bir muayyan qiymatida belgilangan uzunlikdagi ochiq matn bloklari to'plami ustida bitta qaytariluvchi akslantirishni amalga oshiradi. Belgilangan uzunlikdagi matn bloklarini oddiy almashtirish algoritmi hisoblanadi.

Block encryption algorithm – encryption algorithm that implements a fixed value for each key one reversible mapping of open block s of text with a fixed length. Algorithm is simple replacement of text blocks of fixed length.

Алгоритм поточного шифрования – алгоритм зашифрования, реализующий при каждом фиксированном значении ключа последовательность обратимых отображений (различных), действующую на последовательность блоков открытого текста.

Oqimli shifrlash algaritmi – shifrlash algoritmi bo'lib, kalitning har bir muayyan qiymatida ochiq matn bloklari ketma-ketligiga ta'sir etuvchi qaytariluvchi (turli) akslantirish ketma-ketligini amalga oshiradi.

Stream encryption algorithm – encryption algorithm that implements, for each fixed sequence of reversible key mappings (in general, different), acting on a sequence of blocks of text open.

Алгоритм шифрования – криптографический алгоритм, реализующий функцию зашифрования.

Shifrlash algoritmi – shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm.

Encryption algorithm – a cryptographic algorithm that implements the encryption function.

Криптографический алгоритм – алгоритм, реализующий вычисление одной из криптографических функций.

Kriptografik algoritm – kriptografik funksiyalarning birini hisoblashni amalga oshiruvchi algoritm.

Cryptographic algorithm – the algorithm that implements the computation of one of the cryptographic functions.

Алгоритм расшифрования – криптографический алгоритм, обратный к алгоритму зашифрования и реализующий функцию расшифрования.

Rasshifrovkalash algoritmi – rasshifrovkalash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Decryption algorithm – a cryptographic algorithm, the inverse of the algorithm encryption and decryption function implements.

Алгоритм формирования цифровой подписи – составная часть схемы цифровой подписи. Алгоритм (рандомизированный), на вход которого подаются подписываемое сообщение, секретный ключ, а также открытые параметры схемы цифровой подписи. Результатом работы алгоритма является цифровая подпись. В некоторых разновидностях схемы цифровой подписи при формировании подписи используется протокол.

Raqamli imzoni shakllantirish algoritmi – raqamli imzo sxemasining tarkibiy qismi. Kirish yo'liga imzolanuvchi xabar, maxfiy kalit hamda raqamli imzo sxemasining ochiq parametrlari beriluvchi algoritm (randomizatsiyalangan algoritm). Algoritm ishining natijasi raqamli imzo hisoblanadi. Raqamli imzo sxemasining ba'zi turlarida imzoni shakllantirishda protokol ishlatiladi.

The algorithm for generating a digital signature – rart of a digital signature scheme. Algorithm (generally randomized) whose input is fed to sign a message, secret key and public parameters of digital signature schemes. The result of the algorithm is a digital signature. In some species, the digital signature scheme used to generate the signature protocol.

Алгоритм хеширования – в криптографии – алгоритм, реализующий криптографическую хеш-функцию. В математике и программировании – алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале – от всех). Обычно, а. х. преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada – kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o‘zgartiruvchi algoritm. Chiqish yo‘li satrining har bir simvolining qiymati kirish yo‘li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog‘liq. Odatda, xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o‘zgartiradi.

Hashing algorithm – sryptography - an algorithm that implements a cryptographic hash function. In mathematics and programming - algorithm for transforming character strings, usually reduces the length of the string, and such that the value of each character of the output string depends in a complex way on a large number of input symbols (ideally - all). Typically, a. x. converts strings of arbitrary length to fixed-length strings.

Анализ трафика – 1. Заключение о состоянии информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота). 2. Анализ совокупности шифрованных сообщений, передаваемых по системе связи, не приводящий к дешифрованию, но позволяющий противнику и/или нарушителю получить косвенную информацию о передаваемых открытых сообщениях и в целом о функционировании наблюдаемой системы связи. А. т. использует особенности оформления шифрованных сообщений, их длину, время передачи, данные об отправителе и получателе и т. п.

Trafik tahlili – 1. Trafik oqimini kuzatish (borligi, yo'qligi, hajmi, yo'nalishi va chastotasi) asosida axborot holati xususida xulosa qilish. 2. Deshifrlanishga sabab bo'lmaydigan, ammo g'animga yoki buzg'unchiga uzatilayotgan ochiq matn va umuman, kuzatilayotgan aloqa tizimining ishlashi xususidagi bilvosita axborotni olishiga imkon beruvchi aloqa tizimi orqali uzatiluvchi shifrlangan xabarlar majmuining tahlili. Trafik tahlili shifrlangan xabarlarning rasmiylashtirish xususiyatlaridan, ularning uzunligi, uzatilish vaqti, uzatuvchi va qabul qiluvchi xususidagi malumotlardan foydalanadi.

Traffic Analysis – 1. Report on the state information based on observation of traffic flows (presence, absence, amount, direction and frequency. 2. Analysis of all encrypted messages sent over the communication system does not lead to decrypt, but allowing the opponent and / or the offender obtain indirect information about the transmitted Post and generally observed on the functioning of the communication system. A. that uses features of registration messages encrypted, and their length, the transmission time, the data sender and recipient, etc.

Сетевые анализаторы (сниффер) – программы, осуществляющие «прослушивание» сетевого трафика и автоматическое выделение из сетевого трафика имен пользователей, паролей, номеров кредитных карт, другой подобной информации.

Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini «tinglash»ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.

Network analyzers (sniffer) – Programs, asking for "listening" network traffic and automatically selects the network traffic of user names, passwords, credit card numbers, other similar information.

Анонимность – выражает предоставляемую участникам (протокола) возможность выполнять какое-либо действие анонимно, т. е. не идентифицируя себя. Однако при этом, участник обязан доказать свое право на выполнение этого действия. Анонимность бывает абсолютной и отзываемой.

Anonimlik – ishtirokchiga (protokol ishtirokchisiga) qanday-dir harakatni anonim tarzda, ya'ni o'zini identifikatsiyalamasdan, bajarilishini ifodalaydi. Ammo bunda, ishtirokchi ushbu harakatni bajarishga haqli ekanligini isbotlashi lozim. Anonimlik absolyut va chaqiriluvchi bo'lishi mumkin.

Anonymity – a concept related. Expresses provided to participants (protocol) to perform any act anonymously, without identifying themselves. In this case, however, the participant must prove their right to perform this action. Anonymity is absolute and recalls.

Антибот – программное обеспечение для автоматического обнаружения и удаления программ-роботов, программ-шпио-

нов (Spyware), несанкционированно установленного рекламного ПО (Adware) и других видов вредоносного ПО.

Antibot – robot-dasturlarni, ayg'oqchi dasturlarni (Spyware), ruxsatsiz o'rnatilgan reklama dasturiy ta'minotini (Adware) va boshqa zarar keltiruvchi dasturiy ta'minot turlarini avtomatik tarzda aniqlovchi va yo'q qiluvchi dasturiy ta'minot.

Security Code Software for automatic detection and removal of software robots, spyware (Spyware), illegally installed adware (Adware) and other types of malicious software .

Антивирус – программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. Программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также для восстановления исходного состояния зараженных объектов.

Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo'q qiluvchi dastur. Agar virus yo'q qilinmasa, zaharlangan dastur yo'q qilinadi. Shuningdek, viruslardan himoyalashga, zaharlangan dasturiy modullar va tizimli makonlarni aniqlashga hamda zaharlangan obyektlarning dastlabki holatini tiklashga mo'ljallangan dastur.

Antivirus – a program that detects and detects and removes viruses. If the virus is not removed, it is possible, the infected program is destroyed. still - a program designed to protect against viruses, detection of infected software modules and system areas, as well as the original, infected objects.

Аппаратные средства защиты – механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации

от несанкционированного доступа, копирования, кражи или модификации.

Himoyaning apparat vositalari – axborotni ruxsatsiz foydalanishdan, modifikatsiyalanishidan, nusxalashdan, o'g'rilanishidan himoyalashga mo'ljallangan mexanik, elektromexanik, elektron, optik, lazer, radio, radiotexnik, radiolokatsion va boshqa qurilmalar, tizimlar va inshootlar.

Hardware protection – mechanical, electromechanical, electronic, optical, laser, radio, radar and other devices, systems and structures designed to protect the information from unauthorized access, copying, modification or theft.

Аппаратура технической разведки – совокупность технических устройств обнаружения, приема, регистрации, измерения и анализа, предназначенная для получения разведывательной информации.

Texnik razvedka apparaturasi – razvedka axborotini olishga mo'ljallangan aniqlash, qabul qilish, qaydlash, o'lchash va tahlillash texnik qurilmalari majmui.

Equipment and technical intelligence – a set of technical detection devices, receiving, recording, measurement and analysis, designed for intelligence.

Асимметричный шифр – шифр, в котором ключ шифрования не совпадает с ключом дешифрирования.

Asimmetrik shifr – bunday shifrda shifrlash kaliti deshifrlash kalitiga mos kelmaydi.

Asymmetric cipher – a cipher in which the encryption key does not match the decryption key.

Атака – нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой.

Hujum – bosqinchining operatsion muhitini boshqarishiga imkon beruvchi axborot tizimi xavfsizligining buzilishi.

Attack – breach of security of information system, which allows the invader to manage operating environment.

Атака на отказ в обслуживании – атака с целью вызвать отказ системы, то есть, создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo'luvchi hujum, yani shunday sharoitlar tug'diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.

Denial-of-Service attack (DoS attack) – Attack to cause failure of the system, that is to create the conditions under which legitimate users can not get access to the resources provided by the system, or that access will be significantly hampered.

Аттестация – оценка на соответствие определенным требованиям. С точки зрения защиты, аттестации подлежат субъекты, пользователи или объекты, помещения, технические средства, программы, алгоритмы на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

Attestasiya – ma'lum talablarga mosligining bahosi. Himoya nuqtayi nazaridan, mos xavfsizlik sinflari bo'yicha axborotni himoyalash talablariga mosligini aniqlash maqsadida subyektlar,

foydalanuvchilar yoki obyektlar, binolar, texnik vositalar, dasturlar, algoritmlar attestasiya qilinadi.

Attestation – assessment for compliance with certain requirements. From a security standpoint subject to certification facilities, premises, facilities, programs, algorithms, to ensure compliance with the protection of information security in the appropriate classes.

Аудит (безопасности) – ведение контроля защищенности путем регистрации (фиксации в файле аудита) заранее определенного множества событий, характеризующих потенциально опасные действия в компьютерной системе, влияющие на ее безопасность.

Xavfsizlik auditi – kompyuter tizimi xavfsizligiga ta'sir etuvchi, bo'lishi mumkin bo'lgan xavfli harakatlarni xarakterlovchi, oldindan aniqlangan hodisalar to'plamini ro'yxatga olish (audit faylida qaydlash) yo'li bilan himoyalanishni nazoratlash.

Security audit – maintain security control by registering (fixation in the audit file) a predetermined set of events that characterize the potentially dangerous actions in the computer affecting its security.

Аутентификатор – средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.

Authenticator – authentication means representing the hallmark of the user. Means of user.

Аутентификация – проверка идентификации пользователя (проверка подлинности), устройства или другого компонента в системе, обычно, для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Autentifikatsiya – odatda, tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul qilish uchun foydalanuvchining (haqiqiyligini), qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikatsiyasini tekshirish; saqlanuvchi va uzatiluvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Authentication – checking user authentication (authentication), device or other component in the system, usually to make a decision about granting access to system resources; checking the integrity of stored or transmitted data to detect unauthorized modification.

Биометрическая аутентификация – способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.

Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko'z pardasining to'ri va h.) asosidagi autentifikat-

siyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo'lmasligi. Ularni esdan chiqarishning, yo'qotishning yoki boshqa foydalanuvchiga berishning iloji yo'q.

Biometric Authentication – Authentication Method subscriber (user), based on its verification of biometrics (fingerprints, hand geometry, face, voice, retina pattern, etc.). The advantages of this method is the inseparability of the biometric characteristics of the user: they can not be forgotten, lost or transferred to another user.

Двухфакторная аутентификация – аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Two-factor authentication – user authentication based on two different factors are usually based on what the user knows, and what he owns (eg password-based and physical identifier).

