...YEV, A.A. GANIYEV,
D.Y. IRGASHEVA

MA'LUMOTLAR BAZASI XAVFSIZLIGI

TOSHKENT

UO'K: 004.056:004.65 (075.8)
KBK 32.973-018.2
G-19

G-19 **S.K.Ganiyev, A.A. Ganiyev, D.Y. Irgasheva. Ma'lumotlar bazasi xavfsizligi. –T.: «Fan va texnologiya», 2016, 228 bet.**

ISBN 978-9943-11-367-1

"Ma'lumotlar bazasi 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 ma'lumotlar bazasi xavfsizligini ta'minlovchi usullar, vositalar va mexanizmlarning asosiy xarakteristikalari; ma'lumotlar bazasini boshqarish turlari; ma'lumotlar bazasi xavfsizligining texnologik jihatlari; ma'lumotlar bazasidan foydalanishni cheklashning modellari va usullari; ma'lumotlar bazasining taqsimlangan tizimida axborot xavfsizligi; xavfsizlik auditi va ma'lumotlar bazasini rezervli nusxalash masalalari hamda ma'lumotlar bazasini boshqarish tizimlarining himoya prinsiplari muhokama etilib, ma'lumotlar bazasi xavfsizligini ta'minlashdagi me'yoriy hujjatlar keltirilgan.

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

***

Учебник «Безопасность базы данных» подготовлен преподавателями кафедры "Информационная безопасность" базового высшего учебного заведения Ташкентского университета информационных технологий и включает в себя такие вопросы, как основные характеристики методов, средства и механизмов обеспечения безопасности базы данных; виды управления базами данных; технологические аспекты информационной безопасности базы данных; модели и методы разграничения доступа в базы данных; информационная безопасность распределенных систем базы данных; аудит безопасности и резервное копирование базы данных; принципы защиты систем управления базами данных, также приведены нормативные документы обеспечения безопасности базы данных.

Учебник предназначен для студентов высших учебных заведений и может быть использован лицами, занимающимися в сфере безопасности информационной технологии и компьютерных систем.

***

"Data Base Security" textbook is prepared by professor-teachers of department of "Information Security" of base top educational institution, Tashkent University of information technology and it includes features of methods, tools and mechanisms of data base security; methods of data base management; technical aspects of data base security; access control methods and models in database; information security in distributive database systems; security audit and database backup; security principles of database management systems and regulations in database security.

This textbook is designed for students of educational institutions and people that deal in information technologies and computer system security fields can use.

UO'K: 004.056:004.65 (075.8)
KBK 32.973-018.2

Taqrizchilar:

Sagatov M.V. – TDTU, "Axborot tizimlari" kafedrasi mudiri, t.f.d., professor;

Mirzayev O.N. – O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi, Axborot xavfsizligini ta'minlash markazi direktorining birinchi o'rinbosari;

Chul Soo LEE – Toshkent axborot texnologiyalari universiteti, AKT bo'yicha prorektor-maslahatchi.

ISBN 978-9943-11-367-1

MUQADDIMA

Avtomatlashtirilgan axborot tizimlaridan foydalanish, holati va ishlashi korxona va tashkilotlar faoliyatiga jiddiy ta'sir etishi mumkin bo'lgan, ma'lumotlar bazasi yoki ma'lumotlar bazasi majmui ko'rinishidagi umumiy axborot resurslarining paydo bo'lishiga sabab bo'ldi. Natijada, korxona va tashkilotlar faoliyatining axborot ta'minoti amaliyotiga avtomatlashtirilgan axborot tizimini tatbiq etish jarayonida, maxsus "ma'lumotlar bazasini himoyalash" atamasini olgan holatlarni alohida o'ziga xos nazoratlash kerak bo'ladi. Ma'lumotlarni himoyalash jarayonida yechiladigan masalalarning vazifalari va mazmuniga qarashlar avtomatlashtirilgan axborot tizimlari industriyasining tashkil topishi bilan birgalikda shakllandi, ularni amalga oshirishdagi dasturiy-texnik jihatlarning o'zgarishi va murakkablashishi natijasida o'zgardi, ammo vaqt o'tgan sari, astasekin ularning qandaydir bazaviy ro'yxati shakllandi va ma'lumotlar bazasini himoyalash atomatlashtirilgan axborot tizimi nazariyasi va amaliyotida ajralmas muhim komponent bo'lib qoldi.

"Ma'lumotlar bazasi xavfsizligi" deganda ma'lumotlar bazasidan ruxsatsiz foydalanishdan, ma'lumotlarni foydalanuvchilar tomonidan o'zgartirilishidan yoki buzilishidan ogohlantirish; apparat va dasturiy vositalarning yanglishishidagi va ekspluatatsiya xodimi xatosidagi ma'lumotlarning o'zgarishidan yoki buzilishidan ogohlantirish tushuniladi.

O'quvchi e'tiboriga tavsiya etilayotgan "Ma'lumotlar bazasini xavfsizligi" darsligi beshta bobdan iborat.

Darslikning birinchi bobida ma'lumotlar bazasi xavfsizligini ta'minlash usullari, vositalari va mexanizmlarining asosiy xarakteristikalari, ma'lumotlar bazasini boshqarish tizimlarining turlari hamda ma'lumotlar bazasi xavfsizligining texnologik jihatlari keltirilgan.

Ikkinchi bobda ma'lumotlar bazasidan foydalanishni cheklash modellari va usullari ko'rilgan. Diskretsion, mandatli va rolli modellar asosidagi ma'lumotlar bazasidan foydalanishni cheklashni

tashkil etish masalalari batafsil tahlillanadi. Yuqorida keltirilgan modellarni xavfsizlikni berilgan tahdidlardan himoyalashning samaradorligi nuqtayi nazaridan qiyosiy baholashga alohida e'tibor berilgan.

Uchinchi bob ma'lumotlar bazasining taqsimlangan tizimlarining axborot xavfsizligi prinsiplariga ajratilgan. Ma'lumotlar bazasining taqsimlangan tizimlarida axborot xavfsizligi konsepsiyasi keltiriladi. "Mijoz-server" texnologiyalari, replikatsiyalash texnologiyalari va obyektli bog'lash texnologiyalari taqsimlangan tizim texnologiyalarining mustaqil yo'nalishlari sifatida batafsil yoritilgan.

Xavfsizlik auditi va ma'lumotlar bazasini rezervli nusxalash masalalari darslikning to'rtinchi bobidan o'rin olgan. Ma'lumotlar bazasini boshqarish tizimlarida xavfsizlik auditini o'tkazish xususiyatlari bayon etiladi. *Oracle MBBT* misolida ma'lumotlar bazasida xavfsizlik auditini o'tkazish va amalga oshirish masalalari batafsil yoritilgan. Asl nusxa yo'qolganida jiddiy muhim ma'lumotlarni tiklash maqsadida davriy takrorlash (replikatsiyalash) yoki zaxira nusxalarini yaratish, ya'ni rezervli nusxalash masalalari ko'rilgan. So'ngra replikatsiyalash texnologiyalari hamda replikatsiyalarni zamonaviy ma'lumotlarni boshqarish tizimlarida sinxronlash jarayonlari keltirilgan.

Beshinchi bobning mazmuni – ma'lumotlar bazasi xavfsizligini ta'minlash bo'yicha standartlar va spetsifikatsiyalar. Ma'lumotlar bazasi xavfsizligi qismtizimining arxitekturasi va ishlash prinsipi, ma'lumotlar bazasini boshqarish tizimining himoya profili muhokama qilinadi. Ma'lumotlar bazasi xavfsizligini ta'minlash sohasidagi me'yoriy hujjatlar keltirilgan.

Ilovalarda qisqartma so'zlar ro'yxati va atamalarning rus, o'zbek, ingliz tillaridagi izohli lug'ati keltirilgan.

1-bob. MA'LUMOTLAR BAZASI XAVFSIZLIGINI TA'MINLASH USULLARI, VOSITALARI VA MEXANIZMLARI

1.1. Ma'lumotlar bazasi xavfsizligini ta'minlash usullari, vositalari va mexanizmlarining asosiy xarakteristikalari

Kompyuter axborotini himoyalash muammolari bo'yicha 70-yillarning oxiri 80-yillarning boshida o'tkazilgan, keyinchalik turli ilovalarda rivojlantirilgan va mos standartlarda qayd etilgan tadqiqotlar *axborot xavfsizligi* tushunchasining tarkibiy elementlari sifatida quyidagilarni belgilaydi:

- *konfidensiallik* (ruxsatsiz foydalanishdan himoyalash);
- *yaxlitlik* (axborotni ruxsatsiz o'zgartirishdan himoyalash);
- *foydalanuvchanlik* (axborotni va resurslarni ushlab qolinishidan himoyalash, buzilishdan himoyalash, ishga layoqatlikni himoyalash).

Axborot xavfsizligi tarkibiy elementlariga mos *tahdidlar* qarshi turadi. Axborot xavfsizligiga tahdid deganda axborot xavfsizligiga bevosita yoki bilvosita zarar yetkazishi mumkin bo'lgan kompyuter tizimida amalga oshirilgan yoki oshiriluvchi ta'sir tushuniladi. Tahdidlarni axborot xavfsizligini *buzuvchi (buzg'unchi)* amalga oshiradi yoki amalga oshirishga urinadi.

Axborot xavfsizligiga u yoki bu tahdidlarni amalga oshirish bo'yicha buzg'unchi imkoniyatlari kompleksining formallashtirilgan tavsifi yoki ifodasi *buzg'unchining (niyati buzuqning)modeli* deb ataladi.

Kompyuter tizimida axborotning himoyalanganligini ta'minlash bo'yicha tashkiliy-texnologik va dasturiy-texnik choralar kompleksining sifatiy tavsifi *xavfsizlik siyosati* deb ataladi. Xavfsizlik siyosatining formal (matematik, algoritmik, sxemotexnik) ifodasi va ta'rifi *xavfsizlik modeli* deb ataladi.

Ma'lumotlar bazasi (MB) xavfsizligini ta'minlashga taalluqli ba'zi atamalar quyida keltirilgan:

- axborotdan foydalanish (access to infopmation) – axborot bilan tanishish, uni ishlash (xususan, nusxalash), modifikatsiyalash, yo'q qilish;

- foydalanish subyekti (access subject) – harakatlari foydalanishni cheklash qoidalari orqali qat'iy belgilanuvchi shaxs yoki jarayon;

- foydalanish obyekti (access object) – avtomatlashtirilgan tizimning axborot birligi bo'lib, undan foydalanish foydalanishning cheklash qoidalari orqali qat'iy belgilanadi;

- foydalanishni cheklash qoidalari (security policy) – subyektlarning obyektlardan foydalanish huquqini qat'iy belgilovchi qoidalar majmui;

- ruxsatli foydalanish (authorized access to information) – foydalanishni cheklash qoidalarini buzmasdan axborotdan foydalanish;

- ruxsatsiz foydalanish (unauthorized access to information) – axborotdan foydalanishni cheklash qoidalarini buzib foydalanish;

- foydalanish subyektining vakolat darajasi (subject privilege) –foydalanish subyektining foydalanish huquqlari majmui ("imtiyozlar");

- foydalanishni cheklash qoidalarini buzuvchi (security policy violator) – axborotdan ruxsatsiz foydalanuvchi foydalanish subyekti;

- foydalanishni cheklash qoidalarini buzuvchining modeli (security policy violator model) – foydalanishni cheklash qoidalarini buzuvchining abstrakt (formallashgan yoki formallashmagan) tavsifi;

- axborot yaxlitligi (information integrite) – axborot tizimining tasodifiy va (yoki) atain buzish sharoitlarida axborotning o'zgarmasligini ta'minlash qobiliyati;

- konfidensiallik belgisi (sensitivity label) – obyekt konfidensialligini xarakterlovchi axborot birligi;

- ko'p sathli himoya (multilevel secure) – turli sathli konfidensiallikga ega obyektlardan foydalanishning turli huquqlariga ega subyektlarning foydalanishlarini cheklashni ta'minlovchi himoya.

Kompyuterning dasturiy ta'minot strukturasida tashqi xotirada ma'lumotlarni tashkil etishga, joylashtirishga va undan foydalanishga operatsion tizim javob beradi. Uning mos tashkil etuvchisi

ko'pincha "fayl tizimi" deb yuritiladi. Kompyuterning tashqi xotirasidagi ma'lumotlar fayllar deb ataluvchi nomlangan majmua yordamida ifodalanadi. Ko'p hollarda operatsion (fayl) tizimi fayllardagi ma'lumotlarni tashkil etishning ichki mazmunli mantiqini "bilmaydi" va ular bilan baytlarning bir jinsli majmui yoki simvollar satri sifatida muomala qiladi.

Kompyuter tizimining ma'nosi va vazifasi nuqtayi nazaridan, ma'lumotlar fayli kompyuter tizimini predmet sohasining axborot-mantiq (infologik) sxemasini aks ettiruvchi strukturaga ega. Fayllardagi ushbu ma'lumotlar strukturasi ishlash amallarida hisobga olinishi shart. Shu bilan birga, ko'p hollarda ma'lumotlar bazasi fayllarini birdaniga butunligicha kompyuterning asosiy xotirasiga joylash mumkin bo'lmaganligi sababli, ma'lumotlar bazasi fayllaridagi ma'lumotlar strukturasini tashqi xotira fayllariga murojaat amallarini tashkil etishda hisobga olishga to'g'ri keladi.

Bundan ma'lumotlar bazasini boshqarish tizimining (MBBT) dasturiy ta'minot xili sifatidagi asosiy xususiyati kelib chiqadi. Tabiatan *tatbiqiy dasturiy ta'minot* hisoblanuvchi, ya'ni muayyan tatbiqiy masalalarni yechishga mo'ljallangan MBBT avval boshdan tizimli funksiyalarini bajargan – tizimli dasturiy ta'minotning fayl tizimi imkoniyatlarini kengaytirgan. Umuman MBBT amalga oshiruvchi quyidagi funksiyalarni ajratish mumkin:

- ma'lumotlarni mantiqiy strukturasini (ma'lumotlar bazasi sxemalarini) tashkil etish va madadlash;
- tashqi xotiradagi ma'lumotlarning fizik strukturasini tashkil etish va madadlash;
- ma'lumotlardan foydalanishni tashkil etish va ularni asosiy va tashqi xotirada ishlash.

Ma'lumotlarning mantiqiy strukturasini (ma'lumotlar bazasi sxemalarini) tashkil etish va madadlash *ma'lumotlarni tashkil etish modeli* ("ma'lumotlar modeli") vositalari yordamida ta'minlanadi.

Ma'lumotlar modeli ma'lumotlarni tashkil qilish usuli, yaxlitlikning cheklanishlari va ma'lumotlarni tashkil qilish obyektlari ustida joiz amallar to'plami orqali aniqlanadi. Ma'lumotlar modeli uchta tarkibiy qismga - *strukturali, yaxlitli* va *manipulyatsion* qismlarga ajratiladi.

Ma'lumotlarni tashkil etishning quyidagi uchta asosiy modellari mavjud:

- ierarxik;
- tarmoqli;
- relyatsion.

Ma'lumotlarni tashkil etish modeli, aslida, avtomatlashtirilgan axborot tizimini amalga oshiruvchi avtomatlashtirilgan ma'lumotlar bankining *ichki axborot tilini* belgilaydi. MBBT orqali madadlanuvchi ma'lumotlar modeli MBBTni tasniflashda ko'pincha mezon sifatida ishlatiladi. Unga binoan *ierarxik MBBT*, *tarmoq MBBT* va *relyatsion MBBT* farqlanadi.

MBBTning boshqa muhim funksiyasi – tashqi xotiradagi ma'lumotlarning fizik strukturasini tashkil etish va madadlash. Ushbu funksiya ba'zida *ma'lumotlar bazasining fayllar formati* deb ataluvchi ma'lumotlar bazasi fayllarining ichki strukturasini tashkil etadi va madadlaydi hamda ma'lumotlardan samarali va tartibli foydalanish uchun maxsus strukturalarni (indekslarni, sahifalarni) yaratadi va madadlaydi. Ushbu jihatdan bu funksiya MBBTning uchinchi funksiyasi –ma'lumotlar bazasidan foydalanishni tishkil etish bilan uzviy bog'langan.

Tashqi xotiradagi ma'lumotlarning fizik strukturasini tashkil etish va madadlash fayllar tizimining shtatga oid vositalari asosida hamda tashqi xotira qurilmalarining MBBTni bevosita boshqarish sathida amalga oshirilishi mumkin.

Ma'lumotlardan foydalanishni va ularni asosiy va tashqi xotirada ishlashni tashkil etish tranzaksiya deb ataluvchi jarayonlarni amalga oshirish orqali bajariladi. *Tranzaksiya* – ma'lumotlar bazasining joriy holatiga nisbatan alohida ma'noli qiymatga ega amallarning ketma-ket majmui. Masalan, ma'lumotlar bazasidagi alohida yozuvni olib tashlash tranzaksiyasi quyidagilarni o'z ichiga oladi: ko'rsatilgan yozuv bo'lgan ma'lumotlar fayli sahifasini aniqlash; mos sahifani o'qish va asosiy xotira buferiga uzatish; asosiy xotira buferidagi yozuvni olib tashlash; olib tashlangandan so'ng bog'lanishlar va boshqa parametrlar bo'yicha yaxlitlikni tekshirish; ma'lumotlarni mos sahifasining yangi holatini ma'lumotlar bazasi faylida qaydlash.

Tranzaksiyaning ikki xilini ajratish qabul qilingan – tranzaksiya tugallanganidan so'ng ma'lumotlar bazasi holatini o'zgartiruvchi va ma'lumotlar bazasi holatini vaqtincha o'zgartiruvchi (tranzaksiya tugallanganidan so'ng dastlabki holat tiklanadi). MBBTning tranzaksiyalarni tashkil etish va boshqarish bo'yicha funksiyalarining majmui *tranzaksiya monitori* deb ataladi.

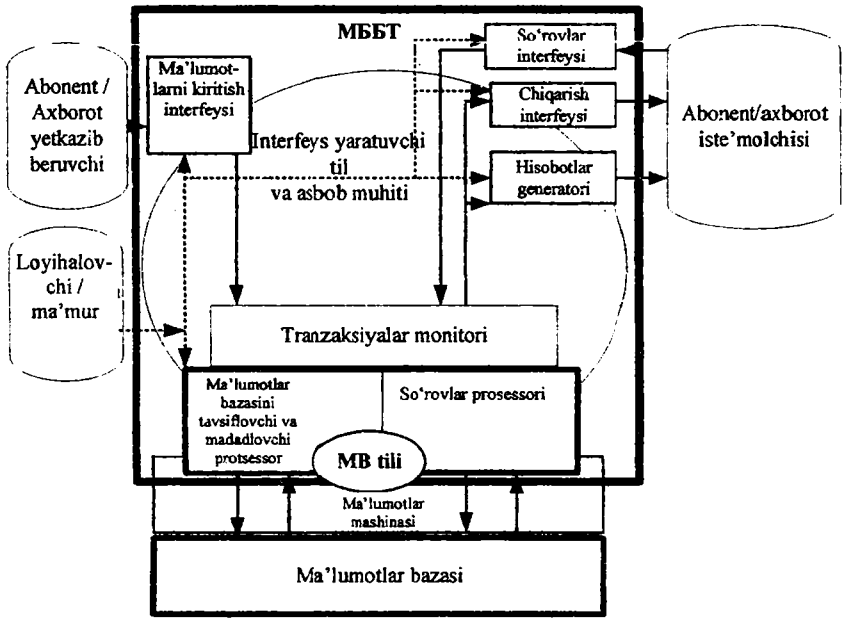
Ma'lumotlar bazasiga nisbatan tranzaksiyalar ma'lumotlar banki foydalanuvchilari harakatlariga tenglashtiriluvchi tashqi jarayonlar bilan ishtirok etadi. Bunda tranzaksiyalarning manbai, boshlab beruvchisi bitta yoki birdaniga bir nechta foydalanuvchi bo'lishi mumkin. Ushbu mezon bo'yicha *bitta odam foydalanuvchi MBBT* va *ko'pchilik foydalanuvchi MBBT* farqlanadi. Odatda, bitta odam foydalanuvchi MBBTlarida tranzaksiyalar monitori MBBTning alohida funksional elementi sifatida amalga oshirilmaydi. Ko'pchilik foydalanuvchi MBBTlarda tranzaksiyalarni monitorlashning asosiy vazifasi – birdaniga bir nechta foydalanuvchilarning umumiy ma'lumotlar ustida tranzaksiyalarning birgalikda samarali bajarishlarini ta'minlash.

Aksariyat MBBTlarda ma'lumotlardan foydalanish va ularni ishlash asosiy xotirada operatsion tizimning shtatga oid vositalari yoki tizimning vositalari yordamida *asosiy xotira buferlarini* tashkil etish orqali amalga oshiriladi. Ma'lumotlardan foydalanish va ularni ishlash vaqtida ma'lumotlar bazasi faylining alohida tashkil etuvchilari asosiy xotira buferlarida joylashtiriladi. Shu sababli, MBBTning ma'lumotlardan foydalanish va ularni ishlashini tashkil etish bo'yicha funksiyasining boshqa bir tarkibiy qismi *asosiy xotira buferlarini boshqarish* hisoblanadi.

MBBTning ma'lumotlardan foydalanish va ularni ishlashini tashkil etish bo'yicha funksiyasining yana bir muhim tarkibiy qismi ma'lumotlar bazasining barcha joriy o'zgarishlarini jurnallashtirish hisoblanadi. *Jurnallashtirish* ma'lumotlarning bo'lishi mumkin bo'lgan yanglishishlar va buzilishlarda but saqlanishini ta'minlovchi asosiy vosita hisoblanadi. Aksariyat MBBTlarda bunday tahdidlarni neytrallash uchun saqlash va joylashtirishning o'zgacha rejimli ma'lumotlar bazasining o'zgarishlari jurnali tashkil etiladi.

Ma'lumotlar bazasining o'zgarishlar jurnalining zaxirali nusxasi, odatda, ma'lumotlar bazasining asosiy faylidan alohida eltuvchilarda joylashtiriladi.

Quyida MBBT komponentlarining o'zaro bog'lanish sxemasi keltirilgan.



1.1-rasm. MBBT komponentlarining o'zaro bog'lanish sxemasi.

Ma'lumotlar bazasi strukturasini tavsiflash va madadlash protsessor MBBTning yadrosi hisoblanadi. U ma'lumotlarni tashkil etish modelini amalga oshiradi. Ushbu model vositalari yordamida loyihachi kompyuter tizimi predmet sohasining infologik sxemasiga mos *ma'lumotlar bazasining mantiqiy strukturasini (sxemasini)* quradi va *ma'lumotlar bazasining ichki sxemasini* qurishni va modellashni ta'minlaydi.

Ma'lumotlar bazasi strukturasini tavsiflash va madadlash protsessor ishlatiluvchi ma'lumotlar modeli (ierarxik, tarmoqli, relyatsion) atamalarida ma'lumotlar bazasining berilgan mantiqiy struktu-

rasini o'rnatishni hamda ma'lumotlar bazasi strukturasini ma'lumotlar bazasining ichki sxemasiga (ma'lumotlarning fizik strukturasiga) translyatsiyalashni (o'tkazishni) ta'minlaydi. Kompyuter tizimida relyatsion MBBT asosida ma'lumotlar bazasi strukturasini tavsiflash va madadlash prosessor strukturalangan so'rov tili SQLning tarkibiy qismi bo'lgan *ma'lumotlar bazasi tilida* amalga oshiriladi.

MBBTning ma'lumotlarni kiritish interfeysi abonentlarni – axborot yetkazib beruvchilarni axborotni tavsiflash va axborot tizimiga kiritish vositalari bilan ta'minlab, *ma'lumotlar bankining kirish yo'li axborot tilini amalga oshiradi.* MBBT rivojining zamonaviy tendensiyalaridan biri kirish yo'li axborot tillarini va kirish yo'li interfeysini foydalanuvchi bilan muloqotdagi tabiiy tilga yaqinlashtirishga intilishdan iborat. Bu "tayyorlanmagan" foydalanuvchilar tomonidan axborot tizimini ekspluatatsiya qilinishiga imkon yaratadi. Ushbu muammo interfeysni tashkil etishning dialog usullarini qo'llash va *kirish yo'li shakllaridan* foydalanish orqali yechiladi. Kirish yo'li shakllari, mohiyatan, ish yuritishda keng qo'llaniluvchi, ko'pchilik odamlarga (tayyorlanmagan foydalanuvchilarga) intuitiv ravishda tushunarli turli xil anketalarning elektron analoglaridan, standartlashtirilgan blankalardan va jadvallardan iborat. Bunda kirish yo'li interfeysi shakllar orqali kiritiluvchi ma'lumotlarni tavsiflash prosessorga uzatish va ma'lumotlar bazasi strukturasini madadlash uchun kirish yo'li shakllarini yaratish, saqlash va ularni ma'lumotlar bazasining mantiqiy strukturasini tavsiflash atamalarida sharxlash vositalarini ta'minlaydi.

So'rovlar interfeysi so'rovlar prosessori bilan birgalikda tizim foydalanuvchilari-abonentlarining axborot ehtiyojlarini akslantiruvchi axborot tizimidan (standart namunaviy so'rovlar qismidan) foydalanishning konseptual modelini ta'minlaydi. So'rovlar interfeysi foydalanuvchiga o'zining axborot ehtiyojini ifodalashiga vositalar taqdim etadi. MBBT rivojining zamonaviy tendensiyalaridan biri so'rovlarni shakllantirishning maxsus "konstruktorlar" yoki qadamba-qadam "masterlar" ko'rinishidagi dialog-ko'rgazmali vositalaridan foydalanishdan iborat.

So'rovlar protsessor shakllantirilgan so'rovlarni *ma'lumotlarni manipulyatsiyalovchi til* atamalarida sharxlaydi va ma'lumotlar ba-

zasi strukturasini tavsiflash va madadlash prosessor bilan birgalikda so'rovlarni bajaradi. Relyatsion MBBTlarda so'rovlar prosessorning asosini SQL tilining asosiy qismi hisoblanuvchi ma'lumotlarni manipulyatsiyalovchi til tashkil etadi. Shunday qilib, so'rovlar protsessor va ma'lumotlar bazasi strukturasini tavsiflash va madadlash prosessor bazasida, ba'zida *ma'lumotlar mashinasi* deb yuritiluvchi, MBBTdagi ma'lumotlar bilan ish ko'ruvchi eng past sath vujudga keladi. Ma'lumotlar mashinasining standart funksiyalaridan va imkoniyatlaridan MBBTning tartibi yuqoriroq komponentlari foydalanadi. Bu MBBT komponentalarini va ma'lumotlar bankini uchta sathga – mantiqiy sathga, ma'lumotlar mashinasiga va ma'lumotlarning o'ziga ajratishga va standartlashga imkon beradi.

Tranzaksiyalar monitorining vazifasi, yuqorida aytib o'tilganidek, umumiy ma'lumotlar ustida bir necha foydalanuvchilar tomonidan birgalikda tranzaksiyani tashkil etishdan iborat. Bunda, xususan, asosiy funksiya bilan ham uzviy bog'langan qo'shimcha funksiya – ma'lumotlarning yaxlitligini va kompyuter tizimi predmet sohasi qoidalari orqali aniqlanuvchi cheklashlarni ta'minlash hisoblanadi.

MBBTning *chiqarish interfeysi* so'rovlar protsessordan so'rovlarning (ma'lumotlar bazasiga murojaatlarning) bajarilishi natijalarini oladi va ularni axborot tizimi foydalanuvchisi – abonentning o'zlashtirishiga qulay holdagi shaklga o'tkazadi. Zamonaviy MBBTda so'rovlarning bajarilishi natijalarining tayyorlanmagan foydalanuvchiga odatdagidek va intuitiv ravishda tushunarli shaklda ma'lumotlarni "vizuallashtirish"ga imkon beruvchi turli usullardan foydalaniladi. Buning uchun, odatda, strukturalangan ma'lumotlarni jadvallar usulida ifodalashdan hamda ma'lumotlarni chiqarishning maxsus shakllaridan foydalaniladi.

Chiqarish shakllari "hisobot"ni shakllantirish asosida ham yotadi. Hisobot chiqarilgan ma'lumotlarni hujjatlash uchun ma'lumotlar bazasidan axborotni qidirish va tanlash natijalarini yozma ravishda ifodalaydi. Shu kabi maqsadlar uchun zamonaviy MBBTlar tarkibiga *hisobot generatorlari* kiritiladi.

U yoki bu MBBTni amalga oshiruvchi zamonaviy dasturiy vositalar ma'lumotlar modelining (relyatsion, tarmoqli, ierarxik yoki aralash) ma'lum doirasidagi *ma'lumotlar bazasini yaratish va foydalanishning* instrumental muhiti va MBBT tili (ma'lumotlarni tav-

siflash tili, ma'lumotlarni manipulyatsiyalash tili, interfeysni yaratish tili va vositalari) majmui hisoblanadi.

MBBTdan foydalanuvchilarni uchta guruhga ajratish mumkin:

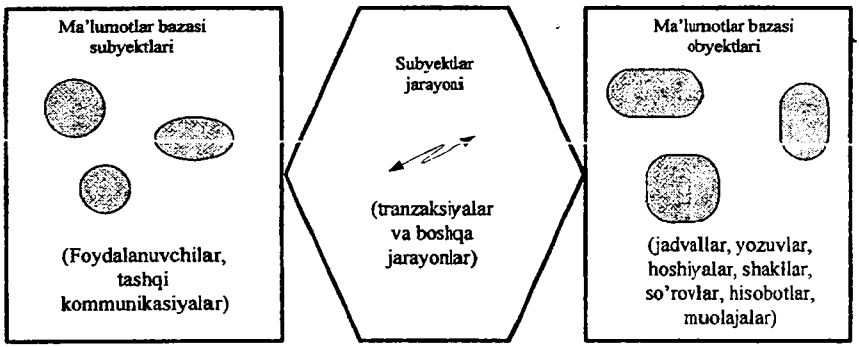
- tatbiqiy dasturchilar – ma'lumotlar bazasi asosida dastur yaratilishiga javobgar. Ma'lumotlarni himoyalash ma'nosida dasturchi ma'lumot obyektlarini yaratish va ularni manipulyatsiyalash imtiyoziga yoki faqat ma'lumotlarni manipulyatsiyalash imtiyoziga ega foydalanuvchi bo'lishi mumkin;
- ma'lumotlar bazasidan oxirgi foydalanuvchilar – ma'lumotlar bazasi bilan bevosita terminal yoki ishchi stansiya orqali ishlashadi. Odatda, ular ma'lumotlarni manipulyatsiyalash bo'yicha imtiyozlarning qat'iy chegaralangan naboriga ega bo'ladilar. Ushbu nabor oxirgi foydalanuvchi interfeysini konfiguratsiyalashda aniqlanishi va o'zgarmasligi mumkin. Bu holda xavfsizlik siyosatini xavfsizlik ma'muri yoki ma'lumotlar bazasi ma'muri (agar bu bir xil lavozimli shaxs bo'lsa) aniqlaydi;
- ma'lumotlar bazasi ma'muri – MBBT foydalanuvchilarining o'zgacha toifasini tashkil etadi. Ma'murlar o'zlari ma'lumotlar bazasini yaratadilar, MBBT ishlashining texnik nazoratini amalga oshiradilar, tizimning kerakli tezkorligini ta'minlaydilar. Undan tashqari, ma'mur vazifasiga foydalanuvchilarni kerakli ma'lumotlardan foydalanishlarini ta'minlash hamda foydalanuvchilarga kerakli ma'lumotlarning tashqi tasavvurini yozish kiradi. Ma'mur xavfsizlik qoidasini va ma'lumotlar yaxlitligini belgilaydi.

Ma'lumotlar xavfsizligi modellari. Xavfsizlik modeli quyidagilarni o'z ichiga oladi:

- kompyuter (axborot) tizimining modeli;
- axborotning tahdidlardan himoyalanganlik mezonlari, prinsiplari, cheklanishlari va maqsad funksiyalari;
- tizimning xavfsiz ishlashining formallashtirilgan qoidalari, cheklanishlari, algoritmlari, sxemalari va mexanizmlari.

Aksariyat xavfsizlik modellari asosida kompyuter tizimlarini subyekt-obyekt modeli yotadi, xususan, avtomatlashtirilgan axborot tizimlarining yadrosi sifatidagi ma'lumotlar bazasi ham. Kompyuter tizimlarining ma'lumotlar bazasi ma'lumotlar bazasining subyektiga (mohiyatan aktiv), ma'lumotlar bazasining obyektiga (mohiyatan

passiv) va subyektlar harakati natijasidagi obyektlar ustidagi jarayonlarga ajratiladi (1.2-rasm).



1.2-rasm. Ma'lumotlar xavfsizligi modellaridagi kompyuter tizimlarining ma'lumotlar bazasi.

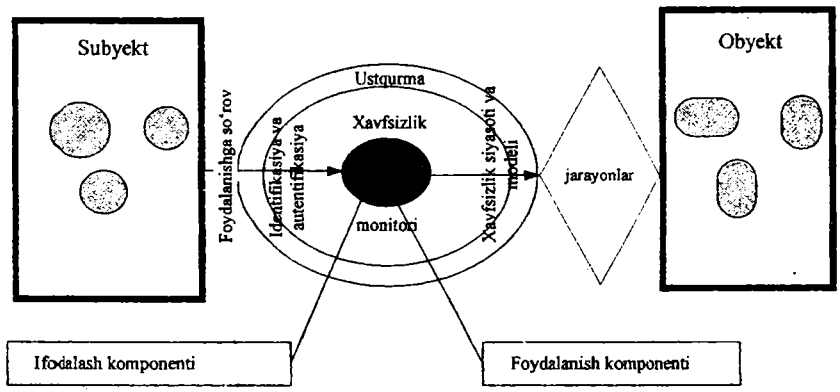
Axborot tizimlari ishlashi xavfsizligining ikkita eng muhim prinsipi ma'lum:

- obyektga nisbatan barcha subyektlar va jarayonlarning identifikatsiyasi va autentifikatsiyasi;
- obyektga nisbatan subyektlar vakolatlarini cheklash va ma'lumotlar ustidagi har qanday vakolatlarni tekshirish shartligi.

Mos holda MBBT yadrosi strukturasida ma'lumotlarni ishlashning barcha jarayonlarida belgilangan xavfsizlik siyosatini amalga oshiruvchi, xavfsizlik monitori (serveri, menedjeri, yadrosi) deb ataluvchi qo'shimcha komponent ajratiladi (Trusted Computing Base – TCB). Ushbu komponent ma'lumotlarni ishlashning barcha jarayonlarida xavfsizlikning ma'lum siyosatini amalga oshiradi. Sxemotexnika nuqtayi nazaridan, kompyuter tizimini ma'lumotlarni ifodalash va ulardan foydalanish (manipulyatsiyalash) komponentlarini hamda interfeys va tatbiqiy funksiyalarni amalga oshiruvchi ustqurmani o'z ichiga oluvchi yadro majmui sifatida tasavvur etilsa, xavfsizlik monitorining roli va o'rnini 1.3-rasmda keltirilgan sxema orqali izohlash mumkin.

Tor ma'noda kompyuter tizimi monitori amalga oshiruvchi xavfsizlik siyosatining o'zi xavfsizlik modelini aniqlaydi (ikkinchi va uchinchi komponentlar).

Ma'lumotlar xavfsizligining eng sodda (bir sathli) modeli foydalanishni cheklashning diskretsion (tanlash) prinsipiga asosan quriladi. Unga binoan obyektdan foydalanish "foydalanish subyekti – foydalanish turi – foydalanish obyekti" uchlik ko'rinishidagi foydalanishning ruxsat etilgan to'plami asosida amalga oshiriladi. Diskretsion foydalanishni formallashtirilgan ifodasini foydalanish matritsasi orqali tasvirlash mumkin. (1.4-rasm)



1.3-rasm. Kompyuter tizimlarida axborotni himoyalashning sxematik jihati.

Foydalanish matritsasi ma'lumotlar bazasining har bir obyektiga (jadvallar, so'rovlar, shakllar, hisobotlar) nisbatan foydalanuvchilar (subyektlar) ro'yxatini va ruxsat etilgan amallar (jarayonlar) ro'yxatini o'rnatadi.

Foydalanishni boshqarish xavfsizlik modelining muhim jihati hisoblanadi. Ikkita yondashish mavjud:

- foydalanishni ixtiyoriy boshqarish;
- foydalanishni majburiy boshqarish;

Foydalanishni ixtiyoriy boshqarishda obyektlarga egalik tushunchasi kiritiladi. Foydalanishni ixtiyoriy boshqarishda obyektdan foydalanish huquqini obyekt egasi belgilaydi. Boshqacha aytganda,

foydalanish matritsasining mos kataklari ma'lumotlar bazasi obyektlariga egalik huquqli subyektlar (foydalanuvchilar) tomonidan to'ldiriladi. Aksariyat tizimlarda obyektlarga egalik huquqi boshqa subyektlarga uzatilishi mumkin. Foydalanishni ixtiyoriy boshqarishda foydalanishni cheklash jarayonini tashkil etishning va boshqarishning to'liq markazlashtirilmagan prinsipi amalga oshiriladi.

		JADVALLAR				
		Xodim. O'rnatilgan ma'lumotlar	Xodim. Konfidensial ma'lumotlar	Amallar	Komandirovka	Topshiriqlar
Foydalanuvchilar	Karimov	O', M				
	Salimov	O'	O'	O', YA, M	O', YA, M	O', YA, M
	A'loev	O', M, YA, Y	O', M, YA, Y			
	Ruziev	O', M, YA, Y	O', M, YA, Y	O', M, YA, Y	O', M, YA, Y	O', M, YA, Y

Belgilashlar:
O' – o'qish;
M – modifikatsiyalash;
YA – yaratish;
Y – yo'qotish (yozuvlarni).

1.4-rasm. Foydalanish matritsasi asosidagi xavfsizlik modeli.

Bunday yondashishda ma'lumotlar bazasida foydalanishni cheklash tizimini foydalanuvchilar va resurslarning muayyan majmuiga sozlashning moslanuvchanligi ta'minlanadi, ammo tizimdagi ma'lumotlar xavfsizligi holatining umumiy nazorati va auditi qiyinlashadi.

Foydalanishni boshqarishga majburiy yondashish foydalanishni yagona markazlashtirilgan ma'murlashni ko'zda tutadi. Ma'lu-

motlar bazasida maxsus ishonchli subyekt (ma'mur) ajratiladi va u (faqat u) ma'lumotlar bazasi obyektlaridan foydalanuvchi barcha qolgan subyektlarni belgilaydi. Boshqacha aytganda, foydalanish matritsasi kataklarini to'ldirish va o'zgartirish faqat tizim ma'muri tarafidan amalga oshiriladi.

Majburiy usul foydalanishni qat'iy markazlashtirilgan boshqarishni ta'minlaydi. Shu bilan birga bu usulning foydalanuvchilarning ehtiyojlari va vakolatlariga, foydalanishni cheklash tizimini sozlash nuqtayi nazaridan, moslashuvchanligi kamroq, aniqligi pastroq, chunki obyektlar (resurslar) tarkibi va konfidensialligi xususidagi eng to'liq tasavvurga ularning egalari ega bo'ladilar.

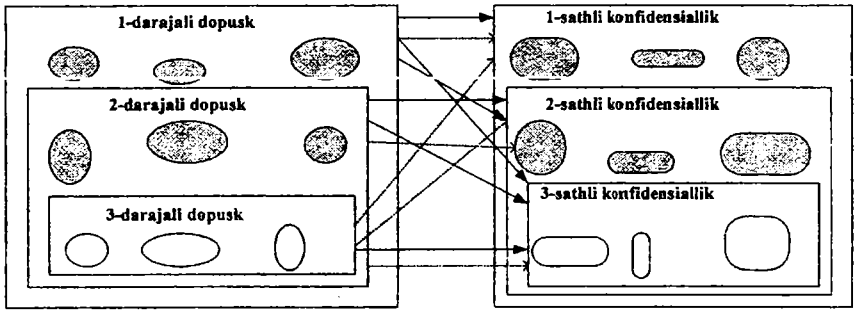
Amalda foydalanishni boshqarishning kombinatsiyalangan usuli qo'llanishi mumkin. Unga binoan obyektlardan foydalanish vakolatining ma'lum qismi ma'mur tomonidan, boshqa qismi esa obyekt egalari tomonidan o'rnatiladi.