Многофакторная аутентификация – реализация контроля доступа, представляющая собой идентификацию пользователя на основе нескольких независимых факторов.

Ko'p faktorli autentifikatsiya – bir necha mustaqil faktorlar asosida foydalanuvchini identifikatsiyalash orqali foydalanish nazoratini amalga oshirish.

Multifactor Authentication – implementing access control, which is a user identification based on several independent factors.

Аутентичность – 1.Подлинность. 2.Свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Аутентичность применяется к таким субъектам, как пользователи, процессы, системы и информация.

Asliga to‘g‘rilik – 1. Haqiqiylik 2. Subyekt yoki resursning so‘ralganiga muvofiqligi kafolatlanuvchi xususiyat. Asliga to‘g‘rilik foydalanuvchilar, jarayonlar, tizimlar va axborot kabi subyektlarga qo‘llaniladi.

Authenticity – 1. Authenticity. 2. Feature ensures that the subject or resource identical stated. Authenticity applies to entities such as people, processes, systems and information.

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ.

Ma’lumotlar bazasi – tatbiqiy dasturlarga bog‘liq bo‘lmagan holda ma’lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy prinsiplarini ko‘zda tutuvchi ma’lum qoidalar bo‘yicha tashkil etilgan ma’lumotlar majmui.

Database – a set of data organized according to certain rules, general principles providing descriptions, storing and manipulating data, regardless of the application.

Банк данных – автоматизированная информационная система централизованного хранения и коллективного использования данных.

Ma’lumotlar banki – ma’lumotlarni markazlashgan saqlashning va kollektiv foydalanishning avtomatlashtirilgan axborot tizimi.

Databank – automated information system for centralized storage and sharing of data.

Безопасная операционная система – операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов.

Xavfsiz operatsion tizim – ma'lumotlar va resurslar mazmuniga mos himoyalash darajasini ta'minlash maqsadida apparat va dasturiy vositalarni samarali boshqaruvchi operatsion tizim.

Secure operating system – an operating system that effectively manages the hardware and software to provide the level of protection corresponding to the content data and resources controlled by the system.

Безопасность – свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательное ее состояние. Состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонала системы), компьютерами или программами.

Xavfsizlik – ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifan, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Ma'lumotlar fayllarining va dasturlarning ishlatilishi, ko'rib chiqilishi va avtorizatsiyalanmagan shaxslar (jumladan, tizim xodimi), kompyuterlar yoki dasturlar tomonidan modifikatsiyalanishi mumkin bo'lmagan holat.

Security – property system to withstand external or internal factors destabilizing effect of which may be undesirable its state or behavior. Also, a state in which data files and programs may not be

used, viewed and modified by unauthorized persons (including staff system) computers or programs.

Безопасность автоматизированной информационной системы – совокупность мер управления и контроля, защищающий APIS от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения АИС и данных.

Avtomatlashtirilgan axborot tizim xavfsizligi – avtomatlashtirilgan axborot tizimini xizmatdan voz kechishidan va ruxsatsiz (atayin yoki tasodifan) fosh etilishidan, modifikatsiyalanishidan yoki uning va ma'lumotlarning buzilishidan himoyalovchi boshqarish va nazorat choralari majmui.

Automated information system security – a set of measures of management and control, protecting APIS denial of service and unauthorized (intentional or accidental) disclosure, modification or destruction of AIS data.

Безопасность информации – состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение. Состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность /конфиденциальность/, целостность и доступность.

Axborot xavfsizligi – axborot holati bo'lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta'sir etishga yoki uning olinishiga yo'l qo'yilmaydi. Axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydala-

nuvchanlik kabi xarakteristikalarining (xususiyatlarining) saqlanishini ta'minlovchi axborotning himoyalanish sathi holati.

Information security – state information, which prevents accidental or intentional tampering or unauthorized information to receive it, also - state -level data protection during processing technologies to support the preservation of its qualitative characteristics (properties) as privacy / confidentiality / integrity and availability.

Информационная безопасность – способность системы противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение.

Axborot xavfsizligi – ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifan, ichki va tashqi informatsion ta'sirlarga qarshi tizimning tura olish xususiyati.

Safety information – the system's ability to resist accidental or intentional, internal or external information influences, that could result in an undesirable state or her behavior.

Безопасность информационно – коммуникационных технологий – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информационно-телекоммуникационных технологий.

Axborot – kommunikatsiya texnologiyalar xavfsizligi – axborot - telekommunikatsiya texnologiyalarining konfidensialligini, yaxlitligini, foydalanuvchanligini, bosh tortmasligini, hisobotdorligini, asliga to'g'riligini va ishonchliligini aniqlash, ularga erishish va madadlash bilan bog'liq barcha jihatlar.

ICT security – communication technology (ICT security) - All aspects related to the definition, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and telecommunication technologies.

Сетевая безопасность – меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает в себя защиту оборудования, программного обеспечения и данных.

Tarmoq xavfsizligi – axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy ishlashiga tasodifan yoki atayin aralashishdan yoki tarmoq komponentlarini buzishga urinishdan ehtiyot qiluvchi choralar. Asbob-uskunalarni, dasturiy ta'minotni, ma'lumotlarni himoyalashni o'z ichiga oladi.

Network Security – measures that protect the network information from unauthorized access, accidental or intentional interference with normal activities or attempts to destroy its components. Includes the protection of hardware, software, data.

Безотказность – способность системы выполнять возложенные на нее функции в требуемый момент времени в задаваемых условиях.

Buzilmaslik – tizimning unga yuklatilgan vazifalarini, berilgan sharoitda istalgan vaqt onida bajarish qobiliyati.

Reliability – The ability of the system to fulfill its function in the desired time in the given conditions.

Биометрические данные – средства аутентификации, представляющие собой такие личные отличительные признаки пользователя, как тембр голоса, форма кисти руки, отпечатки

пальцев и т.д., оригиналы которых в цифровом виде хранятся в памяти компьютера.

Biometrik ma'lumotlar – autentifikatsiya vositasi bo'lib, foydalanuvchining barmoq izlari, qo'l panjasining geometrik shakli, yuz shakli va o'lchamlari, ovoz xususiyatlari, ko'z yoyi va to'r pardasining shakli kabi shaxsiy, farqli alomatlari. Asl nusxalari raqam ko'rinishida kompyuter xotirasida saqlanadi.

Biometric data – authentication, which are personal features such as user tone of voice, the shape of the hand, fingerprints, etc., The originals of which are stored digitally in a computer memory.

Бот – (сокр. от робот) специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь. При обсуждении компьютерных программ термин употребляется в основном в применении к Интернету.

Bot – ("robot" so'zining qisqartirilgani) oddiy foydalanuvchi interfeysi orqali avtomatik tarzda va / yoki berilgan jadval bo'yicha qandaydir harakatlarni bajaruvchi maxsus dastur. Kompyuter dasturlari muhokama qilinganida bot atamasi asosan Internetga qo'llash bilan ishlatiladi.

Bot – 1. (Short for robot) Special program will be executed automatically and / or on the schedule any action through the same interface as a normal user. In the discussion, the term computer program is used mainly in the application to the Internet.

Ботнет – компьютерная сеть, состоящая из нескольких хостов с запущенными ботами. Обычно используются для координации сетевых атак на компьютеры – рассылки спама, хищения личных данных пользователей, перебора паролей на уда-

лённой системе, атак на отказ в обслуживании и т.п. (от англ. слов robot и network).

Botnet – ishga tushurilgan botlarga ega bir qancha sonli xostlardan tashkil topgan kompyuter tarmog'i. Odatda, kompyuterlarga bo'ladigan tarmoq hujumlarini – spamni tarqatish, foydalanuvchilarning shaxsiy ma'lumotlarini o'g'rilash, masofadagi tizimda parollarni saralash, xizmat qilishdan voz kechishga undash hujumlarini muvofiqlashtirish uchun ishlatiladi. (inglizcha robot va network so'zlaridan olingan.)

Botnet – computer network consisting of a number of hosts running bots. Usually used to coordinate attacks on network computers - spam, identity theft users of brute force on the remote system attacks denial of service, etc. (from the English. words robot and network).

Брандмауэр – метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами. Является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).

Brandmauer – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan hamda tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli. Bir necha komponentlardan (masalan, brandmauer dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan himoya to'sig'i hisoblanadi.

Firewall – a method of protecting the network from security threats from other systems and networks by centralizing network

access and control of hardware and software. Also, is a protective barrier, consisting of several components (such as a router or gateway that is running firewall software).

Брандмауэр с фильтрацией пакетов – является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отбраковывать определенные виды входящих и исходящих пакетов.

Paketlarni filtrlovchi brandmauer – kiruvchi va chiquvchi paketlarni ma'lum xillarini brakka chiqarish maqsadida konfiguratsiyalangan dasturiy ta'minot ishlaydigan marshrutizator yoki kompyuter.

Packet-filtering firewall – a router or computer on which the software is running, configured so as to reject certain types of incoming and outgoing packets.

Брандмауэр экспертного уровня – проверяет содержимое принимаемых пакетов на трех уровнях модели OSI - сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Ekspert sathidagi brandmauer – olinadigan paketlarni ISO modelining uchta sathida tarmoq, seans va tatbiqiy sathlarda tekshiradi. Ushbu vazifani bajarishda paketlarni filtrlashning maxsus algoritmlari ishlatiladi. Ular yordamida har bir paket avtorizatsiyalangan paketlarning ma'lum shablonlari bilan taqqoslanadi.

Stateful inspecthion firewall – checks the contents of the packets received on the three levels of the model OSI - network, session and application. To perform this task, use special packet

filtering algorithms by which each packet is compared with the known pattern of authorized packets.

Верификация – процесс сравнения двух уровней спецификации средств вычислительной техники или их комплексов на надлежащее соответствие. В программировании доказательство правильности программ. Различают два подхода к верификации: статические и конструктивные методы.

Verifikatsiya – hisoblash vositalari yoki ularning kompleksi spetsifikatsiyasining ikki sathini tegishli moslikka taqqoslash jarayoni. Dasturlashda – dastur to‘g‘riligining tasdig‘i. Verifikatsiyaga ikkita yondashish farqlanadi: statik va konstruktiv usullar.

Verification – the process of comparing two levels of specification of computer equipment or systems for proper alignment. Also - programming proof of the correctness of programs. There are two approaches to verification: static and constructive methods.

Взламывание пароля – техника (способ) тайно получать доступ к информационной системе (сети), в которой нападающая сторона с помощью вскрывателя паролей пробует угадать (подобрать) или украсть пароли.

Parolni buzib ochish – axborot tizimidan (tarmog‘idan) yashirincha foydalanish texnikasi (usuli) bo‘lib, hujum qiluvchi taraf parollarni fosh qiluvchi yordamida parollarni aniqlashga (tanlashga) yoki o‘g‘rilashga urinib ko‘radi.

Cracking password – tech (method) secretly to access the system (network) information, in which the attacker using opener tries to guess passwords (pick) or steal passwords.

Виды механизмов защиты – некоторыми видами механизмов защиты являются: шифрование, аспекты административного управления ключами, механизмы цифровой подписи,

механизмы управления доступом, механизмы целостности данных, механизмы обмена информацией аутентификации, механизмы заполнения трафика, механизм управления маршрутизацией, механизм нотаризации, физическая или персональная защита, надежное аппаратное/программное обеспечение.

Himoya mexanizmlari turlari – himoya mexanizmlarining ba'zi turlari - shifrlash, kalitlarni ma'muriy boshqarish jihatlari, raqamli imzo mexanizmlari, foydalanishni boshqarish mexanizmlari, ma'lumotlar yaxlitligi mexanizmlari, augentifikatsiya axborotini almashish mexanizmlari, trafikni to'ldirish mexanizmlari, marshrutlashni boshqarish mexanizmi, notarizatsiya mexanizmi, fizik yoki shaxsiy himoya, ishonchli apparat.

Types of protection mechanisms – some kinds of protection mechanisms are: encryption, key management aspects of administrative, digital signature mechanisms, access control mechanisms, mechanisms for data integrity, information exchange mechanisms authentication mechanisms fill traffic routing control mechanism, the mechanism of notarization, physical or personal protection, reliable hardware / software.