An'anaviy sohalarda (kompyuter sohasida emas) va texnologiyalarda axborot xavfsizligini ta'minlashga yondashishlarning tadqiqi ko'rsatadiki, ma'lumotlar xavfsizligining bir sathli modeli real ishlab chiqarish va tashkiliy sxemalarni adekvat akslantirishga yetarli emas. Xususan, an'anaviy yondashishlar axborot resurslarini konfidensiallik darajasi (mutlaqo maxfiy-SS, maxfiy-S, konfidensial-K va h.) bo'yicha kategoriyalashdan foydalanadi. Mos holda axborot resurslaridan foydalanuvchi subyektlar (xodimlar) ham mos ishonch darajasi bo'yicha kategoriyalanadi. Ularga 1-darajali dopusk, 2-darajali dopusk va h. beriladi. Dopusk tushunchasi axborotdan foydalanishni cheklashning mandatli (vakolatli) prinsipini belgilaydi. Mandatli prinsipga binoan 1-darajali dopuskga ega xodim "SS", "S" va "K" darajali har qanday axborot bilan ishlash huquqiga ega. 2-darajali dopuskga ega xodim "S"va "K" darajali har qanday axborot bilan ishlash huquqiga ega. 3-darajali dopuskga ega xodim "K" darajali har qanday axborot bilan ishlash huquqiga ega.

MBBTda foydalanishni cheklash tizimini qurishning mandatli prinsipi Bell-LaPadula modeli deb ataluvchi ma'lumotlar xavfsizligining ko'p sathli modelini amalga oshiradi. (1.5-rasm).

Bell-La Padula modelida obyektlar va subyektlar foydalanishning ierarxik mandatli prinsipi bo'yicha kategoriyalanadi. 1- (eng yuqori) darajali dopuskga ega subyekt konfidensiallikning 1- (eng

yuqori) sathli obyektlaridan va avtomatik tarzda konfidensiallik sathlari ancha past obyektlardan (ya'ni 2- va 3-sathli obyektlardan) foydalana oladi. Mos holda, 2-darajali dopuskga ega subyekt konfidensiallikning 2- va 3-sathli obyektlaridan foydalana oladi.



1.5-rasm. Ma'lumotlar xavfsizligining Bell-LaPadula modeli.

Bell-LaPadula modelida xavfsizlik siyosatining ikkita asosiy cheklashlari o'rnatiladi va madadlanadi:

- yuqorini o'qish man etiladi (no read up - NRU);
- pastga yozish man etiladi (no write down - NWD).

NRU cheklash foydalanishni cheklashning mandatli prinsipini mantiqiy natijasi hisoblanadi, ya'ni subyektlarga dopusklari imkon bermaydigan yuqori sathli konfidensiallikka ega obyektlardan foydalanish man etiladi.

NWD cheklash konfidentsialligi yuqori sathli obyektlardan axborotni nusxalash yo'li bilan konfidensialligi bo'lmagan yoki konfidensialligi past sathli obyektlarga konfidensial axborotning o'tkazilishini (sirqib chiqishini) bartaraf etadi.

Amalda ma'lumotlar bazasi xavfsizligi monitorining real siyosatlarida ko'pincha mandatli prinsip elementlari bilan foydalanishni ixtiyoriy boshqarishli prinsipi birgalikda "kuchaytirilgan" foydalanishni majburiy boshqarishli diskresion prinsip ishlatiladi (subyektlar dopuskini faqat ma'mur belgilaydi va o'zgartiradi, obyektlarning konfidensiallik sathini faqat obyekt egalari belgilaydi va o'zgartiradi).

Nazorat savollari

1. "Axborot xavfsizligi" tushunchasining tarkibiy qismlarini sanab o'ting.
2. Ma'lumotlar bazasini boshqarish tizimi qanday funksiyalarni amalga oshiradi?
3. Ma'lumotlarni tashkil etishning qanday modellarini bilasiz?
4. "Tranzaksiya" tushunchasiga izoh bering.
5. Ma'lumotlar bazasini boshqarish tizimi strukturasi va komponentlarining o'zaro bog'lanishlarini tushuntirib bering.
6. Ma'lumotlar bazasi xavfsizligi modelining tashkil etuvchilarini sanab o'ting.
7. Ma'lumotlar bazasini boshqarish tizimida foydalanishning diskretsion va mandatli cheklash prinsiplarini tushuntiring.

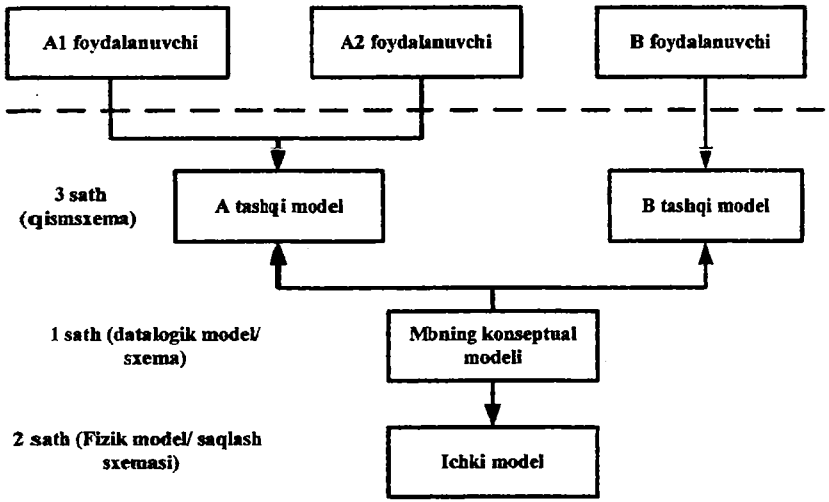
1.2. Ma'lumotlar bazasini boshqarish tizimlarining turlari

Muloqot tillari bo'yicha ochiq, yopiq va aralash MBBTlari farqlanadi. Ochiq tizimlarda ma'lumotlar bazasiga murojaat uchun dasturlarning universal tillari ishlatiladi. Yopiq tizimlar ma'lumotlar bazasi foydalanuvchilari bilan muloqotda xususiy tillardan foydalanadi.

Arxitekturadagi sathlar soni bo'yicha bir sathli, ikki sathli, uch sathli tizimlar farqlanadi. Umuman, sathlarning katta sonini ajratish mumkin. MBBTning arxitekturaviy sathi deganda mexanizmlari ma'lumotlar abstraktsiyasining qandaydir sathini madadlashga xizmat qiluvchi funksional komponent tushuniladi. (Mantiqiy va fizik sath hamda foydalanuvchi "nigohi" - tashqi sath). (1.6-rasm).

Bajariladigan funksiyalari bo'yicha axborot va operatsion MBBTlari farqlanadi. Axborot MBBTlari axborotni saqlashga va undan foydalanishni tashkil etishga imkon beradi. Murakkabroq ishlashni bajarish uchun maxsus dasturlar tuzish lozim. Operatsion MBBTlari yetarlicha murakkab ishlashni bajaradi, masalan, bevosita ma'lumotlar bazasida saqlanmagan agregirlangan ko'rsatkichlarni avtomatik tarzda olishga imkon beradi, ishlash algoritmini o'zgartirishi mumkin va h.

Qo'llanishi mumkin bo'lgan soha bo'yicha universal va ixtisoslashtirilgan (muammoga yo'naltirilgan) MBBTlari farqlanadi.



1.6-rasm. MBBTning arxitekturadagi sathlar soni bo'yicha tasnifi (uch sathli arxitektura misoli).

Ma'lumotlar bazasini boshqarish tizimlari turli xil ma'lumotlarni madadlaydi. Turli MBBTdagi joiz ma'lumotlarning turlar nabori har xil. Undan tashqari, qator MBBTlar ishlab chiqaruvchiga ma'lumotlarning yangi turlarini va bu ma'lumotlar ustida bajariluvchi yangi amallarni qo'shishga imkon beradi. Bunday tizimlar ma'lumotlar bazasining kengayuvchi tizimlari deb yuritiladi.

Ma'lumotlar bazasining kengayuvchi tizimlari konsepsiyasining keyingi rivoji – murakkab obyektlarni bevosita modellashda yetarlicha *quvvatli ifodalash* imkoniyatlariga ega bo'lgan ma'lumotlar bazasining obyektga yo'naltirilgan tizimi hisoblanadi.

Quvvati bo'yicha bitta odam foydalanuvchi va ko'pchilik foydalanuvchi (korporativ) MBBTlari farqlanadi. Bitta odam foydalanuvchi MBBTlar texnik vositalarga qo'yiladigan talablarning yuqori emasligi, oxirgi foydalanuvchiga mo'ljallanganligi, narxining pastligi bilan xarakterlanadi.

Korporativ MBBTlar taqsimlangan muhitda ishlashni, yuqori unumdorlikni, tizimni loyihalashda jamoa ishining madadini ta'minlaydi, rivojlangan ma'murlash vositasiga va yaxlitlikni madadlashning keng imkoniyatlariga ega. Ushbu tizimlar murakkab, qimmat, ko'pgina hisoblash resurslarini talab etadi.

Bitta odam foydalanuvchi va korporativ MBBTlarning qiyosiy xarakteristikalari 1.1-jadvalda keltirilgan.

Bitta odam foydalanuvchi va korporativ foydalanuvchi MBBTlarning qiyosiy xarakteristikasi

1.1- jadval

Mezon	Bitta odam foydalanuvchi	Korporativ foydalanuvchi
Foydalanish osonligi	+	
Dasturiy ta'minot narxi	+	
Ekspluatatsiya narxi	+	
Funksional imkoniyatlari: ma'murlash, Internet/Intranet bilan ishlash va h.		+
Ishlash ishonchligi		+
Madadlanuvchi ma'lumotlar hajmi		+
Tezkorligi		+
Masshtablash imkoniyatlari		+
Geterogen muhitda ishlash		+

Ikkala sinf tizimlari jadallik bilan rivojlanmoqda, uning ustiga rivojning ba'zi tendensiyalari ushbu sinflarning har biriga taalluqli. Birinchi navbatda, ilovalarni ishlab chiqishda yuqori sathli vositalardan foydalanish (avval asosan bitta odam foydalanuvchi tizimlarga taalluqli edi), unumdorlikning va funksional imkoniyatlarning o'sishi, lokal va global tarmoqlarda ishlash va h. Keng tarqalgan korporativ MBBTlariga Oracle, DB2, Sybase, MS SQL Server, Progress va boshqalar taalluqli.

Ishlab chiquvchilarga va oxirgi foydalanuvchilarga mo'ljallangan MBBTlar farqlanadi. Ishlab chiqaruvchilarga mo'ljallangan

MBBTlar samarali murakkab tizimlarni qurishga imkon beruvchi sifatli kompilyatorlarga va sozlashning rivojlangan vositalariga, loyihani hujjatlash vositalariga va boshqa imkoniyatlarga ega bo'lishlari shart. Oxirgi foydalanuvchiga mo'ljallangan MBBTlarga qo'yiladigan talablar quyidagilar: interfeysning qulayligi, til vositalari sathining yuqoriligi, yo'l-yo'riqlarning intellektual modullarining mavjudligi, bexosdan qilingan xatolardan himoyaning yuqoriligi va h.k.

MBBTlarni avlodlar bo'yicha ajratish mavjud. Birinchi avlod MBBTlari (XX asrning 60–70-yillari) ierarxik va tarmoqli modellarga asoslangan, ikkinchi avlod MBBTlariga relyatsion tizimlar taalluqli. Uchinchi avlod MBBTlari ma'lumotlarning murakkab strukturalarini va ma'lumotlar yaxlitligini ta'minlovchi rivojlangan vositalarni madadlashi, ochiq tizimlarga qo'yiladigan talablarni qondirishi lozim.

Nazorat savollari

1. Muloqot tillari bo'yicha qanday MBBTlar farqlanadi?
2. Arxitekturadagi sathlar soni bo'yicha qanday MBBTlar farqlanadi?
3. Ma'lumotlar bazasini boshqarish tizimi quvvati bo'yicha qanday MBBTlar farqlanadi?
4. Bitta odam foydalanuvchi va korporativ MBBTlarining qiyosiy xarakteristikalari.

1.3. Ma'lumotlar bazasi xavfsizligining texnologik jihatlari

Yuqorida keltirilgan xavfsizlik siyosatlari va modellarining hamda himoyalangan ma'lumotlar bazasini qurishning va ishlashining aksiomatik prinsiplarini amalga oshirilishi quyidagi yo'nalishlar bo'yicha guruhlash mumkin bo'lgan qator dasturiy – texnologik masalalarni yechish zaruriyatini keltirib chiqaradi:

- identifikatsiya va autentifikatsiya texnologiyalari;
- ma'lumotlar bazasi xavfsizligi tillari;

- obyektlardan takroran foydalanish xavfsizligini ta'minlash texnologiyalari;
- ishonchli loyihalash va ma'murlash texnologiyalari.

1.3.1. Identifikatsiya va autentifikatsiya texnologiyalari

Identifikatsiya va autentifikatsiya texnologiyalari himoyalangan tizimning majburiy elementi hisoblanadi, chunki u subyektlarni personalizatsiyalashning aksiomatik prinsipini ta'minlaydi va natijada kompyuter tizimlarida axborotni himoyalashning birinchi (dastlabki) dasturiy – texnik chegarasini amalga oshiradi.

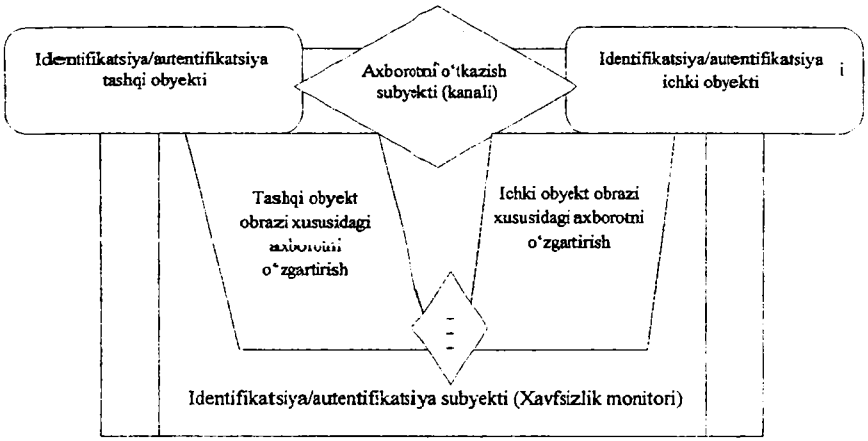
Identifikatsiya deganda subyektlarni, obyektlarni, jarayonlarni nomlari bilan ifodalanuvchi obrazlari bo'yicha farqlash tushuniladi.

Autentifikatsiya deganda identifikatsiyalangan subyektlar, obyektlar, jarayonlar obrazining haqiqiyligini tekshirish va tasdiqlash tushuniladi.

Sistemotexnik jihatdan identifikatsiya/autentifikatsiya tizimi strukturasini 1.7-rasmda keltirilgan sxema orqali tasvirlash mumkin.

Tizimda identifikatsiyalash/autentifikatsiyalash obyekti xavfsizlik monitori tomonidan ro'yxatga olinganda uning obrazi shakllanadi. Ushbu obraz bo'yicha axborot kriptografik o'zgartiriladi va tizimda faqat xavfsizlik monitori foydalana oluvchi resurs ko'rinishida saqlanadi. Shu tariqa identifikatsiya/autentifikatsiya obyektlari ichki obrazlarining axborot massivlari shakllanadi.

Keyinchalik identifikatsiyalashda/autentifikatsiyalashda obyekt o'zining obrazi xususidagi axborotni axborot eltuvchi kanal orqali xavfsizlik monitoriga o'zgartirish uchun uzatadi. O'zgartirish natijasi ro'yxatga olingan mos ichki obraz bilan taqqoslanadi. Ularning mosligida obyektning aniqlanganligi (identifikatsiyalanganligi) va haqiqiyligi (autentifikatsiyalanganligi) xususida qaror qabul qilinadi.



1.7-rasm. Identifikatsiya / autentifikatsiyaning sxemotexnik jihati.

Identifikatsiya/autentifikatsiya obyektlari ichki obrazining axborot massivi tizimning jiddiy resursi hisoblanadi va undan ruxsatsiz foydalanish butun xavfsizlik tizimini obro'sizlantiradi. Shuning uchun undan ruxsatsiz foydalanishga yo'l qo'ymaslikning barcha choralaridan tashqari axborot massivining o'zi shifrlangan bo'lishi lozim.

Umuman, kompyuter tizimlarida subyektlarni (foydalanuvchilarni) identifikatsiyalash/autentifikatsiyalash uchun ularning biometrik parametrlari (barmoq izlari, qo'l panjasining geometrik shakli, yuzning shakli va o'lchamlari, ko'z yoyi va to'r pardasining naqshi, ovoz xususiyatlari va h.) yoki maxsus qurilmalar (smart-kartalar, magnit kartalar va h.) ishlatilishi mumkin. Ammo bevosita kompyuter tizimidan (ma'lumotlar bazasidan) foydalanilganda, ko'pincha identifikatsiya/autentifikatsiyaning parol tizimi ishlatiladi.

Parol tizimlari autentifikatsiyalash onida foydalanuvchi tomonidan maxsus maxfiy (faqat haqiqiy foydalanuvchiga ayon) so'zni yoki simvollar naborini-parolni taqdim etishga asoslangan. Parol foydalanuvchi tomonidan klaviaturadan kiritiladi, kriptografik o'zgartiriladi va o'zining tizimdagi shifrlangan nusxasi bilan taq-

qoslanadi. Tashqi va ichki parol identifikatori mos kelganda mos subyektni aniqlash va haqiqiyligini tasdiqlash amalga oshiriladi.

Parol tizimlari oddiy, ammo parollarni to'g'ri tanlash va foydalanish sharoitida, xususan, foydalanuvchilar parollarni so'zsiz yashirincha saqlashlari sharoitida, autentifikatsiyalashning yetarlicha ishonchli vositasi hisoblanadi. Shu sababli parol tizimlari keng tarqalgan.

Parol tizimlarining asosiy kamchiligi autentifikatorning subyekt-eltuvchidan ajralganligi. Natijada parol u yoki bu usul bilan qonuniy foydalanuvchidan olinishi yoki klaviaturadagi nabordan mo'ralanishi, tizimga kirish yo'lida u yoki bu usul bilan ushlab qolinishi va tizimga niyati buzuq tomonidan taqdim etilishi mumkin.

Shu sababli ba'zi hollarda parol tizimlari kollektiv murojaat tizimi bilan kuchaytirilishi mumkin. Kollektiv murojaat tizimida autentifikatsiyani tizimda ro'yxatga olingan barcha foydalanuvchilar birdaniga o'tishlari shart. Boshqacha aytganda, foydalanuvchilar yakka holda tizimda ishlay olmaydilar. Niyati buzuq tomonidan birdaniga barcha parollarni saralash, ushlab qolish va h. ehtimolligi juda kam, demak, bunday autentifikatsiya tizimining ishonchliligi yuqori.

Taqsimlangan axborot tizimlarida obyektlarni (resurslarni, qurilmalarni) hamda jarayonlarni (so'rovlarni, paketlarni va h.) autentifikatsiyalash lozim. Autentifikatsiyalangan (haqiqiy) foydalanuvchi tizim obyektlariga murojaat etish jarayonida, o'z navbatida, ularning haqiqiy ekanligiga ishonch hosil qilishi lozim.

Jarayonlarni autentifikatsiyalashda belgi (deskriptor) texnologiyalari keng tarqalgan. Foydalanishning belgi yoki deskriptor texnologiyasi xavfsizlikning bir sathli va ko'p sathli modellarining birikmasini aks ettiradi va tizim ma'muri tomonidan ma'lumotlar bazasining barcha obyekt va subyektlariga foydalanishning maxsus deskriptorlarini berishga asoslangan. Foydalanishning deskriptori tarkibida konfidensiallik sathi parametrlarining, joiz amallarning, foydalanish obyektlari yoki subyektlarining joiz nomlarining va foydalanishning boshqa shartlarining nabori bo'ladi. Foydalanish subyekti o'zining deskriptoriga (belgisiga) binoan ruxsat etilgan jarayonni boshlab, unga o'zining foydalanish belgisini uzatadi.

MBBT xavfsizlik yadrosi jarayon belgisini foydalanuvchi – subyektning foydalanish belgisi bilan taqqoslab, jarayon belgisining haqiqiyligini tekshiradi, ijobiy natijada jarayonning foydalanish belgisi obyektining foydalanish belgisi bilan taqqoslanadi. Agar jarayonning va obyektning foydalanish deskriptorlari bir-biriga mos kelsa, xavfsizlik monitori foydalanishga, ya'ni jarayonni (amalni) amalga oshirishga ruxsat beradi.

Belgilarning haqiqiyligini tekshirish uchun tizimda maxsus yozuvlarni qayd etish fayli (massivi) shakllantiriladi. Yangi foydalanuvchini ro'yxatga olishda uning uchun tarkibida uning identifikatsiya nomeri (identifikatori), parol autentifikatori va ma'lumotlar bazasi obyektlaridan foydalanish deskriptorlari nabori (foydalanish belgisi) bo'lgan qaydlash yozuvi yaratiladi. Foydalanuvchi (subyekt) ma'lumotlar bazasida qandaydir jarayonni boshlab, unga o'zining foydalanish belgisini uzatganida, MBBT xavfsizligi yadrosi jarayon belgisini kriptografik o'zgartiradi, uni qaydlash yozuvlari massividagi mos subyektga (foydalanuvchiga) tegishli shifrlangan belgi bilan taqqoslaydi va belgining haqiqiyligi xususida qaror qabul qiladi.

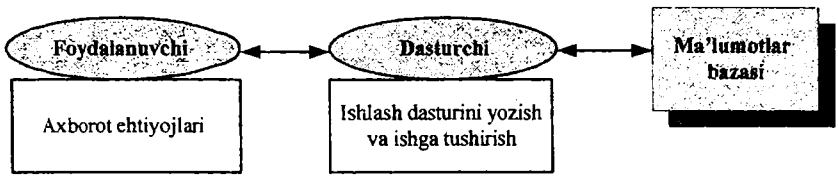
Qaydlash yozuvi massivi, o'z navbatida, tizimdagi yuqori darajali konfidensiallikka ega obyekt hisoblanadi va undan faqat ma'mur foydalanishi mumkin. Butun tizimning xavfsizligi uchun qaydlash yozuvlari massivining nihoyatda muhimligi tufayli, uni shifrlashdan tashqari qo'shimcha qator choralar ko'riladi, xususan, uni joylashtirish, uning yaxlitligini tekshirishning maxsus rejimlari. Shunday qilib, hozirda himoyalangan kompyuter tizimlarida identifikatsiya/autentifikatsiya texnologiyasining rivojlangan nabori ishlab chiqilgan va ishlatiladi. Shuning bilan birga, xavfsizlikning asosiy raxnalarini niyati buzuq aynan shu yo'nalishda topadi.

1.3.2. Ma'lumotlar bazasi xavfsizligi tillari

Kompyuter tizimining ma'lumotlar bazasini loyihalashda foydalanishning muayyan vazifalarini yoki foydalanish qoidalari va cheklashlarini o'rnatish hamda foydalanishni cheklash tizimini boshqarish maqsadida tizim ma'muriga maxsus vosita zarur. Bunday vosita foydalanishning u yoki bu vazifalarini va muayyan

kompyuter tizimida xavfsizlik siyosatining boshqa zarur yo'l-yo'riqlarini tavsiflash va o'rnatishga imkon beruvchi ma'lum tilga asoslanishi lozim.

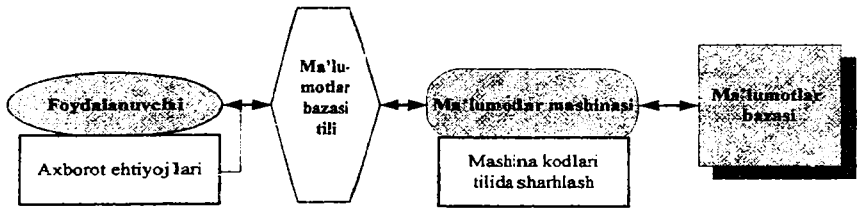
Ma'lumotlar bazasining ichki sxemasidan ko'rinib turibdiki, ma'lumotlar bazasini boshqarish tizimining asosiy vazifasi-ma'lumotlarni joylashtirish va ularni tashqi (diskli) xotira va asosiy xotira orasida almashishning xususiy tizimini yaratish va madadlash. Har bir muayyan MBBT tomonidan ushbu vazifani (ma'lumotlar fayllarining formati, indekslash, xeshlash va buferlash) samarali amalga oshirilishi butun MBBTning samarali ishlashini ta'minlaydi. Shu sababli, 60-yillar oxiri va 70-yillar boshidagi dastlabki MBBT yaratuvchilarining asosiy kuchlari aynan ushbu yo'nalishga qaratilgan edi. Natijada ma'lumotlarni kiritish, ishlash yoki chiqarish bo'yicha har qanday funksiyalarni amalga oshirish uchun yuqori darajali algoritmik tillarida (70-yillar FORTRAN, KOBOL va h.) maxsus dasturlarni yaratuvchi, ma'lumotlar strukturasini tashqi va asosiy xotirada joylashtirish usullarining xususiyatlarini "biluvchi" malakali dasturchilar talab etilar edi. Oqibatda, ma'lumotlar bazasi bilan ishlash foydalanuvchining axborotga bo'lgan ehtiyojini mashina kodiga "o'tkazuvchi" yuqori malakali dasturchi – vositachi orqali amalga oshirilar edi (1.8-rasm).



1.8-rasm. Ilk MBBTlarda foydalanuvchilarning ma'lumotlar bazasi bilan o'zaro aloqasi.

Bunday vaziyat avtomatlashtirilgan axborot tizimini yaratishda va ekspluatatsiyasida katta qo'shimcha xarajatlarga olib keldi hamda korxona va tashkilot faoliyatidagi axborot ta'minoti jarayonlarida hisoblash texnikasining tarqalishini ma'lum darajada to'xtatdi.

Relyatsion MBBTlar nazariyasining asoschisi E.Kodd tomonidan ma'lumotlar bazasi bilan dasturchi bo'lmagan foydalanuvchining muloqoti uchun maxsus tilni yaratish xususida taklif kiritildi. Ushbu til ingliz tilining bir nechta sodda iboralari ("tanlash", "yangilash", "kiritish", "yo'qotish") naboridan tashkil topgan bo'lib, ular orqali dasturchi bo'lmagan foydalanuvchi o'zining axborotga bo'lgan ehtiyoji bo'yicha MBBTga "savollar" qo'yishi mumkin. Bunda ma'lumotlarni bevosita ishlash va foydalanuvchiga natijalarni taqdim etish uchun ushbu "savollarni" mashina kodlarining past darajali tilida sharhlash MBBTning qo'shimcha vazifasi hisoblanadi. Shu tariqa MBBT strukturasidagi "ma'lumotlar mashinasi" paydo bo'ldi. Boshqacha aytganda, ma'lumotlar mashinasi ma'lumotlar bazasi tilini "tushunadi", natijada ma'lumotlarni va ularni ishlash bo'yicha masalalarni ajratadi. Bunday yondashishda foydalanuvchining ma'lumotlar bazasi bilan o'zaro aloqasini 1.9-rasm orqali tasvirlash mumkin.



1.9-rasm. Foydalanuvchining ma'lumotlar bazasi bilan ma'lumotlar bazasi tili orqali o'zaro aloqasi.

Ushbu g'oyalar ilk bor ma'lumotlar bazasi sohasidagi yana bir mashhur mutaxassis Kris Deyt ishtirokida System R (1975 – 1979 yy.) loyihasi amalga oshirilishida tatbiq etildi. Loyihani amalga oshirish jarayonida keyinchalik strukturalangan so'rovlar tili SQL (Structured Query Language)ga aylantirilgan SEQUEL yaratildi. Bunda foydalanuvchiga ma'lumotlar bazasiga "so'rovlarni" shakllantirish imkoniyatiga qo'shimcha tarzda ma'lumotlar strukturalarini, ma'lumotlarni kiritishni va ularni o'zgartirishni tavsiflash imkoniyati ham taqdim etildi. Taxminan shu vaqtda IBM firmasi to-

monidan yana bir relyatsion til – QBE (Query – By – Example) yaratildi. Ushbu til keyinchalik jadval ma'lumotlarini ishlovchi tijorat tizimlarida ishlatildi va zamonaviy MBBTlarida so'rovlarning vizual "konstrukturalarini" yaratishda g'oyaviy asos vazifasini o'tadi.

SQL tilining g'oyasi tezda ommaviylashib, 70-yillar oxiri va 80-yillarning boshida yaratilgan relyatsion MBBTlarda keng qo'llanildi. Natijada SQL tili 1986-yil standartlarning Amerika milliy instituti (ANSI) va standartlashtirishning Xalqaro tashkiloti (ISO) tomonidan relyatsion MBBTlarda ma'lumotlarni tavsiflash va ishlashning standart tili sifatida e'tirof etildi. 1989-yil SQL tilining mukammalashtirilgan SQL2 va 1992-yili SQL3 versiyalari ANSI/ISO tomonidan qabul qilindi.

SQL tili dasturlashning deklarativ (muolajaviy bo'lmagan) tillariga mansub. Muolajaviy tillardan (C, paskal, Fortran, Kobol, Beysik) farqli o'laroq SQL tilida "nima qilish kerak", ammo "qanday qilmoq kerak, qanday olish lozim" emas xususida takliflar (yo'riqnomalar) ifodalanadi. MBBTdagi ma'lumotlar mashinasi sharhlash rolini bajaradi va SQL – yo'riqnomalari belgilagan natijani olish usulini amalga oshiruvchi mashina kodini tuzadi.

SQL tili ikki qismdan iborat:

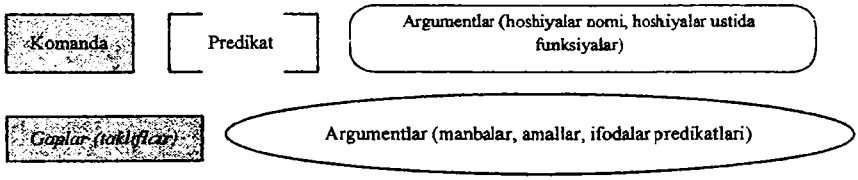
- ma'lumotlarni tavsiflash tili DDL (Data Definition Language);
- ma'lumotlarni manipulyatsiyalash tili DML (Data Manipulation Language).

SQL – yo'riqnomalari sintaksisining tarkibi:

- yo'riqnoma (komanda) nomi;
- manbalarni, amal shartlarini belgilovchi gaplar;
- gaplar belgilagan yozuvlarni tanlash usullarini va rejimlarini aniqlovchi predikatlar;
- mazmunlari yo'riqnomalar va gaplar bajarilishi xususiyatlarini va parametrlarini belgilovchi ifodalar.

SQL – yo'riqnomalarini ikki qismga ajratish mumkin (1.10-rasm).

Birinchi qism tarkibiga SQL – yo'riqnomaning nomi (komandasi), predikat (majburiy bo'lmagan) va yo'riqnoma argumentlari kiradi. Bir yoki bir necha jadvallar hoshiyalarining vergul oralab yozilgan nomlari yo'riqnoma argumentlarini tashkil etadi.



1.10-rasm. SQL-yo'riqnomalari strukturasi.

Ikkinchi qismi argumentlari ma'lumotlar manbaini (jadvallar nomini, jadvallar ustidagi amallarni), komandalar bajarilishi usullari, shartlari va rejimlarini (taqqoslash predikatlarini, jadvallar hoshiyalari mazmunlari bo'yicha mantiqiy va matematik ifodalarni) belgilashlari mumkin bo'lgan bitta yoki bir nechta gaplardan iborat. SQL – yo'riqnomalarining ro'yxati SQL tilining qismlari bo'yicha ajratiladi.

DDL tili tarkibiga relyatsion jadvallarni va ular orasidagi bog'lanishlarni yaratishda asosiy funksiyalar naborini ta'minlovchi bir necha bazaviy yo'riqnomalar kiradi:

CREATETABLE . . . – jadval tuzish;

CREATEINDEX . . . – indeks yaratish;

ALTERTABLE . . . – avval tuzilgan jadval strukturasin o'zgartirish;

DROP . . . – mavjud jadvalni va ma'lumotlar bazasini yo'q qilish.

CREATEABLE va ALTERTABLE yo'riqnomalar strukturasida CONSTRAINT gapi (ma'lumotlar qiymatlariga cheklashlar tashkil etish) NOT NULL (mos hoshiya bo'yicha nullik qiymatlar nojoiz), AYTOINC (qiymatlari inkremental xarakterli, ya'ni har bir yangi yozuv bilan qiymatlar xarakterining ketma-ket o'suvchi hoshiya) va PRIMARY KEY (noyob hoshiya uchun aniqlash) ko'rsatmalari bilan muhim rolni o'ynaydi.

DML tili tarkibiga ma'lumotlarni kiritish, ishlash va chiqarish bo'yicha quyidagi bazaviy yo'riqnomalar ham kiradi:

SELECT . . . – ma'lumotlar bazasidan ma'lumotlarni tanlash;

INSERT . . . – ma'lumotlar bazasiga ma'lumotlarni qo'shish;

UPDATE . . . – ma'lumotlar bazasidagi ma'lumotlarni yangilash;

DELETE . . . – ma'lumotlarni chiqarib tashlash;

GRANT . . . – foydalanuvchiga imtiyozlarni taqdim etish;

REVOKE . . . – foydalanuvchi imtiyozlarini bekor qilish;

COMMIT . . . – joriy tranzaksiyani qaydlash;

ROLLBACK . . . – joriy tranzaksiyani to'xtatish.

SELECT yo'riqnomasining bir turi – SELECT . . . INTO . . . (bir yoki bir necha jadvaldan yozuvlar naborini tanlash va u yordamida yangi jadvalni tuzish) va jadvallarni birlashtirish amalini bajaruvchi dastlabki SELECT yo'riqnomasiga qo'shimcha (SELECT. . . UNION SELECT . . .) UNION SELECT yo'riqnomalari muhim ahamiyatga ega.

SQL – yo'riqnomalarida CONSTRAINT gapidan tashqari quyidagi gaplar ishlatiladi:

FROM . . . – SELECT yo'riqnomalarida sanab o'tilgan hoshiyalardagi jadvallarni yoki so'rovlarni ko'rsatadi;

WHERE . . . – FROM gapida sanab o'tilgan jadvallardagi qaysi yozuvlarni SELECT, UPDATE yoki DELETE yo'riqnomalarining bajarilishi natijasiga qo'shish lozimligini aniqlaydi;

GROUP BY . . . – hoshiyalar ro'yxatida ko'rsatilgan bir xil qiymatli yozuvlarni bitta yozuvga birlashtiradi;

HAVING . . . – SELECT yo'riqnomasi GROUPBY gapi bilan ishlatilganda qanday guruhlangan yozuvlar akslantirilishini aniqlaydi;

IN . . . – MBBT yadrosi aloqa bog'lashi mumkin bo'lgan ma'lumotlarning har qanday tashqi bazasidagi jadvallarni aniqlaydi;

ORDERBY . . . – so'rov natijasida olingan yozuvlarni, ko'rsatilgan hoshiya yoki hoshiyalar qiymatlari asosida, o'sish yoki kamayish tartibida saralaydi.

FROM gapi bo'yicha ma'lumotlarning manbai sifatida jadvallar va so'rovlardan tashqari jadvallarni uch xil ko'rinishda birlashtirish natijalari ham ishlatilishi mumkin. Ushbu birlashtirishlar –

INNEP JOIN . . . ON . . . , LEFT JOIN . . . ON . . . va

RIGHT JOIN . . . ON . . . (mos holda, ichki bog'lanish, chapga yoki o'ngga tashqi bog'lanish).

Predikatlardan SQL – yo'riqnomalaridagi shartlar asosida tanlab olingan yozuvlarni ishlatish usullarini va rejimlarini belgilash uchun foydalaniladi. Bunday predikatlar quyidagilar:

ALL . . . – SQL – yo'riqnomalari shartlariga mos barcha yozuvlarni tanlab oladi;

DISTINCT . . . – tanlangan hoshiyalarda takrorlanuvchi qiymatlarga ega yozuvlarni chiqarib tashlaydi;

DISTINCTROW . . . – butunlay takrorlanuvchi yozuvlarga asoslangan ma'lumotlarni tushirib qoldiradi;

TOP . .. – ORDER BY gapi yordamida tavsiflangan diapazonning boshlanishidagi yoki oxiridagi yozuvlarni qaytaradi.

SQL – yo'riqnomalarida matematik iboralar qoidalari bo'yicha qurilgan va natijasi muayyan, jumladan mantiqiy qiymat bo'lgan har qanday operatorlar, konstantalar, matnli konstantalar qiymatlari, funksiyalar, hoshiyalar nomi kombinatsiyalari ifoda hisoblanadi.

Foydalanuvchilarga imtiyozlarni taqdim etuvchi yoki bekor qiluvchi GRANT va REVOKE yo'riqnomalari SQL tili yo'riqnomalarining asosini tashkil etadi.

GRANT yo'riqnomasining strukturasi quyidagi ko'rinishga ega:

GRANT imtiyozlari ro'yxati vergul orqali ON Obyekt Nomi
TO foydalanuvchilar ismlari vergul orqali
[WITH GRANT OPTION];

bu erda:

- obyekt (jadval) ustida ruxsat etilgan yo'riqnomalar (amallar) – SELECT, INSERT, UPDATE, DELETE – imtiyozlar ro'yxatini tashkil etadi;

- foydalanuvchilar ro'yxati ularning ismlari – identifikatorlari orqali ifodalanishi yoki tizimda ro'yxatga olingan, barcha foydalanuvchilarni identifikatsiyalovchi tayanch so'z PUBLIC bilan almashtirilishi mumkin;

- WITH GRANT OPTION direktivasi sanab o'tilgan foydalanuvchilarga boshqa foydalanuvchilarga ro'yxatda ko'rsatilgan imtiyozlar – vakolatlarni berish bo'yicha qo'shimcha alohida vakolatlar ato etadi.

Aksariyat hollarda muayyan obyekt bo'yicha GRANT va REVOKE komandalarini berish huquqiga avtomatik tarzda ushbu

obyektni yaratuvchilari ega bo'ladilar. Boshqa yondashishlarda ushbu huquqqa ishonchli subyektlar, ya'ni ma'murlar ega bo'ladilar. Bunday yondashish ochiq holda foydalanish matritsasini tuzishni ko'zda tutmasa-da, foydalanishni cheklashning diskresion prinsipi foydalanishning ixtiyoriy va majburiy boshqarishni qo'shib amalga oshiriladi.

Aslida aksariyat MBBTda imtiyozlar va foydalanishni o'rnatish, ma'lumotlar bazasi strukturasi kabi ma'lumotlar bazasining tizimli jadvallarida, ya'ni foydalanish matritsasi sifatida ham qabul qilish mumkin bo'lgan ma'lumotlar bazasining tizimli katalogida "qaydlanadi".

Yuqorida aytib o'tilganidek, diskresion prinsipi ma'lumotlar bazasidan foydalanishni cheklash tizimini predmet sohasining xususiyatlariga va foydalanuvchilar ehtiyojiga sozlash bo'yicha yuqori moslanuvchanlikka ega, ammo samarali boshqaruvchanlik ta'minlanmaydi va tizimda qanday bo'lsa ham aniq bir maqsadga yo'naltirilgan xavfsizlik siyosatini o'tkazishni qiyinlashtiradi. Ushbu kamchilikni bartaraf etishga ikkita yo'l bilan, ya'ni "tasavvur etish" texnikasini ishlatish va SQL tilini maxsus kengaytirish orqali erishiladi. "Tasavvur etish" deganda ma'lumotlarni tanlashdagi global avtorizatsiyalangan so'rov tushuniladiki, ushbu so'rov foydalanuvchilar uchun ma'lum obyekt (obyektlar) xususida "o'zining" tasavvurini shakllantiradi. O'zining sxemasiga (obyektiga va ma'lumotlariga tanlangan yoki maxsus o'zgartirilgan) qandaydir virtual ma'lumotlar bazasini shakllantiradi. Foydalanuvchining tizimga kirishida uni identifikatsiyalash va autentifikatsiyalash jarayonida xavfsizlik yadrosi foydalanuvchi uchun mos tasavvur-so'rovlar qidirib topadi va so'rovni bajarish uchun MBBTning asosiy yadrosiga uzatadi. So'rovni bajarish natijasida foydalanuvchi faqat uning vakolatiga va vazifalariga mos obyektlarni "ko'radi" va ulardan foydalanadi.

Umuman, tasavvur etish texnikasi vositasida foydalanishni cheklash tizimini yaratish, bevosita GRANT yo'riqnomasidan foydalanishga nisbatan oddiyroq usul hisoblanadi va quyidagi ikkita bosqichda amalga oshiriladi:

- barcha ro'yhatga olingan foydalanuvchilar uchun tizimda CREATE VIEW konstruktsiyasi yordamida o'zlarining ma'lumotlar bazasi xususidagi tasavvurlari vujudga keltiriladi;

- vujudga keltirilgan tasavvurlar "GRANT SELECT ON Tasavvur Ismi TO. Foydalanuvchi Ismi" yo'riqnoma yordamida o'zining foydalanuvchilari bilan avtorizatsiyalanadi.

Shu bilan birga, bunday yondashish ma'lumotlar bazasi obyektlariga bevosita qo'llanuvchi GRANT yo'riqnomasiga nisbatan qo'polroq hisoblanadi, chunki obyektlardan foydalanish ko'rsatmalarining alohida amallar (SELECT, INSERT, UPDATE, DELETE) darajasida bo'lishligini ta'minlamaydi.

Shu sababli xavfsizlikning maxsus qoidalari (RULE) kiritilgan hodisa-muolaja ideologiyasiga asoslangan SQL tilining maxsus kengaytirishlari ishlatiladi:

CREATESECURITYRULE – Ism Qoidalar
GRANT- imtiyozlar ro'yxati-vergul orqali ON – Obyekt Ismi
WHERE – shartlar
TO- Foydalanuvchilar Ismlari- vergul orqali.

Xavfsizlik qoidalarining kiritilishi turli xavfsizlik siyosatini yuqori darajali nazoratlash va boshqaruvchanlik bilan amalga oshirish imkoniyatini ta'minlaydi. Ammo, tasavvur etish texnikasi va GRANT yo'riqnomalaridan bevosita foydalanish mandatli cheklash tizimini qurishga imkon bermaydi.

Ushbu masalani yechish uchun konfidensiallik belgisi kiritilgan, ma'lumotlar bazasi obyektlarini yaratish imkoniyati bilan kengaytirilgan SQL tili tavsiya etilishi mumkin. Ammo tijorat va xavfsizlik jarayonlariga binoan sertifikatsiyalangan MBBTida bunday misollar juda kam uchraydi.

Ma'lumotlar bazasi xavfsizligi bo'yicha ta'kidlash lozimki, zamonaviy MBBTda SQL tilining mos konstruktsiyasini avtomatik tarzda shakllantiruvchi va aksariyat hollarda bevosita dasturlashsiz foydalanish ko'rsatmalarini, qoidalarini va cheklashlarni amalga oshirish uchun maxsus dialog – ko'rgazmali interfeys ishlab chiqiladi va ishlatiladi.

1.3.3. Obyektlardan takroran foydalanish xavfsizligini ta'minlash texnologiyalari

Umuman, kompyuter tizimi, xususan, asosiy va tashqi (diskli) xotira, ko'p marta takroran ishlatiluvchi obyektlarga klassik misol hisoblanadi. Obyektlardan takroran foydalanish xavfsizligini ta'minlovchi texnologiyalar niyati buzuqni qiziqtiruvchi axborotning oldingi faoliyat izi bo'yicha yoki texnologik "chiqindi"dan tasodifiy yoki atayin chiqarib olinishi tahdidini bartaraf etishga yo'naltirilgan.

Ushbu texnologiyaning bir qismi operatsion tizimi sathida amalga oshirilsa, boshqa qismi MBBTning avtomatlashtirilgan axborot tizimida amalga oshiriluvchi o'ziga xos funksiyalar hisoblanadi.

Bu texnologiyalar shartli ravishda quyidagi uchta guruhga ajratiladi:

- jarayonlarni yakkalash (izolyatsiyalash);
- jarayon tugaganidan so'ng xotirani tozalash;
- axborot sirqib chiqadigan bilvosita kanallarni to'sish.

Jarayonlarni yakkalash ko'pchilik foydalanuvchi (ko'p protsessorli) tizimlar ishonchliligini ta'minlovchi standart prinsip va usul hisoblanadi. Unga binoan har bir jarayonga o'zining boshqalar (avvalo asosiy xotira makonlari) bilan kesishmaydigan hisoblash resurslari ajratiladi. MBBTda ushbu masalalar tranzaksiya monitori yordamida yechiladi.

Jarayon tugagach xotirani tozalash, vakolatli foydalanuvchilarning konfidensial ma'lumotlar bilan ishlash jarayoni tugaganidan so'ng konfidensial axborotni ruxsatsiz foydalanishdan bevosita bartaraf etishga yo'naltirilgan. Ushbu funksiya jarayonlarni yakkalash kabi, ko'pincha operatsion tizim yordamida bajariladi. Ta'kidlash lozimki, nafaqat jarayon bajarilishi vaqtida konfidensial ma'lumotlar joylashgan asosiy xotiraning qismi, balki virtual-xotira tizimida ishlatiluvchi diskli xotira qismi ham tozalanishi lozim.

Yuqorida aytilganidek, foydalanishni cheklash tizimi amalga oshirilganida axborot sirqib chiqadigan bilvosita kanallar bo'lishi mumkin. Undan tashqari ma'lumotlarni ishlash jarayonlarining xarakteristikalari bilan bog'liq qator texnologik jihatlar axborot sirqib chiqadigan bilvosita kanallar manbai bo'lishi mumkin. Bu

nuqtayi nazaridan "vaqtli" va "xotira bo'yicha" bilvosita kanallar farqlanadi.

Birinchi holda vakolatsiz foydalanuvchi konfidensial axborotning ba'zi elementlariga vakolatli foydalanuvchi tomonidan alohida jarayonlarni bajarilishi vaqtini tahlillash asosida ega bo'ladi (masalan, shubhasiz oddiy yoki qandaydir namunaviy amal uchun haqiqatga to'g'ri kelmaydigan katta vaqt bo'yicha).

Ikkinchi holda ba'zi obyektlarning (fayllarning, jadvallarning) egallagan hajmi "shubha" tug'diradi, ya'ni foydalanuvchiga ko'ra ular tarkibining hajmi aslidagi hajmiga shubhasiz mos kelmaydi.

Boshqacha aytganda, ma'lumotlarni ishlovchi barcha amallar foydalanuvchi "tasavvuriga" mos ma'lumotlar hajmi ustidagina bajarilishi lozim.

Axborot xavfsizligi nuqtayi nazaridan, jiddiy holatlardan yana biri, eng qat'iy variant - ruxsat etilgan muolajalar texnologiyasi ishlatiladi. Bunda tizimdan foydanuvchilarga ma'lumotlar bazasi bilan ishlashga faqat ruxsat etilgan muolajalarni ishga tushirish orqali ruxsat beriladi. Ushbu yondashish ham yuqorida ko'rilgan saqlanuvchi (stored) muolajalar texnologiyasiga asoslangan. Har bir foydalanuvchi uchun, uning vakolatlari va funksiyalariga binoan, tizim ma'muri tomonidan ma'lumotlarni ishlash muolajalari nabori shakllantiriladi. Xavfsizlikni ta'minlash uchun faylda saqlanuvchi muolajalar shifrlanadi.

Foydalanuvchi tizimga kirishida identifikatsiya va autentifikatsiyadan o'tganidan so'ng unga MBBT yadrosi tomonidan muolajalarning ruxsat etilgan nabori taqdim etiladi. Foydalanuvchi ma'lumotlarning o'zidan bevosita foydalana olmaydi va faqat ularni mos muolajalar bo'yicha ishlanishi natijalari bilan ishlaydi.

Kompyuter tizimi ma'lumotlari strukturasi buzg'unchiga ma'lum bo'lishi mumkin bo'lgan ma'lumotlar fayllarida joylashtiriladi. Shu sababli, ma'lumotlar fayllaridan, kompyuter tizimi MBBT dasturiy ta'minotidan tashqarida operatsion tizim yoki diskli muharrir vositalari orqali ruxsatsiz foydalanish imkoniyati kompyuter tizimi ma'lumotlari xavfsizligiga yana bir tahdid hisoblanadi. Ushbu tahdidni betaraflashtirish uchun kriptografik himoya usullari va vositalaridan foydalaniladi. Aksariyat hollarda himoyaning kriptografik vositalari bevosita MBBT dasturiy ta'minotiga o'rnatiladi.

Ma'lumotlar bazasining fayli (fayllari) diskli xotira qurilmalarida joylashtirilganida shifrlanadi. Mos holda, fayl ochilganida kriptografik qismtizim uni deshifrlaydi. MBBTning o'ziga mos xususiyati – asosiy xotira sahifalarini maxsus buferlashni tashkil etish orqali ma'lumotlar bazasi fayllari bilan ishlashning alohida tartibi.

Rivojlangan MBBTlarda ma'lumotlar bazasi obyektlarini ularning konfidensiallik darajasiga asosan tanlab, shifrlash imkoniyati mavjud (yozuvlarning alohida hoshiyalarigacha).

1.3.4. Ishonchli loyihalash va ma'murlash texnologiyalari

Axborot xavfsizligiga tahdidlarning bir qismi kompyuter tizimlari hayotiy siklining bosqichlarida bilmasdan (yoki atayin) qilingan xatoliklar natijasida paydo bo'ladi. Bularga quyidagilar taalluqli: MBBT dasturiy ta'minotini ishlab chiqishda; MBBT bazasida muayyan kompyuter tizimini loyihalashda va yaratishda, xususan, foydalanishni cheklash tizimini loyihalashda; tizimni ma'murlashda, xususan, shtatdan tashqari vaziyatlarda foydalanuvchilar xarakatiga munosabat bildirishda; yanglishishdan so'ng rezervlash, arxivlash va axborotni tiklash bo'yicha texnologik amallarda; kompyuter tizimini ekspluatatsiyadan chiqarishda. Ushbu tahdidlarni betaraflashtirish yoki ehtimolliklarini pasaytirish maqsadida ishonchli loyihalash va ma'murlash texnologiyalarining umumiy guruhiga birlashtiriluvchi qator tashkiliy-texnologik va texnik vositalar, yechimlar ishlatiladi. Bularni shartli ravishda quyidagi qismguruhlarga ajratish mumkin:

- dasturiy ta'minotni ishonchli ishlab chiqish texnologiyasi;
- kompyuter tizimlarini ishonchli loyihalash va yaratish texnologiyasi;
- kompyuter tizimlarini ma'murlashning texnik vositalari va maxsus asboblari;
- xavfsizlik jarayonlarining bayonnomasini tuzish va auditi.

Dasturiy ta'minotni ishonchli ishlab chiqish texnologiyasi tizim yadrosi va konsepsiyasida (ma'lumotlarni ifodalash qismtizimi va ma'lumotlardan foydalanish qismtizimi) ma'lumotlar xavfsizligining u yoki bu modelini va texnologiyalarini avvaldan hisobga olishga asoslangan dasturiy kodni ishlab chiqishda xatoliklarni ka-

maytiruvchi umumiy yondashishlarni va qator o'ziga xos jihatlarni o'z ichiga oladi. Kompyuter tizimi xavfsizligi tizimida aniqlangan zaifliklarning tahlili ko'rsatadiki, raxnalarning mavjudligi va niyati buzuqlar tomonidan topilish ehtimolligi himoya tizimi dastlabki himoyalanmagan tizimni yadrosi va interfeysi ustida ustqurma yoki tashqi qobiq ko'rinishida amalga oshirilganida jiddiy katta bo'ladi.

MBBT dasturiy ta'minoti asosida muayyan avtomatlashtirilgan axborot tizimini ishonchli loyihalash va yaratish texnologiyasi tizim infrastrukturasida va foydalanishni cheklash qismtizimida mantiqiy xatoliklarni bartaraf etishga yo'naltirilgan. Bunda struktura-funksional yondashish asosiy hisoblanadi va keng tarqalgan.

Foydalanuvchilarning (subyektlarning) va axborot tizimi obyektlarining (ma'lumotlar bazasining) katta sonida foydalanishni cheklash sxemasi juda murakkab va chigal bo'lishi mumkin. Bu esa ma'murlash uchun qiyinchiliklar tug'ilishiga sabab bo'ladi va mantiqiy xatoliklarga asos tug'diradi. Ushbu tahdidni bartaraf etish uchun struktura-funksional yondashish doirasida ishchi guruh texnikasi ishlatiladi.

Ishchi guruh ma'lumotlar bazasiga qandaydir umumiy daxldorlikga (o'xshash amallarni bajaruvchi) va umumiy ma'lumotlarga nisbatan konfidensiallikning yaqin parametrlariga ega foydalanuvchilarni birlashtiradi.

Tizim ma'muri ishchi guruhlarini ma'lum identifikatsiyali va vakolatlar naboriga ega kollektiv foydalanuvchilar sifatida tuzishi mumkin. Har bir foydalanuvchi qandaydir ishchi guruhning a'zosi bo'lishi shart. Ishchi guruhga belgilangan vakolatlar avtomatik tarzda barcha foydalanuvchilarga – guruh a'zolariga tarqatiladi. Bu foydalanishni cheklashning zonal-funksional prinsipining ba'zi elementlarining ifodasi hisoblanadi. Qo'shimcha ravishda har bir foydalanuvchining shaxsiy hisob yozuvida vakolatlari aniqlanishi mumkin.

Aksariyat hollarda bunday yondashish tizimdan foydalanuvchi subyektlar sonini jiddiy kamaytirishga, foydalanishni cheklash sxemasini oddiyroq, "shaffof" va boshqariluvchan bo'lishiga imkon beradi. Natijada muayyan foydalanuvchining muayyan obyektdan foydalanishga noto'g'ri ruxsat berish, vakolatlarini oshirish, ortiq-

cha huquqlarini taqdim etish va h. kabi xatoliklar ehtimolligi kamayadi.

Ishchi guruh texnologiyalarida ma'lumotlar bazasidagi jarayonlar foydalanuvchi belgisi va ishchi guruh belgisi bilan ta'minlanadi va mos holda MBBT xavfsizligi yadrosi ikkala belgining haqiqiyligini tekshiradi.

Ishchi guruh texnologiyalari asosida foydalanish tizimini loyihalash "yuqoridan" (deduktiv) va "pastdan" (induktiv) amalga oshirilishi mumkin.

Deduktiv usulga binoan avval foydalanuvchilarning (subyektlarning) funksional strukturasini va tashkiliy ierarxiyasini tahlillash asosida ishchi guruhlar shakllantiriladi va foydalanishning guruhli vazifalari belgilanadi. So'ngra har bir foydalanuvchi tizimda ro'yxatga olinganida, uning vazifalariga muvofiq bir yoki bir necha guruh tarkibiga kiritiladi. Oxirida har bir foydalanuvchi uchun uning funksional vakolat ehtiyojlari xarakteristikalarining xususiyatlari tahlil etiladi va zaruriyat tug'ilganida foydalanishning alohida qo'shimcha vazifasi amalga oshiriladi. Bunda guruhlarni shakllantirish, foydalanishni guruhli va alohida o'rnatish tizim ma'muri tomonidan amalga oshiriladi. Bu foydalanishni boshqarishning majburiy usuliga mos keladi.

Bunday yondashish foydalanishning xatolik bilan taqdim etilish ehimolligini pasaytirishga imkon beradi va foydalanish tizimining qat'iy markazlashgan boshqarilishini ta'minlaydi. Ammo, o'z navbatida, bunday yondashish subyektlarning obyektlardan foydalanishning guruhli va alohida vakolatlarining takrorlanishiga (takrorlanish muammosi) hamda subyektning bitta obyektning o'zidan turli guruhlarda qatnashish orqali foydalanishning ortiqchaligiga (guruhlarning kesishishi muammosi yoki, umumiy ma'noda, guruhlarni optimallash muammosi) sabab bo'lishi mumkin.

Induktiv usulida ishchi guruhlarni loyihalash dastlab subyektlarning (foydalanuvchilarning) obyektlardan foydalanishning alohida vazifalarining taqdimi amalga oshiriladi. Vazifalarni taqdim etish foydalanuvchilarning funksional ehtiyojlarini va vakolat xarakteristikalarini so'rov va tahlillash asosida bajariladi va tizim ma'muri tomonidan (foydalanishini boshqarishning majburiy usuli) yoki obyekt egalarini foydalanish subyektlari tomonidan alohida so'roq-

lash (foydalanishni boshqarishning ixtiyoriy prinsipi) orqali amalga oshirilishi mumkin. So'ngra tizim ma'muri tomonidan turli subyektlardan foydalanishning umumiy yoki o'xshash dasturlari tahlil etilib, uning asosida subyektlar ishchi guruhlarga birlashtiriladi. Ajratilgan foydalanishning umumiy dasturlari foydalanish vazifalarining guruhli taqdimoti sifatida ishlatiladi. Subyektlar va obyektlarning katta sonida foydalanishning o'xshashligini tahlil etish oson masala emas. Ushbu masalani tizim ma'muri ko'pincha evristik hal etadi.

Tizimni ma'murlash va kuzatish jarayonida ishonchlilikni va xavsizlikni oshirishning qo'shimcha tashkiliy usuli umumiy ma'murlashni va xavfsizlikni ma'murlashni bir-biridan ajratish hisoblanadi. Umumiy ma'mur tizimning axborot infrastrukturasini quradi, madadlaydi va boshqaradi. Axborot infrastrukturasi tarkibiga axborot-mantiqiy sxema, obyektlar (resurslar va qurilmalar) konfidensialligini kategoriyalash, interfeys va dialog elementlari, shakllar, so'rovlar kutubxonasi, lug'at-tasnif baza, ma'lumotlarni rezervlash va arxivlash kiradi. Xavfsizlik ma'muri foydalanishni cheklash tizimini tashkil etadi va boshqaradi. Ushbu tizim tarkibiga foydalanuvchilarning vakolat xarakteristikalari (dopusklar), foydalanishning muayyan vazifalari, foydalanuvchilarning foydalanish belgilarini shakllantirish va qaydlash kiradi.

Foydalanuvchilarning hisob yozuvi massividan faqat xavfsizlik ma'muri foydalana oladi. Bitta shaxs tomonidan bir vaqtning o'zida asosiy ma'murlash va xavfsizlikni ma'murlash vazifalarini bajarilishiga yo'l qo'yilmaydi. Bu esa tizim ishonchliligini oshiradi.

Xavfsizlik hodisalarining bayonnomasini tuzish va auditi xavfsizlik holati va jarayonlarining boshqariluvchanligini ta'minlashda muhim vosita hisoblanib, axborot xavfsizligini buzish omillarini tekshirish, sabablarini tahlillash va bartaraf etish, ular yetkazadigan salbiy oqibatlarni va zararlarni pasaytirish uchun sharoitlar yaratadi.

Tizimda xavfsizlik nuqtayi nazaridan barcha jiddiy hodisalar hujjatlanishi shart:

- foydalanuvchilarning kirishi/chiqishi;
- yangi foydalanuvchilarni ro'yxatga olish, foydalanish imtiyozlarini va vazifalarini (hisob yozuvlari massiviga barcha murojaatlarni) almashtirish;

- fayllar ustidagi barcha amallar (yaratish, yo'qotish, nomini o'zgartirish, nusxalash, ochish, bekitish);

- masofadagi tizimga murojaat, masofadagi tizimdan murojaat.

Bunda har bir bunday hodisaga quyidagi qaydlanuvchi minimal kerakli parametrlar ro'yxati o'rnatiladi:

- hodisa kuni va vaqti;
- foydalanuvchi - boshlab beruvchi identifikatori;
- hodisa turi;
- so'rov manbai (taqsimlangan tizim uchun terminalning, ishchi stansiyaning tarmoqdagi nomi va h.);
- tilga olingan obyektlar nomi;
- tizimdagi hisoblarga kiritilgan o'zgartirishlar, xususan, hisob yozuvi massivlariga kiritilgan o'zgartirishlar;
- subyektlarning va obyektlarning foydalanish belgilari.

Bunday yondashish MBBTda jurnallashtirish texnologiyasidan foydalanuvchi hodisa – muolaja texnologiyasiga mos keladi. Bunda hodisalar jurnalidan faqat xavfsizlik ma'muri foydalanadi va u xavfsizlikning buzilishi faktlari yoki alomatlari aniqlanganida hodisalar jarayonini tiklash, tizim xavfsizligining buzilishi sabablarini va manbalarini tahlillash va bartaraf etish imkoniyatiga ega.

Shu nuqtayi nazaridan, xavfsizlikning hodisalar jurnali xavfsizlik auditining kerakli vositasi hisoblanadi. Xavfsizlik auditining maqsadi xavfsizlik muammolari yoki buzilishlarini o'z vaqtida aniqlash va xavfsizlik ma'muriga xabar berish uchun tizimdagi hodisalarni nazoratlash va kuzatishdan iborat. Kompyuter tizimlaridan foydalanish, turli muolajalar, amallar, axborot oqimlari jarayonlari ko'p jihatli, qat'iy determinatsiyalanmagan, ya'ni qisman yoki to'la stoxastik bo'lganligi sababli, axborot xavfsizligining buzilishi faktlarini va alomatlarini aniqlashning avtomatlashtirilgan muolajalarini ishlab chiqish juda murakkab va noaniq masala hisoblanadi. Shu sababli, hozirda qator evristik va neyrotarmoq texnologiyalari ishlab chiqilmoqda. Ular ba'zi hollarda muvaffaqqiyatli ravishda xavfsizlik ma'murining dasturiy vositasida ishlatilib, tizim xavfsizligining avtomatlashtirilgan auditini ta'minlamoqda.

Oddiy holda o'zgarishlarni jurnallashtirish deganda ma'lumotlar bazasidagi barcha o'zgarishlarni ketma-ket tashqi xotiraga yozish tushuniladi. Quyidagi axborot yoziladi:

- o'zgarishlarning tartib raqamlari, turi va vaqti;
- tranzaksiya identifikatori;
- o'zgarishga chalingan obyekt (saqlanuvchi fayl tartib raqami va undagi ma'lumotlar blokining tartib raqami, blok ichidagi qator tartib raqami);
- obyektning oldingi va yangi holati.

Shu tariqa shakllangan axborot ma'lumotlar bazasining o'zgarish jurnali deb ataladi. Jurnal tarkibida tranzaksiyaning boshlanishi va nihoyasining belgilari va nazorat nuqtasining olinish belgisi bo'ladi.

Ajratilgan yozuvli MBBT da tashqi xotira ma'lumotlari bloki ushbu blok ustida bajarilgan oxirgi o'zgartirishning tartib raqami belgisi bilan ta'minlanadi. Tizim adashganda ushbu belgi ma'lumotlar blokining qaysi versiyasi tashqi xotiraga kirishga ulgirganligini bilishga imkon beradi.

Ajratilgan yozuvli MBBT vaqti-vaqti bilan nazorat nuqtalarini bajaradi. Ushbu jarayon bajarilishi vaqtida barcha yozilmagan ma'lumotlar tashqi xotiraga o'tkaziladi, jurnalga esa nazorat nuqtasining olinishi xususida belgi yoziladi. Undan keyin jurnaldagi nazorat nuqtasigacha yozilgan yozuvlar yo'qotilishi mumkin.

O'zgarishlar jurnali bevosita tashqi xotiraga yozilmasligi, ammo asosiy xotirada to'planishi mumkin. Tranzaksiyaning tasdig'i holida MBBT jurnalning qolgan qismini tashqi xotiraga yozilishini kutadi. Shu tariqa tasdiq signalidan keyin kiritilgan barcha ma'lumotlarning, diskli keshdan barcha o'zgargan bloklarni ko'chirilishini kutmasdan turib, tashqi xotiraga o'tkazilishi kafolatlanadi. MBBT jurnalning qolgan qismini nazorat nuqtasini ishlashida ham kutadi.

Bitta tranzaksiyaning mantiqiy rad etilishi yoki ortga qaytish signali holida jurnal teskari tarafga skanerlanadi va bekor qilingan tranzaksiyaning barcha yozuvlari, jurnaldan tranzaksiya boshlanishi belgisigacha chiqariladi. Chiqarilgan axborotga mos holda tranzaksiya harakatini bekor qiluvchi harakat bajariladi, jurnalga esa kompensatsiyalovchi yozuv yoziladi. Ushbu jarayon "Ortga qaytish" (rollback) deb ataladi.

Fizik rad etilganida, na jurnal, na ma'lumotlar bazasi shikastlanmagan bo'lsa, progonka (boshdan-oyoq ko'rikdan o'tkazish -

rollforward) jarayoni bajariladi. Jurnal oldingi nazorat nuqtasidan boshlab to'g'ri yo'nalishga skanerlanadi. Barcha yozuvlar jurnaldan oxirigacha chiqariladi. Jurnaldan chiqarilgan axborot tashqi xotiraning ma'lumotlar blokiga kiritiladi. Agar progonka jarayonida yana yanglishish paydo bo'lsa, jurnalni skanerlash yana boshidan boshlanadi, ammo tiklash uzilish nuqtasidan davom ettiriladi.

MBBTning barqarorligini oshirish uchun o'zgarish jurnalining bir necha bir xil nusxasini bir vaqtda yozish mumkin. Jurnal nusxalarining biridan foydalanish mumkin bo'lmasa, MBBT foydalanish mumkin bo'lgan nusxalarining ixtiyoriy biridan foydalanib, ma'lumotlarni tiklaydi. Bunday strategiya o'zgarish jurnalini multiplekslash deb ataladi.

Nazorat savollari

1. Ma'lumotlar bazasi xavfsizligini ta'minlashda qanday dasturiy-texnologik masalalar yechiladi?
2. Identifikatsiya/autentifikatsiyaning himoyalangan tizimdagi o'rni.
3. Identifikatsiya/autentifikatsiyaning qanday vositalarini bilasiz?
4. Ma'lumotlar bazasini boshqarish tizimlarida asosan autentifikatsiyaning qanday turi ishlatiladi?
5. Parolli autentifikatsiya tizimining asosiy kamchiliklari.
6. Ma'lumotlar bazasini boshqarish tizimining asosiy va qo'shimcha vazifalari nimadan iborat?
7. Ilk MBBTlarda foydalanuvchilarning ma'lumotlar bazasi tili orqali o'zaro aloqasini tushuntiring.
8. SQL-yo'riqnomalari strukturasini tushuntiring.
9. "Tasavvur etish" deganda nima tushuniladi?
10. Obyektlardan takroran foydalanish xavfsizligini ta'minlash texnologiyalari.
11. Ishonchli loyihalash va ma'murlash texnologiyalari.
12. Jurnallashtirish texnologiyasini tushuntiring.
13. O'zgarish jurnallariga qanday axborot yoziladi?
14. O'zgarish jurnalini multiplekslash nima?

2-bob. MA'LUMOTLAR BAZASIDAN FOYDALANISHNI CHEKLASH MODELLARI VA USULLARI

2.1. Ma'lumotlar bazasi xavfsizligi modellari

Axborot xavfsizligining asosiy yo'nalishlaridan biri, foydalanishni cheklash modellari deb ham ataluvchi, axborot xavfsizligining formal modelini yaratish hisoblanadi. Axborot xavfsizligining modeli deganda xavfsizlik siyosatining formal tavsifi tushuniladi. 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.

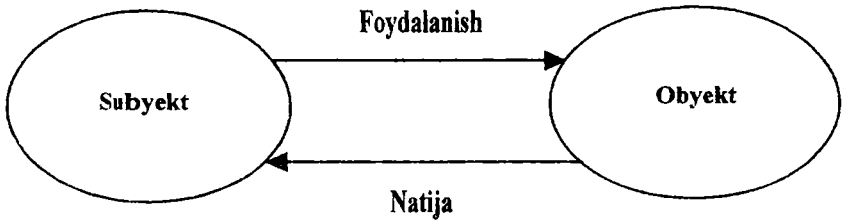
Xavfsizlik modellari himoyalangan kompyuter tizimlarini yaratish va tadqiqlash jarayonlarida muhim rolni o'ynaydi, chunki ular quyidagi o'ta muhim masalalarni yechishni qamrab oluvchi sistemotexnik yondashishni ta'minlaydi:

- axborotni himoyalash vositalari va usullarini amalga oshirish mexanizmlarini belgilovchi himoyalangan kompyuter tizimlari arxitekturasining bazaviy prinsiplarini tanlash va asoslash;
- xavfsizlik siyosatiga (talablar, shartlar, mezonlar) rioya qilinishning rasmiy isboti yo'li bilan ishlab chiqariluvchi tizim xususiyatlarini (himoyalanganligini) tasdiqlash;
- ishlab chiqariluvchi himoyalangan kompyuter tizimining muhim tarkibiy qismi hisoblanuvchi xavfsizlik siyosatining formal tafsilotli ro'yxatini tuzish.

Mohiyatan, xavfsizlik modellari " Buyurtmachi (Iste'molchi) – Ishlab chiqaruvchi (Mutaxassis) – Ekspert (Auditor)" uchlikdagi dastlabki bog'lovchi element hisoblanadi. Buyurtmachilar xavfsizlik modellari asosida o'zlarining tashkilotlari va korxonalarida qabul qilingan xavfsizlik siyosatiga, axborotni ishlashning texnologik jarayonlariga mos keluvchi himoyalangan kompyuter tizimlariga talablarni ifodalashlari mumkin. Ishlab chiqaruvchilar xavfsizlik

modellari asosida ishlab chiqariluvchi tizimlar bo'yicha texnik-texnologik talablarni va dasturiy-texnik yechimlarni shakllantiradilar. Ekspertlar xavfsizlik modellariga asoslanib, muayyan tizimlar himoyalanganligini baholash usulini va tafsilotli ro'yxatini yaratadilar, axborotni himoyalash talablari bo'yicha ishlab chiqarilgan tizimni sertifikatsiyalashni amalga oshiradilar.

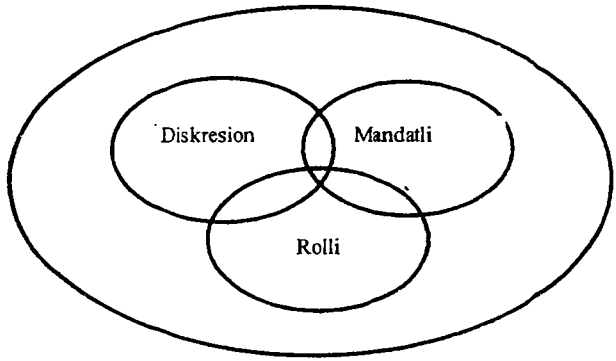
Foydalanishni boshqarish modeli deganda subyektning obyektdan foydalanish tartibini belgilovchi struktura tushuniladi (2.1-rasm).



2.1-rasm. Foydalanishni boshqarish modelining strukturasi.

Ushbu modelning qoidalarini va maqsadlarini amalga oshirishda foydalanishni boshqarish texnologiyalaridan va xavfsizlik mexanizmlaridan foydalaniladi. Ko'pgina xavfsizlik modellarining ichidan asosiylarini ajratish mumkin: diskresion modellar, mandatli modellar va foydalanishni cheklashning rolli modellari. Har bir model subyektlarning obyektlardan foydalanishni boshqarishda turli usullardan foydalanadi. Har biri o'zining afzalliklariga va kamchiliklariga ega.

Ta'kidlash lozimki, ushbu modellardan alohida-alohida foydalanish shart emas, balki tizim xavfsizligiga qo'yiladigan turli talablarni qondirish uchun ular kombinatsiyalanishi mumkin (2.2-rasm).



2.2-rasm. Foydalanishni nazorat tizimi sxemasi.

Nazorat savollari

1. Xavfsizlik siyosati va xavfsizlik modeli tushunchalariga izoh bering.
2. Xavfsizlik modellarining himoyalangan kompyuter tizimlarining yaratilishidagi va tadqiqidagi o'rni.
3. Foydalanishni boshqarish modelining strukturasi.
4. Foydalanishni nazorat tizimi sxemasini tushuntiring.

2.2. Diskretsion model asosida ma'lumotlar bazasidan foydalanishni cheklashni tashkil etish

Xavfsizlikning diskretsion modeli – foydalanishni diskretsion boshqarishga (Discretionary Access Control) asoslangan model. Foydalanishni diskretsion cheklash – nomlangan subyektlar va nomlangan obyektlar orasida foydalanishni cheklash. Foydalanishni diskretsion cheklash quyidagi qoidalarni hisobga olgan holda amalga oshiriladi:

– har bir foydalanuvchi ma'lumotlardan foydalanishidan oldin autentifikatsiyalanishi shart;

– autentifikatsiyalovchi axborotga (identifikator va parol) muvofiq foydalanuvchiga uning vakolatlari tizimi belgilanadi. Foydalanuvchi vakolatiga muvofiq, faqat ma'lumotlarning va ularni

ishlovchi muolajalarning belgilangan naboridan foydalanishi mumkin. Bunda foydalanuvchining hech qanday so'rovi u erishib bo'lmaydigan ma'lumotlarning ishlov jarayoniga jalb qilinishiga yo'l qo'ymasligi shart. Foydalanuvchini autentifikatsiyalovchi axborot va uning ma'lumotlar segmenti hamda ularni ishlash funksiyalaridan foydalanish vakolatlari majmui foydalanish darajasini belgilovchi foydalanish markerini hosil qiladi.

Vakolatlarni belgilash va tekshirishda subyekt-obyekt munosabatlarini xavfsizlik matritsasi ko'rinishida ifodalash qulay hisoblanadi (2.3-rasm). Xavfsizlik matritsasida qatorlar bo'yicha barcha foydalanuvchilar, ustunlar bo'yicha esa ma'lumotlarning barcha fragmentlari yozib qo'yiladi. Qator va ustunlar kesishgan joylarga ma'lumotlar ustidagi joiz amallar yoziladi.

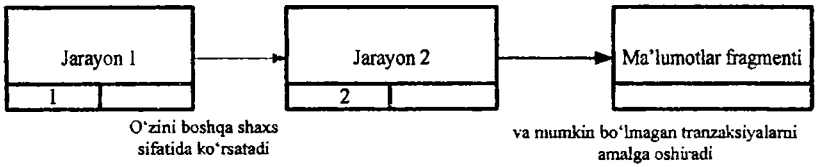
Foydalanuvchi	1-jadval				..	M-jadval			
	1-hoshiya	2-hoshiya	...	N-hoshiya	..	1-hoshiya	2-hoshiya	..	N-hoshiya
User 1	RWCD	RWCD		RW		RW	RWD		R
User 2	RWC	RWCD		RWC		R	RW		RWCD
...									
User X	R	RWD		RWCD		RWD	R		RWC

2.3-rasm. Xavfsizlik matritsasi misoli.

Xavfsizlik matritsasiga asoslangan vakolatlarni tekshirish tizim himoyalanganligini kafolatlamaydi, chunki ma'lumotlarni so'rovchi foydalanuvchining (jarayonning) haqiqiyligini tekshiruvchi vositalarni taqdim etmaydi. Bu esa ruxsatsiz foydalanishga olib kelishi mumkin (2.4-rasm).

Xavfsizlik matritsasi

Jarayon	Ma'lumotlar fragmenti
Jarayon 1	NONE
Jarayon 2	RWCD



2.4-rasm. Ma'lumotlardan ruxsatsiz foydalanish misoli.

Shu sababli himoyalangan MBBT foydalanuvchi yoki jarayon taqdim etgan identifikatorlarning tasdig'ini amalga oshiruvchi, foydalanishni cheklash qismtizimida haqiqiylikni tekshirishni ko'zda tutishi lozim.

Ammo foydalanishni cheklash qismtizimida markerlarning ishlatilishi konfidensiallik darajasi turli bo'lgan ma'lumotlardan foydalanishni cheklashni tashkil etishga imkon bermaydi. Haqiqatan, agar foydalanuvchi konfidensiallik darajasi turli bo'lgan axborotni ma'lumotlarning L qismiga ruxsatli murojaat etsa, ushbu foydalanuvchi L qismdagi barcha ma'lumotlar bilan ishlash imkoniyatiga ega bo'ladi.

Foydalanishni diskretsion cheklashning afzalligi sifatida himoyaning yaxshi detalizatsiyalanishini va nisbatan oddiy amalga oshirilishini ko'rsatish mumkin. Ammo ushbu foydalanishni cheklash turi kamchiliklardan holi emas. Faqat nomlangan obyektlardan foydalanish cheklanib, saqlanuvchi ma'lumotlarni o'zidan foydalanish cheklanmaydi. Masalan, relyasion MBBTni qo'llash holida obyekt jadval hisoblanadi. Bunda jadvalda saqlanuvchi axborotning faqat qismidan to'la hajmda foydalanishni cheklash mumkin emas. Undan tashqari troyan dasturlari (troyan otlari) muammosi mavjud.

Foydalanuvchi kompyuterda qandaydir dasturni chaqirganida, tizimda ko'pincha foydalanuvchidan yashirin amallar ketma-ketligi

boshlanadi. Ushbu amallar odatda operatsion tizim tomonidan boshqariladi.

Foydalanishni cheklashning diskretsion vositalarining qo'llanilishi axborotni uzatishni nazoratlash masalasini yechishga imkon bermaydi. Bunga sabab, ushbu vositalar avtorizatsiyalangan foydalanuvchiga qonuniy tarzda konfidensial axborotni olib, undan boshqa avtorizatsiyalanmagan foydalanuvchilarning foydalana olishlariga imkon tug'dirishga to'sqinlik qila olmaydi. Chunki, vakolatlar ma'lumotlardan (relyatsion MBBT holida relyatsion jadvallar qatoridan) alohida mavjud. Natijada ma'lumotlar "egasiz" bo'lib qoladi va ularni jadvallardan foydalanib, hatto MBBT vositalari yordamida xohlagan shaxsga uzatishga hech narsa to'sqinlik qilmaydi.

Xavfsizlik modellarining dastlabkilaridan biri foydalanishni diskretsion modeli *ADEPT-50* hisoblanadi. Modelda xavfsizlikka tegishli obyektlarning to'rtta xili ko'rsatilgan: foydalanuvchilar (u), topshiriqlar (j), terminallar (t) va fayllar (f). Shu bilan birga har bir obyekt to'rt o'lchamli kortej orqali tavsiflanadi.

Nazorat savollari

1. Foydalanishni diskretsion boshqarish.
2. Foydalanishni diskretsion boshqarishdagi xavfsizlik matritsasini tushuntiring.
3. Foydalanishni diskretsion cheklashning afzalliklari.
4. Foydalanishni diskretsion cheklashning kamchiliklari.

2.3. Mandatli model asosida ma'lumotlar bazasidan foydalanishni cheklashni tashkil etish

Mandatli modellar subyektlar va obyektlar xavfsizligi atributlari to'plamida aniqlangan foydalanishni taqdim etish qoidalari majmuidan iborat foydalanishni mandatli cheklashga (Mandatory Access Control) asoslangan.

Foydalanishni mandatli cheklash – obyektlardagi axborot konfidensialligi bilan xarakterlanuvchi belgiga va konfidensiallikning bunday darajali axborotga subyektlarning murojaatiga rasmiy rux-

satga (dopuskga) asoslangan subyektlarning ma'lumotlar obyektlaridan foydalanishni cheklash.

Foydalanishni diskretsion cheklashdan farqli holda, mandatli foydalanish axborotni bir foydalanuvchidan boshqasiga uzatishga cheklashlar qo'yadi. Bu troyan otlari muammosini yechishga imkon beradi. Mandatli modellarga Bell-LaPadula, MMS modellarini misol tariqasida ko'rsatish mumkin. Ma'lumki, mandatli modellarda, xususan, Bell-LaPadulaning klassik modelida, tasniflovchi to'plam sifatida konfidensiallik darajalarining chiziqli panjarasidan foydalaniladi. Foydalanish subyektlarining konfidensiallik darajasi panjarasidagi aksi darajalangan ishonch paradigmasini ifodalasa, foydalanish obyektlarining aksi esa konfidensiallikning rutbali o'lchovi (maxfiylik griflari) paradigmasini, ya'ni mos axborotning nazoratsiz tarqalishi natijasidagi zarar darajasini ifodalaydi.

Konfidensiallik belgilari asosan ma'lumotlarni xarakterlaydi: ularning mansubligini, muhimligini, e'tiborligini, konfidetsiallik darajasini, obyekt ma'lumotlarining (jadvallar, ustunlar, qatorlar yoki hoshiyalar) qiymatini va h. Konfidensiallik belgilari himoya obyektining mavjudligi mobaynida o'zgarmaydi (ular faqat himoya obyekti bilan birgalikda yo'q qilinadi) va himoyalanuvchi ma'lumotlar bilan birgalikda joylashtiriladi.

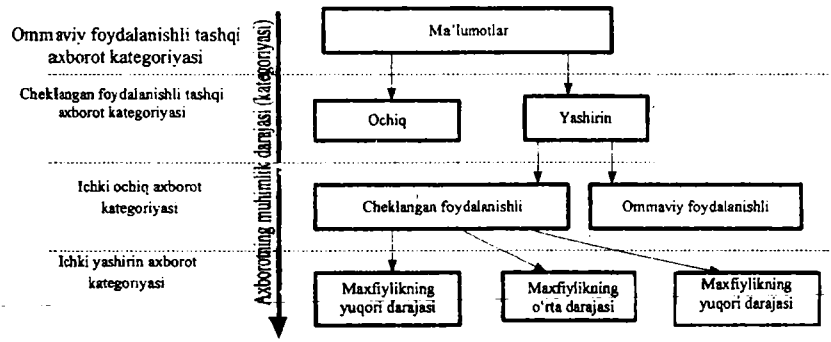
MBBTning foydalanishni cheklash qismtizimida bunday xil cheklashni amalga oshirish axborotdan foydalanishga ruxsat olishda konfidensiallik belgilarini e'tiborsiz qoldirmaydi. Foydalanishni cheklash qismtizimining bunday amalga oshirilishi, odatda, server mashinasida va mijoz mashinasida vositalar kompleksidan iborat bo'ladi. Bunda operatsion tizimning maxsus himoyalangan versiyasidan foydalanish mumkin.