Вирус – небольшая программа, которая вставляет саму себя в другие программы при выполнении. Программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии.

Virus – o'zini boshqa dasturlar bajarilayotganida ularga kirituvchi unchalik katta bo'lmagan dastur. Nusxalarini beixtiyor yaratish, shuningdek, keyinchalik yangi nusxasini boshqarish va

qayta yaratishga erishish maqsadida fayllardagi va tizimli sohalardagi boshqa dasturlarni modifikatsiyalash imkoniyatiga ega dastur.

Virus – a small program that inserts itself into other programs when executed. Still - a program which can spontaneously create their copies and modifies other programs stored in files or system areas for subsequent management and reproduction of a new copy.

Загрузочный вирус – вирус, заражающий загрузочные части жестких и/или гибких дисков.

Yuklama virus – qattiq va/yoki qayishqoq disklarning yuklama qismini zaharlovchi virus.

Boot virus – a virus that infects the boot of the hard and / or floppy disks.

Вирус невидимка – вирус, использующий специальные алгоритмы, маскирующие его присутствие на диске (в некоторых случаях в оперативной памяти).

Ko'rinmas virus – diskda (ba'zida asosiy xotirada) ekanligini niqoblovchi maxsus algoritmdan foydalanuvchi virus.

Stealth virus – a virus that uses special algorithms, masking its presence on the disk (in some cases in RAM).

Полиморфные (зашифрованные) вирусы – вирусы, предпринимающие специальные меры для затруднения их поиска и анализа. Не имеют сигнатур, то есть, не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения.

Polimorf (shifrlangan) viruslar – qidirishlarini va tahlillashlarini qiyinlashtirish uchun maxsus choralarni ko'ruvchi viruslar. Signaturalarga ega emas, ya'ni kodning birorta ham doimiy qismiga

ega emas. Aksariyat holda bitta polimorf virusning ikkita namunasi birorta ham moslikka ega bo'lmaydi.

Polymorphic viruses (encrypted) – viruses take special measures to obstruct their search and analysis. Do not have a signature, not contain any permanent part of the code. In most cases, two samples of the same polymorphic virus does not have any overlap.

Восстанавливаемость – свойство загружаемого модуля, состоящее в возможности защиты его в процессе выполнения от модификации как им самим, так и любым другим модулем. Программа восстановления может заменить такой модуль новым экземпляром, не повлияв при этом ни на порядок обработки, ни на конечный результат.

Tiklanuvchanlik – yuklanuvchi modulning bajarilishi jarayonida modifikatsiyalanishidan o'zi yoki ixtiyoriy boshqa modul tomonidan himoyalash mumkinligi hususiyati. Tiklash dasturi bunday modulni, ishlash tartibiga, yakuniy natijaga ta'sir etmasdan, yangi nusxasi bilan almashtirishi mumkin.

Recoverability (refreshable) – loadable module property of being able to protect it during the execution of the modification of both themselves and any other module. The recovery program can replace a module with a new instance, without affecting neither an order processing or the end result.

Вскрыватель паролей – компьютерная программа, которая осуществляет подбор или похищение паролей.

Parollarni fosh qiluvchi – parollarni tanlashni yoki o'g'rilashni amalga oshiruvchi kompyuter dasturi.

Password cracker – computer program that carries out the selection or stealing passwords.

Вторжение – неправомочный доступ или проникновение любого рода (физическое или информационное) в компьютеры, информационные системы и сети непосредственно или опосредованно через корреспондирующие сети или системы.

Bostirib kirish – noqonuniy foydalanish yoki kompyuterga, axborot tizimi va tarmog'iga bevosita yoki bilvosita, tarmoq yoki tizim orqali ixtiyoriy xil (fizik yoki axborot) kirish.

Intrusion – Unauthorized access or penetration of any kind (physical or informational) in computers, information systems and networks, or indirectly through offsetting network or system.

Вычислительная сеть (компьютерная сеть) – система взаимосвязанных между собой компьютеров, а также технического и программного обеспечения для их взаимодействия.

Hisoblash tarmog'i (kompyuter tarmog'i) – bir-birlari bilan o'zaro bog'langan kompyuterlar tizimi hamda ularning o'zaro harakatlari uchun texnik va dasturiy ta'minot.

Area network (computer network) – a system of interconnected computers, as well as hardware and software for their interaction.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные.

Gammalash – ochiq ma'lumotlarga ma'lum qonuniyat bo'yicha gamma shifrini singdirish jarayoni.

Gamming - the process of applying for a specific law on the open range of the cipher data.

Гарантия защиты – наличие сертификата соответствия для технического средства обработки информации или аттестата на объект информатики, подтверждающих, что безопасность

обрабатываемой информации соответствует требованиям стандартов и других нормативных документов.

Himoyaning kafilligi – ishlanadigan axborot xavfsizligining standartlar va boshqa me'yoriy hujjatlar talablariga mosligini tasdiqlovchi axborotni ishlovchi texnik vositalarga moslik sertifikatining yoki informatika obyektiga attestatning mavjudligi.

Security accredidation – a certificate of conformity to the technical means of information processing or certificate for Informatics to confirming that the security of information processed complies with the standards and other normative documents.

Генератор – составная часть транслятора, выполняющая генерацию машинных команд.

Generator – mashina komandalarini generatsiyalovchi translyatorning tarkibiy qismi.

Generator – part of the translator performs the generation of machine instructions.

Генератор ключей – техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), последовательности ключевой, векторов инициализации и т. п.

Kalitlar generatori – kalit (kriptotizim kaliti), kalit ketmaketligi, initsializatsiya vektorlari va h. sifatida ishlatiluvchi son massivlari yoki boshqa ma'lumotlarni ishlab chiqarishga mo'ljallangan texnik qurilma yoki dastur.

Key generator – technical device or program designed to generate arrays of numbers or other data to be used as keys (cryptographic) key sequence, initialization vectors, and so on.

Генератор псевдослучайных последовательностей – техническое устройство или программа для выработки псевдослучайных последовательностей.

Psevdotasodifiy ketma-ketliklar generatori – psevdotasodifiy ketma-ketliklarni ishlab chiqaruvchi texnik qurilma yoki dastur.

Pseudorandom generator – technical device or a program for generating pseudo-random sequences.

Генератор случайных паролей – программно – аппаратное средство, представляющее собой генератор случайных чисел, используемых в качестве паролей.

Tasodifiy parollar generatori – parollar sifatida ishlatiluvchi tasodifiy sonlar generatoridan iborat dasturiy-apparat vosita.

Randompassword generator – tools of software and hardware agent representing a random number generator to be used as passwords.

Генератор случайных чисел – программа или устройство, предназначенные для выработки последовательности псевдослучайных чисел по заданному закону распределения.

Tasodifiy sonlar generatori – berilgan taqsimlanish qonuniyati bo'yicha psevdotasodifiy ketma-ketlikni shakllantirish uchun mo'ljallangan dastur yoki qurilma.

Random number generator – program or device designed to generate a sequence of pseudorandom numbers from a given distribution law.

Государственная тайна – сведения, охраняемые государством, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для ее обороноспособности, государственной безопасности, эконо-

мических и политических интересов. К государственной тайне относится секретная информация с грифами «особой важности» и «совершенно секретно».

Davlat siri – davlat tomonidan muhofaza qilinuvchi, fosh qilinishi davlatning harbiy-iqtisodiy potensialining sifatiy holatiga salbiy ta'sir etuvchi yoki uning mudofaa imkoniyati, davlat xavfsizligi, iqtisodiy va siyosiy manfaatlari uchun boshqa og'ir oqibatlarga olib kelishi mumkin bo'lgan ma'lumotlar. Davlat siriga "juda muhim" va "mutlaqo maxfiy" grifli axborot taalluqli.

State secret – information protected by the state, the disclosure of which could have a negative impact on the qualitative state of military-economic potential of the country or cause other serious consequences for its defense, national security, economic and political interests. To state secret is secret information classified "special importance" and "top secret".

Готовность системы – мера способности системы выполнять свои функции при нахождении в рабочем состоянии. Количественно готовность можно оценивать с помощью коэффициента готовности.

Tizimning tayyorligi – tizimning ishlash holatida o'z vazifalarini bajarish qobiliyatining o'lchovi. Miqdoran, tayyorlikni tayyorlik koeffitsienti yordamida baholash mumkin.

System availability – measure the system's ability to perform its functions when in working condition. Readiness can be assessed quantitatively by the coefficient of readiness.

Данные – информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека либо автоматическими средствами.

Ma'lumotlar – odam ishtirokida yoki avtomatik tarzda uzatishga, izohlashga yoki ishlashga yaroqli, formallashgan ko'rinishda ifodalangan axborot.

Data – information presented in a formalized manner suitable for communication, interpretation or processing involving human or automated means.

Идентификационные данные – совокупность уникальных идентификационных данных, соответствующие конкретному участнику и позволяющие осуществить однозначную его идентификацию в системе.

Identifikatsiya ma'lumotlari – tizimda bir ma'noli identifikatsiyalanishiga imkon beruvchi, muayyan qatnashchiga tegishli noyob identifikatsiya ma'lumotlari majmui.

Data identification – a set of unique identification data corresponding to a specific party, it allows an unambiguous identification of the system.

Дезинформация – сознательное искажение передаваемых сведений с целью ложного представления у лиц, использующих эти сведения; передача ложной информации.

Dezinformatsiya – foydalanuvchi shaxslarda yolg'on tasavvurni shakllantirish maqsadida ularga uzatiluvchi xabarni atayin buzib ko'rsatish; yolg'on axborotni uzatish.

Misinformation – deliberate distortion of transmitted data with the purpose of the false representations in individuals using this information; transmission of false information.

Длина (размер) ключа – длина слова в определённом алфавите, представляющего ключ. Длина ключа бинарного измеряется в битах.

Kalit uzunligi (o'lchovi) – kalitni ifodalovchi ma'lum alfavitdagi so'z uzunligi. Ikkili kalit uzunligi bitlarda o'lchanadi.

Key length – word length in a certain alphabet, representing the key. The key length is measured in binary bits.

Доверие – основа для уверенности в том, что продукт или система информационных технологий отвечают целям безопасности.

Ishonch – axborot texnologiyalari mahsuloti yoki tizimining xavfsizlik maqsadlariga javob berishiga ishonish uchun asos.

Assurance – basis for confidence that the product or system information technology meet the security objectives.

Доверительность – свойство соответствия безопасности некоторым критериям.

Ishonchlilik – xavfsizlikning qandaydir mezonlarga moslik xususiyati.

Trusted funcionality – property according security with some critiries

Конфиденциальный документ – документ ограниченного доступа на любом носителе, содержащий конфиденциальную информацию.

Maxfiy hujjat – maxfiy axborotli ixtiyoriy eltuvchidan foydalanish cheklangan hujjat.

Confidential document – document restricted in any medium, containing confidential information.

Документированная информация – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Hujjatlangan axborot – rekvizitlari identifikatsiyalanishiga imkon beruvchi, material eltuvchida qaydlangan axborot.

Documented information – fixed in a tangible medium with requisites allowing its identification.

Домен безопасности – ограниченная группа объектов и субъектов безопасности, к которым применяется одна методика безопасности со стороны одного и того же администратора безопасности.

Xavfsizlik domeni – xavfsizlikning bitta ma'muri tomonidan xavfsizlikning bir xil usuli qo'llaniladigan xavfsizlik subyektlari va obyektlarining cheklangan guruhi.

Secyrity domain – limited group of objects and subjects of security, to which the one method of security from the same security administrator.

Достоверность – свойство информации быть правильно воспринятой; вероятность отсутствия ошибок.

Ishonchlilik – axborotninig to'g'ri o'zlashtirilish xususiyati; xatolik yo'qligining ehtimolligi.

Validity – property information to be correctly perceived; the probability of no errors.

Доступ – предоставление данных системе обработки данных или получение их из нее путем выполнения операций поиска, чтения и (или) записи данных.

Foydalanish – ma'lumotlarni ishlash tizimiga ma'lumotlarni taqdim etish yoki undan qidirish, o'qish va/yoki yozish amallarini bajarish yo'li bilan ma'lumotlarni olish.

Access – providing data processing system or getting them out of it by doing a search, read and (or) data record.

Доступ к информации – процесс ознакомления с информацией, ее документирование, модификация или уничтожение,

осуществляемые с использованием штатных технических средств.