Saqlanuvchi muolajalarning murakkab naborini qo'llash orqali foydalanishni mandatli cheklashning qandaydir modifikatsiyasini amalga oshirish ham mumkin. Bunda jadvalga belgilar qo'shimcha atribut sifatida qo'shilib, jadvallardan foydalanish umuman man etiladi va birorta ham ilova saqlanuvchi muolajadan tashqari interaktiv SQL-so'rovni bajara olmaydi. Bu holda foydalanish yetarlicha murakkab va xavfsizlik ma'muriga ishonchning ma'lum darajasini ko'zda tutadi, chunki xavfsizlik ma'muri ma'lumotlar bazasi strukturasini va demak, saqlanuvchi muolajalarni o'zgartirish

huquqiga ega va konfidensial (maxfiy) ma'lumotlarni boshqarishdan chetlanmagan.

Ishonchlilik darajasi turli foydalanuvchilarning multikonfidensial ma'lumotlar fragmentlaridan foydalanishlarini cheklashni foydalanishni cheklashning ko'p sathli siyosatini tuzish orqali amalga oshirish imkoniyati aniqlangan. Bunda boshqarish va foydalanishni nazoratlash ma'lumotlar bazasida saqlanuvchi axborotning konfidensiallik darajasiga muvofiq amalga oshiriladi. Foydalanishni cheklashning ko'p sathli siyosati Bell-LaPadula modeli asosida tuziladi. Ushbu model ma'lumotlardan foydalanishni so'rovchi subyektlarni, aktiv jarayonlarni va obyektlarni, ya'ni fayllarni, jadvallarni, yozuvlarni, hoshiyalarni boshqarishga mo'ljallangan. Bell-LaPadula bo'yicha modellashning mohiyati obyektlarni konfidensiallik darajasi bo'yicha, subyektlarni esa ishonchlilik darajasi bo'yicha tasniflashdan iborat. So'ngra konfidensiallik sinfiga nisbatan foydalanish sathi vakolatlarining naborini tavsiflovchi qoida shakllantiriladi.

Bell-LaPadula modeli asosidagi ma'lumotlar bazasini himoyalash mexanizmi axborot kategoriyalarini ma'lumotlar konfidensialligi sinflarining "teskari vorisligi" asosida quriladi. Teskari vorislikning ma'nosi quyidagicha (2.5-rasm).

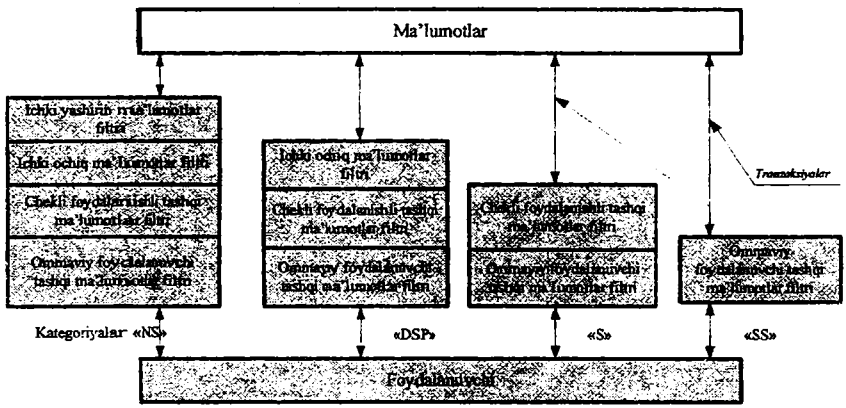


2.5-rasm. Ma'lumotlar konfidensialligi sinflarining ierarxiyasi.

Ma'lumotlar konfidensialligi sinflarning qandaydir ierarxiyasi beriladi. Undan tashqari, muhimlik alomati bo'yicha kategoriyalar

to‘plamini ifodalovchi sinflar doirasida ma’lumotlar guruhlari majmui shakllantiriladi. Axborot muhimligi darajasi oshishi bilan mos axborot kategoriyasi meros qilinadi. Boshqacha aytganda, axborotning mos kategoriyasidan foydalanishga ruxsat oigan foydalanuvchi muhimligi kamroq ma’lumotlami o‘qish huquqiga ega bo‘ladi.

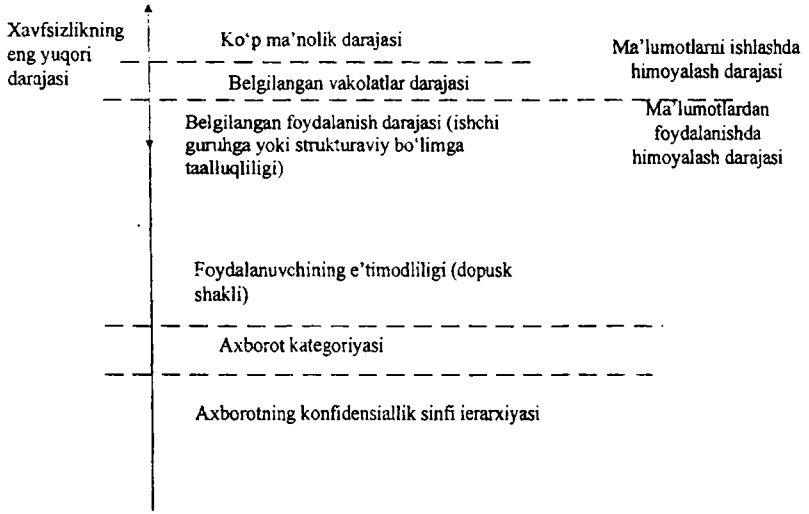
Mos kategoriya ma’lumotlaridan foydalanish foydalanuvchining dopuski darajasiga muvofiq tanlanuvchi foydalanish filtri yordamida ta’minlanadi. Foydalanishni mandatli cheklashli foydalanishni cheklash qismtizimining modeli 2.6-rasmda keltirilgan.



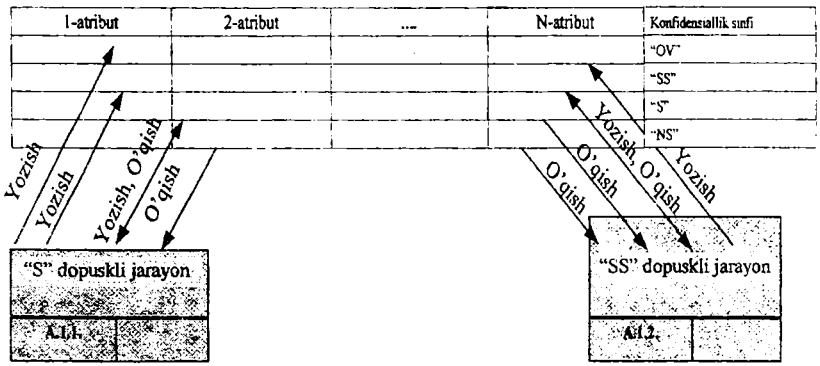
2.6-rasm. Foydalanishni mandatli cheklashli foydalanishni cheklash qismtizimining modeli.

Ma’lumotlar xavfsizligi modelining yuqoriroq sathlarida foydalanuvchining axborotni ishlashi bo‘yicha vakolatlari tizimi aniqlanadi (2.7-rasm).

Agar subyekt sinfi o‘zidagidek yoki yoziluvchi obyektdan past bo‘lgan holdagina subyektga obyektga yozish huquqiga ega bo‘lishi imkoniyatini beruvchi himoya tizimining xususiyati σ-xususiyat (sigma-xususiyat) deb yuritiladi. σ-xususiyatning amalga oshirilishi misoli 2.8-rasmda keltirilgan.



2.7-rasm. Foydalanishni mandatli cheklashda obyekt va subyektlarning tasnifiy alomatlari.



2.8-rasm. Bell-LaPadula qoidalarini qo'llash misoli.

Jadvaldagi ma'lumotlar konfidensiallik darajasi kamayishi tartibida saralangan. "S" dopuskli jarayon ma'lumotlarni faqat mos yoki konfidensiallikning yuqoriroq sinfli kortejlarga yozishi

mumkin, o'qish esa faqat mos yoki konfidensiallikning pastroq sinfli kortejlardan amalga oshirilishi mumkin.

Bell-LaPadula prinsipining amalga oshirilishi bitta jadvalning o'zi uchun himoyaning bir necha sathlarini madadlash talabi bilan bog'liq. Bu esa MBBTning barqarorligini, ishonchliligini va boshqariluvchanligini bir muncha pasayishiga olib keladi.

Yanada murakkab tasniflovchi to'plamlarni kiritish yo'li bilan mandatli modellarni kuchaytirish bo'yicha ishlar ham ma'lum. Bu to'plamlar, xususan, MLS-panjaralar deb ataluvchi tematik klassifikator-rubrikatorlardan (deskriptorli, ierarxik, fasetli) foydalanishga asoslangan tematik jihatni nazarda tutadi. Ammo MLS-panjarali modellar dastlabki mandatli modellarning mohiyatini o'zgartirmaydi. Xususan, aksariyat hollarda foydalanish subyektlari va obyektlarining tasnifini aniqlash va o'zgartirish jarayonlarini qat'iy belgilamaydi. Keng ma'noda esa foydalanish subyektlarini aniqlash jarayonlarini hamda ko'p uchraydigan foydalanishlarni (bitta subyekt - bir vaqtning o'zida bir nechta obyektlardan, bir nechta subyekt bir vaqtning o'zida bitta obyektdan) qat'iy belgilamaydi. Undan tashqari, mandatli modellar MBBTdagi obyektlar tizimi strukturasini hisobga olmaydi va ularga konfidensiallikka (maxfiylikka) nisbatan chiziqli tartibda qamrab olingan obyektlar to'plami sifatida qaraydi. MBBTda mandatli modellarni qo'llash natijasida ma'lumotlarni tashkil etishning va ulardan foydalanishni cheklashning yagona mexanizmi ta'minlanmaydi.

Nazorat savollari

1. Foydalanishni mandatli cheklash mohiyatini tushuntiring.
2. Ma'lumotlar konfidensialligi sinflarining ierarxiyasi.
3. Foydalanishni mandatli cheklashda obyekt va subyektlarning tasnifiy alomatlari.
4. Ma'lumotlar bazasini boshqarish tizimida Bell-LaPadula qoidasini qo'llash misolini tushuntiring.

2.4. Rolli model asosida ma'lumotlar bazasidan foydalanishni cheklashni tashkil etish

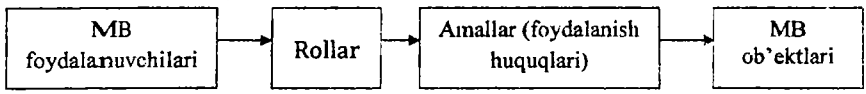
Foydalanishni cheklashning rolli modeli (Role – Based Access Control) foydalanishni cheklashning diskresion siyosatining rivoji hisoblanadi. Tizim subyektlarining obyektlardan foydalanish qoidalari ularning o'ziga xos xususiyatlarini hisobga olgan holda guruhlanadi, ya'ni rollar hosil qilinadi. Bunda ushbu model qoidalari qat'iy aniqlangan axborot qiymati panjarasi asosida qurilgan mandatli model qoidalariga nisbatan moslashuvchanroq hisoblanadi. Rolli modelda "subyekt" tushunchasi "foydalanuvchi" va "rol" tushunchalari bilan almashtiriladi. Foydalanuvchi - tizim bilan ishlovchi va ma'lum xizmat vazifalarini bajaruvchi inson. Rol – tizimda harakatlanuvchi abstrakt tushuncha bo'lib, u bilan ma'lum faoliyatni amalga oshirish uchun zarur bo'lgan vakolatlarning cheklangan, mantiqiy bog'langan nabori bog'liq. Rolli siyosatdan foydalanib foydalanishni boshqarish ikki bosqichda amalga oshiriladi. Birinchi bosqichda har bir rol uchun obyektlardan foydalanish huquqlar naborini ifodalovchi vakolatlar nabori belgilanadi. Ikkinchi bosqichda har bir foydalanuvchiga uning qo'lidan keladigan rollar ro'yxati belgilanadi.

Foydalanishni rolli cheklashli foydalanishni cheklash qism tizimida foydalanuvchilar axborotdan foydalanish huquqini boshqa foydalanuvchilarga uzata olmaydilar. Bu foydalanishni rolli cheklashning foydalanishni diskresion va mandatli cheklashlardan asosiy farqi hisoblanadi.

Foydalanishni rolli cheklashda rol vakolatlarini taqsimlash (diskresion foydalanishdan farqli holda) xavfsizlik ma'muriga bog'liq bo'lmay, tashkilotda va muayyan MBBTda qabul qilingan xavfsizlik siyosatiga bog'liq bo'ladi. Rol deganda foydalanuvchi yoki foydalanuvchilar guruhi tashkilot miqyosida bajaradigan harakatlar to'plami tushunilishi mumkin. Rol tushunchasi vazifalar, mas'uliyatlar va malakalar tavsifini o'z ichiga oladi. Vazifalar rollar bo'yicha MBBT xavfsizlik ma'muri tomonidan taqsimlanadi. Foydalanuvchining roldan foydalanishi ham ushbu ma'mur tomonidan aniqlanadi.

Foydalanishni cheklashning rolli xili foydalanishni abstraktsiya va tashkilotda ishlatiluvchi subyektlar va obyektlarning tavsifi sathida nazoratlashni ko'zda tutadi. Agar foydalanishni cheklash qismtizimi foydalanishni rolli cheklash asosida qurilgan bo'lsa, rollarni qo'shish va yo'q qilish murakkab bo'lmagan jarayonga aylanadi. Shunday qilib, foydalanishni rolli cheklash xavfsizlik ma'muriga diskresion foydalanishda ishlatiluvchi an'anaviy foydalanishni nazoratlash ro'yxatiga nisbatan yuqoriroq sathli abstraktsiyalar bilan ish ko'rishiga imkon beradi.

Foydalanishni rolli cheklash asosidagi xavfsizlik siyosatlari foydalanuvchilar, rollar, amallar va himoyalanuvchi obyektlar atamalarida tavsiflanadi (2.9-rasm).



2.9-rasm. Foydalanishni rolli cheklashda ma'lumotlar bazasida saqlanuvchi axborotdan foydalanuvchilarni foydalanish mexanizmi.

Foydalanishni rolli cheklashli himoyalanuvchi obyekt ustida biror-bir amalni bajarish uchun foydalanuvchi qandaydir rolni bajarishi lozim. Foydalanuvchi ushbu rolni bajarishdan oldin MBBT xavfsizligi ma'muri tomonidan ushbu rol uchun avtorizatsiyalangan bo'lishi shart. Shunday qilib, foydalanishni rolli cheklash ma'murga roldagi avtorizatsiyaga, rolni faollashtirishga, amallarni bajarishga cheklashlarni o'rnatish qobiliyatini bag'ishlaydi.

Rollarning taqdim etilishi, kompyuter tizimlaridan foydalanuvchilar uchun foydalanishni cheklashning aniqroq va tushunarli qoidalarini aniqlashga imkon beradi. Bunda foydalanishni rolli cheklash foydalanuvchilarning vakolatlari va majburiyatlari doirasi aniq belgilangan kompyuter tizimlarida samarali ishlatiladi.

Rol deganda kompyuter tizimi obyektlaridan foydalanish huquqlari majmui tushuniladi. Ammo foydalanishni rolli cheklash foydalanishni diskresion cheklashning xususiy holi hisoblanmaydi, chunki foydalanishni rolli cheklash qoidalari kompyuter tizimi subyektlariga foydalanish huquqlarini taqdim etish tartibini vaqtning

har bir onida, uning ishlash sessiyasi va undagi mavjud yoki mavjud bo'lmagan rollarga bog'liq holda belgilaydi. Bu esa foydalanishni mandatli cheklash tizimiga xos. Shu bilan birga foydalanishni rolli cheklash qoidalari foydalanishni mandatli cheklash qoidalariga nisbatan moslanuvchan hisoblanadi. Ma'lumki, foydalanishni mandatli cheklash qoidalari qat'iy belgilangan axborot muhimligi panjarasi (shkalasi) asosida tuziladi.

Foydalanishni rolli cheklashning bazaviy modelining asosiy elementlari quyidagilar:

U – foydalanuvchilar to'plami;

R – rollar to'plami;

P – kompyuter tizimi obyektlaridan foydalanish xuquqlari to'plami;

S – foydalanuvchilar sessiyalari to'plami;

PA: $R \rightarrow 2^r$ - har bir rol uchun foydalanish huquqlarini belgilovchi funksiya; bunda har bir $p \in P$ uchun shunday $r \in R$ mavjudki, $p \in PA(r)$;

UA: $U \rightarrow 2^R$ - har bir foydalanuvchi uchun, u avtorizatsiyalanishi mumkin bo'lgan rollar to'plamini belgilovchi funksiya;

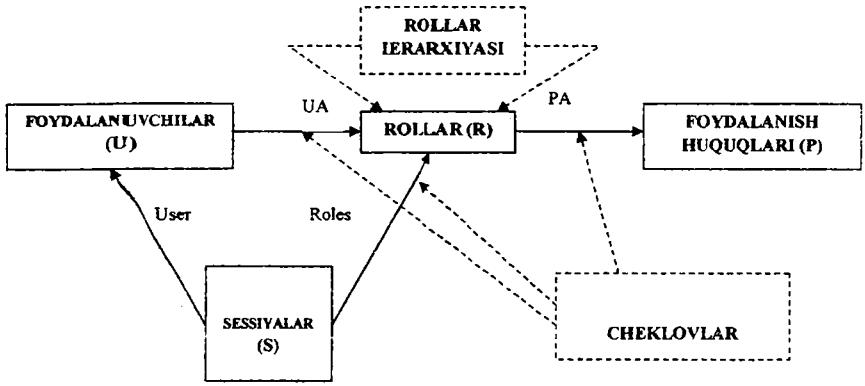
user: $S \rightarrow U$ – nomi orqali faollashgan har bir sessiya uchun foydalanuvchini belgilovchi funksiya;

roles: $S \rightarrow 2^R$ - muayyan sessiyada avtorizatsiyalangan foydalanuvchi uchun rollar to'plamini belgilovchi funksiya; bunda vaqtning har onida har bir $s \in S$ uchun $roles(S) \leq UA(user(S))$ sharti bajariladi.

Bir sessiya mobaynida foydalanuvchi avtorizatsiyalanadigan rollar to'plami foydalanuvchining o'zi tomonidan modifikatsiyalanadi. Foydalanishni rolli cheklashda bir sessiya tomonidan ikkinchi sessiyani faollashtirish mexanizmi mavjud emas. Barcha sessiyalar foydalanuvchi tomonidan faollashtiriladi. Foydalanuvchi avtorizatsiyalanishi mumkin bo'lgan yoki u bir sessiya mobaynida avtorizatsiyalanuvchi rollar to'plamiga qo'yiladigan cheklashlar foydalanishni rolli cheklash bazaviy modelining muhim mexanizmi hisoblanadi. Ushbu mexanizm foydalanishni rolli cheklashni keng qo'llashga ham zarur, chunki u kompyuter tizimlarida axborotni ishlash texnologiyalariga yuqori muvofiqlikni ta'minlaydi.

Foydalanishni rolli cheklashning bazaviy modelida U, R, P to'plamlari va PA, UA funksiyalari vaqt mobaynida o'zgarmaydi yoki ushbu to'plamlar va funksiyalarni o'zgartirishga imkon taqdim etuvchi yagona rol – "xavfsizlik ma'muri" mavjud deb faraz qilinadi. Yuzlab va minglab foydalanuvchilar bir vaqtda ishlovchi real kompyuter tizimlarida rollar strukturasi va foydalanish huquqlari juda murakkab bo'lishi mumkin, ya'ni ma'murlash muammolari o'ta muhim masala hisoblanadi. Ushbu masalani yechish uchun foydalanishni rolli cheklashning bazaviy modeli asosida qurilgan foydalanishni rolli cheklashni ma'murlash modeli ko'riladi.

Foydalanishni rolli cheklashning bazaviy modeli strukturasi 2.10-rasmda keltirilgan.



2.10-rasm. Foydalanishni rolli cheklashning bazaviy modeli strukturasi.

Foydalanishni rolli cheklashni ma'murlash modelida foydalanishni rolli cheklashning bazaviy modelida ishlatiluvchi elementlarga qo'shimcha quyidagi elementlar ko'riladi:

AR — ma'muriy rollar to'plami;

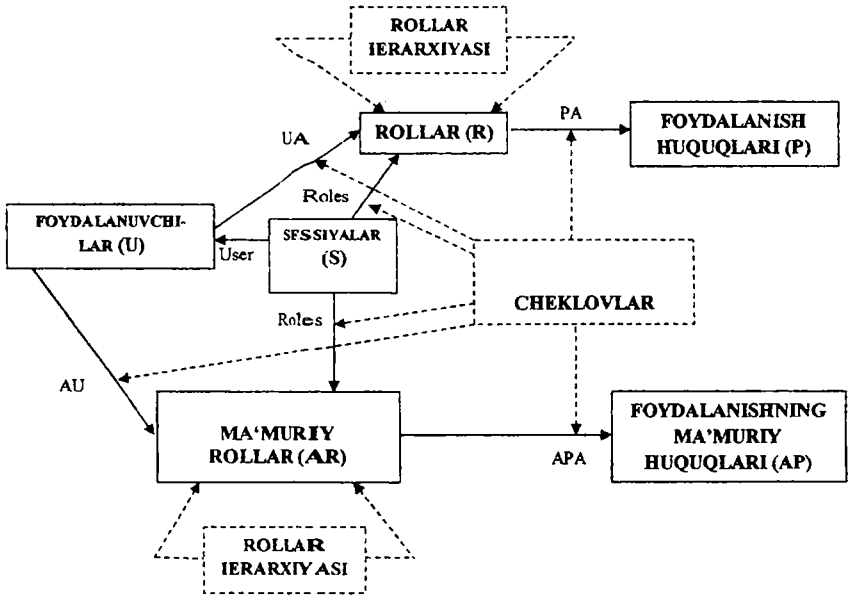
AP — foydalanishning ma'muriy huquqlari to'plami;

APA:AR $\rightarrow 2^{AP}$ - har bir ma'muriy rol uchun foydalanishning ma'muriy huquqlari to'plamini belgilovchi funksiya;

AUA:U $\rightarrow 2^{AR}$ – har bir foydalanuvchi uchun, u avtorizatsiyalanishi mumkin bo'lgan ma'muriy rollar to'plamini belgilovchi funksiya.

Foydalanishni rolli cheklashni ma'murlash modelining strukturasi 2.11- rasmda keltirilgan.

Foydalanuvchilarning avtorizatsiyalangan rollari to'plamini ma'murlashda AUA funksiya qiymatlari o'zgartiriladi. Bu o'zgartirishni amalga oshirish uchun AR to'plamidan maxsus ma'muriy rollar aniqlanadi.

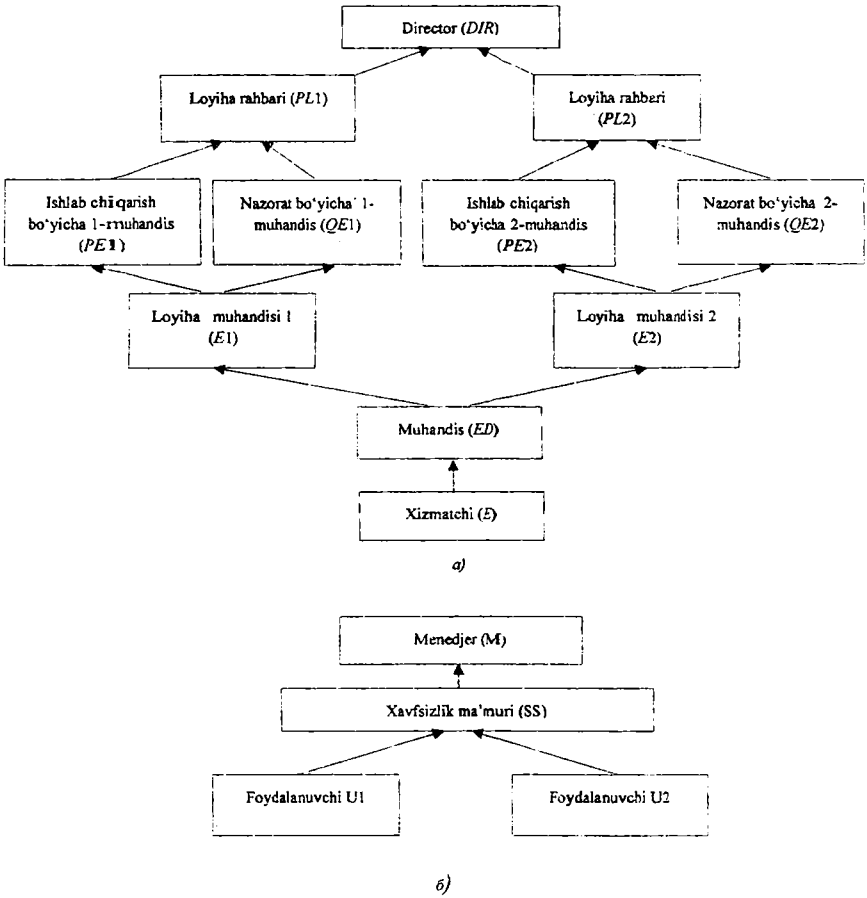


2.11-rasm. Foydalanishni rolli cheklashni ma'murlash modelining strukturasi.

Foydalanuvchilarning avtorizatsiyalangan rollari to'plamini ma'murlash uchun quyidagilarni aniqlash lozim:

- rollar to'plamining har bir ma'muriy roli uchun u o'zgartirishga imkon beruvchi avtorizatsiyalangan foydalanuvchilar to'plamini;
- har bir rol uchun foydalanuvchilar mos keladigan dastlabki shartni.

Ma'muriy rollar ierarxiyasining namunaviy strukturasi 2.12-rasm "a" va "b" da keltirilgan.



2.12-rasm. Ma'muriy rollar ierarxiyasining namunaviy strukturasi.

Ierarxiyadagi eng kichik rol – xizmatchi (E), loyihalarni ishlab chiqarish rollari ierarxiyasidagi eng katta rol – direktor (DIR), eng kichik rol – muhandis (ED). Boshqarishda ikkita loyiha bo'yicha ishlar bajariladi. Har bir loyihada eng katta rol – loyiha rahbari

(PL1, PL2), eng kichik rol – loyiha muhandisi (E1, E2) va o'zaro taqqoslab bo'lmaydigan rollar – ishlab chiqarish bo'yicha muhandis (RE1, RE2) va nazoratlash bo'yicha muhandis (QE1, QE2) aniqlangan. Ma'muriy rollar ierarxiyasi to'rtta roldan iborat bo'lib, eng katta rol – xavfsizlik ma'muri (SS).

Foydalanishni rolli cheklash modelida ko'riladigan rollar ierarxiyasini o'zgartirishga imkon beruvchi ma'murlash qoidalarini aniqlash eng murakkab masala hisoblanadi. Ushbu masalani yechish uchun foydalanuvchilarning avtorizatsiyalangan rollari to'plamini va rollardan foydalanish huquqlarini ma'murlash qoidalarini aniqlashda amalga oshirilgan yondashishlardan foydalaniladi.

Elementlari quyidagilardan iborat bo'lgan uchta ierarxiya beriladi:

- imkoniyatlar – foydalanish huquqlari va boshqa imkoniyatlar to'plami;
- guruhlar – foydalanuvchilar va boshqa guruhlar to'plami;
- birlashmalar – foydalanuvchilar, foydalanish huquqlari, guruhlar, imkoniyatlar to'plami va boshqa birlashmalar to'plami.

Birlashmalar ierarxiyasi umumiyroq hisoblanadi va imkoniyatlar va guruhlar ierarxiyasini qamrab olishi mumkin. Imkoniyatlarni va guruhlarni aniqlash modeldagi rollarni ma'murlash qoidalarining amalda qo'llaniluvchi axborotni ishlash texnologiyasiga mosligini ta`minlash va tashkilotning ma'muriy strukturasini yaratish uchun talab qilinadi. Masalan, foydalanuvchiga o'zining vazifasini bajarishi uchun foydalanish huquqlarining qandaydir nabori zarur bo'lishi mumkin. Buning ustiga, ushbu naborda foydalanishning qandaydir huquqining yo'qligi mavjud huquqlarga egalikning ma'nosiz qilib qo'yishi mumkin.

Imkoniyatlar, guruhlar va birlashmalar ierarxiyalari asosida elementlari – imkoniyatlar roli, guruhlar roli, birlashmalar roli hisoblanuvchi rollar ierarxiyasi belgilanadi.

Imkoniyatlar roli – faqat aniq va foydalanish huquqlari mos imkoniyatlarga ega rollar.

Guruhlar roli – mos guruh foydalanuvchilarining barchasi bir vaqtda avtorizatsiyalanishi mumkin bo'lgan rollar.

Birlashmalar roli - foydalanuvchilar guruhi va alohida foydalanuvchilar avtorizatsiyalanishi mumkin bo'lgan va foydalanish huquqlariga va imkoniyatlariga ega rollar.

Nazorat savollari

1. Foydalanishni rolli cheklash modeli mohiyatini tushuntiring.
2. Foydalanishni rolli cheklash modelining diskresion va mandatli modellardan farqi.
3. Foydlanishni rolli cheklash modelida axborotdan foydalanish mexanizmini tushuntiring.
4. Foydalanishni rolli cheklashning bazaviy modeli strukturasi.
5. Foydalanishni rolli cheklashni ma'murlash modelining strukturasi.
6. Ma'muriy rollar ierarxiyasini tushuntiring.

3-bob. MA'LUMOTLAR BAZASINING TAQSIMLANGAN TIZIMIDA AXBOROT XAVFSIZLIGI

3.1. Ma'lumotlar bazasining taqsimlangan tizimida axborot xavfsizligi konsepsiyasi

Ma'lumki, korporativ tarmoqlar asosida qurilgan yirik avtomatlashtirilgan axborot tizimlarida har doim ham tarmoqning bitta uzelida barcha ma'lumotlar bazasini va MBBTni markazlashgan joylashtirishni tashkil etib bo'lmaydi. Bu esa taqsimlangan ma'lumotlar bazasini bashqarish tizimi bilan uzviy bog'langan taqsimlangan hisoblash tizimlarining paydo bo'lishiga sabab bo'ldi.

Taqsimlangan ma'lumotlar bazasi – kompyuter tarmog'ida taqsimlangan, o'zaro mantiqiy bog'langan ma'lumotlar bazalari majmui.

Taqsimlangan ma'lumotlar bazasini boshqarish tizimi – taqsimlangan ma'lumotlar bazasini boshqarishni va foydalanuvchilar uchun uning taqsimlanganligining shaffofligini ta'minlovchi dasturiy tizim.

Taqsimlangan ma'lumotlar bazasi yagona global sxema doirasida har qanday modelni (ierarxik, tarmoq, relyatsion va obyektga mo'ljallangan ma'lumotlar bazasini) madadlovchi ma'lumotlar bazalarini birlashtirishi mumkin. Bunday konfigurasiya, barcha ilovalar uchun joylashgan yeri va formatidan qat'iy nazar, har qanday ma'lumotlardan shaffof foydalanishni ta'minlashi lozim.

Taqsimlangan ma'lumotlar bazasini yaratish va ishlashining asosiy prinsiplari quyidagilar:

- ma'lumotlar joylashishining foydalanuvchilar uchun shaffofligi (boshqacha aytganda, taqsimlangan mal'umotlar bazasi foydalanuvchi uchun taqsimlanmagandek ko'rinishi lozim);
- foydalanuvchilarning bir-biridan izolyatsiyalanganligi (foydalanuvchi ma'lumotlarni o'zgartirishi, yangilashi, yo'q qilishi onida boshqa foydalanuvchilar ishini "sezmasligi", "ko'rmasligi" lozim);

- vaqtning har qanday onida ma'lumotlar holatining sinxronlanganligi va uyg'unligi (zid emasligi).

Asosiy prinsiplardan quyidagi qo'shimcha prinsiplar kelib chiqadi:

- lokal avtonomiya (har bir hisoblash qurilmasi muvaffaqiyatli ishlashi uchun, har qanday boshqa qurilmaga bog'liq bo'lmasligi kerak);
- markaziy qurilmaning mavjud emasligi (oldingi bandning natijasi);
- joylashgan yeriga bog'liq emasligi (ma'lumotlar xuddi foydalanuvchining lokal qurilmasida joylashganidek);
- ishlashining uzluksizligi (tizimning rejali uzilishining mavjud emasligi);
- ma'lumotlarning fragmentlanishiga bog'liq emasligi (gorizontal fragmentlash - bitta jadval yozuvlarining turli guruhlari turli qurilmalarda yoki turli lokal bazalarda joylashtiriladi; vertikal fragmentlash — bitta jadvalning turli hoshiyalari – ustunlari turli qurilmalarda joylashtiriladi);
- ma'lumotlarning replikatsiyalanishiga (takrorlanishiga) bog'liq emasligi (ma'lumotlar bazasining qandaydir jadvali turli qurilmalarda joylashgan bir necha nusxalari orqali ifodalanishi mumkin);
- so'rovlarning taqsimlangan ishlanishi (so'rovlarning optimizatsiyalash taqsimlangan xarakterga ega bo'lishi lozim – avval global optimizatsiya, so'ngra ishga tushirilgan qurilmalarning har birida lokal optimizatsiya);
- tranzaksiyalarni taqsimlangan boshqarish (taqsimlangan tizimda alohida tranzaksiya turli qurilmalarda harakatlarning bajarilishini talab etishi mumkin, tranzaksiya barcha qatnashgan qurilmalarda tugallangan bo'lsa u tugallangan hisoblanadi);
- apparaturaga bog'liq emasligi (turli xil kompyuterlari bo'lgan qurilmalarda tizimning ishlashi mumkinligi maqbul hisoblanadi);
- operatsion tizim xiliga bog'liq emasligi (tizim turli hisoblash qurilmalardagi operatsion tizimlarning farqlanishiga bog'liq bo'lmagan holda ishlashi lozim);
- kommunikatsiya tarmog'iga bog'liq emasligi (turli kommunikatsiya muhitida ishlash imkoniyati);

- MBBTga bog'liq emasligi (turli qurilmalarda turli MBBT ishlashi mumkin, amalda SQLni madadlovchi MBBTlar ishlatiladi).

Odatda, MBBT asosida yaratiluvchi taqsimlangan axborot tizimlari ham "taqsimlangan MBBTlari" atamasi orqali xarakterlanadi va mos holda "taqsimlangan ma'lumotlar bazasi" atamasi ishlatiladi.

Taqsimlangan hisoblashlarni amalga oshirish yuqorida ko'rsatilgan taqsimlangan tizimlarni yaratish va ishlashi prinsiplarining ba'zilaridan chekinish orqali amalga oshiriladi. Qanday prinsip "qurbon" qilinishiga bog'liq holda taqsimlangan tizim texnologiyalarida bir necha mustaqil yo'nalishlar ajralib chiqdi – "mijoz - server" texnologiyalari, takrorlash texnologiyalari, obyektli bog'lash texnologiyalari.

Real taqsimlangan axborot tizimlari, odatda, uchchala texnologiyalarni biriktirish asosida qurilgan. Metodik nuqtayi nazaridan ularni alohida muhokama qilish maqsadga muvofiq hisoblanadi.

"Mijoz - server" texnologiyalarida taqsimlangan tizimlarni yaratish va ishlashi prinsiplarining asosiylaridan biri - markaziy qurilmaning mavjud emasligidan chekiniladi. Shu sababli, «mijoz – server» texnologiyalarining negizida yotuvchi quyidagi ikkita asosiy g'oyani ajratish mumkin:

- bitta yoki bir nechta serverlardagi ma'lumotlarning barcha foydalanuvchilar uchun umumiyligi;

- umumiy ma'lumotlarni birgalikda (parallel va bir vaqtda) turli hisoblash qurilmalarida ishlovchi foydalanuvchilarning (mijozlarning) ko'pligi.

Boshqacha aytganda, "mijoz - server" texnologiyalariga asoslangan tizimlar faqat foydalanuvchilarga nisbatan taqsimlangan. Shu sababli, ko'pincha ularni "haqiqiy" taqsimlangan tizimlarga tegishli emas, balki ko'pchilik foydalanuvchi tizimlarning alohida sinfi deb hisoblaydilar.

"Mijoz - server" texnologiyalarida server va mijoz tushunchalari muhim qiymatga ega. Keng ma'noda *server* deganda qandaydir hisoblash resurslariga (xotira, vaqt, prosessor unumdorligi va h.) ega har qanday tizim, jarayon, kompyuter tushuniladi.

Mijoz deganda serverdan qandaydir resursni so'rovchi, qandaydir resurslardan foydalanuvchi yoki server tomonidan o'zgacha

usul bilan xizmat ko'rsatiluvchi har qanday tizim, jarayon, kompyuter, foydalanuvchi tushuniladi.

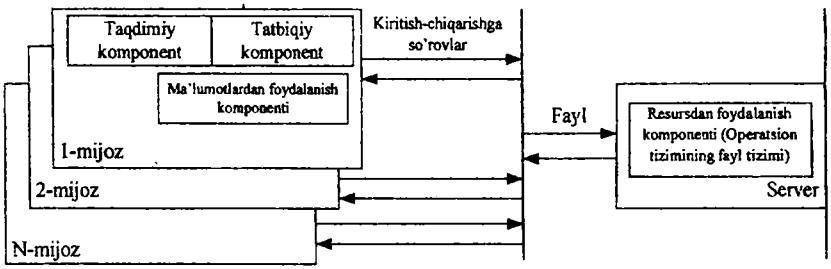
"Mijoz - server" tizimlari o'zining rivojida bir necha bosqichlarni bosib o'tish jarayonida uning turli modellari shakllandi. Ularni amalga oshirish, demak, to'g'ri tushunish MBBT strukturasini quyidagi uchta komponentga ajratishga asoslangan:

- taqdimiy komponent – ba'zida oddiygina foydalanuvchi interfeysi deb ataluvchi, ma'lumotlarni kiritish va aks ettirish funksiyasini amalga oshiruvchi;
- tatbiqiy komponent – muayyan predmet sohasidagi avtomatlashtirilgan axborot tizimi vazifalarini amalga oshiruvchi so'rovlar, hodisalar, qoidalar, muolajalar va boshqa hisoblash funksiyalari nabori;
- ma'lumotlardan foydalanish komponenti – ma'lumotlarni olish, saqlash, fizik yangilash va o'zgartirish funksiyalarini amalga oshiruvchi.

Ushbu uchta komponentning tizimda amalga oshirish va taqsimlash xususiyatlaridan kelib chiqqan holda "mijoz - server" texnologiyalarining to'rtta modeli farqlanadi:

- fayl serveri modeli (File Server - FS);
- ma'lumotlardan masofadan foydalanish modeli (Remote Data Access - RDA);
- ma'lumotlar bazasi serveri modeli (Data Base Server - DBS);
- ilovalar serveri modeli (Application Server - AS).

Fayl serveri modeli eng sodda bo'lib, qanchalik axborot tizimini yaratish usulini xarakterlasa, shunchalik lokal tarmog'idagi komponentlarning o'zaro aloqasining umumiy usulini xarakterlaydi. Tarmoq kompyuterlaridan biri ajratilib, fayl serveri, ya'ni har qancha ma'lumotlar saqlanuvchi umumiy joy deb belgilanadi. FS – modelining mohiyatini 3.1-rasm orqali tushuntirish mumkin.



3.1-rasm. Fayl serveri modeli.

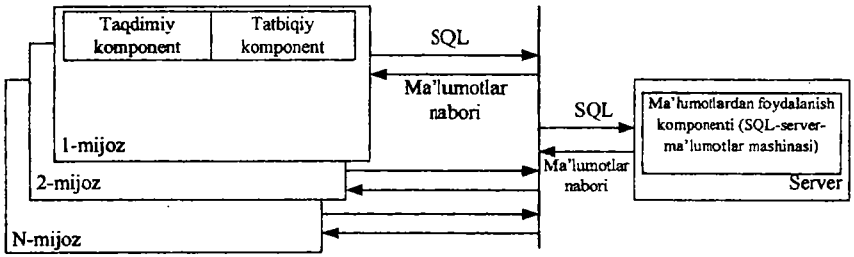
FS – modelida barcha asosiy komponentlar mijoz qurilmasida joylashtiriladi. Ma'lumotlarga murojaat qilinganida MBBT, o'z navbatida, fayl tizimiga ma'lumotlarni kiritish – chiqarishga so'rovlar bilan murojaat etadi. Seans vaqtida operatsion tizim funksiyalari yordamida mijoz qurilmasining asosiy xotirasiga ma'lumotlar bazasi fayli to'laligicha yoki qisman nusxalanadi. Bu holda server passiv funksiyani bajaradi.