Axborotdan foydalanish – shtatga oid texnik vositalardan foydalanib axborot bilan tanishish, uni hujjatlash, nusxalash, modifikatsiyalash yoki yo‘q qilish jarayoni.

Access to information – the process of reviewing the information, documenting, modification or destruction, implemented by the staff of technical means. still - familiar with the information, information processing, in particular, copying, modification or destruction of information.

Доступ к конфиденциальной информации – санкционированное полномочным должностным лицом ознакомление конкретного лица с информацией, содержащей сведения конфиденциального характера.

Konfidensial axborotdan foydalanish – muayyan shaxsga tarkibida konfidensial xarakterli ma’lumot bo‘lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati

Access to confidential information – authorized official introduction of a particular person with the information containing confidential information.

Несанкционированный доступ к информации – получение защищаемой информации заинтересованным субъектом с нарушением прав или правил доступа к защищаемой информации установленных правовыми документами или собственником, владельцем информации.

Axborotdan ruxsatsiz foydalanish – manfaatdor subyekt tomonidan o‘rnatilgan huquqiy hujjatlarni yoki mulkdor, axborot egasi tomonidan himoyalanuvchi axborotdan foydalanish huquqlari yoki qoidalarini buzib, himoyalanuvchi axborotga ega bo‘lishi.

Unauthorized access to information – preparation of protected information interested entity in violation of the legal instruments or by the owner, the owner of the information or rights of access to protected information.

Ограниченный доступ – доступ к информационному ресурсу, разрешаемый установленными для данного ресурса правилами доступа только определенному кругу лиц, обладающих соответствующими полномочиями.

Cheklangan foydalanish – axborot resursidan, ushbu resursga faqat mos vakolatlarga ega shaxslarning ma'lum doirasiga o'rnatilgan foydalanish qoidalari bo'yicha ruxsatli foydalanish.

Restricted access – access to the resources of the information allowed by the established rules for the resource access only certain persons with appropriate authority.

Доступность – свойство логического объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

Foydaluvchanlik – avtorizatsiyalangan mantiqiy obyekt so'rovi bo'yicha mantiqiy obyektning tayyorlik va foydalanuvchanlik holatida bo'lish xususiyati.

Availability - property of an object in a state of readiness and usage upon request authorized entity.

Живучесть – свойство системы оставаться работоспособной в условиях внешних воздействий.

Yashovchanlik – tizimning tashqi ta'sirlar sharoitida ishga layoqatli qolishi xususiyati.

Viability – property of the system to remain operational under external influences.

Журнал восстановления – журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в Б.Д. (файле) с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

Tiklash jurnali – ma'lumotlar bazasi yoki faylni tiklash imkoniyatini ta'minlovchi jurnal. Unda ma'lumotlar bazasidagi (fayldagi) ma'lumotlarning haqiqiyligi aniqlangan va oxirgi rezerv nusxa olingan ondan boshlab, barcha o'zgarishlar xususida axborot mavjud.

Recovery log – magazine, providing the ability to restore a database or file. Contains information about all the changes in DB (file) from the moment when it was found that the data is reliable and has been made the last backup.

Заверение – регистрация данных у доверенного третьего лица для дальнейшей уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Ishontirish – mazmuni, ma'lumotlar manbai, yetkazish vaqti kabi xarakteristikalarning to'g'riligiga bundan buyon ishonish uchun ma'lumotlarni ishonchli uchinchi shaxsda qaydlash.

Notalization – registration data from a trusted third party for further confidence in the correctness of such properties as the source of data, the time of delivery.

Заполнение трафика – генерация фиктивных сеансов обмена данными, фиктивных блоков данных и/или фиктивных данных в составе блоков данных.

Trafikni to‘ldirish – ma’lumotlar almashishining soxta seanslarini, ma’lumotlarning soxta bloklarini va/yoki ma’lumotlar bloklari tarkibida soxta ma’lumotlarni generatsiyalash.

Filling traffic – generate dummy data exchange session, dummy data units and / or the dummy data comprising data blocks.

Запрос идентификации – запрос, заданный ведущей станцией ведомой станции для ее идентификации или определения ее состояния.

Identifikatsiya so‘rovi – boshqaruvchi stansiyaning boshqariluvchi stansiyaga uni identifikatsiyalash yoki holatini aniqlash uchun bergan so‘rovi.

Request identification – query specified slave master station to identify it or determine its status.

Заражение – процесс создания в вычислительной технике вирусом своей копии, связанный с изменением кодов программ, системных областей или системных таблиц.

Zaharlash – hisoblash texnikasida virusning dastur, tizimli zona yoki tizimli jadvallarning o‘zgarishi bilan bog‘liq o‘zining nusxasini yaratish jarayoni.

Infection – in computing the process of creating copies of its virus associated with changes in program codes, system areas or system tables.

Зарегистрированный пользователь – пользователь, имеющий приоритетный номер в данной системе коллективного пользования.

Ro‘yxatga olingan foydalanuvchi – berilgan kollektiv foydalanuvchi tizimda ustuvor nomerli foydalanuvchi.

Authorized user – a user with a priority number in the system of collective use.

Защита – средство для ограничения доступа или использования всей или части вычислительной системы; юридические, организационные и технические, в том числе программные меры предотвращения несанкционированного доступа к аппаратуре, программам и данным.

Himoyalash – hisoblash tizimidan yoki uning qismidan foydalanishni cheklash vositasi; apparaturadan, dasturdan va ma'lumotlardan ruxsatsiz foydalanishni bartaraf etuvchi tashkiliy va texnik, jumladan, dasturiy choralar.

Protection, security, lock out – means for restriction of access or use of all or part of the computing system; legal, organizational and technical, including program, measures of prevention of unauthorized access to the equipment, programs and data.

Антивирусная защита – комплекс организационных, правовых, технических и технологических мер, применяемых для обеспечения защиты средств вычислительной техники и автоматизированной системы от воздействия программных вирусов.

Virusga qarshi himoya – hisoblash texnikasi va avtomatlashtirilgan tizim vositalarini dasturiy virus ta'siridan himoyalashni ta'minlashda ishlatiluvchi tashkiliy, huquqiy, texnik va texnologik choralar kompleksi.

Protection anti-virus – the complex of the organizational, legal, technical and technological measures applied to ensuring protection of computer aids and system of automated from influence of viruses program.

Защита информации – включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание

целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Axborotni himoyalash – axborot xavfsizligini ta'minlashga yo'naltirilgan tadbirlar kompleksi. Amalda axborotni himoyalash deganda ma'lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar kerak bo'lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

Information protection – includes a complex of the actions aimed at providing information security. In practice is understood as maintenance of integrity, availability and if it is necessary, confidentiality of information and the resources used for input, storage, and processing and data transmission.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Axborotni kriptografik himoyalash – axborotni kriptografik o'zgartirish yordamida himoyalash.

Cryptographic protection of information – information security by means of its cryptographic transformation.

Организационная защита информации – защита информации, осуществляемая путем принятия административных мер.

Axborotni tashkiliy himoyalash – ma'muriy choralarni qo'llash yo'li bilan amalga oshiriluvchi axborot himoyasi.

Information security organizational – the Information security which is carried out by acceptance of administrative measures.

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных

субъектов (потребителей), не имеющих права доступа к этой информации.

Axborotni fosh qilinishdan himoyalash – himoyalanuvchi axborotni, ushbu axborotdan foydalanish huquqiga ega bo'lmagan manfaatdor subyektlarga (iste'molchilarga) ruxsatsiz yetkazishni bartaraf etishga yo'naltirilgan axborot himoyasi.

Information security from disclosure – the information security directed on prevention of unauthorized finishing of protected information to interested subjects (consumers), not having right of access to this information.

Защита информации от технических разведок – деятельность, направленная на предотвращение или существенное снижение возможностей технических разведок по получению разведывательной информации путем разработки и реализации системы защиты.

Axborotni texnik razvedkadan himoyalash – himoyalash tizimini ishlab chiqish va amalga oshirish yo'li bilan texnik razvedkaning axborot olish imkoniyatlarini bartaraf qilishga yoki jiddiy kamaytirishga yo'naltirilgan faoliyat.

Information security from technical investigations – the activity directed on prevention or essential decrease in opportunities of technical investigations on obtaining prospecting information by development and realization of system of protection.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (ино-

странными) разведками и другими заинтересованными субъектами.

Axborotni sirqib chikishidan himoyalash – himoyalanuvchi axborotning fosh qilinishi va undan ruxsatsiz foydalanish natijasida, nazoratsiz tarqalishini bartaraf etishga hamda (ajnabiy) razvedka va boshqa manfaatdor subyektlar tomonidan o'zlashtirilishini istisno qilishga (qiyinlashtirishga) yo'naltirilgan axborot himoyasi.

Information security from leak – the information security directed on prevention of uncontrollable distribution of protected information as a result of its disclosure and unauthorized access to it, and also on an exception (difficulty) of obtaining protected information (foreign) investigations and other interested subjects.

Защита от несанкционированного доступа – предотвращение или существенное затруднение несанкционированного доступа к программам и данным путем использования аппаратных, программных, криптографических методов и средств защиты, а также проведение организационных мероприятий. Наиболее распространенным программным методом защиты является система паролей.

Ruxsatsiz foydalanishdan himoyalash – apparat-dasturiy va kriptografik usullar va vositalar yordamida hamda tashkiliy tadbirlarni o'tkazib, dasturlardan va ma'lumotlardan ruxsatsiz foydalanishni bartaraf etish yoki jiddiy qiyinlashtirish. Himoyalishning eng keng tarqalgan dasturiy usuli parollar tizimi hisoblanadi.

Protection from unauthorized access – prevention or essential difficulty of unauthorized access to programs and this way of use of hardware, program and cryptographic methods and means of protection, and also carrying out organizational actions. The most

widespread program method of protection is the system of passwords.

Злоумышленник – лицо или организация, заинтересованные в получении несанкционированного доступа к программам или данным, предпринимающие попытку такого доступа или совершившие его.

Niyati buzuq – dasturlardan yoki ma'lumotlardan ruxsatsiz foydalanishdan manfaatdor, bunday foydalanishga uringan yoki amalga oshirgan shaxs yoki tashkilot.

Intruder – the person or the organization interested in receiving unauthorized access to programs or data, making an attempt of such access or made it.

Идентификатор – средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

Identifikator – subyekt yoki obyektning farqlanuvchi alomatidan iborat foydalanishning identifikatsiya vositasi. Foydalanuvchilar uchun asosiy identifikatsiya vositasi parol hisoblanadi.

Identifier – means of identification of the access, representing a distinctive sign of the subject or object of access. The main means of identification of access for users is the password.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Foydalanish identifikatori – foydalanuvchi subyekt yoki obyektning noyob alomati.

Access identifier – unique sign of the subject or object of access.

Идентификатор пользователя – символическое имя, присваиваемое отдельному лицу или группе лиц, разрешающее использование ресурсов вычислительной системы.

Foydalanuvchi identifikatori – hisoblash tizimi resurslaridan foydalanish uchun alohida shaxsga yoki shaxslar guruhiga beriladigan ramziy ism.

User identifier, userid – symbol the check name appropriated to the individual or a group of persons and allowing use of resources of the computing system.

Идентификация – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Identifikatsiya – foydalanish subyektlari va obyektlariga identifikator berish va/yoki taqdim etilgan identifikatorni berilganlari ro'yxati bilan taqqoslash.

Identification – assignment to subjects and objects of access of the identifier and/or comparison of the shown identifier with the list of the appropriated identifiers.

Избирательное управление доступом – метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит.

Foydalanishni tanlab boshqarish – foydalanuvchini, jarayonni va/yoki u tegishli guruhni identifikatsiyalashga va tanishga asoslangan tizim subyektlarining obyektlardan foydalanishni boshqarish usuli.

Discretionary access control (DAC) – method of control over access of subjects of system to. To the objects, based on iden-

tification and an identification of the user, process and/or group to which it belongs.

Имитация – активная атака на криптографический протокол, целью которой является навязывание противником и/или нарушителем одной из сторон сообщения от имени другой стороны, которое не будет отвергнуто при приеме.

Imitatsiya – qabul qilinishida rad etilmaydigan, dushman va/yoki buzg'unchi tomonidan taraflarning biri xabarini taraflarning ikkinchisi nomidan majburan qabul qildirish maqsadida kriptografik protokolga faol hujum.

Imitation – attack active on the protocol cryptographic which purpose is imposing by the opponent and/or the violator of one of the message parties on behalf of other party which won't be rejected at reception.

Имитовставка – отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа, добавленный к зашифрованным данным для обеспечения имитозащиты.

Imitovstavka – imitohimoyani ta'minlash maqsadida ochiq ma'lumotlardan va kalitdan ma'lum qoida bo'yicha olingan va shifrlangan ma'lumotlarga qo'shilgan axborotning belgilangan uzunlikdagi bo'lagi.

Massage authentication code – piece of information of the fixed length, received by a certain rule from open data and a key and added to the ciphered data for providing imitation protection.

Имитозащита – защита системы шифрованной связи от навязывания ложных данных.

Imitohimoya – shifrlangan aloqa tizimini yolg'on ma'lumotlarning majburan kiritilishidan himoyalash.

Integrity protection, protection from imitation – protection of system of encoded communication against imposing of false data.

Имитостойкость – свойство криптографической системы (криптографического протокола), характеризующее способность противостоять активным атакам со стороны противника и/или нарушителя, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных.

Imitobardoshlik – maqsadi yolg'on xabarni majburan kiritish, uzatiluvchi xabarni almashtirish yoki saqlanuvchi ma'lumotlarni o'zgartirish bo'lgan dushman yoki/va buzg'unchi tomonidan qilinadigan faol hujumlarga qarshi tura olish qobiliyati orqali xarakterlanuvchi kriptografik tizim (kriptografik protokol) xususiyati.

Imitation resistance – property of system cryptographic (the protocol cryptographic), characterizing ability to resist to attacks active from the opponent and/or the violator which purpose is imposing of the untrue report, substitution of the transferred message or change of stored data.

Социальная инженерия – обход системы информационной безопасности с помощью информации, получаемой из контактов с обслуживающим персоналом и пользователям путем введения их в заблуждение различными уловками, обмана и т.д.

Ijtimoiy injeneriya – xizmatchi xodimlar va foydalanuvchilar bilan muloqotda turli nayranglar va aldashlar orqali chalg'itish yo'li bilan olingan axborotdan foydalanib, axborot xavfsizligi tizimini chetlab o'tish.

Social engeneering – round system of information security with using information obtained from contacts with serves staff and

users by introducing them in delusion different tricks, deception, etc.

Инсайдер – член группы людей, имеющий доступ к закрытой информации, принадлежащей этой группе. Как правило, является ключевым персонажем в инциденте, связанным с утечкой информации. С этой точки зрения различают следующие типы инсайдеров: халатные, манипулируемые, обиженные, нелояльные, подрабатывающие, внедренные и т.п.

Insayder – guruhga tegishli yashirin axborotdan foydalanish huquqiga ega guruh a'zosi. Odatda, axborot sirqib chiqish bilan bog'liq mojaroda muhim shaxs hisoblanadi. Shu nuqtayi nazardan insayderlarning quyidagi xillari farqlanadi: beparvolar, manipulyatsiyalanuvchilar, ranjiganlar, qo'shimcha pul ishlovchilar va h.

Insider – the member of group of the people having access to the classified information, belonging this group. As a rule, is the key character in the incident, connected with information leakage. From this point of view distinguish the following types of insiders: negligent, manipulated, offended, disloyal, earning additionally, introduced, etc.

Информационная надежность – 1. Способность алгоритма или программы правильно выполнять свои функции при различных ошибках в исходных данных. 2. Способность информационной системы обеспечивать целостность хранящихся в ней данных.

Axborot ishonchliligi – 1. Dastlabki ma'lumotlardagi turli xatoliklarda algoritm yoki dasturning o'z vazifasini to'g'ri bajarish qobiliyati. 2. Axborot tizimining unda saqlanayotgan ma'lumotlar yaxlitligini ta'minlash qobiliyati.

Information reliability – 1.Abilityofalgorithm or the program it is correct to carry out the functions at various mistakes in basic data. 2. Ability of information system to provide integrity of the data which were stored in it.

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Axborot tizimi – hujjatlarning (hujjatlar massivining) va axborot texnologiyalarining, xususan, axborot jarayonlarini amalga oshiruvchi hisoblash texnikasi va aloqa vositalaridan foydalanib, tashkiliy tartibga solingan majmui.

Information system – organizationally ordered set of documents (document files) and information technologies, including with use of computer aids and the communications, realizing information processes.

Информационная технология – система технических средств и способов обработки информации.

Axborot texnologiyasi – axborotni ishlash usullari va texnik vositalari tizimi.

Information technology – system of technical means and ways of information processing.

Инфраструктура открытых ключей – подсистема системы ключевой асимметричной шифрсистемы. Предназначена для обеспечения (с помощью сертификатов ключей) доверия законных пользователей к подлинности ключей, соответствия ключей пользователям и оговоренным условиям их применения.

Ochiq kalitlar infrastrukturasi – asimmetrik shifrtizim kalitlari tizimining qismtizimi. Qonuniy foydalanuvchilarning kalitlarning haqiqiyligiga, kalitlarning foydalanuvchilarga va ular oldindan kelishilgan ishlatish shartlariga mosligiga ishonishlarini (kalitlar sertifikatlari yordamida) ta'minlashga mo'ljallangan.

Public Key Infrastructure (PKI) – subsystem of system key cipher system of asymmetric. It is intended for providing (by means of certificates of keys) trust of users of lawful keys to authenticity, compliance of keys to users and the stipulated conditions of their application.

Инцидент – зафиксированный случай попытки получения несанкционированного доступа или проведения атаки на компьютерную систему.

Mojaro – ruxsatsiz foydalanish huquqiga ega bo'lishga yoki kompyuter tizimiga hujum o'tkazishga urinishning qayd etilgan holi.

Incident – the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.

Искажение – отклонение значений параметров сигнала данных от установленных требований. Изменение содержимого сообщения, передаваемого по линии связи.

Buzilish – ma'lumotlar signali parametrlari qiymatlarining o'rnatilgan talablardan chetlanishi. Aloqa liniyasi bo'yicha uzatiluvchi xabar tarkibining o'zgarishi.

Distortion – deviation of values of parameters of a signal of data from the established requirements. Still - change of contents of the message transferred on the communication lines.

Канал передачи данных – физическая среда, по которой передается информация из одного устройства в другое.

Ma'lumotlarni uzatuvchi kanal – fizik muhit, u orqali axborot bir qurilmadan ikkinchisiga uzatiladi.

Data transmission channel – the physical environment on which information from one device is transferred to another.

Канал проникновения – путь от злоумышленника к источнику конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям.

Kirib olish kanali – niyati buzuqdan to konfidensial axborot manbaigacha bo'lgan yo'l. U orqali himoyalanuvchi ma'lumotlardan ruxsatsiz foydalanish mumkin.

Insecurity channel – actual path from the malefactor to a source of confidential information by means of which unauthorized access to protected data is possible.

Канал утечки информации – физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможно несанкционированное получение охраняемых сведений (совокупность источника коммерческой тайны, физической среды и средства промышленного шпионажа).

Axborot sirqib chiqaruvchi kanal – qo'riqlanuvchi ma'lumotlardan (tijorat siri, fizik muhit va sanoat ayg'oqchilik vositalari majmui) ruxsatsiz foydalanishga imkon beruvchi konfidensial axborot manbaidan to niyati buzuqgacha bo'lgan fizik yo'l.

Information leakage channel – actual path from a source of confidential information to the malefactor, on which probably unauthorized obtaining protected data (set of a source of a trade secret, the physical environment and means of industrial espionage).

Киберпреступность – действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хи-

щение или разрушение информации в корыстных или хулиганских целях.

Kiberjinoyatilik – g‘arazli yoki xuliganlik maqsadlarda himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxs yoki guruh harakatlari.

Cyber cryme – actions of individuals or the groups, directed on breaking of systems of computer protection, on plunder or information destruction in the mercenary or hooligan purposes.

Кибертерроризм – действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных общественно опасных последствий.

Kiberterrorizm – insonlar halokati, aytarlicha moddiy zarar xavfini va boshqa jamiyatga xavfli oqibatlarni tug‘diruvchi kompyuter tizimlarini chalg‘itish bo‘yicha harakatlar.

Cyber terrorism – actions on disorganization of the computer systems creating danger of death of people, significant property damage or other socially dangerous consequences.

Открытый ключ – несекретный ключ асимметричной шифросистемы.

Ochiq kalit – asimmetrik shifrtizimning maxfiy bo‘lmagan kaliti.

Public key – unclassified key the asymmetric cryptosystem.

Разовый ключ – ключ, однократно используемый для шифрования в цикле (в жизненном цикле ключей). Обычно не подлежит хранению и является элементом составного ключа.

Bir martali kalit – siklda (kalitlarning hayot siklida) shifrlash uchun bir marta ishlatiluvchi kalit. Odatda saqlanmaydigan va tarkibiy kalit elementi hisoblanadi.

Once-only key – the key which is once used for enciphering in a cycle (vital keys). Usually isn't subject to storage and is an element of a key compound.

Ключ расшифрования – ключ, используемый при расшифровании.

Deshifrlash kaliti – deshifrlashda ishlatiluvchi kalit.

Decryption key – the key used for decryption.

Сеансовый ключ – ключ, специально сгенерированный для одного сеанса связи между двумя участниками (протокола).

Seans kaliti – ikkita qatnashchilar (protokol qatnashchilari) orasidagi bitta aloqa seansi uchun maxsus generatsiyalangan kalit.

Session key – the key which has been specially generated for one communication session between two participants (protocol).

Секретный ключ – ключ, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной симметричной шифросистемы или к использованию некоторых функций данной асимметричной шифросистемы.

Maxfiy kalit – ma'lum simmetrik shifrtizim kalitlaridan yoki ma'lum asimmetrik shifrtizimning ba'zi funksiyalaridan foydalanish huquqiga ega bo'lmagan shaxslardan maxfiy sanaluvchi kalit.

Secret key – the key kept in a secret from persons, not having the admission to keys given symmetric cryptosystem or to use of some functions given the asymmetric cryptosystem.

Код – 1. Представление символа двоичным кодом. 2. Криптографический прием, в котором используется произ-

вольная таблица или кодировочная книга для преобразования текста в закодированную форму.

Kod – 1. Simvolni ikkilik kod orqali ifodalash. 2. Matnni kodlangan shaklga o'zgartirishda ixtiyoriy jadvaldan yoki kodlash kitobidan foydalanuvchi kriptografik usul.

Code – 1. Symbol representation by a binary code. 2. Cryptographic reception in which any table or the quoted book for transformation of the text to the coded form is used.

Код аутентификации – вид алгоритма имитозащищающего кодирования информации. Как правило, к. а. сопоставляет сообщению его код аутентичности сообщения. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения.

Autentifikatsiya kodi – axborotni imitohimoyalovchi kodlash algoritmining turi. Odatda, autentifikatsiya kodi xabarni uning asliga to'g'ri kodi bilan taqqoslaydi. Axborotning haqiqiyligi xususida qaror qabul qilish algoritmi xabarning asliga to'g'ri kodi qiymatini tekshirishga asoslangan.

Authentication code – type of algorithm of coding imitation secure information. As a rule, authentication code compares to the message its code of authenticity of the message. The algorithm of decision-making on authenticity of information is based on check of value of a code of authenticity of the message.

Код аутентичности сообщения – Специальный набор символов, добавляемый к сообщению в протоколах аутентификации сообщений с доверяющими друг-другу участниками, предназначенный для обеспечения его целостности и аутентификации источника данных.

Xabarning asliga to‘g‘riligi kodi – bir-biriga ishonuvchi ishtirokchilar tomonidan xabarlarni autentifikatsiyalash protokollarida xabarga qo‘shiladigan va uning yaxlitligini va ma’lumotlar manbaining autentifikatsiyasini ta’minlashga mo‘ljallangan simvollarning maxsus nabori.

Message authentication code, seal, integrity check value – in protocols of authentication of messages with participants trusting each other – the special character set added to the message and intended for ensuring its integrity and authentication of data source.

Компрометация – утеря значительной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т.д.).