Ushbu modelning afzalligi – uning soddaligi, server unumdorligiga yuqori talablarning mavjud emasligi (asosiysi, disk muhitining istalgan hajmi). Ta'kidlash lozimki, bu holda MBBTning dasturiy komponentlari taqsimlanmagan, ya'ni MBBTning hech qanday qismi serverga o'rnatilmaydi va joylashtirilmaydi.

Ushbu modelning kamchiligi – foydalanuvchilarning tizimdan ommaviy foydalanishida, masalan, ish kunining boshida avj qiymatiga erishuvchi yuqori tarmoq trafigi. Ammo, ma'lumotlarning umumiy bazasi bilan ishlash nuqtayi nazaridan, MBBT tomonidan ma'lumotlar bazasi fayli (fayllari) xavfsizligining maxsus mexanizmlarining mavjud emasligi jiddiyroq kamchilik hisoblanadi. Boshqacha aytganda, foydalanuvchilar orasida ma'lumotlarni taqsimlash (ma'lumotlarning bitta fayli bilan parallel ishlash) faqat operasion tizimning fayl tizimi vositalari yordamida amalga oshiriladi. Kamchiliklariga qaramay, fayl serveri modeli ko'pchilik foydalanuvchi rejimni madadlash yo'nalishida shaxsiy MBBTning imkoniyatlarini kengaytirishning tabiiy vositasi hisoblanadi, shu jabhada o'zining ahamiyatini saqlab qoladi.

Ma'lumotlardan masofadan foydalanish modeli relyatsion MBBTlar uchun tashqi xotirada ma'lumotlarni joylashtirishning va fizik manipulyatsiyalashning o'ziga xos xususiyatlarini hisobga olishga asoslangan. RDA – modelda MBBTda ma'lumotlardan foydalanish komponenti ikkita boshqa komponentlardan (taqdimiy va tatbiqiy komponentlardan) to'laligicha ajratilgan va tizim serverida joylashtiriladi.

Ma'lumotlardan foydalanish komponenti SQL – server deb ataluvchi MBBT dasturiy qismining mustaqil qismi sifatida amalga oshiriladi va tizim serverining hisoblash qurilmasida o'rnatiladi. Boshqacha aytganda, SQL – server ma'lumotlar mashinasi rolini o'ynaydi. 3.2-rasmda RDA – modeli sxemasi keltirilgan.



3.2-rasm. Ma'lumotlardan masofadan foydalanish modeli.

Tizim serverida joylanuvchi ma'lumotlar bazasi faylida (fayllarida) ma'lumotlar bazasining tizimli katalogi ham mavjud bo'lib, unda, jumladan, ro'yxatga olingan mijozlar, ularning vakolatlari va h. xususidagi ma'lumotlar ham joylashtiriladi.

Mijoz qurilmalarida interfeys va tatbiqiy funksiyalarni amalga oshiruvchi MBBTning dasturiy qismi o'rnatiladi. Foydalanuvchi tizimning mijoz qismiga kirib, u orqali tizim serverida ro'yxatdan o'tadi va ma'lumotlarni ishlashni boshlaydi.

Tizimning tatbiqiy komponenti (so'rovlar kutubxonasi, ma'lumotlarni ishlash muolajalari) to'laligicha mijoz qurilmasida joylashtiriladi va bajariladi. Tatbiqiy komponent o'z funksiyasini amalga oshirishda SQL – serverga yo'naltiriluvchi kerakli SQL – yo'riqnomalarni shakllantiradi. SQL – server turli mijozlardan SQL –

yo'riqnomalarni qabul qiladi va muvofiqlashtiradi, ularni bajaradi, ma'lumotlar yaxlitligiga cheklashlarning tekshirilishini va bajarilishini ta'minlaydi va mijozlarga SQL – yo'riqnomalarni ishlash natijalarini ma'lumotlar (jadvallar) nabori ko'rinishida yuboradi.

Shu tariqa, mijozning server bilan muloqoti SQL – yo'riqnomalar orqali o'tadi, serverdan mijoz qurilmalariga esa faqat ishlash natijalari, ya'ni hajmi bo'yicha ma'lumotlar bazasidan jiddiy kam bo'lgan ma'lumotlar nabori uzatiladi. Natijada tarmoq yuklanishi keskin kamayadi, server esa faol markaziy funksiya maqomiga ega bo'ladi. Undan tashqari SQL – server ko'rinishidagi MBBTi yadrosi bir necha foydalanuvchilarning birgalikda ishlashida ma'lumotlarning cheklangan yaxlitligini va xavfsizligini ta'minlash bo'yicha an'anaviy va muhim funksiyalarni ta'minlaydi.

RDA – modelning boshqa, ko'rinmaydigan afzalligi – axborot tizimlarining tatbiqiy komponentlarining o'zaro aloqa interfeysining umumiy ma'lumotlar bilan unifikatsiyalanganligi. Bunday o'zaro aloqa SQL tili doirasida maxsus protokol ODBC (Open Database Connectivity – ma'lumotlar bazasidan oshkora foydalanish) orqali standartlashtirilgan. Ushbu protokol ko'p protokollikni, ya'ni taqsimlangan tizimlardagi mijoz qurilmalarida MBBT xiliga bog'lik emaslikni ta'minlashda muhim o'rin tutadi.

MBBTining ko'p protokolligi – MBBTning dastlab turli xil MBBTiga mo'ljallangan tatbiqiy dasturlarga xizmat qilish qobiliyati. Boshqacha aytganda, serverdagi MBBT yadrosining maxsus komponenti (ODBC drayveri deb ataluvchi) so'rovlarni qabul qilish, ishlash va natijalarni boshqa, "begona" relyatsion MBBT boshqaruvida ishlovchi mijoz qurilmalariga jo'natish qobiliyatiga ega.

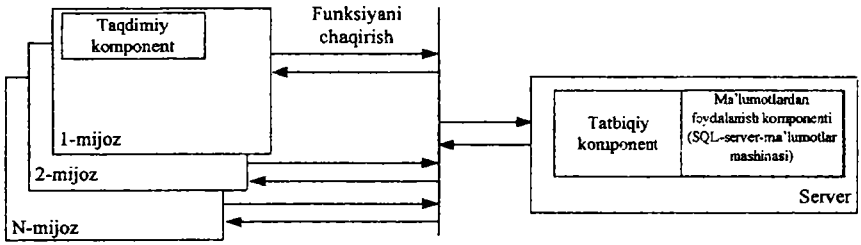
Bunday imkoniyat qandaydir tashkilotda mavjud lokal ma'lumotlar bazasi asosida shaxsiy yoki boshqa xil relyatsion MBBT boshqaruvida taqsimlangan axborot tizimini yaratishda moslashuvchanlikni jiddiy oshiradi.

Mijoz hisoblash qurilmalariga qo'yiladigan yuqori talablar RDA – modelining kamchiligi hisoblanadi, chunki axborot tizimi predmet sohasining o'ziga xos xususiyati orqali aniqlanuvchi ma'lumotlarni ishlashning tatbiqiy dasturlari ularda bajariladi.

Boshqa bir kamchiligi – tarmoq trafigining jiddiyligi, ya'ni ma'lumotlar bazasi serveridan ba'zi hollarda yetarlicha jiddiy

hajmni egallovchi ma'lumotlar (jadval) naborlari mijozlarga jo'natiladi.

Ma'lumotlar bazasi serveri modeli – RDA-modelining rivoji. Saqlanuvchi muolajalar mexanizmi uning o'zagi hisoblanadi. RDA – modelidan farqli o'laroq, axborot tizimining muayyan predmet sohasi uchun belgilangan, SQL tili vositalari orqali tavsiflangan hodisalar, qoidalar va muolajalar ma'lumotlar bilan birga tizim serverida saqlanadi va unda bajariladi. Boshqacha aytganda, tatbiqiy komponent to'laligicha tizim serverida joylanadi va bajariladi. Ma'lumotlar bazasi serveri modeli sxematik tarzda 3.3-rasmda keltirilgan.



3.3-rasm. Ma'lumotlar bazasi serveri modeli.

DBS – modelining mijoz qurilmalarida faqat interfeys komponenti (taqdimiy komponent) joylanadi. Bu esa mijozning hisoblash qurilmasiga talablarning jiddiy kamayishiga olib keladi. Foydalanuvchi mijoz qurilmasidagi tizim interfeysi orqali ma'lumotlar bazasiga ma'lumotlarni ishlash bo'yicha faqat kerakli muolajalar, so'rovlar va boshqa funksiyalar chaqiriqlarini jo'natadi. Ma'lumotlardan foydalanish va ularni ishlash bo'yicha barcha chiqimli amallar serverda bajariladi va mijozga faqat ishlash natijalari jo'natiladi (RDA modelida esa ma'lumotlar nabori jo'natiladi). Bu esa DBS – modelida tarmoq trafigining RDA – modeliga qaraganda jiddiy kamayishiga olib keladi.

Ta'kidlash lozimki, tizim serverida barcha tizim foydalanuvchilarining tatbiqiy masalalari bir vaqtda bajariladi. Natijada server hisoblash qurilmalariga (disk muhiti va asosiy xotira hajmiga,

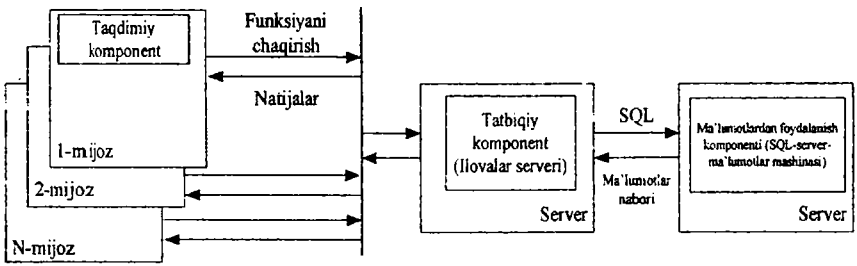
tezkorligiga) talablar keskin oshadi. Bu DBS – modelining asosiy kamchiligi hisoblanadi.

Tarmoq yukining kamayishidan tashqari, tarmoq serverining aktiv roli, unda hodisalar, qoidalar va muolajalar mexanizmini saqlash va bajarish, taqsimlangan axborot tizimini predmet sohasini barcha nyuanslariga adekvatroq va samarali "sozlash" imkoniyati DBS – modelining afzalligi hisoblanadi.

Undan tashqari, ma'lumotlar holati va o'zgarishining bir-biriga muvofiqligining ishonchli ta'minlanishi natijasida ma'lumotlarni saralash va ishlash imkoniyati oshadi, foydalanuvchilarning umumiy ma'lumotlar bilan kollektiv ishlashi o'zaro samarali muvofiqlashtiriladi.

Server hisoblash resurslari tezkorligi va xotirasiga nisbatan talablarni turli hisoblash qurilmalari bo'yicha tarqatish uchun *ilovalar serveri modeli* ishlatiladi.

AS-modelida axborot tizimining tatbiqiy komponenti tizim resurslarining yuqori tezkorligi bo'yicha ixtisoslashtirilgan qo'shimcha serverga o'tkaziladi. Ushbu modelning sxemasi 3.4-rasmda keltirilgan.



3.4-rasm. Ilovalar serveri modeli.

DBS – modeliga o'xshab, mijoz qurilmalarida tizimning faqat interfeys qismi, ya'ni taqdimiy komponenti joylashtiriladi. Ammo ma'lumotlarni ishlash funksiyalarining chaqiriqlari ilovalar serveriga jo'natiladi va unda ushbu funksiyalar tizimning barcha foydalanuvchilari uchun birgalikda bajariladi. Foydalanish va ma'lumotlarni o'zgartirish bo'yicha past darajali amallarni bajarish uchun

ilovalar serveri, RDA – modelidagidek, SQL – serverga murojaat etadi, unga SQL – muolajalari chaqiriqlarini jo'natadi va mos holda, undan ma'lumotlar naborini oladi.

Ma'lumki, alohida ma'noli qiymatga ega ma'lumotlar (SQL – yo'riqnomalari) ustida bajariladigan amallarning ketma-ket majmui tranzaksiya deb ataladi.

Bu nuqtayi nazaridan, ilovalar serveri SQL – server bajaradigan tranzaksiyalarni shakllantirishni boshqaradi. Shu sababli, ilovalar serverida o'rnatiluvchi MBBTning dasturiy komponenti tranzaksiyani ishlash monitori (Transaction Processing Monitors - TPM) yoki oddiygina tranzaksiya monitori deb ham yuritiladi.

AS – model, DBS – modelining kuchli tomonlarini saqlagan holda axborot tizimi hisoblash sxemasining optimal qurilishiga imkon beradi, ammo RDA – modelidek tarmoq trafigini oshiradi.

Amalda aralash modellar ishlatiladi. Oddiy tatbiqiy funksiyalar va ma'lumotlar yaxlitligini ta'minlash serverda saqlanuvchi muolajalar orqali madadlanadi (DBS – model), predmet sohasining murakkabroq funksiyalari esa mijoz qurilmalaridagi (RDA – model) yoki ilovalar serveridagi (AS – model) tatbiqiy dasturlar yordamida amalga oshiriladi.

Nazorat savollari

1. Taqsimlangan ma'lumotlar bazasini yaratish va ishlashining asosiy prinsiplari.
2. "Mijoz-server" texnologiyasi modellarini sanab o'ting.
3. Fayl serveri modelini tushuntiring.
4. Ma'lumotlardan masofadan foydalanish modelini tushuntiring.
5. Ma'lumotlar bazasi serveri modelini tushuntiring.
6. Ilovalar serveri modelini tushuntiring.

3.2. Markazlashtirilgan ko'pchilik foydalanuvchi axborot tizimlarida ma'lumotlar bazasi xavfsizligi

Taqsimlangan ma'lumotlar bazasi yaxlitligini ta'minlashda qator muammolar mavjud:

- bir necha foydalanuvchilarning bitta axborotdan bir vaqtda foydalanish imkoniyati (ayniqsa, ma'lumotlar bazasiga murojaatlar, tuzatishlar kiritish bilan bog'liq bo'lsa);

- ma'lumotlar bazasining alohida qismlarining turli kompyuterlar bo'yicha fizik tarqoqligi;

- axborot manbalarining har xilligi.

Birinchi muammo har qanday taqsimlangan ma'lumotlar bazasiga taalluqli bo'lsa, ikkinchi muammo – agar ma'lumotlar bazasi taqsimlangan bo'lsa, uchinchi muammo – agar tizim geterogen bo'lsa, sodir bo'ladi.

Muammolarning birinchi guruhi, asosan, turli foydalanuvchilarning bir vaqtda tuzatishlar kiritishi natijasida ma'lumotlarning buzilishi xavfi bilan bog'liq.

Ko'pchilik foydalanish rejimida tuzatish kiritishli murojaatlarni bajarishda ma'lumotlar yaxlitligini ta'minlashning quyidagi sxemalarini ko'rsatish mumkin:

- boshqa foydalanuvchi axborotga tuzatish kiritayotganida axborotga tuzatish kiritishni taqiqlash (blokirovka);

- axborot birligining turli nusxalariga tuzatish kiritish, so'ngra ro'y bergan kolliziyalarni bartaraf etish.

Agar MBBT ko'pchilik foydalanuvchi murojaatlarda yaxlitlikni ta'minlash usulini tanlash imkoniyatini taqdim etsa, ushbu tanlash natijasiga ko'p omillar ta'sir etadi, jumladan:

- tuzatish murojaatlarini bajarishda raqobat darajasi – axborot birligiga bir vaqtda tuzatish kiritish vaziyati qanchalik tez-tez sodir bo'ladi;

- tizim reaksiyasi vaqtiga cheklashlar;

- vaqtning har bir onida ma'lumotlarning dolzarbligiga va zid emasligiga talablar;

- texnik vositalar xarakteristikasi.

Taqsimlangan tizimlarda yaxlitlikni ta'minlash muammolarining ikkinchi guruhiga ma'lumotlarni taqsimlanishi va natija sifatida ularni ishlash muolajalarining taqsimlanishi sabab bo'ladi, ya'ni ushbu muammolar aynan ma'lumotlarni tizimning turli uzellariga tarqatish bilan bog'liq.

Ma'lumki, taqsimlangan axborot tizimlarida yaxlitlikni ta'minlashda ikkita yondashish mavjud – qat'iy yaxlitlik (tight

consistency) va qat'iy bo'lmagan yaxlitlik (loose consistency). Qat'iy yaxlitlik vaqtning har qanday onida ma'lumotlar yaxlitligini kafolatlaydi. Bunda ikki fazali qaydlash protokolidan (2RS) foydalaniladi. Qat'iy yaxlitlash kommunikatsiyaning yuqori sifatini talab qiladi, chunki barcha uzellar doimo foydalanuvchan bo'lishi lozim. Ikkinchi yondashishga binoan bazaga o'zgartirishlar kiritish va ularning iste'molchi uzellarida akslantirish orasida vaqtiy kechikish joiz hisoblanadi.

Tranzaksiyani ikki fazali qaydlash – tranzaksiyani ikkita bosqich yordamida bajarish jarayonida ma'lumotlar bazasining ketmaket o'tishidan iborat. Birinchi bosqichda (birinchi fazada) – tranzaksiya nomidan murojaat qilingan ma'lumotlar bazasining barcha obyektlari sinxronlangan tarzda egallanadi. Ma'lumotlar obyekti barcha serverlarda egallanadi. Ikkinchi bosqichda (ikkinchi fazada) barcha serverlarda barcha o'zgarishlar sodir bo'ladi, yoki garchand bitta xato holida, birinchi bosqich bajarilishigacha ma'lumotlar bazasi bo'lgan holatga qaytiladi.

Tranzaksiyaning ikki fazali qaydlash mexanizmining quyidagi kamchiliklari mavjud:

- barcha serverlardagi barcha kerakli ma'lumotlarning egallanishi ma'lumotlardan foydalanishni uzoq muddatga blokirovka qilinishiga sabab bo'lishi mumkin;
- qandaydir, garchand yagona xato hisobiga yangilashdan voz kechish ehtimolligi katta;
- agar qandaydir serverdan foydalanishning yoki global tarmoqqa chiqishning iloji bo'lmasa, tranzaksiyani yo'qotish sodir bo'ladi;
- tarmoq strukturasida muvofiqlashtiruvchi uzelning ishlatilishi qo'shimcha xatar bilan bog'liq, chunki uning ishdan chiqishi, tranzaksiya ta'siridagi ma'lumotlaming blokirovka qilinishiga olib keladi;
- tranzaksiyani ishlash murakkabligi. Ushbu protokol qo'llanilganda, protokolning o'zi qo'shimcha trafik manbai hisoblanadi. Bu esa tizim reaktsiyasi vaqtini oshiradi.

Undan tashqari tarmoqning yetarli bo'lmagan o'tkazish qobiliyati va ma'lumotlarni uzatishning kichik tezligi reaksiya vaqtining nojoiz darajaga kattalashishiga olib kelishi mumkin.

Turli MBBT yaxlitlikni ta'minlashning turli texnologiyalarini madadlaydi.

Ma'lumotlarni himoyalash usullari. Ko'pchilik foydalanuvchi rejimda ishlashda ma'lumotlarni ruxsatsiz foydalanishdan himoyalash alohida dolzarblikni kasb etadi. Ma'lumotlar bazasidan foydalanishni boshqarishning turli usullari mavjud. Ushbu usullar xavfsizlikning turli darajasini ta'minlaydi. Ularning ba'zilari har qanday axborot tizimiga, boshqalari esa muayyan MBBTga taalluqli.

Ma'lumotlar bazasini shifrlash. Ma'lumotlar bazasini shifrlash himoyalashning eng oddiy usuli hisoblanib, unda ma'lumotlar bazasi faylining ko'rinishi o'zgaradi va uni standart xizmatchi dasturlar yoki matn redaktori yordamida o'qib bo'lmaydi. Shifrlash odatda, ma'lumotlar bazasini elektron uzatishda yoki tashqi eltuvchida saqlashda ishlatiladi.

Ma'lumotlar bazasini deshifrlash. Ushbu amal shifrlashga teskari amal.

Obyektlarni bekitish. Ma'lumotlar bazasini begona foydalanuvchilardan himoyalash usullaridan biri-uni bekitish. Unga binoan butun ma'lumotlar bazasi operatsion tizim vositalari yordamida kataloglarni kuzatishda bekitiladi yoki ma'lumotlar bazasining alohida obyektlari muayyan MBBTi vositalarining ma'lumotlar bazasi bilan ishlashida bekitiladi. Ushbu usul yetarlicha ishonchli emas, chunki bekitilgan obyektlarni nisbatan oson akslantirish mumkin.

Ishga tushirish parametrlaridan foydalanish. Ushbu parametrlar ma'lumotlar bazasi ochilganida avtomatik tarzda ochiluvchi start usulini berishga imkon yaratadi. Usul aniqlanganida MBBT taqdim etgan ma'lumotlar bazasi darchasini bekitish mumkin va xususiy tugmacha usulini o'rnatish mumkin. Bunda foydalanuvchi ma'lumotlar bazasi ustida faqat ushbu ilova taqdim etgan interfeys joiz hisoblovchi harakatlarni bajarishi mumkin.

Parollardan foydalanish. Himoyalanishning oddiygina usuli – ma'lumotlar bazasini ochish uchun parollarni o'rnatish. Parol o'rnatilganidan so'ng ma'lumotlar bazasining har bir ochilishida dialog darchasi paydo bo'ladi va unga parolni kiritish talab qilinadi. Faqat haqiqiy parol kiritgan foydalanuvchi ma'lumotlar bazasini ochishi mumkin.

Umuman, ma'lumotlar bazasidan foydalanuvchilarning barchasi uchun yagona parol belgilanishi mumkin. Ammo ma'lumotlar bazasini himoyalashning moslanuvchan va keng tarqalgan usuli foydalanuvchi sathida himoyalash bo'lib, unda har bir foydalanuvchiga parol beriladi. MBBT ishga tushirilishida foydalanuvchi identifikatsiyalanishi lozim. Tizim foydalanuvchi identifikatori va parolining bir-biriga mosligini tekshiradi.

Har bir foydalanuvchi uchun nafaqat noyob kod, balki foydalanish darajasi va foydalanuvchi foydalana oladigan obyektlar belgilanishi mumkin.

Aksariyat MBBT yagona foydalanuvchilardan tashqari ularning guruhini yaratishi mumkin.

Ma'lumotlar bazasining takrorlanishini taqiqlash. Yuqorida aytilganidek, takrorlash (replikatsiya) foydalanuvchilarga ma'lumotlarning umumiy bazasining nusxasini yaratishga imkon beradi. Takrorlangan ma'lumotlar keyinchalik noqonuniy tarqatish uchun ishlatilishi mumkin. Shu sababli, ba'zi hollarda ma'lumotlar bazasini takrorlashni taqiqlashga to'g'ri keladi.

Foydalanuvchilar tomonidan parollarni o'rnatishni va ishga tushirish parametrlarini sozlashni taqiqlash. Ma'lumotlardan ko'pchilik foydalanishda nafaqat ma'lumotlarning buzilmaganligini va konfidensialligini ta'minlash, balki ma'lumotlardan tegishli foydalanuvchilarning foydalanish imkoniyati muhim hisoblanadi. Shu sababli MBBT har qanday foydalanuvchining ma'lumotlar bazasida parol o'rnatishiga to'sqinlik qiluvchi mexanizmga ega bo'lishi lozim.

Undan tashqari ishga tushirish parametrlariga o'zgartirish kiritishni taqiqlovchi mexanizmning mavjudligi maqsadga muvofiq hisoblanadi, chunki ushbu parametrlar sozlanuvchi menyu, instrumentlarning sozlanuvchi panellari va start usullari kabi xususiyatlarni belgilaydi.

Foydalanuvchilarni yaratish va yo'q qilish. Ko'pchilik foydalanuvchi muhitda ma'lumotlar bazasidan foydalanuvchi – ma'lumotlar bazasi obyektlarining ma'lum nabori egasi tushunchasi katta ahamiyat kasb etadi.

Tizim foydalanuvchilarini ikkita sinfga ajratish mumkin. Har qanday o'lchamli tizimda doimo superfoydalanuvchilarning ba'zi

turlari – avtomatik tarzda ko'pchilik (yoki barcha) imtiyozlarga ega va o'zining superfoydalanuvchi maqomini kimgadir imtiyozlar yoki imtiyozlar guruhi yordamida uzata oladigan foydalanuvchilar mavjud. *Ma'lumotlar bazasi ma'muri* atamasi bunday superfoydalanuvchilar va ularning imtiyozlari uchun tez-tez ishlatiluvchi atama hisoblanadi.

Boshqa foydalanuvchilarni ma'lumotlar bazasining ma'murlari yaratadi va ularga boshlang'ich imtiyozlarni beradi. Foydalanuvchilarni faqat ma'murlar yaratadi. Foydalanuvchilarga huquqlarni berish va qaytarib olish nafaqat ma'murlar, balki mos huquqlarga ega boshqa foydalanuvchilar tomonidan bajarilishi mumkin.

Foydalanuvchilar guruhlarga birlashishlari mumkin. Foydalanuvchilar guruhi - imtiyozlarning bir xil naboriga ega foydalanuvchilar. Umuman, bir foydalanuvchi turli guruhlarda ishtirok etishi mumkin. Har bir foydalanuvchi maxsus identifikatsiya nomiga yoki nomeriga ega (Authorization ID).

Aksariyat ekspluatatsiyadagi korporativ MBBTlari SQL – serverlari hisoblanadi. Shu sababli SQL – tizimlar misolida foydalanuvchilarni boshqarish masalalarini ko'raylik.

Foydalanuvchilarni boshqarish jarayonining muayyan shakllari turli MBBTlarda bir-biridan ancha farqlanishi mumkin. Foydalanuvchilarni boshqarish jarayoni ishlatiluvchi operatsion tizimga, ma'lumotlar bazasi arxitekturasiga bog'liq. Shu sababli SQL ning mos qismida ishlab chiqaruvchi platformasiga ham ko'proq bog'liqlik ko'zga tashlanadi.

Foydalanuvchilarni boshqarish jarayonini uchta asosiy bosqichga ajratish mumkin. Avval ma'lumotlar bazasida foydalanuvchini hisobga olish yozuvini yaratish lozim. So'ngra foydalanuvchiga u ma'lumot bazasi doirasida, taxminan yechuvchi masalalarga muvofiq imtiyozlar beriladi. Nihoyat, foydalanuvchiga ma'lumotlar bazasidan foydalanish kerak bo'lmaganida uni hisobga olish yozuvi yo'qotilishi yoki oldin unga berilgan imtiyozlar bekor qilinishi lozim.

Ma'lumotlar bazasi bilan ishlashdan oldin foydalanuvchi, uning ismi va parolini so'rashdan iborat kirish muolajasi yordamida identifikatsiyalanishi shart. Kirilgandan so'ng MBBT bilan ishlash seansi harakatga keltiriladi.

Imtiyozlarni belgilash va bekor qilish. Taqsimlangan ma'lumotlar bazasi ko'pchilik foydalanuvchilarning ma'lumot bazalari bilan ishlashni ko'zda tutadi. Ammo barcha foydalanuvchilarga ham ma'lumotlar bazasi bilan har qanday harakatlarni bajarishga ruxsat berilmaydi. Shu sababli foydalanuvchilarga imtiyozlar belgilanadi.

Ma'lumotlar bazasida imtiyozlar ikki kategoriyaga bo'linadi: tizimli imtiyozlar (system privileges) va obyektli imtiyozlar (object privileges). Tizimli imtiyozlar ma'lumotlar bazasidan umumiy foydalanishni nazoratlaydi. Unga jadvallarni va boshqa obyektlarni yaratish hamda ma'lumotlar bazasini ma'murlash huquqi taalluqli.

Obyektli imtiyozlar ma'lumotlar bazasining muayyan obyekti bilan bog'liq. Obyektli imtiyozlar uch qismdan iborat:

- imtiyoz qo'llanuvchi obyekt;
- imtiyoz ruxsat beruvchi amallar;
- imtiyozlar beriluvchi foydalanuvchi.

Belgilanishi lozim bo'lgan dastlabki imtiyozlardan biri – jadval yaratuvchilari imtiyozlari. Agar barcha foydalanuvchilar tizimda bazaviy jadvallarni yaratish imkoniyatlariga ega bo'lsalar, ma'lumotlarning ortiqchaligi, ularning nomuvofiqligi ro'y berishi mumkin, natijada tizim samarador bo'lmaydi.

Jadval yaratgan foydalanuvchi uning egasi hisoblanadi. Bu degani, foydalanuvchi o'zi yaratgan jadvalda barcha imtiyozlarga ega va imtiyozlarni boshqa foydalanuvchilarga uzatishi mumkin. Har bir foydalanuvchi SQL muhitida maxsus identifikatsiya nomiga (yoki nomeriga) ega.

Imtiyozlar GRANT (BERMOQ) operatori yordamida beriladi va REVOKE (BEKOR QILMOQ) operatori yordamida bekor qilinadi.

GRANT operatori quyidagi sintaksisga ega:

```
GRANT imtiyoz.,...– ON obyekt nomi
TO {imtiyoz taqdim etiluvchi foydalanuvchi} [PUBLIS]
[WITH GRANT OPTION];
imtiyoz:=
{ALL PRIVILEGES}
|SELECT
|DELETE
|{INSERT [(ustun nomi.,...)]}
```

|{UPDATE [(ustun nomi.,...)]}
|REFERENCES [(ustun nomi.,...)]}
|USAGE}

SQL GRANT operatorini olganida, ushbu operatorning joizligini aniqlash maqsadida komanda bergan foydalanuvchining imtiyozlarini tekshiradi.

Jadvaldan foydalanuvchi uchun imtiyozlarning quyidagi xillari belgilanishi mumkin:

- SELECT – jadvalda so'rovlarni bajarishga ruxsat;
- INSERT – jadvalda INSERT (yangi qatorni kiritish) operatorini bajarishga ruxsat;
- UPDATE – jadvalda UPDATE (hoshiyalar qiymatini yangilash) operatorini bajarishga ruxsat;
- DELETE – jadvalda DELETE (yozuvlarni yo'qotish) operatorini bajarishga ruxsat;
- REFERENCES – tashqi kalitni aniqlashga ruxsat.

GRANT operatorining bittasida bir necha imtiyozlar, ularni vergul orqali sanash yoki foydalanuvchiga ushbu jadval uchun barcha imtiyozlar berilishini anglatuvchi ALL argumentini ishlatib, belgilanishi mumkin.

GRANT operatorining bittasida bir vaqtning o'zida bir necha foydalanuvchiga imtiyozlar, ularni vergul orqali sanash yoki imtiyozlar barcha foydalanuvchiga berilishini anglatuvchi PUBLIS argumentini ishlatib, belgilanishi mumkin. Ammo bu imkoniyatdan ehtiyotkorona foydalanish zarur, chunki PUBLIS nafaqat joriy foydalanuvchilarni, balki tizimga keyinchalik kiritilishi mumkin bo'lgan barcha foydalanuvchilarni anglatadi. Faraz qilaylik, foydalanuvchi Mansurov "Sotrudnik" jadvalining egasi va u foydalanuvchi Karimovga jadvalga so'rov yuborishga rozi. Bu holda foydalanuvchi Mansurov quyidagi komandani kiritishi lozim:

GRANT SELECT ON Sotrudnik TO Karimov;

WITH GRANT OPTION gapi foydalanuvchiga ushbu jadval uchun imtiyozlarni belgilashga imkon yaratadi. Agar, masalan, komanda quyidagi ko'rinishni olsa:

GRANT SELECT ON Sotrudnik
TO Karimov WITH GRANT OPTION:

foydalanuvchi Karimov, o'z navbatida imtiyozlarni belgilash huquqini boshqa foydalanuvchilarga uzatish imkoniyatiga ega bo'ladi, ya'ni foydalanuvchi Karimov quyidagi komandani berishi mumkin:

GRANT SELECT ON Mansurov Sotrudnik
TO Salimov WITH GRANT OPTION:

Demak, sxema egasi bo'lmagan foydalanuvchi jadvalga havola qilganida, jadval nomi oldida sxema nomi ko'rsatiladi.

Obyektning aksariyat imtiyozlari bir xil sintaksisdan foydalanadi. Yuqorida keltirilgan imtiyozlardan UPDATE va REFERENCES istisno.

UPDATE imtiyozlari berilganida yuqorida qo'llanilgan sintaksisdan foydalanish mumkin, ya'ni foydalanuvchiga jadvalning barcha ustunlarini yangilash huquqi beriladi. Imtiyoz nomidan keyin qavs ichida ushbu imtiyoz tatbiq etiluvchi ustunlar nomi ko'rsatilishi mumkin. Masalan, UPDATE imtiyozi quyidagi ko'rinish olishi mumkin:

GRANT UPDATE (doljnost, oklad) ON Sotrudnik TO Karimov; REFERENCES imtiyozi berilganida ham ustunlar nomi beriladi.

Jadvalni faqat alohida ustunlari bo'yicha ko'zdan kechirishni cheklash uchun tasavvur yaratish mexanizmidan foydalanib, imtiyozni real jadval uchun emas, tasavvur uchun belgilash lozim. Jadvalni faqat alohida qatorlar bo'yicha ko'zdan kechirishni cheklash uchun ham tasavvurdan foydalanish mumkin.

Imtiyozni bekor qilish REVOKE operatori yordamida amalga oshiriladi. Ushbu komandaning sintaksisi GRANT operatorining sintaksisiga o'xshash. Masalan, Karimov uchun "Sotrudnik" jadvalini ko'zdan kechirish imtiyozini bekor qilish quyidagi ko'rinishga ega:

REVOKE SELECT ON Sotrudnik TO Karimov.

Muayyan MBBTda yuqorida keltirilgan imtiyozlardan farqli imtiyozlar mqdadlanishi mumkin. Masalan, ba'zi MBBTda foydalanuvchilarga indekslarni yaratishga imkon beruvchi INDEX imtiyozini berish mumkin. Ammo INDEX obyekti SQL standartida aniqlanmagan va ushbu imtiyozni berish komandasining sintaksisi tizimdan tizimga o'zgarishi mumkin.

Imtiyozni bekor qilish huquqiga kim egalik qilishi SQL standartida aniqlanmagan. Ammo, odatda, imtiyozni bekor qilish, ushbu imtiyozni bergan foydalanuvchi tomonidan amalga oshiriladi.

Nazorat savollari

1. Taqsimlangan ma'lumotlar bazasi yaxlitligini ta'minlashda qanday muammolar mavjud?
2. Tranzaksiyaning ikki fazali qaydlash mexanizmini tushuntiring.
3. Ma'lumotlar bazasini shifrlash va deshifrlash qanday amalga oshiriladi?
4. Obyektlarni akslantirish va bekitish qanday amalga oshiriladi?
5. Ishga tushirish parametrlaridan foydalanishni tushuntiring.
6. Taqsimlangan ma'lumotlar bazasini himoyalashda parollardan foydalanish.
7. Imtiyozlar qanday belgilanadi va bekor qilinadi?

3.3. Ma'lumotlarni obyektli bog'lash texnologiyasi

Mijoz – server tizimi uchun ishlangan tatbiqiy komponentlarning SQL – serverlar ko'rinishidagi axborot tizimi yadrosi bilan o'zaro ta'sirini unifikatsiyalash, shaxsiy MBBT boshqaruvidagi tarqoq ma'lumotlar bazasini murakkab detsentralizatsiyalangan getrogen taqsimlangan tizimlarga integratsiyalash uchun ham o'xshash yechimlarni ishlab chiqishga imkon yaratdi. Bunday yondashish *ma'lumotlarni obyektli bog'lash* nomini olgan.

Tor ma'noda, ma'lumotlarni obyektli bog'lash texnologiyasi bir foydalanuvchi tomonidan tashkil qilingan bitta lokal bazaning boshqa foydalanuvchi tomonidan tashkil etilgan va ekspulatatsiya qilinuvchi, balkim boshqa hisoblash qurilmasidagi, lokal baza ma'lumotlaridan foydalanishni ta'minlash masalasini yechadi.

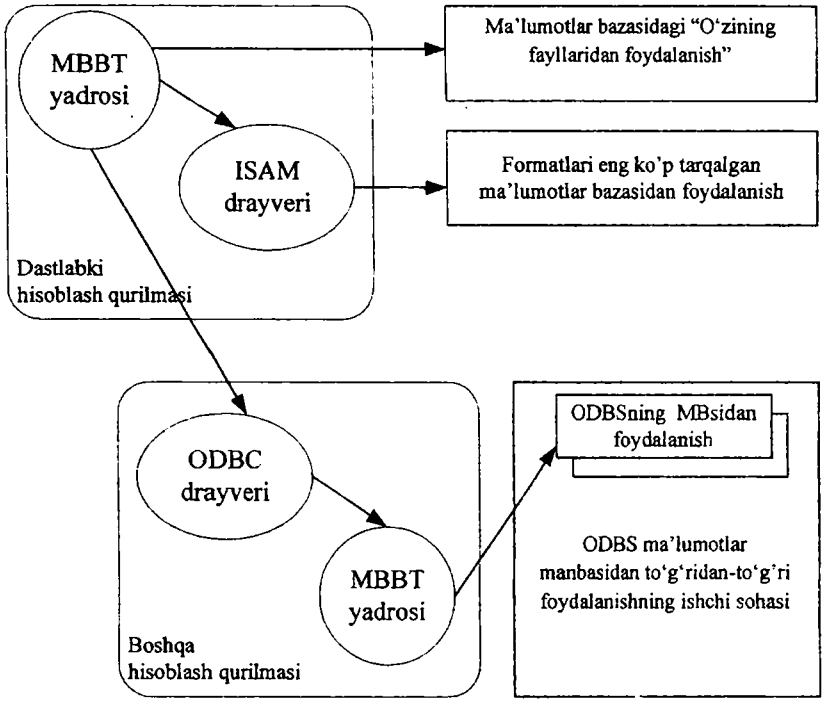
Ushbu masalaning yechimi "*ma'lumotlardan foydalanish obyektlari*" – dBase texnologiyasini zamonaviy shaxsiy MBBT texnologiyalari (MS Access, MS FoxPro va h.) tomonidan madadlashga asoslangan. Ta'kidlash lozimki, obyekt deganda obyektga mo'l-

jallangan dasturlash va zamonaviy obyektga mo'ljallangan operatsion muhit asoslanuvchi ma'lumotlar va ularni ishlash usullarining bir butunga (obyektga) integratsiyasi tushuniladi. Boshqacha aytganda, "*ma'lumotlardan foydalanish obyektlari*" texnologiyasini madadlovchi MBBT lokal bazalarga boshqa fayllardagi, balkim boshqa hisoblash qurilmalaridagi va boshqa MBBT boshqaruvidagi ma'lumotlardan foydalanish obyektlarini kiritish va ishlatish imkoniyatiga ega bo'ladi.

Texnik nuqtayi nazaridan, "*ma'lumotlardan foydalanish obyektlari*" texnologiyasi yuqorida aytib o'tilgan *ODBC protokoliga* asoslangan. ODBC protokoli nafaqat mijoz – server tizimlaridagi SQL serverlari ma'lumotlaridan *foydalanish standarti* sifatida, balki relyatsion MBBT boshqaruvidagi har qanday ma'lumotlardan foydalanish standarti sifatida qabul qilingan. ODBC protokoli asosida ma'lumotlardan bevosita foydalanish uchun *ODBC drayverlari* deb ataluvchi ma'lumotlar bo'lgan qurilmalarda initsializatsiyalanuvchi maxsus dasturiy komponentlar yoki boshqaruvida tashqi ma'lumotlar bazasi yaratilgan va ekspluatatsiya qilinayotgan MBBTning initsializatsiyalanuvchi yadrolari ishlatiladi. Obyektli bog'lash asosida tashqi ma'lumotlar bazalaridan foydalanish prinsipi va xususiyati sxema ko'rinishida 3.5-rasmda keltirilgan.

Zamonaviy shaxsiy MBBT avvalo. "*o'zining*" *formatidagi tashqi ma'lumotlar bazasidagi obyektlardan* (jadvallardan, so'rovlardan, shakllardan) *to'g'ridan-to'g'ri foydalanish* imkoniyatini ta'minlaydi. Boshqacha aytganda, ishlashning joriy seansida tashkil etilgan ma'lumotlar bazasiga foydalanuvchi maxsus havola – obyektlarini kiritishi va boshqa (tashqi, ya'ni ushbu seansda maxsus tashkil etilmagan) ma'lumotlar bazasi bilan ishiash imkoniyatiga ega. *Joriy ma'lumotlar bazasiga kiritilgan tashqi ma'lumotlar bazasi obyektlari bog'langan deb ataladi* va odatda, ichki obyektlardan farqlash maqsadida maxsus belgiga ega. Ta'kidlash lozimki, ma'lumotlarning o'zi joriy ma'lumotlar bazasi fayliga (fayllariga) sig'maydi va "o'zining" ma'lumotlar bazasi fayllarida qoladi. Joriy ma'lumotlar bazasining tizimli katalogiga foydalanish uchun bog'langan obyektlar xususidagi barcha zaruriy ma'lumotlar joylashtiriladi. Bu ma'lumotlar – bog'langan obyektlarning ichki nomi va

tashqi nomi, ya'ni tashqi ma'lumotlar bazasidagi obyektning haqiqiy nomi, tashqi baza fayliga to'liq yo'l va h.



3.5-rasm. ODBC protokoli asosida tashqi ma'lumotlardan foydalanish prinsipi.

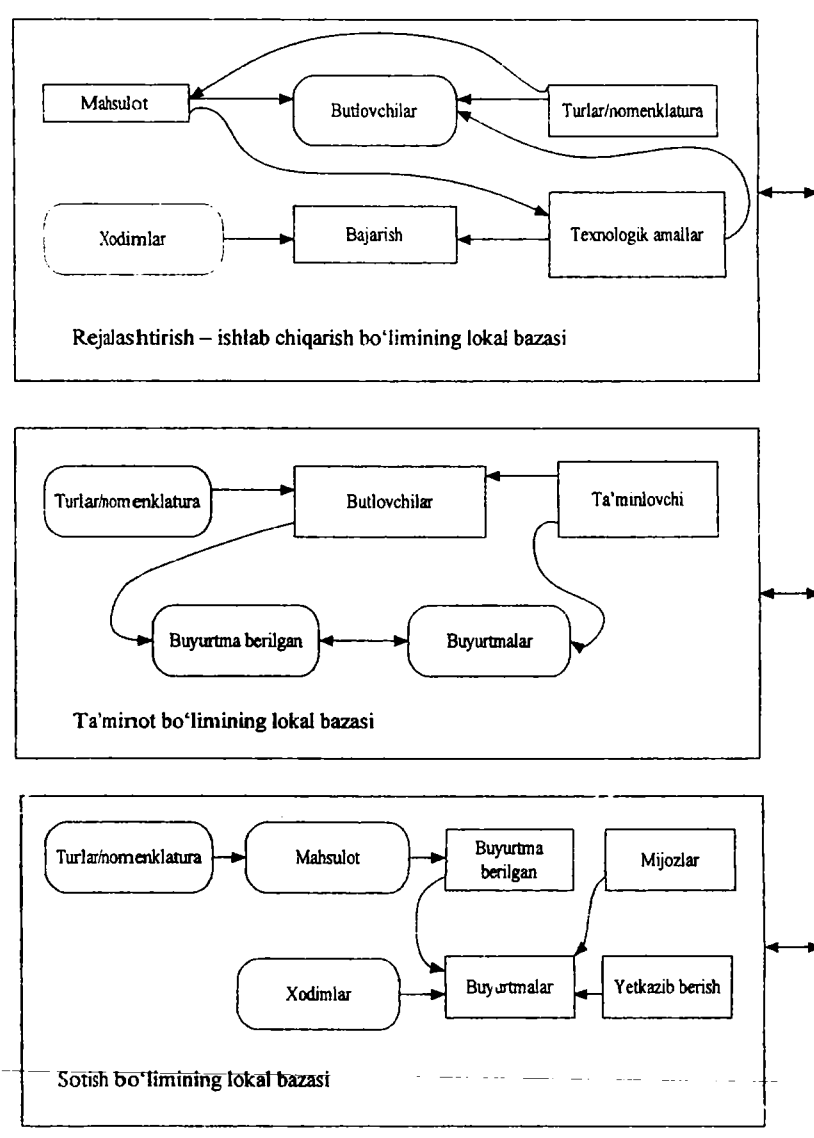
Foydalanuvchi uchun *bog'langan obyektlar* ichki obyektlardan hech nimasi bilan ham farqlanmaydi. Foydalanuvchi tashqi bog'langan bazalarda ma'lumotlar jadvalini tashkil etishni, qidiruvni, ma'lumotlarni o'zgartirishni, yo'q qilishni va qo'shishni, bunday jadvallar bo'yicha so'rovlarni tuzishni va h. bajarishi mumkin. Bog'langan obyektlarni ichki ma'lumotlar bazasiga integratsiyalash, *ya'ni ichki va tashqi jadvallar orasida bog'lanishni* o'rnatish mumkin.

Texnik nuqtayi nazaridan, tashqi ma'lumotlar bazasining bog'langan obyektlari bilan ishlash joriy ma'lumotlar bazasining ma'lu-

motlar bilan ishlashidan unchalik farq qilmaydi. Joriy ma'lumotlar bazasining tizimli katalogi bo'yicha bog'langan obyekt ma'lumotlariga murojaat qilinganda MBBT yadrosi tashqi ma'lumotlar bazasining mos faylining (fayllarining) makoni va boshqa parametrlari xususidagi ma'lumotlarni topadi va foydalanuvchiga bildirmasdan ushbu faylni (fayllarni) ochadi. So'ngra ma'lumotlardan bevosita foydalanish va ularni manipulyatsialash maqsadida oddiy tartib bo'yicha asosiy xotirada ma'lumotlarning tashqi fayli sahifalarini buferlashni tashkil etadi. Ta'kidlash lozimki, zamonaviy operatsion tizimlari ma'lumotlari fayllari bilan ko'pchilik foydalanuvchi rejim imkoniyatlari bilan ishlash asosida tashqi ma'lumotlar bazasi bilan (agar u boshqa hisoblash qurilmasida bo'lsa) *shu vaqtning o'zida boshqa foydalanuvchi ishlashi mumkin.* Bu esa umumiy taqsimlangan ma'lumotlarning kollektiv ishlanishini ta'minlaydi.

3.6-rasmda mahsulotni ishlab chiqarish va sotishning axborot ta'minoti nuqtayi nazaridan birgalikda foydalanuvchi ma'lumotlarning lokal bazalari sxemasining misoli keltirilgan. Rasmda strelkalar yordamida "yakkadan-ko'plarga" xilidagi bog'lanishlar ko'rsatilgan bo'lib, strelka uchi "ko'plar" tomoniga mos keladi.

Bog'langan jadvallarda ma'lumotlar hajmining ortishi bilan taqsimlangan tizimlarni qurishning bunday prinsipining tarmoq trafigining jiddiy oshishiga olib kelishini sezish qiyin emas, chunki tarmoq bo'yicha doimo, hatto ma'lumotlar nabori emas, balki ma'lumotlar bazasi fayllarining sahifalari uzatiladi.



3.6-rasm. Obyektli bog'lash texnologiyasi asosida tashkil etilgan lokal ma'lumotlar bazalari sxemasining namunasi.

Bu esa, o‘z navbatida, tarmoqning avj yuklanishiga olib keladi. Shu sababli, taqdim etilgan o‘zaro bog‘langan obyektli lokal ma’lumotlar bazasining sxemalari ishlab chiqarish – texnologik va tashkiliy jarayonlarga bog‘lik axborot texnologiyalariga tayangan holda lokal bazalari orasidagi tarmoqdagi ma’lumotlar oqimining jadalligi, yo‘nalganligi nuqtayi nazaridan keyingi sinchiklab o‘rganib chiqishni talab etadi.

Ma’lumotlar xavfsizligini va yaxlitligini ta’minlashning ishonchli mexanizmlarining mavjud emasligi ham jiddiy muammo hisoblanadi. Fayl serveri modelidagidek bir necha foydalanuvchilarning bir xil ma’lumotlar bilan birgalikda ishlashi, faqat operatsion tizimning bir necha ilovalar faylidan bir vaqtda foydalanish bo‘yicha funksiyalari yordamida ta’minlanadi. Xuddi shu tarzda keng tarqalgan Fox Pro, dBASE kabi boshqa MBBTining ma’lumotlar bazasidagi ma’lumotlardan hamda jadval ma’lumotlaridan foydalanish ta’minlanadi. Bunda foydalanish bevosita MBBT yadrosi yordamida hamda odatda, MBBT komplekti tarkibiga kiruvchi maxsus qo‘shimcha ISAM (Indexed Sequential Access Method) drayverlar yordamida ta’minlanadi. Bunday yondashish shu tariqa qurilgan taqsimlangan getrogen tizimlarining ko‘p protokolligini, ya’ni lokal ma’lumotlar bazalarini madadlovchi MBBT turlarining “xilma-xilligini” amalga oshiradi. Ammo obyektli bog‘lash, amalga oshirilishi va madadlanishi muayyan MBBTning o‘ziga xos xususiyatiga bog‘liq ma’lumotlar bazasining boshqa obyektlarini (so‘rovlar, shakllar, hisobotlar) istisno qilgan holda, faqat bevosita ma’lumotlar jadvali bilan chegaralanadi.

Boshqa MBBT bazalaridan foydalanish (3.5-rasmga qaralsin) masofadagi ma’lumotlar joylashgan hisoblash qurilmalarida o‘rnatiluvchi va bajariluvchi ODBC drayverlarining texnikasi orqali amalga oshiriladi. Bu holda “g‘oya” quyidagicha: lokal ma’lumotlar bazasini madadlovchi shaxsiy MBBT tarkibiga ODBC drayveri deb ataluvchi qo‘shimcha dasturiy komponentni o‘rnatish mumkin. O‘rnatiluvchi ODBC drayveri operatsion tizim katalogining maxsus qism katalogida “ro‘yxatga olinadi”. Shu tariqa ODBC ma’lumotlari manbaidan to‘g‘ridan – to‘g‘ri foydalanishning ishchi zonasi hosil qilinadi.

ODBC ma'lumotlari manbaidan bevosita foydalanish uchun MBBT yadrosi ichki lokal ma'lumotlar bazasining tizimli katalogi bo'yicha manba joylashgan joyni aniqlaydi, ilovalaming o'zaro ta'siri protokoli (API) bo'yicha hisoblash qurilmasida ODBC drayverining masofadagi ma'lumotlarini chaqiradi ODBC protokoli bo'yicha ma'lumotlardan foydalanish va ishlashi uchun SQL – yo'riqnomalarni yo'llaydi. Bunday foydalanish rejimi qator parametrlar orqali tartibga solinadi (muolajalarni chaqirish intervali, so'rov ishlanishining maksimal vaqti, so'rovlar bo'yicha shakllantiriluvchi ma'lumotlar naboridan tarmoq bo'yicha bir marta jo'natiluvchi yozuvlar soni, yozuvlarni blokirovka qilish vaqti va h.). Ushbu parametrlar ODBCning mos drayverini o'rnatishda va ro'yxatga olishda operatsion tizimning maxsus reestriga yoziladi.

Bunday yondashishda har bir lokal MBBT, tashqaridan (boshqa hisoblash qurilmalaridan) "uning" ma'lumotlar fayli ma'lumotlaridan foydalanishga murojaat qilinganida o'zining hisoblash qurilmasida SQL – server rolini, ya'ni ma'lumotlar mashinasi rolini bajaradi. Bu holda ma'lumotlarni bevosita ishlashni "o'zining" ma'lumotlar faylining mantiqiy va fizik strukturasi xususiyatlarini biluvchi MBBT tomonidan amalga oshirilishi odatda, ishlashning yuqori samaradorligini ta'minlaydi, eng asosiysi esa, ma'lumotlar manbaining predmet sohasi mantiqi bo'yicha ma'lumotlar yaxlitligiga cheklashlar bajariladi.

Ma'lumotlarni himoyalash va foydalanishni cheklash tizimlarida "raxnalar"ning paydo bo'lishi, obyektli bog'lash texnologiyasining ma'lum muammosi hisoblanadi. Ma'lumotlardan foydalanish muolajalarini bajarish uchun ODBC drayverlarining chaqiriqlari tarkibida, yo'ldan, fayllar va so'raluvchi obyektlar (jadvallar)dan tashqari (agar mos bazalar himoyalangan bo'lsa) ochiq holdagi foydalanish parollari bo'ladi, natijada foydalanish va ma'lumotlarni himoyalash tizimlari tahlillanishi va ochilishi mumkin.

Nazorat savollari

1. Ma'lumotlarni obyektli bog'lash texnogiyasining mohiyatini tushuntiring.
2. ODBC protokoli asosida tashqi ma'lumotlardan foydalanish prinsipi.
3. Obyektli bog'lashli lokal ma'lumotlar bazalarining sxemalarini tushuntiring
4. Ko'p protokollik (interperabelnost) qanday yondashishni amalga oshiradi?

4-bob. XAVFSIZLIK AUDITI VA MA'LUMOTLAR BAZASINI REZERVLI NUSXALASH

4.1. Ma'lumotlar bazasini boshqarish tizimlarida xavfsizlik auditini o'tkazish xususiyatlari

Axborot tizimi yoki axborot texnologiyasining auditi deganda tizimning, texnologiyaning joriy holati, unda kechuvchi texnologiyalar va hodisalar xususidagi obyektiv ma'lumotlarni olish va baholashning, ularning ma'lum mezonga moslik darajasini o'rnatish va natijalarni buyurtmachiga taqdim etishning tizimli jarayoni tushuniladi.

Audit o'tkazilishi axborot texnologiyasining joriy xavfsizligini baholashga, xavf-xatarlarni baholash va boshqarishga, ularning tashkilot biznes jarayonlariga ta'sirini boshqarishga, tashkilot axborot aktivlarining xavfsizligini ta'minlash masalasiga to'g'ri va asoslangan yondashishga imkon beradi.

Tashkilotning asosiy aktivlari quyidagilar:

- g'oyalar;
- bilimlar;
- loyihalar;
- ichki tekshirish natijalari.

Auditning umumiy tushunchasi. 1844-yili Angliyada aksioner shirkatlar xususida qonun qabul qilingan. Ushbu qonunga binoan shirkat boshqarmasi har yili aksionerlar oldida hisob berishi lozim. Buning ustiga hisobot maxsus kishi - mustaqil auditor tomonidan tekshirilishi va tasdiqlanishi shart. Ushbu yil auditning tug'ilgan yili hisoblanadi.

Hozirda audit o'z rivojining bir necha bosqichlarini o'tib, davlatlar xo'jalik hayotining qismiga aylandi. Aksionerlik shirkatining buxgalteriya hisoblarini alohida professional auditorlar tekshirishidan boshlab audit tarkibida professional auditorlar va auditorlik firmalar ko'rsatuvchi qator xizmatlar (buxgalteriya hisobotini tekshirish, moliyaviy tahlil, maslahat berish) bo'lgan kompleks tushun-

chagacha rivojlandi. Bunday firmalarning orasida o'nlab xodimlari bo'lgan - katta bo'lmaganlari va minglab xodimlari bo'lgan - juda kattalari mavjud.

Audit turlari. Axborot tizimi xavfsizligining auditini odatda, tashqi va ichkilariga ajratishadi.

Tashqi audit asosan tashkilotdan tashqarida va odatda, axborot xavfsizligi auditi bilan shug'ullanuvchi ixtisoslashgan tashkilotlar tomonidan o'tkaziladi. Bunda tashqi hujumlar natijasidagi xavf-xatar o'lchamlari tahlillanadi (xatto tashkilot tarmoqlararo ekranlar bilan himoyalangan bo'lsa ham). Tashqi auditni o'tkazishda portlarni skanerlash, tarmoq va tatbiqiy dasturiy ta'minot zaifliklarini qidirish amalga oshiriladi. Web – serverlari, pochta va fayl serverlari bilan o'zaro bog'lanishga hamda tashkilot lokal tarmog'iga kirishga urinishlar amalga oshiriladi. Tashkilot rahbariyatining xohishi bilan tashqi auditning maxsus turi - Ethical Hacking o'tkazilishi mumkin. Bunda maxsus tashkilot (bunday tashkilot maxsus Tiger Team nomiga ega) tashkilot serverlariga, saytlariga va xostlariga tanlab olingan hujumlarni amalga oshiradi. Bunday hujumlar tashkilot axborot tizimining zaifliklarini namoyish etishi mumkin.

Ichki audit odatda tashkilot xodimlaridan tashkil topgan maxsus komanda tomonidan o'tkaziladi. Ichki auditning vazifasi mavjud axborot tizimi texnologiyasidan foydalanishdagi xavf-xatarni baholash hisoblanadi. Auditning bu turi qandaydir standartni amalga oshiruvchi auditni avtomatlashtirish vositasini jalb qilish orqali bajariladi. Ichki audit tashkilotning tarmoqlararo ekran bilan chegaralangan tarmoq muhitining ichida o'tkaziladi. Tashkilotning ichki xost portlarini va zaifliklarini skanerlash ham uning vazifasi hisoblanadi. Undan tashqari, tashkilotda o'rnatilgan xavfsizlik siyosatining bajarilishi, resurslardan foydalanishning nazorati va boshqarilishi, tashkilot xodimining parol siyosati va uning bajarilishi tahlillanadi. Auditning bu turi audit o'tkazishning standart usulini tarmoq zaifliklarini mukammal ko'rib chiqish bilan to'ldiradi.

Oracle MBBT misolida ma'lumotlar bazasi xavfsizligi auditini o'tkazish. Oracle MBBT – funksional rivojlangan mahsulot hisoblanadi va unda audit o'tkazishning bir necha imkoniyatlari mavjud.

Oracle auditi ma'lumotlar bazasi tarkibidagi axborotdan avtorizatsiyalanmagan foydalanishni yoki axborotning ichki suiiste'mol qilinishini aniqlashda yordam berishi mumkin.

Oracle dagi audit uchta qismga ajratilgan:

- CREATE TABLE yoki CREATE SESSION kabi iboralarning auditi;
- ALTER USER imtiyozlar auditi;
- SELECT TABLE obyekt sathidagi obyektga audit.

Asosiy konfiguratsiya. Audit yozuvini ma'lumotlar bazasining auditorlik jadvaliga yoki operatsion tizimning auditorlik jurnaliga joylashtirish mumkin. Audit yozuvining operatsion tizim jurnaliga yozilishi ba'zi hollarda himoyalanishning yuqoriroq darajasini ta'minlasa-da, ushbu imkoniyat barcha platformalar uchun mumkin emas. Ma'lumotlar bazasiga yozishda audit init.ora fayliga quyidagi qatorni qo'shish orqali ishga tushiriladi.

audit_trail=db

Misollar. *Ma'lumotlar bazasidan foydalanishga urinishga auditni ishga tushirish misoli.*

SQL> audit create session;

Audit succeeded.

SQL>

Ushbu komanda foydalanishning muvaffaqiyatli yoki muvaffaqiyatli emasligidan qat'iy nazar, barcha foydalanuvchilarning foydalanishiarini kuzatadi.

Oracle hujjatlari bo'yicha auditning barcha komanda formatlari quyidagi ko'rinishga ega:

audit {statement_option/privilege_option}

[by user] [by {session/access}] [whenever {successful/unsuccessful}]

Ushbu ifodaning faqat statement_option va privilege_option qismlari majburiy hisoblanadi, qolgan qismlari qo'shimcha parametrlar bo'lib, ularning ishlatilishi auditni yanada o'ziga xos bo'lishiga imkon beradi.

Foydalanuvchi audit komandasini berishi uchun unda "AUDIT SYSTEM" imtiyozi bo'lishi shart. Ushbu imtiyozga ega foydalanuvchilarni topish uchun quyidagilarni bajarish lozim:

SQL> select *

```
2 from dba_sys_privs
3 where privilege like '%AUDIT%';
GRANTEE                        PRIVILEGE                ADM
------------------------------ ------------------------ ----------
CTXSYS                         AUDIT ANY                NO
CTXSYS                         AUDIT SYSTEM             NO
DBA                            AUDIT ANY                YES
DB                             AUDIT SYSTEM             YES
IMP_FULL_DATABASE              AUDIT ANY                NO
MDSYS                          AUDIT ANY                YES
MDSYS                          AUDIT SYSTEM             YES
WKSYS                          AUDIT ANY                NO
WKSYS                          AUDIT SYSTEM             NO
9 rows selected.
SQL>
```

Yuqorida keltirilgan natijalar Oracle 9i ma'lumotlar bazasiga tegishli. MDSYS, CTXSYS va WKSYS foydalanuvchilar hujumchi uchun yaxshigina nishon bo'lishlari mumkin, chunki qilinuvchi har qanday harakatlarni bekitish uchun foydalanuvchilarning ixtiyoriy biri tomonidan auditning har qanday harakati to'xtatilishi mumkin.

Endi qandaydir foydalanuvchi tizimga kirib, o'z ishini boshlasa, audit foydalanishning barcha urinishlarini kuzatadi.

Ma'lumotlar bazasida o'zgarishlarni nazorat qilishga auditni o'rnatish misoli.

Ushbu misolda qisqalikni ta'minlash maqsadida, ma'lumotlar bazasi obyektlaridagi barcha o'zgarishlar kuzatilmaydi. Garchand, umuman, ma'lumotlar bazasining har qanday obyektlaridagi (jadvallaridagi, indekslaridagi, klasterlaridagi, muolajalaridagi, bibliotekalaridagi va h.) o'zgarishlarni kuzatish mumkin. Mazkur misolda audit obyektlarning tanlangan guruhiga ishga tushiriladi. Auditni sozlash quyida ko'rsatilganidek, ikki bosqichda, audit komandalarini yaratish va bajarish uchun ishga tushirish orqali amalga oshirilishi mumkin:

```
set head off
set feed off
set pages 0
spool aud.lis
```

```
select 'audit '//name//';'
from system_privilege_map
where (name like 'CREATE%TABLE%'
or name like 'CREATE%INDEX%'
or name like 'CREATE%CLUSTER%'
or name like 'CREATE%SEQUENCE%'
or name like 'CREATE%PROCEDURE%'
or name like 'CREATE%TRIGGER%'
or name like 'CREATE%LIBRARY%')
union
select 'audit '//name//';'
from system_privilege_map
where (name like 'ALTER%TABLE%'
or name like 'ALTER%INDEX%'
or name like 'ALTER%CLUSTER%'
or name like 'ALTER%SEQUENCE%'
or name like 'ALTER%PROCEDURE%'
or name like 'ALTER%TRIGGER%'
or name like 'ALTER%LIBRARY%')
union
select 'audit '//name//';'
from system_privilege_map
where (name like 'DROP%TABLE%'
or name like 'DROP%INDEX%'
or name like 'DROP%CLUSTER%'
or name like 'DROP%SEQUENCE%'
or name like 'DROP%PROCEDURE%'
or name like 'DROP%TRIGGER%'
or name like 'DROP%LIBRARY%')
union
select 'audit '//name//';'
from system_privilege_map
where (name like 'EXECUTE%INDEX%'
or name like 'EXECUTE%PROCEDURE%'
or name like 'EXECUTE%LIBRARY%')
/
spool off
```

@@aud.lis

Ushbu skript/ssenariy audit komandalari naborini spul-faylga chiqaradi. Spul-fayl audit komandalarini bajarish uchun ishga tushiriladi.

So'ngra ma'lumotlar bazasini qayta ishga tushirish lozim. Haqiqatan, audit ishga tushirilganini oddiy tekshirish ko'rsatadi.

SQL>select name, value from v $parameter 2 where name like 'audit%';

NAME	VALUE
audit_trail	DB
audit_tile_dest	?/rdbms/ audit

SQL>

Ushbu harakatlar aniq berilmaganucha nazoratlanuvchi harakatlar kuzatilmaydi. Ma'lumotlar bazasidan imtiyozli foydalanish, ma'lumotlar bazasini ishga tushirish va to'xtatish, ma'lumotlar faylini qo'shish kabi strukturaviy o'zgarish hollari bundan mustasno.

Ushbu harakatlar init.ora faylida audit_tile_dest qayta aniqlanmaganucha operatsion tizimning $ORACLE_HOME/rdbms/ audit faylida kuzatiladi. Windows da ushbu voqealar Event Viewe da paydo bo'ladi.

Audit uchun qandaydir imtiyozlar yoki iboralar ishlatilganligini tekshirishda quyidagilar ishlatiladi:

```
SQL>select from dba_stm_audit_opts
2 union
3 select from dba_priv_ audit_opts
no rows selected
SQL.
```

Qanday obyektlar nazoratlanganligini aniqlash uchun dba_obj_ audit_opts topshiriqni so'rash lozim.

Nazorat savollari

1. Axborot tizimi auditi nima?
2. Axborot xavfsizligi auditini o'tkazishda tashkilotning qanday aktivlari ko'riladi?
3. Axborot xavfsizligi auditining turlari.
4. *Oracle* dagi audit qanday qismlarga bo'lingan?

4.2. Ma'lumotlar bazasini tiklash

Muhim axborotning yo'qolishidan saqlanish uchun muntazam ravishda ma'lumotlarni rezervli nusxalash lozim. *Rezervli nusxalash* - o'ta muhim ma'lumotlarning asl nusxalari yo'qolganida ularni tiklash maqsadida vaqti-vaqti bilan takrorlash yoki zaxira nusxalarini yaratish. Aytish mumkinki, rezervli nusxalash-uskunaning buzilishi yoki foydalanuvchi tomonidan tasodifan fayllarning yo'q qilinishi holida axborotni yo'qolishidan sug'urtalash. Rezervli nusxalashning ikkita asosiy usuli mavjud: qat'iy disk qiyofasini nusxalash va kompyuter fayl tizimini nusxalash.

Qat'iy disk qiyofasini nusxalash - diskning aniq nusxasini yaratish. Bunda nafaqat foydalanuvchi ma'lumotlarini, balki Windows ni va operatsion tizimi holati xususidagi barcha axborotni tiklashga erishiladi.

Faylli nusxalash - kompyuter fayl tizimini, ya'ni kompyuterda saqlanuvchi papkalar va fayllarni nusxalash. Bunday nusxalash foydalanuvchining papkalarini va fayllarini tiklashga yordam bersa-da, tizimni ishchi holatiga qaytara olmaydi. Nusxalashning bu ikki xilini amalga oshirishning muayyan usuli xususida gap ketganda ularning bir necha asosiy xillarini ajratish mumkin: to'liq nusxalash, differensial nusxalash va inkremental nusxalash.

To'liq nusxalash - ko'rsatilgan ma'lumotlarni butunligicha to'liq nusxalash. Bunda nusxalashlar orasidagi o'zgarishlar hisobga olinmaydi.

Differensial rezervli nusxalash deganda oxirgi to'liq nusxalashdan keyingi vaqtda o'zgargan axborotni nusxalash tushuniladi. Ya'ni har bir keyingi nusxalash birinchi nusxalashdan beri o'zgargan barcha fayllarni o'z ichiga oladi.

Shunday qilib, rezerv nusxani tiklash uchun birinchi to'liq va oxirgi nusxalashlarni olish lozim.

Inkremental nusxalash faqat yangi va oxirgi nusxalashdan keyingi o'zgargan fayllarni nusxalaydi. Shu sababli u eltuvchidan differensial nusxalashga nisbatan kam joyni egallaydi. Ammo inkremental nusxani tiklash murakkabroq, chunki nafaqat birinchi va oxirgi, balki barcha oraliq nusxalangan fayllarni hisobga olishga to'g'ri keladi.

Nusxalashning yana bir usuli "ko'zguli nusxalash" mavjud. Ushbu usulga binoan diskda yangi fayl paydo bo'lishi bilanoq, u nusxada ham (vaqtning real rejimida) paydo bo'ladi. Ba'zi mutaxassislar ushbu usulni ikki tomonlama sinxronlash deb atashadi.

Rezervli nusxalashga quyidagi talablar qo'yiladi:

- axborot saqlanishining ishonchliligi. Saqlash tizimining buzilishlarga bardosh uskunalarni qo'llash, axborotni takrorlash va nusxalardan biri yo'q qilingan holda yo'qolgan nusxani almashtirish orqali erishiladi;
- ekpluatatsiyada soddaligi. Avtomatlashtirish (iloji boricha foydalanuvchi va ma'mur ishtirokini minimallashtirish) orqali erishiladi;
- tezda tatbiq etish (dasturni osongina o'rnatish va sozlash, foydalanuvchilarni tezlik bilan o'rgatish).

Rezerv nusxani saqlovchi qurilmaga uzatish usuli bo'yicha ma'lumotlarni rezervli nusxalashning quyidagi xillarini ko'rsatish mumkin: lokal hisoblash tarmog'i orqali, rezerv nusxalash serverining ishtirokisiz ma'lumotlarni saqlash tarmog'i orqali, "bir lahzali nushalar" mexanizmidan foydalanib ma'lumotlarni saqlash tarmog'i orqali. TCP/IP asosida kompyuter tizimi orqali rezervli nusxalashning afzalligi - amalga oshirilishining va rezervli nusxalash infrastrukturasiga o'zgartirish kiritishning soddaligi. Bunda rezervli nusxalashning tarmoq agentining dastur ta'minotini server-mijozga o'rnatish va tarmoq bo'yicha rezervli nusxalash serveri bilan o'zaro aloqasini sozlash kifoya. Rezervli nusxalash quyidagi sxema bo'yicha amalga oshiriladi: rezervli nusxalash serveri kompyuter tarmog'i orqali server-mijozdagi rezervli nusxalash agentiga komanda jo'natadi. Ushbu agent rezervli nusxalash serveriga ma'lumotlarlarni tayyorlash va jo'natish bo'yicha amallarni bajaradi. Rezervli nusxalash serveri ma'lumotlarni qabul qiladi va saqlash qurilmasiga yozadi. Tarmoq infrastrukturasida qandaydir o'zgarish sodir bo'lganida, tarmoq agenti tezda qayta sozlanishi va rezervli nusxalash tizimi ishini davom ettirishi mumkin. Undan tashqari, ushbu texnologiyaning amalga oshirilishi arzon va server-mijozlarning ma'lumotlarni saqlovchi tarmoqqa to'g'ridan-to'g'ri ulanishini talab etmaydi, ya'ni SANga (Storage Area Network – Ma'lumotlarni saqlash tarmog'i) ulanmagan serverlardagi yoki

ma'lumotlar saqlanuvchi tarmoqqa virtual ulangan serverlardagi ma'lumotlarni himoyalash uchun ishlatilishi mumkin.

Ushbu usulning kamchiligi – kompyuter tizimining rezervli nusxalash trafigi bilan yuklanishi, server – mijozga yuk, kompyuter tizimi va rezervli nusxalash serveri interfeyslarining o'tkazish qobiliyatiga bog'liqligi, rezervli nusxalashni berilgan "vaqt oralig'ida" bajarish zarurligi, masshtablash bo'yicha imkoniyatlarining cheklanganligi. Albatta, rezervli nusxalash trafigini uzatish uchun ajratilgan kompyuter tizimini tashkil etish, rezervli nusxalash serverining tarmoq interfeyslarini yagona "yo'g'on" tarmoq interfeyslarga birlashtirish mumkin. Ammo bu choralar ma'lumotlar himoyasi infrastrukturasining murakkablashishiga va uning masshtablanishining yomonlashishiga olib keladi. Shunday bo'lsa-da, ushbu texnologiya operatsion tizimning tizimli ma'lumotlari va ilovalar kabi kamdan-kam o'zgaruvchi ma'lumotlarni rezervli nusxalashga butunlay mos.

Ma'lumotlar bazasida ma'lumotlar fayllarining ikki xili yaratilishi mumkin.

Birlamchi ma'lumotlar fayli (Primary data file). Ushbu faylning yaratilishi shart bo'lib, unda ma'lumotlar bazasi katalogining yuklama axboroti va ma'lumotlar bazasining boshqa fayllariga ko'rsatkichlar saqlanadi. Ma'lumotlarning birlamchi faylida obyektlar va foydalanuvchilar ma'lumotlari joylashishi mumkin. Birlamchi fayl nomi uchun *mdf* kengaytirish tavsiya etiladi.

Ikkilamchi ma'lumotlar fayli (Secondary data file). Ushbu faylning yaratilishi shart bo'lmay, unda obyektlar va foydalanuvchilar ma'lumotlari saqlanadi. Unumdorlikni oshirish uchun ikkilamchi fayllarni turli disklarda saqlash tavsiya etiladi. Ma'lumotlar bazasida 32766 dan ko'p bo'lmagan ikkilamchi fayllar joylashtirilishi mumkin. Ikkilamchi fayl nomi uchun *ndf* kengaytirish tavsiya etiladi.

Tiklash modeli (recovery model) - ma'lumotlar bazasi konfiguratsiyasining parametri bo'lib, tranzaksiyalarni ro'yxatga olishni, tranzaksiya jurnalining rezervli nusxasini yaratishni va ma'lumotlar bazasini tiklash parametrlarini boshqaradi. Tiklash modelini tanlash, ma'lumotlar bazasini tiklashga va tiklash modelining tranzaksiyani

ro'yxatga olishi yoki olmasligiga bog'liq holda unumdorlikka jiddiy ta'sir ko'rsatadi.

To'liq tiklash modeli deganda, ma'lumotlar bazasi yadrosining tranzaksiyalar jurnalida barcha amallarni ro'yxatga olishi va hech qachon jurnalni qisqartirmasligi tushuniladi. Ushbu model ma'lumotlar bazasini uning yanglishishi onigacha bo'lgan holatini tiklashga imkon beradi.

Tiklashning oddiy modeli aksariyat tranzaksiyalar xususidagi ma'lumotlarning eng oz miqdorini ro'yxatga oladi va har bir nazorat nuqtasidan so'ng tranzaksiyalar jurnalini qisqartiradi. Tiklashning ushbu modeli rezervli nusxalashni va tranzaksiyalar jurnalini tiklashni madadlamaydi. Uning ustiga ma'lumotlarning alohida sahifalarini tiklashga imkon bermaydi.

To'liq bo'lmagan bayonnoma tuzishli modelda ma'lumotlar bazasi yadrosi SELECT INTO va BULKINSERT kabi ommaviy amallarning eng oz miqdorining ro'yxatini olib boradi. Agar jurnalning rezerv nusxasi tarkibida qandaydir ommaviy amallar bo'lsa, ma'lumotlar bazasini tranzaksiyalar jurnalining rezervli nusxasining oxiriga mos holatigacha (vaqtning ma'lum onigacha emas) tiklash mumkin. Tiklashning ushbu modeli faqat katta ommaviy amallar uchun ishlatiladi.

Rezervli nusxalashning asosiy turlari. Rezervli nusxalashning ikkita asosiy turi mavjud:

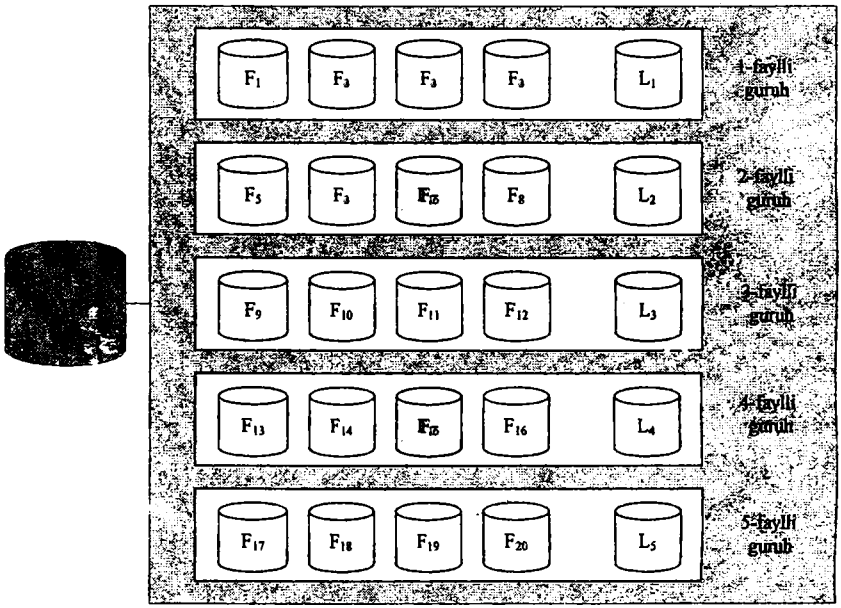
- zid bo'lmagan (sovuq) rezervli nusxalash. Bunda nusxalar foydalanuvchi uchun ma'lumotlar bazasi berk (close) bo'lganida yaratiladi. Avtonom rejimda yaratilgan ma'lumotlar bazasining rezervli nusxasi tarkibida ma'lumotlarning barcha fayllari, takrorlanish jurnallari va boshqaruvchi fayllar bo'ladi. Ma'lumotlar bazasi to'xtatilganidan so'ng barcha fayllar disklarning birida nusxalanadi. Nusxalash tugaganidan so'ng ma'lumotlar bazasini qayta yuklash amalga oshiriladi;
- operativ rejimdagi rezervli (qaynoq) nusxalash. Masalan, ma'lumotlar bazasi doimo operativ rejimda bo'ladi va foydalanuvchilar foydalana oladi.

Tranzaksiyalar jurnalining rezervli nusxasini faqat to'liq tiklash modeli yoki to'liq bo'lmagan bayonnoma tuzishli model o'rnatilgan ma'lumotlar bazasi uchun yaratish mumkin. Shuning-

dek, tranzaksiyalar jurnalini nusxalash faqat rezervli nusxalashdan so'ng amalga oshirilishi mumkin. Tranzaksiyalar jurnali tarkibida ma'lumotlarning faqat qismigina bo'ladi, shuning uchun ma'lumotlar bazasini tiklash uchun uning to'liq nusxasi ham talab etiladi.

Rezervlashning ikki xilidan ishonchlikning eng katta yutug'iga almashtirishli rezervlashda erishiladi. Ammo rezervlashning ushbu xilini amalga oshirish tizim holatini nazoratlovchi avtomatni va ishlab turgan tizim yanglishganida uzib-ulovchi (kommutator) qurilmani talab etadi.

Ma'lumotlar bazasi har biri o'z ichiga ma'lumotlarning qo'shimcha fayllar to'plamini va tranzaksiya jurnallarini oluvchi fayl guruhlari to'plamiga "tarqatilishi" mumkin (4.1-rasm).

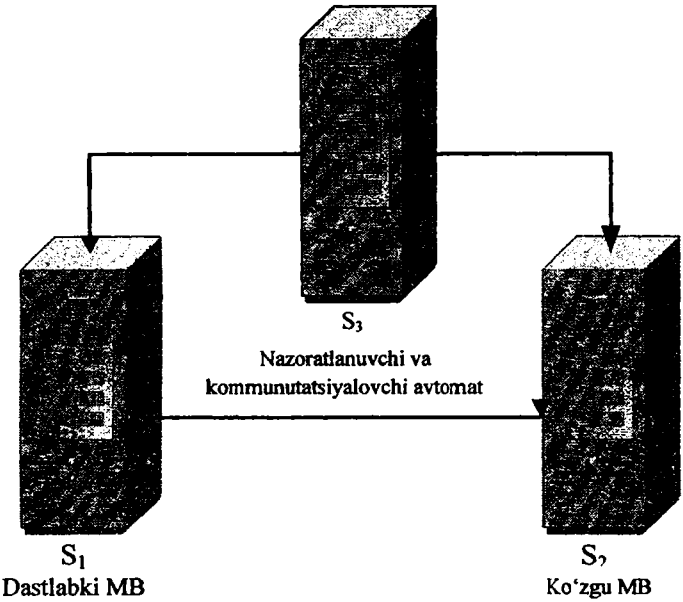


4.1-rasm. Ma'lumotlar bazasi fayllarini fayl guruhlariga tarqatish.

Ma'lumotlar bazasini fayl guruhlariga tarqatishdan eng katta samaraga RAID massivlarini qo'llashda erishiladi. Fayl qism-

tizimlarining unumdorligi, foydalanuvchanligi va ishonchliligi ortadi.

Nazoratlash va kommutatsiyalash avtomati mavjudligida rezervli nusxalash modulining strukturaviy sxemasi 4.2-rasmda keltirilgan.



4.2-rasm. Nazoratlovchi va kommutatsiyalovchi avtomatli rezervli nusxalash modulining strukturaviy sxemasi.

4.2-rasmda quyidagi belgilashlar qabul qilingan:

S_1, S_2 – axborotni himoyalashning asosiy va rezervli tizimlari;

S_3 – asosiy tizimning buzilganligi aniqlanganida himoya va kommutatsiya tizimining to'g'ri ishlashini nazoratlovchi avtomat.

Nazorat savollari

1. Ma'lumotlar bazasini rezervli nusxalash nima?
2. Rezervli nusxalashning asosiy usullari.
3. Rezervli nusxalash tizimiga talablar.

4. Ma'lumotlar bazasida ma'lumotlarning qanday fayllarini yaratish mumkin?

5. Ma'lumotlar bazasini rezervli nusxalashning asosiy turlari.

6. Nazoratlovchi va kommutatsiyalovchi avtomatli rezervli nusxalash modulining strukturaviy sxemasi.

4.3. Ma'lumotlar bazasini boshqarishning zamonaviy tizimlarida replikatsiyani sinxronlash jarayoni

"Mijoz-server" yoki ma'lumotlarni obyektli bog'lash texnologiyalari asosida qurilgan aksariyat taqsimlangan tizimlarning zaif joyi, tarmoq bo'yicha ma'lumotlarning katta miqdori uzatilishi sababli unumdorligining yetarlicha yuqori emasligi. Ma'lumotlarni replikatsiyalash texnologiyasi tezkor taqsimlangan tizimlarni qurishda ma'lum alternativa taqdim etadi.

Foydalanuvchilarning umumfoydalaniluvchi bir xil (muvofiqlashtirilgan) ma'lumotlar bilan avtonom ishlashi maqsadida boshqa kompyuterga joylashtiriluvchi ma'lumotlar bazasining alohida nusxasi *replika* deb ataladi.