Obro‘sizlantirish – jiddiy axborotni yo‘qotish yoki uni avtorizatsiyalanmagan subyektlar (shaxslar, dasturlar, jarayonlar va h.) tomonidan o‘zlashtirilishi.

Compromising – loss of critical information or receiving it the subjects not authorized for this purpose (persons, programs, processes, etc.)

Контроль доступа – определение и ограничение доступа пользователей, программ или процессов к устройствам, программам и данным вычислительной системы.

Foydalanish nazorati – foydalanuvchilarning, dasturlarning yoki jarayonlarning hisoblash tizimlari qurilmalaridan, dasturlaridan va ma’lumotlaridan foydalanishlarini aniqlash va cheklash.

Access control – definition and restriction of access of users, programs or processes to devices, programs and data of the computing system.

Концепция защиты информации – система взглядов и общих технических требований по защите информации.

Axborotni himoyalash konsepsiyasi – axborotni himoyalash bo‘yicha qarashlar va umumiy texnik talablar tizimi.

The concept of information security – frame of reference and the general technical requirements on information security.

Криптографическая система – совокупность технических и/или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

Kriptografik tizim – axborotni kriptografik o‘zgartirishni va kalitlarni taqsimlash jarayonini boshqarishni ta’minlovchi texnik va/yoki dasturiy vositalar, tashkiliy usullar majmui.

Cryptographic system, Cryptosystem – set technical and/or software, the organizational methods providing cryptographic transformation of information and management process of distribution of keys.

Лицензия – разрешение на право продажи или предоставления услуг.

Litsenziya – sotish yoki xizmat ko‘rsatish huquqiga ruxsatnoma.

License – permission to the right of sale or service.

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации, оформленное лицензионным соглашением /договором/.

Axborot himoyasi sohasidagi litsenziya – axborot xavfsizligi sohasida u yoki bu ishlarni bajarish huquqiga litsenzion bitim (shartnoma) bilan rasmiylashtirilgan ruxsatnoma.

License information security – permission to the right of carrying out these or those works in the field of the information security, issued by the license agreement/contract/.

Ложная информация – информация, ошибочно отражающая характеристики и признаки, а также информация о не существующем реальном объекте.

Yolg'on axborot – xarakteristikalarni va alomatlarni noto'g'ri akslantiruvchi axborot hamda real mavjud bo'lmagan obyekt husu-sidagi axborot.

False information – information which is mistakenly reflecting characteristics and signs, and also information on object not existing really.

Макровирусы – программы на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и так далее).

Makroviruslar – qandaydir ma'lumotlarni ishlash tizimiga (matn redaktoriga, elektron jadvallarga va h.) o'rnatilgan tillardagi (makrotillardagi) dasturlar.

Macro viruses – programs in the languages (macrolanguages) which have been built in some systems of data processing (text editors, spreadsheets and so on).

Мандат – разновидность указателя, определяющий путь доступа к объекту и разрешенные над ним операции.

Mandat – obyektdan foydalanish va uning ustida ruxsat etil-gan amallarni bajarish yo'lini aniqlovchi ko'rsatkich turi.

Mandate – kind of the index defining a way of access to object and operations allowed over it.

Мандатное управление доступом – концепция (модель) доступа субъектов к информационным ресурсам по грифу сек-

ретности, разрешенной к пользованию информации, определяемому меткой секретности /конфиденциальности/.

Foydalanishni mandatli boshqarish – maxfiylik (konfidensiallik) belgisi orqali aniqlanuvchi maxfiylik grifi bo'yicha axborotdan foydalanishga ruxcat etilgan subyektlarning axborot resurslaridan foydalanish konsepsiyasi (modeli).

Mandate management access – the concept (model) of access of subjects to information resources on the security classification of information allowed for using determined by a tag of privacy/confidentiality/.

Маскарад – попытка получить доступ к системе, объекту или выполнение других действий субъектом, не обладающим полномочиями на соответствующее действие и выдающим себя за другого, которому эти действия разрешены.

Maskarad – tegishli harakatlarni amalga oshirishga vakolatlari bo'lmagan subektning o'zini boshqa vakolatli shaxs deb ko'rsatib, u shaxs nomidan harakatlarning imkoniyatlariga va imtiyozlariga ega bo'lishga urinishi.

Masquerade – attempt to get access to system, object or performance of other actions by the subject which isn't possessing powers on the corresponding action and giving out for another to which these actions are allowed.

Матрица доступа – таблица, отображающая правила доступа субъектов к информационным ресурсам, данные о которых хранятся в диспетчере доступа. Таблица, отображающая правила разграничения доступа.

Foydalanish matritsasi – Ma'lumotlari foydalanish dispetcherida saqlanuvchi axborot, axborot resurslaridan subyektlarning

foydalanish qoidalarini aks ettiruvchi jadval; foydalanishni cheklash qoidalarini aks ettiruvchi jadval.

Access matrix – the table displaying rules of access of subjects to information resources, given about which are stored in the dispatcher of access. Also, the table displaying rules of differentiation of access.

Матрица полномочий – таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта относительно защищаемых данных.

Vakolatlar matritsasi – elementlari muayyan obyektning himoyalanuvchi ma'lumotlarga nisbatan huquqlarini (vakolatlarini, imtiyozlarini) belgilovchi jadval.

Privilege matrix – the table, which elements define the rights (powers, privileges) a certain object from nositelno protected data.

Менеджмент риска – полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.

Xavf-xatar menedjmenti – axborot-telekommunikatsiya texnologiya resurslariga ta'sir etishi mumkin bo'lgan xavfli hodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to'liq jarayoni.

Risk management – full process of identification, control, elimination or reduction of consequences of dangerous events which can have impact on resources of information and telecommunication technologies.

Модель нарушителя правил доступа – абстрактное описание нарушителя правил доступа к информационному ресурсу. Примерами моделей нарушителя правил доступа являются

такие программы, как троянский конь, логическая бомба, компьютерный вирус и другие.

Foydalanish qoidalarini buzuvchining modeli – axborot resursidan foydalanish qoidalarini buzuvchining abstrakt tavsifi. Axborot resursidan foydalanish qoidalarini buzuvchining modeli sifatida troyan dasturini, mantiqiy bombani, kompyuter virusini va h. ko'rsatish mumkin.

Model intruder access rules – abstract the description of the breaker of rules of access to information resource. Examples of models of the breaker of rules of access are such programs as the Trojan horse, a logical bomb, a computer virus and others.

Модификация информации – изменение содержания или объема информации на ее носителях при обработке техническими средствами.

Axborotni modifikatsiyalash – axborotni texnik vositalarida ishlashda uning mazmunini yoki hajmini o'zgartirish.

Modification of information – to change the content or the amount of information on the processing of technical means.

Мониторинг безопасности информации – постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

Axborot xavfsizligi monitoringi – axborot xavfsizligi talablariga mosligini aniqlash maqsadida axborot tizimidagi axborot xavfsizligini ta'minlash jarayonini muttasil kuzatish.

Information security monitoring – constant monitoring of the process information security in the system information to determine its compliance with information security.

Наблюдаемость – возможность для ответственных за защиту информации лиц восстанавливать ход нарушения или попытки нарушения безопасности информационной системы.

Kuzatuvchanlik – axborot himoyasiga javobgar shaxslar uchun axborot tizimi xavfsizligini buzish jarayonini yoki buzishga urinishlarni tiklash imkoniyati.

Observability – an opportunity for those responsible for data protection officials to restore the course of violations or attempted violations of information system security.

Надежность – характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени.

Ishonchlilik – ma'lum sharoitlarda berilgan vaqt oralig'ida funksional uzelning, qurilmaning, tizimning o'ziga topshirilgan vazifalarni bajarish qobiliyatining xarakteristikasi.

Reliability – the ability of the functional characteristics of node devices, the system under certain circumstances to carry out the desired function during a certain period of time.

Нападающий – субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Hujumchi – harakati ko'rilayotgan kompyuter tizimida axborot xavfsizligini buzadigan subyekt.

Attacker – a subject whose actions violate the information security in a under consideration computer system.

Нарушение полномочий – попытка пользователя или программы выполнить неразрешенную операцию.

Vakolatlarning buzilishi – foydalanuvchining yoki dasturning ruxsat etilmagan amalni bajarishga urinishi.

Privilege violation – user or program attempts to perform an unauthorized operation.

Нарушение системы безопасности – успешное поражение средства управления безопасностью, которое завершается проникновением в систему.

Xavfsizlik tizimining buzilishi – tizimga suqilib kirish bilan tugallanadigan xavfsizlikni boshqarish vositalarining shikastlanishi.

Security system violation – the successful defeat security controls, which concludes with penetration into the system.

Нарушение целостности – искажение содержимого записей файла или базы данных. Происходит вследствие машинных сбоев, программных ошибок, а также ошибочных действий пользователей.

Yaxlitlikning buzilishi – fayl yoki ma'lumotlar bazasidagi yozuvlarning buzilishi. Mashinaning yanglishishi, dasturiy xatoliklar hamda foydalanuvchilarning noto'g'ri harakatlari natijasida ro'y beradi.

Integrity violation – the distortion of the contents of the recorded files or database. Thid is due to machine failures, software errors and erroneous actions of users.

Нарушение целостности информации – утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения.

Axborot yaxlitligining buzilishi – axborotning, uni texnik vositalari yordamida ishlanishida yo'qotilishi, ruxsatsiz modifikat-

siyalanishi yoki yo‘q qilinishi natijasida yaxlitlik xususiyatining yo‘qolishi.

Information integrity violation - the loss of information when it is processed by technical means, the integrity of the property as a result of its unauthorized modification or unauthorized destruction.

Нарушитель – субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Buzg‘unchi – harakatlari ko‘rilayotgan kompyuter tizimida axborot xavfsizligini buzadigan subyekt.

Attacker – a subject whose actions violate the information security in a computer system under consideration.

Обработка данных – систематическое выполнение операций над данными.

Ma’lumotlarni ishlash – ma’lumotlar ustida amallarning muntazam bajarilishi.

Data processing – manipulation of data by a computer.

Ошибка в данных – ошибочное представление одного или нескольких исходных данных может стать причиной аварийного завершения программы либо оказаться необнаруженной, но результаты нормально завершившейся программы будут при этом неверными.

Ma’lumotlardagi xatolik – bir yoki bir necha dastlabki ma’lumotlarning xato ifodalanishi, dasturning avariyali tugallanishiga sabab bo‘lishi mumkin yoki xatolik aniqlanmasligi mumkin, ammo tugallangan dastur natijasi noto‘g‘ri bo‘ladi.

Data error – presentation errors of one or more source data might become cause of accident program crash or be undetected, but the results normally complete the program will under this infidels.

Пакетная фильтрация – процесс пропускания или блокирования пакетов в сети на основе адресов отправителя и получателя, значений портов или протоколов. П.ф., как правило, является частью программного обеспечении firewall, защищающего локальную сеть от нежелательных вторжений.

Paketli filtratsiya – jo'natuvchi va qabul qiluvchi adreslari, portlar yoki protokollar qiymatlari asosida tarmoqdagi paketlarni o'tkazish yoki blokiroqka qilish jarayoni. Paketli filtrlash, odatda, lokal tarmoqni nomaqbul suqilib kirishlardan himoyalovchi tarmoqlararo ekran dasturiy ta'minotining qismi hisoblanadi.

Packet Filtering – missing process or blocking process packets in a network based on the values and destination addresses, ports, or protocols. P.f, as a rule, is a piece of software protection firewall, protecting the local network from unwanted intrusions.

Одноразовый пароль – пароль, действительный только для одного сеанса или транзакции. Наряду с многофакторной аутентификацией о.п. уменьшает риск подключения к системе с незащищенной рабочей станции.

Bir martali parol – faqat bitta seans yoki tranzaksiya uchun haqiqiy parol. Bir martali parol, ko'p faktorli autentifikatsiyalash bilan birga, himoyalanmagan ishchi stansiyali tizimga ulanish xavf-xatarini kamaytiradi.

One-Time Password (OTP) – is a password that is valid for only one login session or transaction, on a computer system or other digital device.

Пароль – уникальная последовательность символов, которую необходимо ввести по запросу компьютера, чтобы исключить доступ к системе, программе или данным.