Replikatsiyalashning asosiy g'oyasiga binoan foydalanuvchilar lokal ma'lumotlar bazasi bo'yicha ko'p miqdorda ko'paytirilgan bir xil (umumiy) ma'lumotlar bilan avtonom ishlaydilar. Natijada, tarmoq bo'yicha ma'lumotlarni uzatish va almashish zaruriyatining yo'qligi sababli, foydalanuvchi hisoblash qurilmasining yuqori unumdorligi ta'minlanadi. Bunday yondashishni amalga oshirish uchun MBBTning dasturiy ta'minoti mos holda ma'lumotlar bazasini tirajlash (replikatsiyalash) funksiyalari, xususan, ma'lumotlarning o'zini va ularning strukturalarini hamda replikalarni joylashtirish xususidagi axborot bo'lgan tizimli katalogni tirajlash funksiyalari bilan to'ldiriladi.

Ammo bunday taqsimlangan tizimlarni qurish va ishlatishning asosiy prinsiplaridan birini - *ma'lumotlarning muvofiqlashtirilgan holatining uzluksizligi* prinsipini - ta'minlashning ikkita muammosi paydo bo'ladi:

- barcha replikalarda umumiy ma'lumotlarning soni va qiymatining muvofiqlashtirilgan holatini ta'minlash;

- barcha replikalarda ma'lumotlar strukturasini muvofiqlashtirilgan holatini ta'minlash.

Umumiy ma'lumotlarning muvofiqlashtirilgan holatini ta'minlash, o'z navbatida, quyidagi *ikkita prinsipdan* birining amalga oshirilishiga asoslanadi:

- yangilashni uzluksiz ko'paytirish prinsipi (har qanday replikadagi har qanday yangilanish darhol ko'paytirilishi shart);
- kechiktirilgan yangilash prinsipi (replikalarni yangilash maxsus komandagacha yoki vaziyatgacha kechiktirilishi mumkin).

Yangilashni uzluksiz ko'paytirish prinsipi "real vaqt tizimlari"ni qurishda asos hisoblanadi. "Real vaqt tizimlari"ga misol tariqasida havodagi harakatni boshqarish tizimini, yo'lovchi transport chiptalarini band etish tizimini va h. ko'rsatish mumkin. Ularda taqsimlangan tizimlarning barcha uzellari va komponentalarida replikalarning yoki tirajlangan boshqa ma'lumotlarning uzluksiz va aniq mosligi talab etiladi. Ushbu prinsipga binoan har qanday tranzaksiya muvaffaqiyatli tugallangan hisoblanadi, qachonki u tizimning barcha replikalarida muvaffaqiyatli tugallansa. Amalda ushbu prinsipning amalga oshirilishi "tupik"lar bilan bog'liq jiddiy qiyinchiliklarga duch keladi. Faraz qilaylik, bitta hisoblash qurilmasida foydalanuvchi o'zinig replikasida ma'lumotlarni yangilaydi. Tranzaksiya (tranzaksiyalar) amalga oshirilishi vaqtida ushbu replikaning ma'lumotlar bazasidan mos yozuvlarning boshqa foydalanuvchilar tomonidan o'zgartirilishi lokal MBBT yadrosi yordamida blokirovka qilinadi. Shuning bilan birga tranzaksiya qaydlanishi mumkin va ushbu tranzaksiya jo'natilgan hamda tizimning boshqa replikalarida tugallangandan so'ngina mos ma'lumotlar razblokirovka qilinadi. Yana faraz qilamiz, tarmoqning boshqa kompyuteridagi tizimning boshqa replikasidagi foydalanuvchi, tabiiyki, ushbu onda boshqa foydalanuvchilar tomonidan o'zgartirilishi blokirovka qilingan yozuvlar bilan o'zining yangilashini (tranzaksiyani) o'tkazadi. Shu tariqa tupik hosil bo'ladi. Bir tranzaksiya o'zining replikasida qaydlanishi mumkin emas, chunki mos yozuvlar boshqa replikada blokirovka qilingan. Ushbu yozuvlarning boshqa replikada razblokirovkasi birinchi replikadagi mos yozuvlar razblokirovka qilinmaguncha, ya'ni birinchi replikada tranzaksiya tugallanmaguncha mumkin emas. Tupik vaziyat sodir bo'ladi.

Replikatsiyalangan tizimlarda tupiklarni aniqlashda markazlashtirilgan "Mijoz-server" tizim tranzaksiyalarini monitorida ishlab chiqilgan algoritmlardan foydalaniladi.

Umuman, taqsimlangan axborot tizimlarining qator predmet sohalarida ma'lumotlarni muvofiqlashtirishning uzluksizligi nuqtayi nazaridan real vaqt rejimi talab qilinmaydi. Bunday tizimlar axborot jarayonlari unchalik dinamik xarakteriga ega bo'lmagan tashkiliy – texnologik strukturalarni avtomatlashtiradi. Agar misol tariqasida avtomatlashtirilgan hujjat aylanish tizimini ko'rsak, xizmatga oid hujjatlar harakatining an'anaviy "tezligi" ish kuniga yoki ish soatlariga mos keladi. Bu holda taqsimlangan axborot tizimi replikalarini faqat bir marta har bir ish soatida yoki har bir ish kunida yangilash talab etiladi.

Bunday xil axborot tizimini *kechiktirilgan yangilash prinsipi* asosida qurish mumkin. Qandaydir replikada to'plangan ma'lumotlar o'zgarishi foydalanuvchining maxsus komandasi bo'yicha tizimning barcha qolgan replikalarini yangilash uchun yuboriladi. Bunday amal replikalarni sinxronlash deb yuritiladi. Replikalarni sinxronlashda ixtiloflar va tupiklarning paydo bo'lishi imkoniyati jiddiy kamayadi, uncha ko'p bo'lmagan ixtilofli vaziyatlar tashkiliy choralar yordamida osongina bartaraf etiladi.

Ma'lumotlarni muvofiqlashtirishning ikkinchi muammosini hal etish, ya'ni ma'lumotlar strukturasini muvofiqlashtirish, "Mijoz-server" tizimdagidek markaziy qurilmaning mavjud emasligi prinsipidan qisman chekinish orqali amalga oshiriladi va "asosiy" replika texnikasiga asoslanadi.

Ushbu texnikaning mohiyatiga binoan, tizim ma'lumotlar bazasining replikalaridan biri asosiy deb e'lon qilinadi. Bunda ma'lumotlar bazasining strukturasini faqat asosiy replikada o'zgartirish mumkin. Ma'lumotlar strukturasining ushbu o'zgarishlari kechiktirilgan yangilash prinsipi, ya'ni replikalarni maxsus sinxronlash orqali tirajlanadi. Markaziy qurilmaning mavjud emasligi prinsipidan qisman chekinishda, haqiqiy markazlashgan tizimlardan farqli holda bosh replikaning ishdan chiqishi, butun taqsimlangan tizimning birdaniga zavol topishiga olib kelmaydi, chunki qolgan replikalar avtonom tarzda ishlayveradi. Uning ustiga, replikatsiya texnologiyasini madadlovchi MBBT amaliyotida ma'lum vakolatga ega

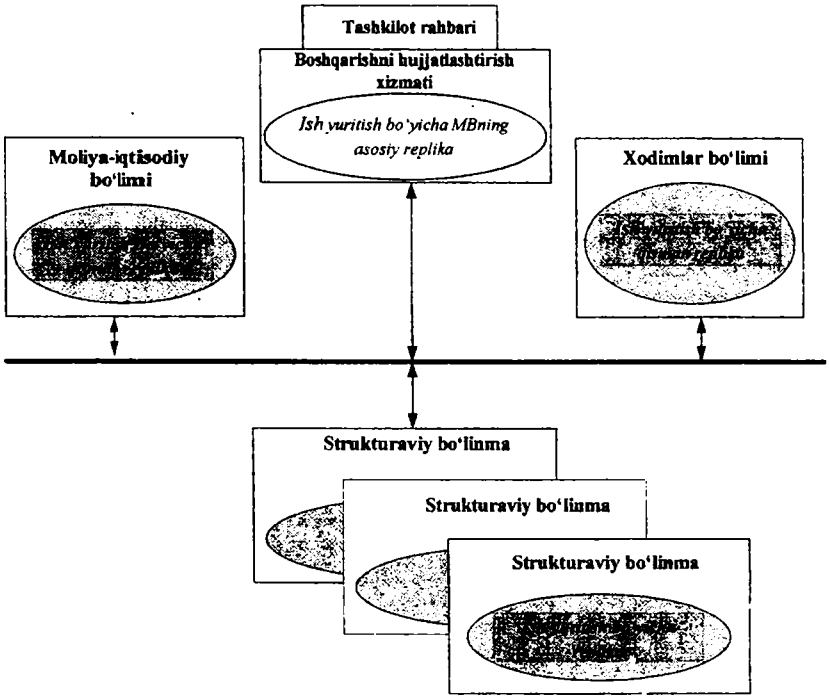
foydalanuvchiga (tizim ma'muriga) har qanday replikani asosiysiga o'zgartirish imkoniyati beriladi. Bu esa butun tizimning ishga layoqatligini to'liq tiklash imkoniyatini beradi.

Zamonaviy MBBTda replikalarni sinxronlash jarayoni. Ushbu jarayonda faqat o'zgartirilgan yoki turli replikalarga qo'shilgan ma'lumotlar almashtiriladi. Buning uchun ma'lumotlar bazasining tizimli katalogida joriy o'zgarishlarning maxsus jadvallari tuziladi va taqsimlangan tizimning barcha obyektlarini, xususan, turli replikalardagi bir xil nomlangan alohida-alohida obyektlarni global identifikatsiyalash (nomlash) tashkil etiladi. Bunday yondashish ma'lumotlar bazasi hajmini birmuncha ko'paytiradi, ammo replikalarni sinxronlashda traneport xarajatini jiddiy cheklaydi.

Qisman replikalarni va replikalarga *replikalanuvchi* va *replikalanmaydigan obyektlarni* kiritish imkoniyati replikatsiya texnologiyalarida qurilgan taqsimlangan axborot tizimlari ishlashining moslanuvchanligi va samaradorligi nuqtayi nazaridan muhim hisoblanadi. Qisman replika deganda tarkibida to'liq replikaning cheklangan qismto'plami bo'lgan ma'lumotlar bazasi tushuniladi. To'liq (asosiy) replikaning muayyan jadvallari uchun o'rnatiladigan filtrlardan foydalanish qisman replikani yaratishning keng tarqalgan usuli hisoblanadi. Qisman replikalar ma'lumotlardan foydalanishni cheklash bilan bog'liq ba'zi muammolarni yechishga imkon beradi va ma'lumotlarni ishlash unumdorligini oshiradi. Masalan, ma'lumotlar bazasi replikasiga ma'lum bo'linma uchun faqat ushbu bo'linmaga tegishli jadvallar yozuvini replikatsiyalash maqsadga muvofiq hisoblanadi. Bu esa boshqa yozuvlardan foydalanishni istisno etadi. Qisman replikalar texnikasi replikalarni sinxronlashga ketgan xarajatni ham kamaytiradi, chunki tarmoq bo'yicha uzatiladigan o'zgargan ma'lumotlar sonini cheklaydi.

Replikalarga replikatsiyaga loyiq bo'lmagan ma'lumotlar bazasi obyektlarini kiritish imkoniyati ma'lumotlar bazasi sxemasini va boshqa obyektlarini (so'rovlar, shakllar va hisobotlarni) predmet sohasining o'ziga xos xususiyatiga, ma'lumotlarni kiritish xususiyatiga va taqsimlangan tizimning muayyan elementi bo'yicha yechiladigan axborot masalalariga yuqori moslanuvchan va adekvat sozlashga imkon beradi. 4.3-rasmda replikatsiya texnologiyasi asosida qandaydir tashkiliy strukturaning ish yuritish bo'yicha taqsim-

langan axborot tizimi sxemasini tashkil etishga yondashish tasvirlangan.



4.3-rasm. Replikatsiya texnologiyasi asosida ish yuritish bo'yicha taqsimlangan axborot tizimi sxemasini tashkil etishga yondashish misoli.

Axborot tarmoqlarida ma'lumotlarning katta oqimi va yangilanishi jadalligi talab qilinmagan hollarda ma'lumotlarni replikatsiyalash texnologiyalari, markazlashgan elementlariga ega taqsimlangan axborot tizimlarini yaratish muammosining qimmatli "og'ir" mijoz-server tizimlaridan foydalanishga nisbatan tejamli yechimi hisoblanadi.

Amalda ma'lumotlarni birgalikda kollektiv ishlash uchun ma'lumotlarni obyektli bog'lash, replikatsiya va mijoz-server yechimlari elementlarini o'z ichiga oluvchi aralash texnologiyalardan foy-

dalaniladi. Bunda mantiqiy loyihalash, ya'ni ma'lumotlarni (jadvallarni, hoshiyalarni, kalitlarni, bog'lanishlarni, yaxlitlikni cheklashni) tashkil etishning mantiqiy loyihalash muammosiga axborot oqimlarini transport-texnologik loyihalash, foydalanishni cheklash va h. murakkab muammolari qo'shiladi. Afsuski, hozircha predmet sohasining mantiqiy va axborot-texnologik infrastrukturasi omillarini hisobga oluvchi taqsimlangan axborot tizimlarini loyihalashni avtomatlashtirish uchun nazariy-metodologik va instrumental yondashishlar ishlab chiqilmagan. Shunday bo'lsa-da, axborot oqimlari va texnologiyalarining taqsimlangan tabiatining o'zi belgilovchi taqsimlangan axborot tizimlarining yanada keng tarqalishi avtomatlashtirilgan axborot tizimlari rivojining asosiy istiqboli hisoblanadi.

Nazorat savollari

1. Ma'lumotlami replikatsiyalash nima?
2. Qisman replikalarni tashkil etishni tushuntiring.
3. "Tupik"lar paydo bo'lish holatlarini tushuntiring.
4. Replikalarni sinxronlash jarayonini tushuntiring.

5-bob. MA'LUMOTLAR BAZASI XAVFSIZLIGINI TA'MINLASH BO'YICHA STANDARTLAR VA SPETSIFIKATSIYALAR

5.1. Ma'lumotlar bazasi xavfsizligi qismtizimining arxitekturasi va ishlash prinsipi

Ma'lumotlar bazasini boshqarish tizimlari, ayniqsa relyatsion MBBTlari, axborotning katta massivlarini saqlashda ustun instrument bo'lib qoldi. Bir qadar rivojlangan ilovalar operasion tizimning fayl strukturalariga emas, balki mijoz/server texnologiyasida bajarilgan ko'pchilik foydalanuvchi MBBTga ishonadi. Shu sababli MBBTning, birinchi navbatda uning server komponentlarining, axborot xavfsizligini ta'minlash butun tashkilot xavfsizligi uchun hal qiluvchi ahamiyatga ega. Yuqorida aytib o'tilganidek, MBBT uchun axborot xavfsizligining uchta asosiy jihatlari – konfidensiallik, yaxlitlik va foydalanuvchanlik muhim hisoblanadi. Ma'lumotlar bazasini himoyalashning umumiy g'oyasi "Ishonchli kompyuter tizimlarini baholash mezonlari"da S2 xavfsizlik sinfi uchun ta'riflangan tavsiyalarga rioya qilishdan iborat. Umuman, ba'zi MBBTlar V1 sinfiga xos qo'shimchalar taklif etadi, ammo bunday qo'shimchalarni amalda qo'llash faqat tashkilot axborot strukturasining barcha komponentlari xavfsizlikning V kategoriyasiga ega bo'lgandagina ma'no kasb etadi. Bunga erishish texnik va moliya nuqtayi nazaridan murakkab. Undan tashqari quyidagi ikkita jihatni hisobga olish kerak. Birinchidan, aksariyat tijoriy tashkilotlar uchun xavfsizlikning S2 sinfi yetarli. Ikkinchidan, yaxshi himoyalangan versiyalar ma'nodorligi va imkoniyatlari bo'yicha oddiy "kasbdoshlar"idan orqada qoladi. Shuning sababli maxfiylik uchun kurashuvchilar aslida ma'naviy eskirgan (garchi sinchiklab tekshirilgan) mahsulotlardan foydalanishga majburlar.

Identifikatsiya va foydalanuvchilarning haqiqiyligini tekshirish.

Odatda, MBBTda foydalanuvchilarni identifikatsiyalash va ularni haqiqiyligini tekshirish uchun operatsion tizimning mos mexanizmlari, yoki SQL-CONNECT operatori qo'llaniladi. Masalan, *ORACLE* MBBT holida CONNECT operatori quyidagi ko'rinishga ega bo'ladi:

CONNECT foydalanuvchi [parol] [@ma'lumotlar_bazasi].

Har holda, ma'lumotlar bazasi serveri bilan ishlash seansining boshlanishi onida foydalanuvchi o'zining nomi bilan identifikatsiyalanadi, autentifikatsiya vositasi sifatida esa parol ishlatiladi. Ushbu jarayonning tafsilotlari ilovaning mijoz qismining amalga oshirilishi orqali aniqlanadi.

UNIX kabi ba'zi operatsion tizimlar dastur ishga tushirilishi vaqtida amaldagi foydalanuvchi identifikatorini o'zgartirishga imkon beradi. Ma'lumotlar bazasi bilan ishlovchi ilova odatda, oddiy foydalanuvchilar imtiyozlariga nisbatan ancha ortiqcha imtiyozlarga ega. Tabiiyki, bunda ilova puxtalik bilan o'ylangan, qat'iy belgilangan imkoniyatlar naborini taqdim etadi. Agar foydalanuvchi u yoki bu usul yordamida ilovani nihoyasiga yetkaza olsa, ammo ma'lumotlar bazasining serverga ulanishini asray olsa, u ma'lumotlar bilan har qanday harakatlarni bajarishi mumkin.

Foydalanishni boshqarish. Foydalanishni boshqarish bilan bog'liq masalalarni oydinlashtirish uchun *INGRES* MBBT ishlatiladi.

Odatda MBBTda foydalanishni ixtiyoriy boshqarish qo'llaniladi. Bunda obyekt egasi undan foydalanish huquqini (ko'pincha imtiyozini deb yuritishadi) o'z ixtiyoricha beradi. Imtiyozlar subyektlarga (alohida foydalanuvchilarga), guruhlarga, rollarga yoki barcha foydalanuvchilarga berilishi mumkin.

Rollar imtiyozlari foydalanuvchilar va guruhlar imtiyozlaridan ustun turadi. Boshqacha aytganda, subyekt sifatidagi foydalanuvchining ma'lum rolli ilovalar ishlov beruvchi obyektlardan foydalanish huquqiga ega bo'lishi shart emas. Ta'kidlash lozimki, *ORACLE* MBBTda rol deganda imtiyozlar nabori tushuniladi. Bunday rollar imtiyozlarni strukturalash vositasi sifatida xizmat qiladi va ularning modifikatsiyalanishini osonlashtiradi.

Barcha foydalanuvchilar majmui PUBLIC deb ataladi. PUBLICga imtiyozlar berilishi – foydalanishning ko'zda tutilgan

huquqlarini berishning qulay usuli. Turli foydalanuvchilar zimmasiga turli ma'lumotlar bazasini ma'murlashni yuklash ma'noga ega bo'ladi, qachonki ushbu bazalar mustaqil va ularga nisbatan imtiyozlarni ajratishning kelishilgan siyosatini yoki rezervli nusxalashni o'tkazishga to'g'ri kelmasa. Bu holda har bir ma'mur qancha zarur bo'lsa, shuncha biladi. Bir tomondan INGRES foydalanuvchisi va ma'lumot bazasi, ikkinchi tomondan operatsion tizim superfoydalanuvchi (OS UNIX holida root) va xizmatchi foydalanuvchilar (OS UNIXda bu-bin, Ip, IJUCP va h. bo'lishi mumkin) orasidagi o'xshashlikni kuzatish mumkin. Xizmatchi foydalanuvchilarning kiritilishi superfoydalanuvchi imtiyozlarini olmasdan funksional qismtizimlarni ma'murlashga imkon beradi. Xuddi shu tarzda serverda saqlanuvchi ma'lumotlarni bo'lmalarga ajratish mumkin. Bitta bo'lma ma'murining obro'sizlantirilishi, albatta boshqa bo'lma ma'murining obro'sizlantirilishi degani emas.

Imtiyoz turlari. MBBTda imtiyozlarni ikkita kategoriyaga ajratish mumkin: xavfsizlik imtiyozlari va foydalanish imtiyozlari.

Xavfsizlik imtiyozlari doim muayyan foydalanuvchiga uning yaratilishi (CREATE USER operatori yordamida) yoki xarakteristikalarini o'zgartirish (ALTER USER operatori yordamida) vaqtida ajratiladi. Bunday imtiyozlar beshta:

- security – MBBT xavfsizligini boshqarish va foydalanuvchi harakatlarini kuzatish huquqi. Foydalanuvchi ushbu imtiyoz bilan har qanday ma'lumotlar bazasiga ulanishi, foydalanuvchilar, guruhlar va rollar xarakteristikalarini yo'q qilishi va o'zgartirishi, ma'lumotlar bazasidan foydalanish huquqini boshqa foydalanuvchiga berishi, qayd qilinuvchi axborotning yozilishini boshqarishi, boshqa foydalanuvchilar so'rovini kuzatishi va nihoyat, boshqa foydalanuvchilar nomidan INGRES-komandalarni ishga tushirishi mumkin. Security imtiyozi ma'lumotlar bazasi serverining ma'muriga hamda axborot xavfsizligiga shaxsan javobgar shaxsga zarur. Ushbu imtiyozni boshqa foydalanuvchilarga berish (masalan, ma'lumotlar bazasi ma'muri tomonidan) ma'lumotlar bazasi serverining himoyasidagi bo'lishi mumkin bo'lgan zaif joylarni ko'paytiradi;
- createdb – ma'lumotlar bazasini yaratish va yo'q qilish huquqi. Ushbu imtiyozga server ma'muridan tashqari foyda-

lanuvchilar ega bo'lishlari lozim. Foydalanuvchilar ixtiyoriga alohida ma'lumotlar bazasining ma'murlari roli taqdim etiladi;

- operator – odatda operator ixtiyoridagi harakatlarni bajarish huquqi. Serverni ishga tushirish va to'xtatish, axborotni saqlash va tiklash ko'zda tutiladi. Ushbu imtiyozni server va ma'lumotlar bazasi ma'muridan tashqari operatsion tizim ma'muriga ham berish maqsadga muvofiq hisoblanadi;
- maintain locations – ma'lumotlar bazasi serveri ma'murining bazasi va operatsion tizim o'rnashgan joyni boshqarish huquqi;
- trace – sozlovchi trassirovka flaglari xolatlarini o'zgartirish huquqi. Ushbu imtiyoz murakkab, tushunarsiz vaziyatlarni tahlillashda ma'lumotlar bazasi serveri ma'muriga va boshqa tajribali foydalanuvchilarga foydali.

Xavfsizlik imtiyozlari ma'muriy harakatlar bajarishga imkon beradi.

Foydalanish imtiyozlari, nomiga muvofiq, subyektlarning ma'lum obyektlardan foydalanish huquqini belgilaydi va foydalanuvchilarga, guruhlarga, rollarga yoki barchaga GRANT operatori yordamida ajratiladi va REVOKE operatori yordamida olib qo'yiladi. Ushbu imtiyozlar odatda, mos obyekt egasi (ma'lumotlar bazasi ma'muri) yoki security imtiyoziga ega shaxs (odatda ma'lumotlar bazasi serveri) tomonidan beriladi.

Guruhlarga va rollarga imtiyozlarni berishdan oldin ularni CREATE GROUP va CREATE ROLE operatorlari yordamida yaratish lozim.

Guruh tarkibini o'zgartirish uchun ALTER GROUP operatori xizmat qiladi.

DROP GROUP operatori guruhlarni yo'q qilishga imkon beradi (faqat guruh a'zolari ro'yxati yo'q qilinganidan so'ng).

ALTER ROLE operatori rollar parollarini o'zgartirishga, DROP ROLE operatori esa rollarni yo'q qilishga xizmat qiladi.

Yuqorida aytib o'tilganidek, imtiyozlarning nomlangan eltuvchilarini yaratish va yo'q qilish hamda ularning xarakteristikalarini o'zgartirish, faqat security imtiyoziga ega foydalanuvchi tomonidan amalga oshirilishi mumkin. Bunday harakatlar amalga oshirilganda, tarkibida subyektlar va ularning imtiyozlari saqlanuvchi ma'lumotlar bazasiga ulanishga ega bo'lish lozim.

Foydalanish imtiyozlarini ular taalluqli obyektlar turi bo'yicha ajratish mumkin. INGRES MBBTda bunday turlar beshta:

- jadvallar va tasavvurlar;
- muolajalar;
- ma'lumotlar bazasi;
- ma'lumotlar bazasi serveri;
- hodisalar.

Foydalanish imtiyozlarini berish GRANT operatori yordamida amalga oshiriladi. GRANT operatori umumiy ko'rinishda quyidagi formatga ega:

- GRANT imtiyozlar;
- ON obyektlar;
- TO kimga.

Jadvallar va tasavvurlarga muvofiq quyidagi foydalanish huquqlarini boshqarish mumkin:

SELECT - ma'lumotlarni tanlash huquqi;

INSERT - ma'lumotlarni qo'shish huquqi;

DELETE - ma'lumotlarni yo'q qilish huquqi;

UPDATE - ma'lumotlarni yangilash huquqi (yangilanishga ruxsat bo'lgan ma'lum ustunlarni ko'rsatish mumkin);

REFERENCES - berilgan jadvalga (ma'lum ustunlarni ko'rsatish mumkin) havola qiluvchi tashqi kalitlardan foydalanish huquqi.

Odatda, foydalanuvchi jadvallardan va tasavvurlardan foydalanishning hech qanday huquqiga ega emas. Bu huquqlarni GRANT operatorlari yordamida berish mumkin.

Muolajalarga nisbatan bajarish huquqi berilishi mumkin. Bunda muolajalar ishlov beruvchi obyektlardan foydalanish huquqlarining ajratilishi xususida o'ylash kerak emas, ularning mavjudligi shart emas. Shunday qilib, ma'lumotlar bazasi muolajalari ma'lumotlar ustida qat'iy belgilangan harakatlarni bajarish uchun nazoratli foydalanishni taqdim etishning qulay vositasi hisoblanadi.

Ma'lumotlar bazasidan foydalanish huquqlarini uning ma'muri yoki security imtiyoziga ega foydalanuvchi taqdim etishi mumkin. Ushbu "huquqlar" aslida ma'lumotlar bazasidan foydalanishga qator cheklashlar o'rnatadi, ya'ni mohiyatan taqiqlovchi hisoblanadi. Kiritish/chiqarish amallar soniga yoki bitta so'rov bilan qaytariluvchi qator soniga cheklash, jadvallar va muolajalar va h. yaratish

huquqiga cheklash ko'zda tutiladi. Odatda foydalanuvchi miqdoriy limitlar bilan qoniqmaydi va bazada obyektlar yaratish huquqini oladi.

Ta'kidlash lozimki, ma'lumotlar bazasini yaratishda uning maqomi (umumiy yoki shaxsiy) ko'rsatiladi. Bu bazadan nazarda tutilgan foydalanish huquqiga ta'sir etadi. Odatda umumiy bazaga ulanish huquqi barchaga beriladi. Shaxsiy bazaga ulanish huquqi oshkora ravishda berilishi lozim. Ulanishga huquq baza va undagi obyektlar bilan boshqa barcha amallarni bajarish uchun kerak.

QUERY_IO_LIMIT va QUERY_ROW_LIMIT imtiyozlar (bu holda cheklashlar deb atash to'g'riroq bo'lar edi) so'rovlar optimizatori bergan baho asosida tekshiriladi. Agar optimizator oldindan so'rov kiritish/chiqarish amaliga yoki qaytariluvchi qatorga ajratilgan limit sonidan oshganini aytsa, so'rov rad etiladi. Bu xildagi miqdoriy cheklashlarning qo'yilishi serverning bitta mijoz tomonidan monopoliya qilinishiga to'sqinlik qiladi va yuqori tayyorlikni madadlash instrumentining biri sifatida ishlatilishi mumkin.

Oldin berilgan imtiyozlarni (ruxsat beruvchi va taqiqlovchi) bekor qilishda REVOKE operatori xizmat qiladi.

Foydalanishni boshqarishda tasavvurlardan foydalanish. MBBT foydalanishni boshqaruvchi o'ziga xos vosita – tasavvurlarni taqdim etadi. Tasavvurlar subyektlar uchun bazaviy jadvallarning ma'lum qatorlarining ko'rinarli bo'lishiga (proeksiyani amalga oshirishga) yoki ma'lum qatorlarni tanlashga (seleksiyani amalga oshirishga) imkon beradi. Ma'lumotlar bazasining ma'muri subyektlarga bazaviy jadvallardan foydalanish huquqini bermasdan va munosib tasavvurlarni tuzib, jadvallarni ruxsatsiz foydalanishdan himoyalaydi va har bir foydalanuvchini o'zining ma'lumotlar bazasiga qarashi bilan ta'minlaydi.

Quyida tarkibida dastlabki jadvalning ikkita ustuni bo'lgan va o'z ichiga faqat ustunlarni birining ma'lum qiymatli qatorini qamrab oluvchi tasavvumi yaratish misoli keltirilgan:

```
CREATE VIEW empview AS
SELECT name, dept
FROM employee
WHERE dept = 'shoe';
```

Ushbu tasavvurdan tanlash huquqi barchaga berilganida:

```
GRANT SELECT
ON empview
TO PUBLIC;
```

empview tasavvurdan foydalanishni amalga oshiruvchi subyektlar "shoe"dan farqlanuvchi bo'limlar xususidagi ma'lumotlami so'rashga intilishlari mumkin, masalan:

```
SELECT *
FROM empview
WHERE dept = 'toy';
```

ammo javob tariqasida foydalanish huquqlarining buzilganligini ko'rsatuvchi javob kodini emas, balki oddiygina nulli qatorli natijani oladilar. Bu juda muhim, chunki niyati buzuqni bo'limlar ro'yxatini javob kodlarini tahlillash orqali bilvosita tarzda olish imkoniyatidan mahrum etadi.

Foydalanish huquqlarining ierarxiyasi. GRANT operatori va MBBTdan foydalanishni boshqaruvchi boshqa vositalar foydalanishning quyidagi cheklashlar turini amalga oshirishga imkon beradi:

- amaliy cheklashlar (jadvalning barcha yoki faqat ba'zi ustunlariga qo'llaniluvchi SELECT, INSERT, UPDATE, DELETE foydalanish huquqlari hisobiga);
- muhimligi bo'yicha cheklashlar (tasavvurlar mexanizmi hisobiga);
- resurslarga cheklashlar (ma'lumotlar bazasidan foydalanish imtiyozlari bo'yicha).

So'rovlarni ishlashda MBBT avval obyektlardan foydalanish huquqini tekshiradi. Agar amaliy cheklashlar buzilgan bo'lsa, so'rov mos tashxis chiqarilib, rad etiladi. Muhimligi bo'yicha cheklashlarning buzilishi faqat natijaviy qatorlarning soniga ta'sir etadi, bunda hech qanday tashhis chiqarilmaydi. Nihoyat, oldingi ikkita cheklashlar hisobga olinganidan so'ng, so'rov ishlanish uchun optimizatorga beriladi. Agar optimizator resurslarga cheklashlar oshirilganini aniqlasa, so'rov mos tashhis chiqarilib, rad etiladi.

Imtiyozlar ierarxiyasiga boshqa nuqtayi nazardan qarash mumkin. Har bir foydalanuvchi o'zinikidan tashqari PUBLIC imtiyoziga ega. Undan tashqari, u turli guruhlarda bo'lib, ma'lum rollar bilan ilovalarni ishga tushirishi mumkin. Quyida imtiyozlarning

nomlangan turli eltuvchilari taqdim etgan huquqlarning o'zaro munosabati xususida so'z ketadi.

INGRES MBBT uchun avtorizatsiya ierarxiyasi quyidagi ko'rinishga ega:

- rol (yuqori ustuvorlik);
- foydalanuvchi;
- guruh;
- PUBLIC (past ustuvorlik).

Har bir foydalanuvchi obyekt uchun INGRES foydalanishning so'raluvchi turiga (SELECT, EXECUTE va h.) tegishli ierarxiyadagi imtiyozni qidirishga urinadi. Masalan, yangilash maqsadida jadvaldan foydalanishga urinishda INGRES rolning, foydalanuvchining, guruhning va barcha foydalanuvchilarning imtiyozlarini tekshiradi. Agar ierarxiyaning bitta sathida UPDATE imtiyozi bo'lsa ham, so'rov keyingi ishlash uchun uzatiladi. Aks holda, so'rovni rad etishni ko'zda tutuvchi foydalanish huquqi ishlatiladi.

Resurslarga cheklashlarning batafsil talqinini ko'raylik. Aytaylik, ierarxiyaning barcha to'rtta sathida so'rovning natijaviy qatori soniga cheklashlar tasniflangan (QUERY_ROW_LIMIT imtiyozi):

- rol – 1700;
- foydalanuvchi – 1500;
- guruh – 2000;
- PUBLIC – 1000.

Agar foydalanuvchi MBBT bilan ishlash seansining boshlanishida rolni va guruhni bergan bo'lsa, rol yuklagan cheklash 1700 ishlatiladi. Agar QUERY_ROW_LIMIT imtiyozi rol uchun mavjud bo'lmasa yoki foydalanuvchi ish seansi boshlanishida rolni bermagan bo'lsa, foydalanuvchi 1500dan ko'p bo'lmagan qatordan natijalarni olishi mumkin va h. Agar QUERY_ROW_LIMIT imtiyozi ierarxiyaning birorta bir sathida tasniflangan bo'lmasa, MBBT nazarda tutilgan qiymatdan foydalanadi. Nazarda tutilgan qiymat deganda natijaviy qator soniga cheklashlarning yo'qligi tushuniladi.

Odatda ishlatiluvchi rol va guruh mos holda ilovani ishga tushiruvchi komanda qatorining -R va -G – opsiyalarning argumentlari sifatida beriladi. Misol:

QBF -Gaccounting company_db

Agar G- opsiya mavjud bo'lmasa, foydalanuvchining nazarda tutuvchi guruhi (agar u mavjud bo'lsa) ishlatiladi.

Nihoyat, agar sql komanda qatorida –u foydalanuvchi opsiya berilgan bo'lsa, tekshiruvchilar qatoriga ko'rsatilgan foydalanuvchi ham kiradi.

Xavfsizlik belgilari va foydalanishni majburiy nazoratlash. Yuqorida xavfsizlikning S sathiga xos foydalanishni ixtiyoriy boshqarish vositalari tavsiflangan edi. Ma'lumki, ular umuman aksariyat tijoriy ilovalarga yetarli. Shunday bo'lsa-da, ular bitta juda muhim masalani – axborot uzatilishini kuzatish masalasini yechmaydi. Foydalanishni ixtiyoriy boshqarish vositalari avtorizatsiyalangan foydalanuvchiga maxfiy axborotni qonuniy tarzda olishga va so'ngra undan boshqa avtorizatsiyalanmagan foydalanuvchilarning foydalanishlariga xalaqit bermaydi. Chunki foydalanishni ixtiyoriy boshqarishda imtiyozlar ma'lumotlardan alohida joylashadi (relyatsion MBBTlarda esa relyatsion jadvallar qatoridan alohida joylashadi). Natijada ma'lumotlar "egasiz qoladi" va ularning kimga bo'lsa ham uzatilishiga hech nima xalaqit bermaydi (hatto MBBT vositalari ham).

Xavfsizlik sathi tizimi Bga muvofiq "Ishonchli kompyuter tizimlarini baholash mezonlari"da INGRES/Enhanced Security (xavfsizligi oshirilgan INGRES) versiyada amalga oshirilgan xavfsizlik belgilari mexanizmi tavsiflangan. Ushbu versiyani amalda qo'llash faqat operatsion tizim va xavfsizlik B sathiga ega boshqa dasturiy komponentlar bilan birgalikda amalga oshirilganida ma'noga ega bo'ladi. Shunday bo'lsa ham, INGRES MBBTda belgili xavfsizlikning amalga oshirilishini ko'rish, bilish nuqtayi nazaridan qiziqarli, ma'lumotlarni maxfiylik sathlari va foydalanish kategoriyalariga ajratishga asoslangan yondashishning o'zi esa, ko'pgina foydalanuvchilarning ma'lumotlarning katta massivlariga nisbatan imtiyozlari tizimini loyihalashda foydali bo'lishi mumkin.

INGRES/Enhanced Security MBBTda har bir relyatsion jadvalga yashirincha jadval qatori xavfsizligi belgisi bo'lgan ustun qo'shiladi. Xavfsizlik belgisi uchta komponentdan iborat:

Maxfiylik sathi. Ushbu komponentning mazmuni ilovaga bog'liq. Xususan, sathlarning an'anaviy spektri "mutlaqo maxfiy"dan "maxfiy emas"gacha bo'lishi mumkin.

Kategoriyalar. Kategoriya tushunchasi ma'lumotlarni "bo'lmalar"ga ajratishga va natijada xavfsizlik tizimi ishonchliligini oshirishga imkon beradi. Tijoriy ilovalarda kategoriya sifatida "moliyalar", "kadrlar", "moddiy boyliklar" va h. xizmat qilishi mumkin.

Hududlar. Axborotni bo'lmalarga ajratishda qo'shimcha vosita hisoblanadi. Amalda "hudud" komponenti, haqiqatan geografik mazmunga (masalan, ma'lumot taalluqli mamlakatga) ega bo'lishi mumkin.

INGRES/Enhanced Security MBBTining har bir foydalanuvchisi ishonchlilik darajasi orqali xarakterlanadi. Ishonchlililk darajasi foydalanuvchiga berilgan xavfsizlik belgisi orqali ham aniqlanadi. Foydalanuvchi, agar uning ishonchlilik darajasi mos xavfsizlik belgisi talablarini qondirsa, ma'lumotlardan foydalanishi mumkin, yanada aniqrog'i:

- foydalanuvchining maxfiylik sathi ma'lumotlarning maxfiylik sathidan past bo'lmasligi shart;
- ma'lumotlar xavfsizligi belgisidagi kategoriyalar nabori butunlay foydalanuvchi xavfsizligi belgisida bo'lishi shart;
- foydalanuvchi xavfsizligi belgisidagi hududlar nabori butunlay ma'lumotlar xavfsizligi belgisida bo'lishi shart.

Maxsus imtiyoz DOWNGRADE ma'lumotlar bilan assotsiatsiyalangan xavfsizlik belgisini o'zgartirishga imkon beradi. Bunday imkoniyat, masalan, u yoki bu sabab bilan noto'g'ri bo'lib qolgan belgilarni tuzatish uchun zarur.

Tabiiyki, INGRES/Enhanced Security MBBTi relyatsion jadvallarga xavfsizlik belgisini nafaqat yashirincha, balki ochiq holda kiritishga yo'l qo'yadi. Mos taqqoslash amallarini madadlovchi ma'lumotlarning yangi turi security label paydo bo'ladi.

INGRES/Enhanced Security – xavfsizlikning V sinfiga sertifikat (attestatsiyaga ekvivalent) olgan birinchi MBBT hisoblanadi. Ehtimol, xavfsizlik belgilari asta-sekin ma'lumotlar bazasini boshqarish tizimining standart repertuariga kiradi.

MBBTda ma'lumotlar yaxlitliligini madadlash. Tijoriy tashkilotlar uchun ma'lumotlar yaxlitligini ta'minlashning konfidensiallikni ta'minlashga nisbatan muhimligi kam emas. Shubhasiz, mijozlarning hisob raqamidagi mablag'ni mo'ralab ko'rish ko'ngilsiz hodisa hisoblanadi. Hisob raqamidan hisob raqamiga pul o'tka-

zishda mablag'ning noma'lum yo'nalishda yo'qolishi esa undan battar noxush hodisa hisoblanadi.

Ma'lumki, ma'lumotlar bazasining asosiy dushmani tashqaridagi niyati buzuq emas, balki uskunaning, ma'murlarning, tatbiqiy dasturlarning va foydalanuvchilarning yanglishishi.

MBBTi foydalanuvchisi nuqtayi nazaridan ma'lumotlar yaxlitligini madadlashning asosiy vositalari cheklashlar va qoidalar hisoblanadi.

Cheklashlar. Cheklashlar jadvallarga yoki alohida ustunlarga taalluqli bo'lishi mumkin. Ustunlarga cheklashlar CREATE TABLE operatorida jadvalni yaratishda beriladi.

Jadval cheklashlari ustunlar guruhiga taalluqli va jadval yaratishda, yoki kechroq, ALTER TABLE operatori yordamida berilishi mumkin.