Parol – tizimdan, dasturdan yoki ma'lumotlardan foydalanishga ruxsat olish uchun kompyuter so'rovi bo'yicha kiritiladigan simvollarning noyob ketma-ketligi.

Password – a password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user.

Перестановка – криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных.

Joyini o'zgartirish – ma'lumotlar blokida alohida bitlar yoki simvollarning joylashish tartibini o'zgartirish bilan bog'liq kriptografik amal.

Permutation – cryptographic operations, connected to the change in the order of the individual bits or symbols in the data block.

Подделка информации – умышленная несанкционированная модификация информации при ее обработке техническими средствами с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

Axborotni soxtalash – axborotning texnik vositalarda ishlanishida raqibning oldida muayyan foyda (afzallik) olish maqsadida axborotni atayin ruxsatsiz modifikatsiyalash.

Fake information (Forgery) – intentional unauthorized modification of data when it is processed by technical means to obtain certain benefits (benefits) to a competitor or suffering damage.

Подотчетность – возможность проверки; имеет две стороны: во-первых, любое состояние системы можно вернуть в исходное для выяснения того, как система в нем оказалась; во-вторых, имеющийся порядок проведения аудита безопасности позволяет гарантировать, что система удовлетворяет всем заявленным требованиям.

Hisobdorlik – tekshirish imkoniyati. Ikkita jihatga ega: birinchidan, tizimning har qanday holatini, ushbu holatga qay tarzda tushib qolganini aniqlash uchun dastlabki holatiga qaytarish; ikkinchidan, xavfsizlik auditini o'tkazishning mavjud tartibi tizimning barcha bildirilgan talablarni qoniqtirishini kafolatlashga imkon beradi.

Auditability – ability to test; has two aspects: firstly, any state of the system can be reset to determine how the system was in it; Second, the existing procedures for auditing the security helps ensure that your system meets all the stated requirements.

Цифровая подпись – представляет собой строку в некотором алфавите (например, цифровую), зависящую от сообщения или документа и от некоторого секретного ключа, известного только подписывающему субъекту. Предполагается, что ц. п. должна быть легко проверяемой без получения доступа к секретному ключу.

Raqamli imzo – xabarga yoki hujjatga va faqat imzo chekuvchi subyektga ma'lum qandaydir maxfiy kalitga bog'liq qandaydir alfavitdagi qatordan (masalan, raqamli qatordan) iborat. Raqamli imzoning, maxfiy kalitdan foydalanmasdan, osongina tekshirilishi lozimligi faraz qilinadi.

Digital signature – is a string in some alphabet (eg, digital), depending on the message or document and from a secret key

known only to the signatory subject. It is assumed that digital signatur should be easily verified without access to the secret key.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, которая используется для определения лица, подписывающего информацию.

Elektron imzo – boshqa elektron shakldagi axborotga (imzolanuvchi axborotga) birlashtirilgan yoki boshqa tarzda shunday axborot bilan bog‘langan va axborotni imzolovchi shaxsni aniqlashda ishlatiladigan elektron shakldagi axborot.

Electronic signature – information in electronic form which is attached to the other information in electronic form (signed information) or otherwise relating to such information and is used to determine the person signing the information.

Подстановка – криптографическая операция, связанная с замещением блока другим и использующая определенный код.

O‘rniga qo‘yish – blokni o‘rniga boshqasini qo‘yish va muayyan koddan foydalanish bilan bog‘liq kriptografik amal.

Substitution – cryptographic operations associated with the replacement unit and the other using a specific code.

Подтверждение подлинности – механизм, направленный на подтверждение подлинности и предусматривающий обмен информацией.

Haqiqiylikning tasdig‘i – haqiqiylikni tasdiqlashga yo‘naltirilgan va axborot almashishni ko‘zda tutuvchi mexanizm.

Authentication exchange – mechanism aimed at providing authentication and exchange of information.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Xavfsizlik siyosati (tashkilotdagi axborot xavfsizligi siyosati) – tashkilot o'z faoliyatida rioya qiladigan axborot xavfsizligi sohasidagi hujjatlangan qoidalar, muolajalar, amaliy usullar yoki amal qilinadigan prinsiplar majmui.

Security policy – set of documented policies, procedures, practical methods or guidelines in the field of information security used by the organization in its activities.

Полномочия – право пользователя (терминала, программы, системы) осуществлять те или иные процедуры над защищенными данными.

Vakolatlar – himoyalangan ma'lumotlar ustida u yoki bu muolajani bajarishi bo'yicha foydalanuvchining (terminalning, dasturning, tizimning) huquqi.

Privileges – the right of the user (terminal program, system) to implement certain procedures over the protected data.

Полномочное управление доступом – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении субъектов обращаться к информации такого уровня конфиденциальности.

Foydalanishni vakolatli boshqarish – obyektlar tarkibidagi axborotning konfidensialligini xarakterlovchi belgiga va subyektlarning bunday konfidensiallik darajasiga ega axborotga murojaat

etishlariga rasmiy ruxsatga asoslangan subyektlarning obyektlardan foydalanishlarini cheklash.

Plenipotentiary access control – access control subjects to objects based on the characterized Tagged confidentiality of the information contained in the objects, and the authorization of subjects to access information of such a level of confidentiality.

Предоставление права на доступ – выдача разрешения (санкции) на использование определенных программ и данных.

Foydalanish huquqini taqdim etish – muayyan dasturlar va ma'lumotlardan foydalanishga ruxsat (sanksiya) berish.

Authorization – authorization (approval) to use certain programs and data.

Проникновение – успешное преодоление механизмов защиты системы.

Suqilib kirish – tizimning himoya mexanizmlaridan muvaffaqqiyatli o'tishi.

Penetration – successful resolution mechanisms to protect the system.

Протокол – совокупность правил, определящих алгоритм взаимодействия устройств, программ, систем обработки данных, процессов или пользователей.

Protokol – qurilmalar, dasturlar, ma'lumotlarlarni ishlash tizimlari, jarayonlar yoki foydalanuvchilarning o'zaro harakati algoritmini belgilovchi qoidalar majmui.

Protocol – a set of rules that define the algorithm of interaction devices, software, data processing systems, processes or users.

Профиль защиты – документ, описывающий задачи обеспечения защиты информации в терминах функциональных требований и требований гарантированности.

Himoya profili – axborotni himoyalash masalasini funksional talablar va kafolatlanish talablari atamalarida tavsiflangan hujjat.

Protection Profile – document describing the task of ensuring the protection of information in terms of the functional requirements and the requirements of the warranty.

Разглашение информации – несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Axborotning oshkor qilinishi – axborotni, ushbu axborotdan foydalanish huquqiga ega bo'lmagan iste'molchilarga ruxsatsiz yetkazish.

Disclosure of information – unauthorized bringing protected information to consumers who do not have access to this information.

Разграничение доступа – совокупность методов, средств и мероприятий, обеспечивающих защиту данных от несанкционированного доступа пользователей.

Foydalanishni cheklash – ma'lumotlarni foydalanuvchilarning ruxsatsiz foydalanishlaridan himoyalashni ta'minlovchi usullar, vositalar va tadbirlar majmui.

Access control – a set of methods, tools and measures to ensure the protection of data from unauthorized users.

Разделение привилегий – принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

Imtiyozlarning bo'linishi – ma'lumotlardan foydalanish uchun bitta emas, balki ikkita parolni ko'rsatish (masalan, ikkita shaxs parolini) lozim bo'lgan ma'lumotlarni himoyalash mexanizmini ochish prinsipi.

Privilege sharing – the principle of the opening mechanism of protection of data in which to access them you must specify not one, but two passwords (for example, two persons).

Распределенная атака на отказ в обслуживания – входит в число наиболее опасных по последствием классов компьютерных атак, направленных на нарушение доступности информационных ресурсов. Позволяет генерировать удлиненный трафик, кроме того, её трудно заблокировать, так как поведение различных атакующих компьютеров может отличаться.

Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujumlar – axborot resurslarining foydalanuvchanligini buzishga yo'naltirilgan, oqibati bo'yicha o'ta xavfli kompyuter hujumlari sinfiga mansub. Uzaytirilgan trafikni generatsiyalashga imkon beradi, undan tashqari, uni blokirovka qilish qiyin, chunki turli kompyuterlarning hujumlari turlicha bo'ladi.

Distributed Denial of Service (DDoS) – among the most dangerous consequence of classes on cyber attacks aimed at the violation of the availability of information resources. Allows you to generate a larger graph, in addition, it is difficult to block, since the behavior of the various attacking computers may differ.

Резидентный – постоянно присутствующий в оперативной памяти.

Rezident – asosiy xotirada doimo mavjud.

Resident – constantly present in memory.

Сервер-посредник – брандмауэр, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с брандмауэром, используется процесс, называемый трансляцией адресов (address translation).

Server-vositachi – brandmauer bo'lib, unda barcha avtorizatsiyalangan mijozlarning IP-adreslarini brandmauer bilan assotsiyalangan IP-adreslarga o'zgartirish uchun adreslarni translyatsiyalash (adress translation) deb ataluvchi jarayondan foydalaniladi.

Proxy server – firewall, in which to convert the IP-addresses of all authorized clients in IP-addresses associated with a firewall, use a process called NAT (address translation).

Система обнаружения вторжения – программное или аппаратное средство, предназначенное для выявления фактов несанкционированного доступа в компьютерную систему или сеть.

Bostirib kirishlarni aniqlash tizimi – kompyuter tizimidan yoki tarmog'idan ruxsatsiz foydalanish faktini aniqlashga mo'ljallangan dasturiy yoki apparat vosita.

Intrusion Detection System (IDS) – software or hardware designed to detect cases of unauthorized access to a computer system or network.

Скремблер – кодирующее устройство, используемое в цифровом канале, которое выдает случайную последовательность бит.

Skrembler – raqamli kanalda ishlatiluvchi, bitlarning ketma-ketligini shakllantiruvchi kodlovchi qurilma.

Scrambler – encoder used in the digital channel, which provides a random sequence of bits.

Сниффинг – вид сетевой атаки, также называется «пассивное прослушивание сети».

Sniffing – tarmoq hujumi turi, "tarmoqni yashirincha eshitish" deb ham ataladi.

Sniffing – type of network attack also called "sniffing".

Спамминг – посылка большого числа одинаковых сообщений в различные группы UNINET.

Spamming – UNINETning turli guruhlariga katta sonli bir xil xabarlarni jo'natish.

Spamming – sending a large number of identical messages to different groups UNINET.

Стеганография – отрасль науки, изучающая математические методы сокрытия конфиденциальной информации в открытых информационных массивах.

Steganografiya – ochiq axborot massivlarida konfidensial axborotni yashirishning matematik usullarini o'rganuvchi fan sohasi.

Steganography – a branch of science that studies the mathematical methods of hiding confidential information in open information arrays.

Криптографическая стойкость – фундаментальное понятие криптографии – свойство криптосистемы (криптопротокола), характеризующее её (его) способность противостоять атакам противника и/или нарушителя, как правило, имеющим целью получить секретный ключ или открытое сообщение.

Kriptografik bardoshlilik – kriptografiyaning fundamental tushunchasi – kriptotizimning (kriptoprotokolning), odatda, maqsadi maxfiy kalitga yoki ochiq xabarga ega bo'lish bo'lgan dushmanning va/yoki buzg'unchining hujumlariga qarshi tura olishi qobiliyatini xarakterlovchi xususiyati.

Cryptographic resistance – the basic concept of cryptography - property cryptosystem, which characterizes her (his) ability to withstand enemy attacks and / or the offender, as a rule, have to obtain the secret key or open a message.

Стратегия защиты – формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

Himoyalash strategiyasi – tizimning ma'lum tahdidlardan himoyalashni ta'minlashda amal qilinishi lozim bo'lgan mezonlarni, ayniqsa, operativ mezonlarni rasmiy tavsifi.

Security strategy – a formal definition of the criteria, particularly operational, to be followed while protecting the system against known threats.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Axborotni himoyalash texnikasi – axborotni himoyalashni ta'minlashga mo'ljallangan axborotni himoyalash vositalari, axborotni himoyalash samaradorligini nazoratlash vositalari, boshqarish tizimlari va vositalari.

Security technique - protection of information, tools for monitoring the effectiveness of information security, instrumentation and control systems designed to protect information.

Техническая защита информации – деятельность, направленная на обеспечение безопасности информации инженерно-техническими мерами.

Axborotni texnik himoyalash – injener-texnik choralar yordamida axborot xavfsizligini ta'minlashga yo'naltirilgan faoliyat.

Technical protection of information – activities aimed at ensuring of information security engineering and technical measures.

Техническая разведка – получение сведений путем сбора и анализа информации техническими средствами.

Texnik razvedka – texnik vositalar yordamida axborotni yig'ish va tahlillash yo'li bilan ma'lumotlarni olish.

Technical intelligence – obtain information through the collection and analysis of information by technical means.

Тип доступа – сущность права доступа к определенному устройству, программе, файлу и т.д. (обычно read, write, execute, append, modify, delete).

Foydalanish turi – ma'lum qurilmadan, dasturdan, fayldan va h. foydalanish huquqining ma'nosi (odatda read, write, execute, append, modify, delete).

Access type – essence of the right of access to a particular device, programs, files, etc. (usually read, write, execute, append, modify, delete).

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Tahdid (axborot xavfsizligiga tahdid) – axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug'diruvchi sharoitlar va omillar majmui.

Threat – set of conditions and factors that create potential or actual violations of the existing danger of information security.

Управление доступом – определение и ограничение доступа пользователей, программ и процессов к данным, программам и устройствам вычислительной системы.

Foydalanishni boshqarish – foydalanuvchilarning, dasturlarning va jarayonlarning ma'lumotlardan, hisoblash texnikasi dasturlari va qurilmalaridan foydalanishlarini belgilash va cheklash.

Access control – definition and limitation of access users, programs, and processes the data, programs, and devices of a computer system.

Утечка информации – неконтролируемое распространение информации, которое привело к ее несанкционированному получению.

Axborotni sirqib chiqishi – axborotni ruxsatsiz olinishiga sabab bo'lgan uning nazoratsiz tarqalishi.

Information loss – uncontrolled dissemination of information that led to the elevation of its.

Фальсификация – использование различных технологий для обхода систем управления доступом на основе IP-адресов с помощью маскирования под другую систему, используя ее IP-адрес.

Soxtalashtirish – boshqa tizim IP-adresidan foydalanib, unga o'xshab niqoblanish yordamida IP-adreslar asosida foydalanishni boshqarish tizimini chetlab o'tish uchun turli texnologiyalardan foydalanish.

Spoofing – the use of different technologies to bypass access control systems, IP-based addresses using masking under another system using its IP-address.

Фишинг – технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д.

Fishing – foydalanish paroli, bank va identifikatsiya kartalari ma'lumotlari va h. kabi shaxsiy konfidensial ma'lumotlarni o'g'rilashdan iborat internet-firibgarlik texnologiyasi.

Phishing – Internet-fraud technique, is used for stealing personal confidential data such as passwords, bank and identification cards, etc.

Фрод – обман; мошенничество, жульничество, подделка. Вид интернет-мошенничества, при котором мошенник самыми разными способами незаконно получает какую-то часть денег или услуг, относящихся к какому-либо сервису.

Frod – aldash, firibgarlik, g'irromlik, qalbakilik. Internet-firibgarlik turi bo'lib, firibgar turli usullar yordamida pulning yoki qandaydir serverga tegishli xizmat qismiga noqonuniy ega bo'ladi.

Fraud – deception; fraud scam; fake. Kind of Internet fraud in which the scammer in many ways unlawfully obtains some of the money or services relating to any service.

Хакер – пользователь, который пытается вносить изменения в системное программное обеспечение, зачастую не имея на это право. Хакером можно назвать программиста, который создает более или менее полезные вспомогательные программы, обычно плохо документированные и иногда вызывающие нежелательные побочные результаты.

Xaker – tizimli dasturiy ta'minotga ko'pincha noqonuniy o'zgartirishlar kiritishga urinuvchi foydalanuvchi. Odatda yomon hujjatlangan va ba'zida nojoiz qo'shimcha natijalar tug'diruvchi ozmi-ko'pmi foydali yordamchi dasturlar yaratuvchi dasturchini xaker deb atash mumkin.

Hacker – a user who is trying to make changes to system software, often without that right. Can be called a hacker programmer who creates a more or less useful utility programs are usually poorly documented and sometimes cause unwanted side effects.

Хеш-функция – функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно, фиксированной длины.

Xesh-funksiya – chekli alfavitdagi uzunligi chekli kirish yo'li so'zini berilgan, odatda, qat'iy uzunlikdagi so'zga akslantirish funksiyasi.

Hash function – function mapping input word of finite length over a finite alphabet in a given word, usually a fixed length.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Axborot yaxlitligi – tasodifan va/yoki atayin buzilish hollarida hisoblash texnikasi vositalarining yoki avtomatlashtirilgan tizimning axborotini o'zgartirmasligini ta'minlovchi xususiyati.

Information Integrity – the ability of computers and automated systems to provide consistent information in a casual and / or intentional distortion (destruction).

Ценность информации – свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности человека.

Axborotning muhimligi – axborotning insonning maqsadli faoliyatining turli sohalarida amaliy foydalanishga yaroqliligi orqali aniqlanuvchi xususiyati.

Information value – property information, determine its applicability to practical use in various fields of purposeful human activity.

Червь – программа, внедряемая в систему злонамеренно, в результате которой прерывается ход обработки информации в

системе. В отличие от вирусов, червь не искажает файлы данных и программы. Обычно червь выполняется, оставаясь необнаруженным, и затем самоуничтожается.

Qurt – ko'pincha yomon niyatda tizimga kiritiladigan va axborotning ishlash jarayonini to'xtatuvchi dastur. Viruslardan farqlangan holda, qurt odatda, ma'lumotlar faylini va dasturni buzmaydi. Qurt yashirincha bajariladi va o'z-o'zini yo'qotadi.

Worm – programs implemented in the system, often malicious, and interrupting the flow of processing information in the system. Unlike viruses worm usually does not distort the data files and programs. Typically, the worm is executed, undetected, and then deletes itself.

Сетевой червь – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

Tarmoq qurtlari – lokal va global kompyuter tarmoqlari orqali mustaqil ravishda tarqalish xususiyatiga ega bo'lgan zararli dastur turi.

Network worm – a kind of malicious program, self-propagating through local and global computer networks.

Шлюз прикладного уровня – исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне модели OSI. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Ilova sathi shlyuzi – avtorizatsiyadan o'tgan mijoz va tashqi xost o'rtasidagi to'g'ridan to'g'ri o'zaro aloqa amalga oshishiga yo'l qo'ymaydi. Shlyuz OSI modelining ilova sathida kiruvchi va

chiquvchi tarmoq paketlarining barchasini filtrlaydi. Ilovalar bilan bog'liq dastur-vositachilar TCP/IP aniq xizmatlari generatsiyalaydigan axborotni shlyuz orqali uzatilishini ta'minlaydi.

Application-level gateway – eliminates the direct interaction between an authorized client and the external host. Gateway filters all incoming and outgoing packets at the application layer model OSI. Application-related program intermediary redirect gateway information generated by a particular service TCP/IP.

Шлюз сеансового уровня – исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Он принимает запрос доверенного клиента на определенные услуги и после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом. После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Seans sathi shlyuzi – avtorizatsiyadan o'tgan mijoz va tashqi xost o'rtasidagi to'g'ridan-to'g'ri o'zaro aloqa amalga oshishiga yo'l qo'ymaydi. Shlyuz ishonchli mijozdan so'rov qabul qiladi va so'ralgan seansga ruxsatning joizligi tekshirilganidan so'ng tashqi xost bilan aloqani o'rnatadi. Shundan so'ng ikkala shlyuz yo'nalishda tarmoq paketlarini filtrlamasdan, nusxa oladi.

Circuit-level gateway - eliminates the direct interaction between an authorized client and the external host. It takes a trusted client request for certain services and, after validation of the requested session, establishes the connection with the external host. After this, the gateway simply copies the packets in both directions, not realizing their filtration.

Шпионское программное обеспечение – вид вредоносного программного обеспечения, осуществляющего деятельность

по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Xufiya dasturiy ta'minot – foydalanuvchilarning ruxsatisiz kompyuter konfiguratsiyalari, foydalanuvchilar faoliyati va har qanday boshqa konfidensial axborotni yig'ish bo'yicha faoliyat olib boradigan zararli dasturiy ta'minot turi.

Spyware – type of malicious software, carrying out activities to collect information about your computer configuration, user activity, and any other confidential information without the consent of the user.

Экспертиза системы защиты информации – оценка соответствия представленных проектных материалов по защите информации (на объекте) поставленной цели, требованиям стандартов и других нормативных документов.

Axborotni himoyalash tizimining ekspertizasi – axborotni himoyalash bo'yicha taqdim etilgan loyiha materiallarining qo'yilgan maqsad, standartlar talablariga va boshqa me'yoriy hujjatlarga mosligini baholash.

Expert operation of the system of protection to information – conformity assessment submitted project materials for the protection of information (on-site) goal, the standards and other regulatory documents.

Эксплойт – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему.

Eksployt – kompyuter tizimiga hujum uyushtirish uchun qo'llaniladigan va dasturiy ta'minot zaifliklaridan foydalanuvchi kompyuter dasturi, dasturiy kod fragmenti yoki buyruqlar ketma-ketligi.

Exploit – computer program code snippet or a sequence of commands that use vulnerabilities in software and used for an attack on a computer system.

Эффективность – свойство объекта удовлетворять требованиям к услуге с заданными количественными характеристиками.

Samaradorlik – berilgan miqdoriy xarakteristikalari bilan xizmat ko'rsatishga bo'lgan talablarni qondiruvchi obyektning xususiyati.

Efficiency – object property to satisfy the requirements of the service with the given quantitative characteristics.

Ядро защиты – технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Himoya yadrosi – foydalanish distpetcheri konsepsiyasini amalga oshiruvchi himoyalash vositalari kompleksining texnik dasturiy va mikrodasturiy elementlari.

Security kernel – hardware, software and micro-program elements of remedies tools protection implementing the concept of Access Manager.

MUNDARIJA

V BOB. AXBOROTNI KRIPTOGRAFIK HIMOYALASH

VI BOB. IDENTIFIKATSIYA VA AUTENTIFIKATSIYA

VII BOB. KOMPYUTER VIRUSLARI VA ZARARKUNANDA DASTURLAR BILAN KURASHISH MEXANIZMLARI

VIII BOB. AXBOROTNI HIMOYALASHDA TARMOQLARARO EKRANLARNING O‘RNI

IX BOB. OPERATSION TIZIM HIMOYASI

X BOB. AXBOROT SIRQIB CHIQISH KANALLARI

ОГЛАВЛЕНИЕ

IV глава. МОДЕЛИ БЕЗОПАСНОСТИ

V глава. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

VI глава. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

VII глава. МЕХАНИЗМЫ БОРЬБЫ С КОМПЬЮТЕРНЫМИ ВИРУСАМИ И ВРЕДОНОСНЫМИ ПРОГРАММАМИ

CONTENTS

Chapter V. CRYPTOGRAPHIC PROTECTION OF INFORMATION

Chapter VI. IDENTIFICATION AND AUTHENTICATION

Chapter VII. MECHANISMS TO COMBAT COMPUTER VIRUSES AND MALWARE

Chapter VIII. LOCATION FIREWALLS IN PROTECTION OF INFORMATION

Chapter IX. OPERATING SYSTEM SECURITY

Chapter X. CHANNELS OF INFORMATION LEAKAGE

S.K. GANIYEV, M.M. KARIMOV, K.A. TASHEV

AXBOROT XAVFSIZLIGI

Toshkent – «Fan va texnologiya» – 2017

Muharrir:	Sh.Aliyeva
Tex. muharrir:	M.Holmuhamedov
Musavvir:	D.Azizov
Musahhih:	N.Hasanova
Kompyuterda sahifalovchi:	N.Raxmatullayeva

E-mail: tipografiyacnt@mail.ru Tel: 245-57-63, 245-61-61.
Nashr.lits. AI№149, 14.08.09. Bosishga ruxsat etildi: 16.11.2017.
Bichimi 60x84 $^{1}/_{16}$. «Timez Uz» garniturasi. Ofset bosma usulida bosildi.
Shartli bosma tabog'i 23,5. Nashriyot bosma tabog'i 23,25.
Tiraji 1500. Buyurtma №189.