Quyidagi misol tarkibida ikkita ustundagi qiymatlarni bog'lovchi nomlangan cheklashlar mavjud:

```
CREATE TABLE dept (
dname char (10),
budget money,
expenses money,
CONSTRAINT check_amount CHECK (budget > 0 and expenses <= budget)
);
```

{Byudjet ijobiy bo'lishi shart, xarajatlar esa byudjet doirasidan chiqmasligi shart}

Havolali cheklashlar jadvallar orasidagi aloqaning yaxlitligiga javob beradi. Bunday cheklashning talabiga binoan bitta har bir qiymatga boshqa jadvaldagi roppa-rosa bitta qiymat mos kelishi lozim. Bunday qiymatlar relyatsion modeldagi jadvallar orasida havola rolini o'ynaydi.

Havolali cheklashga misol:

```
CREATE TABLE emp (
ename char (10),
edept char (10) references dept(dname)
);
```

{Birorta ham xizmatchi noma'lum bo'limda hisoblanmasligi shart}

Cheklashlarning barcha turlari jadval egasi tomonidan yuklanadi va keyingi ma'lumotlar bilan amallar natijasiga ta'sir qiladi. SQL-operatorning bajarilishi tugashidan avval mavjud cheklashlar tekshiriladi. Buzilishlar aniqlanganida MBBT nonormal tugallanish xususida xabar beradi va operator kiritgan o'zgarishlarni bekor qiladi.

Ta'kidlash lozimki, havolali cheklashni yuklash uchun havola qilinayotgan jadvalga nisbatan REFERENCES imtiyoziga ega bo'lish lozim (yuqoridagi misoldagi dept).

Cheklashlarni nafaqat yuklash, balki bekor qilish mumkin. Bunda cheklashlar orasida bog'lanishlar bo'lishi mumkin va ulardan birining bekor qilinishi boshqa (havolali) cheklashlarning yo'q qilinishini talab qilishi mumkin.

Quyidagi misolni ko'raylik:

```
CREATE TABLE dept (
name char(10) NOT NULL,
location char(20),
CONSTRAINT dept_unique UNIQUE(name)
);
CREATE TABLE emp (
name char(10),
salary decimal(10,2),
edept char(10) CONSTRAINT empref REFERENCES dept(name)
);
```

Agar dept_unique cheklashni yo'q qilish talab qilinsa, quyidagi operatordan foydalanish mumkin:

```
ALTER TABLE dept
DROP CONSTRAINT dept_unique cascade;
```

cascade so'zi dept_unique bilan bevosita yoki bilvosita bog'liq barcha cheklashlar yo'q qilinishini bildiradi. Ushbu holda empref cheklash olib tashlanadi. Agar cascade o'rniga restrict ko'rsatilsa, ya'ni faqat dept_unique cheklashni yo'q qilishga urinilsa, MBBT xatolikni qaydlaydi.

INGRES MBBTda cheklashlarni nazoratlash bilan ishlash samaradorligini murosaga keltirishga uriniladi. Ma'lumotlarni ommaviy nusxalashda cheklashlarni nazoratlash o'chirib qo'yiladi.

Bu degani, nusxalashni yaxlitlikni tekshirishning global muolajasini ishga tushirish bilan to'ldirish lozim.

Qoidalar. Qoidalar ma'lumotlar bazasidagi ma'lum o'zgarishlar bo'lganida berilgan harakatlarni bajarilishini chaqirishga imkon beradi. Odatda, harakat – muolajani chaqirish. Qoidalar jadvallar bilan assotsiatsiyalanadi va ushbu jadvallar o'zgarganida ishga tushadi.

Qoidalar faqat nisbatan oddiy shartlarni nazoratlash vositalari hisoblanuvchi cheklashlardan farqli holda, bazadagi ma'lumotlar elementlari orasidagi xohlagancha murakkab o'zaro bog'lanishni tekshirishga va madadlashga imkon beradi. Cheklashlar holidagiga o'xshab qoidalarni tekshirish nusxalashning ommaviy amallarida to'xtatiladi. Ma'lumotlar bazasi ma'muri ham SET NOROLES operatoridan foydalanib, qoidalarni tekshirishni oshkora to'xtatishi mumkin. SETRULES operatori qoidalar mexanizmi ishini tiklashi mumkin. Odatda ushbu mexanizm ulangan bo'ladi.

Qoidalarni yo'q qilish DROP RULE qoida operatori orqali amalga oshiriladi. Mos jadval yo'q qilingan holda MBBT avtomatik tarzda qoidalarning yo'q qilinishini ta'minlaydi. Shu tariqa jadvallar va qoidalar yaxlitligi ta'minlanadi.

Axborot xavfsizligi nuqtayi nazaridan ta'kidlash lozimki, jadval bilan assotsatsiyalangan qoidani mos muolajalarni bajarish huquqini ushbu jadval egasi yaratishi mumkin. Harakati qoidani ishlashiga sabab bo'luvchi foydalanuvchi faqat jadvaldan foydalanishning kerakli huquqlariga ega bo'lishi shart. Shu tariqa qoidalar oshkora bo'lmagan holda foydalanuvchilar imtiyozlarini kengaytiradi. Bunday kengayishlar qat'iy ma'muriy nazoratga ehtiyoj sezadi, chunki xatto qoidaning yoki assotsatsiyalangan muolajaning biroz o'zgarishi ma'lumotlar himoyalanganligiga tubdan ta'sir etishi mumkin. Qoidalarning murakkab tizimidagi xatolik esa bashorat qilib bo'lmaydigan oqibatlarga sabab bo'ladi.

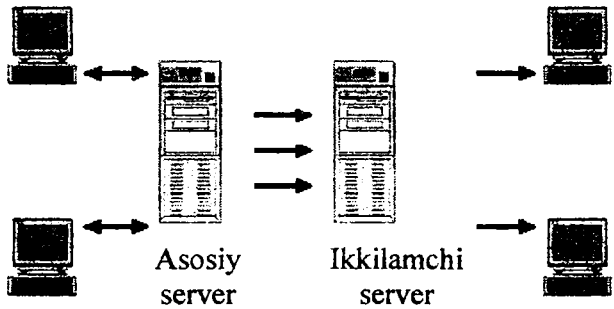
Yuqori tayyorlikni madadlash vositalari. Tijoriy ilovalarda apparat-dasturiy komplekslarning yuqori tayyorligi muhim omil hisoblanadi. MBBTga muvofiq yuqori tayyorlikni madadlovchi vositalar apparat, ayniqsa disklarga tegishli buzilishlarni neytrallashni hamda xizmatchi xodim yoki tatbiqiy dastur xatoliklarini tiklashni ta'minlashi lozim.

Bunday vositalar boshidayoq kompleks arxitekturasiga o'rnatilishi shart. Masalan, ortiqcha disk massivlarining u yoki bu turidan foydalanish kerak. Albatta, apparat-dasturiy yechim qimmatlashadi, ammo ekspluatatsiya vaqtida bo'lishi mumkin bo'lgan zarardan asraydi.

Ma'lumotlar bazasi serverining klaster tashkil etilishi. Odatda klaster tarkibida uzellar-kompyuterlar tomonidan birgalikda ishlatiluvchi bir necha diskli qismtizim va komponentlar orasidagi ortiqcha bog'lanishlar bo'ladi. Tashqi nuqtayi nazaridan klaster bir butun kabi ko'rinadi, bir necha uzellarning mavjudligi esa unumdorlikning va buzilishlarga barqarorlikning oshishiga sabab bo'ladi.

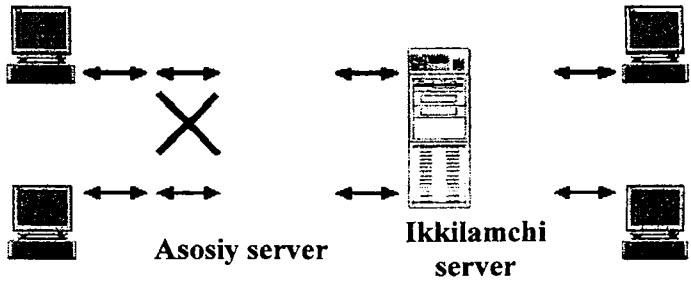
Ma'lumotlarni tirajlash. Axborot xavfsizligi nuqtayi nazaridan tirajlashga ma'lumotlarning foydalanuvchanligini oshirish vositasi sifatida qarash mumkin. San-Fransisko shahridagi baqqol xususidagi hikoya afsona bo'lib qoldi. Baqqol halokatli yer qimirlashidan so'ng boshqa shahardan oldinroq tirajlangan axborotni olib, bazasini 16 daqiqada tikladi.

INGRES MBBT tirajlashning rivojlangan imkoniyatini taqdim etadi. Informix OnLine-DS 7.1da ma'lumotlarni asosiy serverdan to'laligicha ikkilamchi serverga akslantirishdan iborat tirajlash modeli madadlanadi.



5.1-rasm. Asosiy serverga yozish va undan o'qish mumkin, ikkilamchi serverdan faqat o'qiladi.

Tirajlashli Informix OnLine-DS serverlarining konfiguratsiyasida bitta asosiy va qator ikkilamchi serverlar ajratiladi. Asosiy serverda o'qish va ma'lumotlarni yangilash amalga oshiriladi, barcha o'zgarishlar esa ikkilamchi serverlarga uzatiladi. Ikkilamchi serverlardan faqat o'qish mumkin (5.1-rasm). Asosiy server buzilganida, ikkilamchi server avtomatik ravishda yoki qo'lda o'qish va yozish rejimiga o'tkaziladi (5.2-rasm). Asosiy server buzilganida, mijozlarni ochiq-oydin qayta yo'naltirish madadlanmaydi, ammo u ilovalar doirasida amalga oshirilishi mumkin.



5.2-rasm. Asosiy server buzilganida, ikkilamchi server o'qish va yozish rejimiga o'tkaziladi.

Asosiy server tiklanganidan so'ng ushbu server ikkilamchi serverga aylanishi mumkin, endi o'qish-yozish rejimida ishlovchi avvalgi ikkilamchi serverga asosiy server maqomi beriladi va unga ulangan mijozlar ishlarini davom ettiradilar. Shu tariqa ma'lumotlardan uzluksiz foydalanish ta'minlanadi.

Tirajlash axborotni tranzaksiya jurnalidan (mantiqiy jurnaldan) asosiy serverning tirajlash buferiga uzatish yo'li bilan amalga oshiriladi. Undan axborot ikkilamchi serverning tirajlash buferiga o'tkaziladi. Bunday o'tkazish sinxron yoki asinxron rejimida sodir bo'lishi mumkin. Sinxron rejim ma'lumotlar bazasining to'liq muvofiqligini kafolatlaydi, ya'ni asosiy serverda qaydlangan birorta ham tranzaksiya, xatto asosiy server yanglishganida ham ikkilamchi serverda qaydlanmay qolmaydi. Asinxron rejim mutlaqo muvo-

fiqlikni ta'minlamaydi, ammo tizimning ishchi xarakteristikalarini yaxshilaydi.

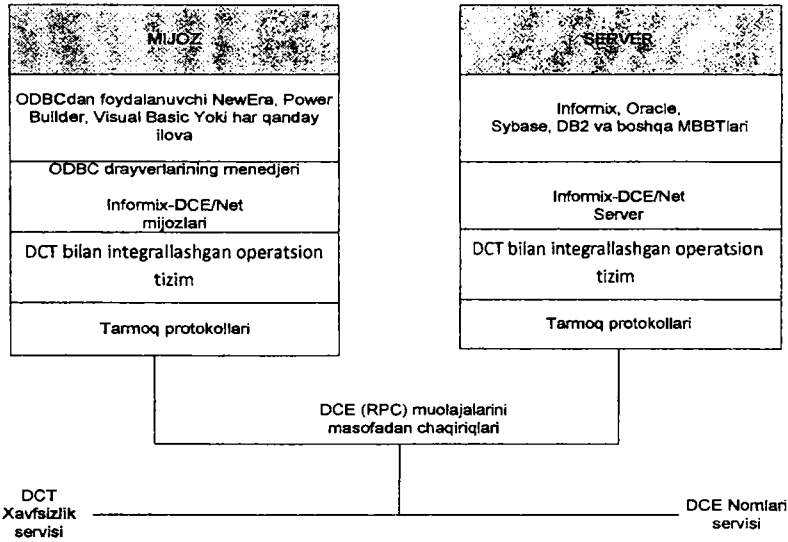
Tirajlashning qo'shimcha ijobiy samarasi - qaror qabul qilishni madadlovchi katta hajmli resursli ilovalarni, asosan, ikkilamchi serverga o'tkazish imkoniyati. Bu holda ular parallel ishlash vositalaridan maksimal foydalanib, asosiy serverda to'plangan tranzaksiyalarni operativ ishlovchi ilovalarga xalaqit qilmasdan, ishlanishi mumkin. Bunga ma'lumotlarning foydalanuvchanligini oshiruvchi omil sifatida ham qarash mumkin.

Server va mijozlar orasidagi kommunikatsiyalarni himoyalash. Server va mijozlar orasidagi kommunikatsiyalarni himoyalash muammosi nafaqat MBBTlarga, balki barcha taqsimlangan tizimlarga taalluqli. Tabiiyki, bu yerda, masalan, OSF konsernining taqsimlangan hisoblash muhitidagi (Distributed Computing Environment, DCE) kabi umumiy yechimlar qidiriladi. MBBT ishlab chiqaruvchilariga o'zining dasturiy mahsulotlarini ushbu muhitga "yuklash" qoladi (masalan, Informix kompaniyasi Informix-DCE/Netni amalga oshirib, shu ishni bajardi).

Informix-DCE/Net Informixning barcha instrumental vositalari hamda har qanday ilovalar yoki ODBC interfeysidan foydalanuvchi mustaqil ta'minotchilardagi instrumental komplekslari uchun DCE serverlaridan foydalanishni tashkil etadi (5.3-rasm).

Xavfsizlik serveri DCE muhitida mijoz-serverning o'zaro aloqalarini amalga oshirishdagi muhim komponent hisoblanadi. Ushbu server taqdim etadigan asosiy funksiyalar – Kerberos vositalari amalga oshiruvchi autentifikatsiya, avtorizatsiya (vakolatlarni tekshirish) va shifrlash. Masalan, mijoz-serverning har bir ilovasi uchun ma'mur himoyaning quyidagi beshta sathidan birini berishi mumkin:

- faqat mijozning server bilan ulanganligi aniqlanganidagina uzatiluvchi ma'lumotlar himoyalanadi;



5.3-rasm. Informix-DCE/Netdan foydalanuvchi mijoz-server muhitining tatbiqiy yoki instrumental konfiguratsiyasi.

- server ilk bor so'rovni olganida, faqat muolajani masofadan chaqirishning boshlang'ich bosqichida ma'lumotlar himoyalanadi;
- ma'lumotlar manbaining haqiqiyligini tasdiqlash. Serverga qabul qilinuvchi barcha ma'lumotlarning ma'lum mijozdan ekanligi tekshiriladi;
- ma'lumotlar manbai va yaxlitligini tasdiqlash. Jo'natilgan ma'lumotlarning o'zgartirilmaganligi tekshiriladi;
- ma'lumotlar manbai, yaxlitligi va konfidensialligini tasdiqlash. Oldingi sathda ko'zda tutilgan tekshirishlar bajariladi va barcha jo'natilgan ma'lumotlar shifrlanadi.

Informix-DCE/Net madadlagan autentifikatsiya servisi DCE taqsimlangan muhit xavfsizligi xarakteristikalarini yaxshilaydi, o'sha vaqtda foydalanuvchilar va ma'murlar faoliyati soddalashadi. Ushbu muhitga joylashtirilgan har qanday ma'lumotlar bazasiga murojaat etish uchun yagona kirish nomiga va DCE uchun parolga ega bo'lish kifoya. Ilova ishga tushirilganda Informix-DCE/Net

DCEdan foydalanuvchining autentifikatsiya axborotini so'raydi va uni istalgan bazaga ulaydi.

Ma'lumotlar bazasidan va ilovalardan foydalanishning kirish nomi va huquqini ma'murlashning yagona nuqtasining mavjudligi xavfsizlikning umumiy vaziyatini tartibga solishga imkon beradi. Masalan, agar DCEning kirish nomi yo'q qilinsa, ushbu foydalanuvchi tizimli resurslarning birortasidan ham foydalana olmaydi.

Nazorat savollari

1. Ma'lumotlar bazasi xavfsizligi qismtizimining arxitekturasi qanday mexanizmlarni o'z ichiga oladi?
2. MBBTda imtiyozlarning qanday turlari mavjud?
3. Foydalanishni boshqarishda tasavvurlardan foydalanishni tushuntiring.
4. Foydalanish huquqlarining ierarxiyasi.
5. Xavfsizlik belgilari va foydalanishni majburiy nazoratlash.
6. Xavfsizlik belgisining komponentlarini tushuntiring.
7. Ma'lumotlar bazasi serverini klaster tashkil etilishini tushuntiring.
8. Ma'lumotlarni tirajlash nima?
9. Server va mijozlar orasidagi kommunikatsiyalarni himoyalash.

5.2. Ma'lumotlar bazasini boshqarish tizimlarining himoya profillari

MBBT, operatsion tizimlari kabi, tarkibida xavfsizlik servislarining kombinatsiyasi mavjud, ammo operatsion tizimdan farqli holda o'z ehtiyojini qoplay olmaydi. MBBT operatsion tizim mexanizmlari va funksiyalaridan foydalanadi. Bunday ikki sathlik o'ziga hos tahdidlarning paydo bo'lishiga olib keladi va mos qarshi harakat vositalarining jalb qilinishini talab etadi. Masalan, ma'lumotlar bazasi operatsion tizimi tomonidan boshqariluvchi fayllarda yoki disklarda joylashadi, demak, ma'lumotlar bazasiga MBBTning shtat vositalari yoki operatsion tizim mexanizmlari yordamida murojaat etib, fayldan yoki qurilmadan foydalanish mumkin. Bunday imko-

niyatlar MBBT himoyasi profilida (uning prototipi "To'q sariq kitob" ning S2 xavfsizlik sinfiga mos keladi) hisobga olinishi shart. Bu yerda autentifikatsiya tushunchasi kiritiladi va u MBBT uchun foydalanuvchi identifikatorining haqiqiyligini tasdiqlovchi mexanizmni taqdim etadi. Yuqorida tilga olingan ikki sathlikning yana bir ko'rinishi – bazaviy konfiguratsiya xavfsizligi faraz qilinadi, ya'ni bazaviy tizim (operatsion tizim va/yoki xavfsizlikning tarmoq servislari, va/yoki maxsus dasturiy ta'minot) o'rnatilgan, konfiguratsiyalangan va xavfsiz boshqariladi.

Bazaviy tizim MBBT bilan bog'liq barcha fayllarni ruxsatsiz foydalanishdan himoyalashga imkon beruvchi foydalanishni boshqarish mexanizmlarini ta'minlashning lozimligini ko'zda tutuvchi xavfsizlik maqsadlari ham ushbu yo'nalishga taalluqli. Undan tashqari, operatsion tizim xavfsizlik funksiyalarini yakkalash va MBBT jarayonlarini himoyalash uchun vositalarni taqdim etadi. Aytish mumkinki, boshqarish va yakkalash nafaqat bazaviy operatsion tizim vositalari tomonidan, balki MBBT komponentlarini tarmoq uzellari bo'yicha tarqatish va tarmoqlararo ekranlardan foydalanish yo'li bilan ham arxitekturaviy madadlanishi mumkin.

Xavfsizlikning funksional talablariga kelsak, xavfsizlik funksiyalari (FPT_TDC) orasida ma'lumotlarning hamda xavfsizlik funksiyalarining taqsimlangan MBBT (FPT_TRC) doirasida takrorlanishdagi ma'lumotlarning muvofiqligiga qo'yiladigan talablarning muhimliligа ishora qilish mumkin. Muvofiqlikka taqsimlangan tranzaksiyalarni ishlashning qandaydir shakli yordamida yoki sinxronlashning qandaydir protokolini qo'llab, takrorlanuvchi ma'lumotlarni yangilash yo'li bilan erishish mumkin.

Foydalanuvchanlikka hujumdan himoyalash uchun himoya profilida foydalanuvchilarga ajratiladigan kvotalarning (FPU-RSA.1) amalga oshirilishi hamda parallel seanslarga (FTA_MCS.1) bazaviy cheklashlar ko'zda tutilgan.

Zamonaviy MBBT xususiyatini, xususan, tranzaksiyalar mexanizmi tomonidan amalga oshiriluvchi ma'lumotlarning dinamik yaxlitligini ta'minlash talabini hisobga olish zarur. Xavfsiz tiklash talablari haddan tashqari umumiy xarakterga ega. Tarmoq muhitidagi standart tahdidlardan himoyalash butunlay bazaviy tizim zimmasiga yuklatilgan.

"Ma'lumotlar bazasini boshqarish tizimining himoya profili" ("Database Management System Protection Profile") ma'lumotlar bazasida saqlanuvchi axborot konfidensialligini, yaxlitligini va foydalanuvchanligini himoyalash uchun talablar mavjud tashkilotlardagi ma'lumotlar bazasini boshqarish tizimi uchun xavfsizlik talablarini belgilaydi. Bunday axborotni fosh etish, modifikatsiyalash yoki xizmat qilishdan voz kechishga undash tashkilot faoliyatiga yomon ta'sir etishi mumkin. Ushbu himoya profili quyidagilarni belgilaydi:

- *asosiy talablar majmuini.* Himoya profiliga mos barcha ma'lumotlar bazasi ushbu talablarni qondirishi shart;
- *autentifikatsiya paketlari* majmuini (bir yoki undan ko'p bunday paketlar himoya profiliga mos ma'lumotlar bazasida ta'minlanishi shart).

Ushbu tizimlar ma'muri quyidagi imkoniyatlarga ega:

- tizim doirasida oxirgi foydalanuvchilar huquqlarining buzilishini bartaraf etish maqsadida ular harakatini boshqarish va doimo nazoratlash;
- yakka foydalanuvchilar tomonidan resursdan foydalanishni boshqarish va foydalanuvchilar harakatini hisobga olish.

Autentifikatsiya paketlari foydalanuvchining haqiqiy ekanligini tasdiqlash uchun vositalar taqdim etadi:

- operatsion tizimda autentifikatsiya (foydalanuvchi xost operatsion tizimida autentifikatsiyalangan va ma'lumotlar bazasida identifikatsiyalangan);
- ma'lumotlar bazasida autentifikatsiya (foydalanuvchi MBBTda identifikatsiyalangan va autentifikatsiyalangan).

Ushbu profilning kelgusi nashrlarida autentifikatsiya paketlari ro'yxatining kengayishi mumkinligini (masalan, autentifikatsiyaga asoslangan katalogni kiritish uchun) ta'minlash maqsadida asosiy talablar va autentifikatsiya paketlarini bir-biridan ajratish qabul qilingan.

Xavfsizlik bo'yicha topshiriqning ushbu himoya profiliga mosligini arz qilish uchun autentifikatsiya paketi o'rnatilishi lozim. Himoya profiliga moslik arzlarini "MBBT operatsion tizim vositalari yordamida autentifikatsiyalash rejimida yoki "MBBT

operatsion tizim vositalari va ma'lumotlar bazasi vositalari yordamida autentifikatsiyalash rejimida" aniqlashi lozim.

MBBT himoyasining profili aktivlarga xavf-xatarning o'rtacha darajali qandaydir umumlashgan muhiti uchun belgilangan. Ishonchlikka talablar va funksiyalarning minimal barqarorligi xavf-xatarning ushbu darajasiga muvofiq tanlangan.

Odatda, MBBT ma'lumotlar bazasidan ko'pgina foydalanuvchilarning bir vaqtda foydalanishlarini ta'minlash uchun ishlatiladi.

MBBT turli usullar orqali konfiguratsiyalanishi mumkin:

- ma'lumotlar bazasidan yakka foydalanishli *avtonom tizim* (masalan, alohida foydalanuvchining shaxsiy kompyuterda ishlashiga asoslangan ilova);

- *markaziy mashina (masalan, meynfreym) bilan bog'langan terminallarda* ishlovchi ma'lumotlar bazasidan ko'pchilik foydalanuvchi;

- *markaziy server bilan bog'lanishni madadlovchi intellektual ishchi stansiyalar tarmog'i* ("mijoz-server" arxitektura);

- o'z navbatida MBBT bilan bog'langan, *server ilovasi bilan bog'lanishni madadlovchi intellektual mijoz ishchi stansiyalari tarmog'i* (masalan, MBBT yordamida dinamik sahifalami shakllantiruvchi Web-server bilan bog'lanishni madadlovchi Web-brauzer).

Yuqorida tilga olingan konfiguratsiyalarning har birida ma'lumotlarning o'zi doimo bitta serverda bo'lishi yoki ko'pgina mustaqil serverlar orasida taqsimlanishi mumkin.

MBBT pastki bazaviy tizim (xostning va/yoki tarmoq servislarining operatsion tizimi va/yoki maxsus buyurtirilgan dasturiy ta'minot) funksiyalarini ishlatuvchi ilova va muayyan tizimning axborot texnologiyasi komponenti hisoblanadi.

MBBT ilovasi tarkibida bajariluvchi bir nechta yuklama modullari yoki ma'lumotlarning bir necha fayllari bo'lishi mumkin. Ular har qanday boshqa asosiy tizim jarayonlari va fayllar kabi asosiy tizim huquqlarining ma'murlanishiga bo'ysundiriladi.

MBBT bazaviy tizim xavfsizligini ta'minlovchi vositalarning funksional imkoniyatlarini kengaytirishi mumkin. Masalan, ma'lumotlar bazasi imtiyozlarining tarmoqlangan mexanizmining operatsion tizimga qaraganda ancha yaxshisini amalga oshirishi mumkin.

Autentifikatsiya paketi ma'lumotlar bazasi uchun foydalanuvchining ma'lum qilgan identifikatorining haqiqiyligini tasdiqlovchi mexanizmni taqdim etadi. Ushbu himoya profili doirasida bu quyidagi ikkita mexanizm yordamida ta'minlanishi mumkin:

Tashqi – xost operatsion tizim yordamida (operatsion tizim vositalari orqali autentifikatsiya). Autentifikatsiyaning ushbu sxemasida ma'lumotlar bazasi foydalanuvchisini identifikatsiyalash va autentifikatsiyalashda xostning operatsion tizimiga ishoniladi. Xostning operatsion tizimi ma'lumotlar bazasidagi foydalanuvchining haqiqiyligini tasdiqlashni ta'minlaydi. Ma'lumotlar bazasi operatsion tizim tomonidan taqdim etilgan identifikatorni ma'lumotlar bazasi identifikatorini o'rnatish uchun ishlatadi.

Bevosita ma'lumotlar bazasi doirasida (ma'lumotlar bazasi vositalari yordamida autentifikatsiya). Autentifikatsiyaning ushbu sxemasida ma'lumotlar bazasi o'zining shaxsiy autentifikatsiyalash mexanizmidan foydalanib, foydalanuvchi bildirgan identifikatorning haqiqiyligini tekshiradi (verifikatsiyalaydi).

Yuqorida tilga olingan autentifikatsiya servislaridan bo'lmaganida bittasi mos ma'lumotlar bazasi tomonidan taqdim etilishi shart. Himoyaga ehtiyoj axborot texnologiyasining aktivlari MBBT doirasida saqlanuvchi, konfidensialligi, yaxlitligi yoki foydalanuvchanligi obro'sizlantirilishi mumkin bo'lgan axborotdan iborat. Ma'lumotlar bazasi obyektlari va ma'lumotlar bazasining ushbu obyektlari doirasidagi ma'lumotlar axborot texnologiyasining aktivlari hisoblanadi.

Ma'lumotlar bazasining boshqa obyektlaridagi ma'lumotlar qismlarining birlashmasi ma'lumotlar bazasining obyektlari bo'lishi mumkin. Boshqarish ma'lumotlari MBBT tomonidan ma'lumotlar bazasi obyektlarini tashkil etish va himoyalash uchun ishlatiladi. Ma'lumotlar bazasi auditining ma'lumotlari MBBT tomonidan uning ishlash jarayonida generatsiyalanadi.

Quyida MBBT xavfsizligiga tahdidlar va ushbu tahdidlarni yuzaga keltirishi mumkin bo'lgan buzg'unchilar aniqlangan.

Ushbu tahdidlarga quyidagilar qarshi tura oladi:

- MBBT taqdim etgan xavfsizlikning texnik choralari;
- bazaviy tizim taqdim etgan xavfsizlikning texnik choralari;

- muhitdagi texnik bo'lmagan xavfsizlikning amaliy choralari (personalga tegishli muolajaviy, fizik choralar).

Quyidagilar buzg'unchi bo'lishi mumkin:

- bazaviy tizimdan (operatsion tizimdan va/yoki tarmoq servislaridan va/yoki maxsus ta'minotdan) vakolatsiz foydalanuvchi shaxslar;

- bazaviy tizimdan vakolatli foydalanuvchi shaxslar.

Quyidagilar tizimdan foydalanuvchi hisoblanishi mumkin:

- ma'lumotlar bazasidan foydalanuvchi bo'lmagan shaxslar;

- ma'lumotlar bazasidan foydalanuvchi shaxslar.

MBBT bartaraf etuvchi tahdidlar. MBBT quyidagi tahdidlarga qarshi tura olishi shart:

T.ACCES – *ma'lumotlar bazasidan ruxsatsiz foydalanish.* Begona yoki ayni vaqtda ma'lumotlar bazasidan foydalanishga vakolati bo'lmagan shaxs MBBTga murojaat etadi.

T.DATA – *axborotdan ruxsatsiz foydalanish.* Ma'lumotlar bazasidan vakolatli foydalanuvchi MBBT doirasidagi axborotga, ma'lumotlar egasi yoki ma'lumotlar himoyasiga javobgar hisoblanuvchi ma'lumotlar bazasidan foydalanuvchining ruxsatisiz murojaat etadi. Ushbu tahdidga MBBT axborotidan, xotiradagi yoki MBBT boshqaradigan saqlash resurslaridagi qoldiq axborotdan ruxsatsiz foydalanish qo'shiladi.

T.RESOURCE — *resurslarning haddan tashqari ishlatilishi.* Ma'lumotlar bazasining autentifikatsiyalangan foydalanuvchisi ma'lumotlar bazasining global resurslaridan shunday foydalanadiki, boshqa foydalanuvchilarning MBBTdan foydalanishlarini xavf ostiga qo'yadi. Ushbu tahdid MBBT doirasidagi axborotdan foydalanuvchanlikka tegishli. Masalan, ma'lumotlar bazasi foydalanuvchisi resurslardan haddan tashqari foydalanish bilan bog'liq harakatlar qilishi boshqa foydalanuvchilarning ma'lumotlardan, resurslardan va servislardan qonuniy foydalanishlariga to'sqinlik qiladi. Bunday tajovuzlar yomon niyat bilan qilinishi mumkin, e'tiborsizlik yoki beparvolik natijasi bo'lishi mumkin yoki foydalanuvchi o'z harakatining oqibatini anglamasligi mumkin. Bunday tajovuzlar ko'p sonli foydalanuvchilarning bir vaqtdagi harakati natijasida kuchayishi mumkin.

T.ATTACK – *aniqlanmagan tajovuz.* MBBTning aniqlanmagan obro'sizlantirilishi buzg'unchining (ma'lumotlar bazasidan vakolatli yoki vakolatsiz foydalanuvchining) vakolati doirasiga kirmagan harakatlarni bajarishga urinishi natijasida ro'y beradi.

T.ABUSE.USER – *imtiyozlardan noto'g'ri foydalanish.* MBBTning aniqlanmagan obro'sizlantirilishi ma'lumotlar bazasi foydalanuvchisining harakati (atayin yoki atayin bo'lmagan) natijasida ro'y beradi. Masalan, ma'lumotlar bazasining foydalanuvchisi o'zi javobgar bo'lgan ma'lumotlar bazasidan foydalanish huquqini boshqa, ushbu axborotdan firibgarlik maqsadida foydalana oluvchi foydalanuvchiga berishi mumkin. Ta'kidlash lozimki, ushbu tahdid ishonchning yuqori darajasiga ega foydalanuvchilarga tarqalmaydi.

Muhit tomonidan bartaraf etiluvchi tahdidlar:

T.OPERATE – *xavfli amal.* Ma'lumotlar bazasining obro'sizlantirilishi murakkab tizimning noto'g'ri konfiguratsiyalanishi, ma'murlanishi va/yoki ishlashi natijasida ro'y berishi mumkin.

T.CRASH – *to'satdan uzilishlar.* MBBT ishlashining to'satdan uzilishlari ma'lumot bazasini boshqarish ma'lumotlari va audit ma'lumotlari xavfsizligi bilan bog'liq ma'lumotlarning yo'qolishiga yoki buzilishiga olib kelishi mumkin. Bunday uzilishlar operator xatosi yoki dasturiy ta'minotdagi, apparat vositalaridagi, ta'minot manbaidagi yoki ma'lumotlar eltuvchisidagi adashishlar natijasi bo'lishi mumkin.

T.PHYSICAL – *fizik tajovuz.* Xavfsizlikka kritik hisoblanuvchi MBBT yoki bazaviy operatsion tizimi va/yoki tarmoq serverlari qismlari fizik tajovuzga duchor bo'lishlari natijasida xavfsizlik buzilishi mumkin.

P.ACCESS – *ma'lumotlar bazasi obyektlaridan foydalanish* quyidagilar tomonidan belgilanadi:

- ma'lumotlar bazasi egasi;
- foydalanishga urinuvchi ma'lumotlar bazasi subyektining identifikatori;
- ma'lumotlar bazasi subyekti egalik qiluvchi ma'lumotlar bazasi obyektidan foydalanish imtiyozlari;
- ma'lumotlar bazasi subyektining ma'muriy imtiyozlari;
- subyektga ajratilgan resurslar.

Ta'kidlash lozimki, ushbu siyosatga binoan ma'lumotlar bazasi obyektlari egalari o'z obyektlari uchun javobgarlar; ma'lumotlar bazasi obyektlari egasi o'zlarining obyektlaridan foydalanishni yoki ularni boshqarishni, *foydalanishni diskresion boshqarish* asosida, boshqa foydalanuvchilarga taqdim etishlari mumkin; ma'lumotlar bazasi foydalanuvchilari faqat o'zlariga taqsimlangan *resurslardan* foydalanish vakolatiga egalar.

P.ACCOUNT – *ma'lumotlar bazasi foydalanuvchilari quyidagilarga javobgarlar:*

- obyekt egasi tomonidan belgilangan obyektdagi amallarga;
- ma'lumotlar bazasi ma'muri tomonidan belgilangan harakatlarga.

MBBT axborot texnologiyasining texnik va muhitining funksional jixatiga bog'liq.

MBBT *bo'yicha taxminlar*:

A.TOECONFIG – MBBT o'rnatilgan, konfiguratsiyalangan va o'zining baholangan konfiguratsiyasiga muvofiq boshqariladi.

Asosiy tizimli taxminlar.

Fizik taxminlar:

A.PHYSICAL – MBBT va bazaviy tizim resurslari foydalanish vositalarini boshqarish doirasida joylashgan bo'lib, begona foydalanuvchilarning va ma'lumotlar bazasidan foydalanuvchilarning tizimdan ruxsatsiz fizik foydalanishlarini bartaraf etadi.

Konfiguratsiya taxminlari:

A.SYS.CONFIG – bazaviy tizim (operatsion tizim va/yoki tarmoq xavfsizligi servislari va/yoki maxsus dasturiy ta'minot) o'rnatilgan, konfiguratsiyalangan va o'zining xavfsiz konfiguratsiyasiga muvofiq boshqariladi.

A.ACCESS – bazaviy tizim shunday konfiguratsiyalanganki, tizimdan faqat shaxslarning ruxsatli guruhi foydalanishi mumkin.

A.MANAGE – MBBTni bazaviy tizimini va axborot xavfsizligini boshqarish uchun bir yoki undan ortiq puxta bilimli ishonchli shaxslar belgilanadi.

Bog'liqlik taxminlari:

A.PEER – faraz qilinadiki, MBBT bilan o'zaro harakatda bo'lgan axborot texnologiyaning har qanday komponentlari o'sha boshqarish ostida bo'ladi va o'sha xavfsizlik siyosati ostida ishlaydi.

A.NETWORK – faraz qilinadiki, taqsimlangan muhitda tarmoqning bazaviy servislari foydalanuvchilarning haqiqiyligini ta'minlovchi o'zaro harakatlarning xavfsiz protokollariga asoslanadi

5.1-jadvalda MBBT xavfsizligi maqsadlari tahdidlarining va xavfsizlik siyosatlarining har biriga munosabati keltirilgan va har qanday tahdidga bo'lmaganida, axborot texnologiyasining bitta maqsadi mos kelishligi va har qanday xavfsizlik siyosati, bo'lmaganida, axborot texnologiyasi xavfsizligining bitta maqsadi bilan ta'minlanganligi ko'rsatilgan. Jadvaldagi "Ha" so'zi axborot texnologiyasi xavfsizligining ko'rsatilgan maqsadi ma'lum tahdid yoki xavfsizlik siyosati uchun o'rinli.

O.ACCESS – MBBT foydalanuvchilarni va ma'murlarni xususiy yoki P.ACCESS xavfsizlik siyosatiga muvofiq javobgarliklaridagi ma'lumotlardan yoki resuslardan foydalanishni boshqarish imkoniyatini ta'minlashi lozim. Buning uchun baholash obyektida quyidagi muayyan maqsadlar mavjud:

Tahdidlar va siyosatlarning baholash obyekti xavfsizligi maqsadlari bilan o'zaro bog'liqligi

5.1-jadval

Siyosatlar / Tahdidlar	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESORCE	O.ADMIN.TOE
T.ACCESS	HA	HA		HA	HA
T.DATA	HA	HA			HA
T.RESORCE	HA	HA		HA	HA
T.ATTACK	HA	HA	HA		HA
T.ABUSEUSER	HA	HA	HA		HA
P.ACCES		HA		HA	
P.ACCOUNT		HA	HA		

O.ACCESS.OBJECTS – MBBT ma'lumotlarning va ma'lumotlar bazasi obyektlarining ruxsatsiz fosh qilinishini, kiritilishini, modifikatsiyalanishini yoki yo'q qilinishini hamda ma'lumotlar bazasining kuzatilishini, ma'lumotlarning boshqarilishini va ma'lumotlar bazasi ma'lumotlarining auditini bartaraf etishi lozim.

O.ACCESS.CONTROL – MBBT ma'lumotlar bazasi foydalanuvchilariga xususiy yoki javobgarliklaridagi ma'lumotlardan boshqa vakolatli foydalanuvchilarning foydalanishlarini boshqarish imkoniyatini taqdim etishi lozim.

O.ACCESS.RESIDUAL – MBBT obyektlar va resurslardan foydalanilgandan so'ng ularda qolgan ma'lumotlardan ruxsatsiz foydalanishni bartaraf etishi lozim.

O.RESOURCE – MBBT o'zining ma'lumotlar bazasi resurslaridan vakolatli foydalanuvchilarga foydalanishni boshqarish vositalarini taqdim etishi lozim.

O.I&A.TOE – MBBT bazaviy tizim yordamida yoki yordamisiz o'zining foydalanuvchilarini identifikatsiyalash va autentifikatsiyalash vositalarini taqdim etishi lozim.

O.AUDIT – MBBT o'zining ma'muriga yetarlicha yordam berish maqsadida xavfsizlikka ahamiyatli hodisalarni batafsil ro'yxatga oluvchi vositalarni taqdim etishi lozim:

- ma'lumotlar bazasini obro'sizlanishidan himoyasiz qolishiga sabab bo'luvchi xavfsizlikni buzishga urinishlarni yoki MBBTni himoyalash vositalari konfiguratsiyasidagi bo'lishi mumkin bo'lgan xatolikni aniqlash;
- ma'lumotlar bazasining individual foydalanuvchilarini, P.ACCOUNT siyosatiga binoan ma'lumotlar bazasi xavfsizligi uchun ahamiyatli har qanday bajariladigan harakatlariga javobgar bo'lishiga majbur qilish.

O.ADMIN.TOE – zarur hollarda MBBT bazaviy tizim bilan birga faqat vakolatli ma'murga baholash obyekti va uning xavfsizlik funksiyalarini samarali boshqarishga imkon beruvchi funksiyalarni taqdim etishi lozim.

Muhit uchun xavfsizlik maqsadlari.

Quyidagi axborot texnologiyasi xavfsizligi maqsadlari MBBT ishlatiluvchi muhit orqali qondirilishi lozim:

O.ADMIN.ENV – zarur hollarda MBBT bazaviy tizim bilan birga faqat vakolatli ma'murga MBBT va uning xavfsizlik funksiyalarini samarali boshqarishga imkon beruvchi funksiyalarni taqdim etishi lozim:

O.FILES – bazaviy tizim MBBT bilan bog'liq barcha fayllar va kataloglarni (jumladan, bajariluvchi dasturlarni, ishchi dastur bibliotekasini, ma'lumotlar bazasi fayllarini, eksport qilinuvchi fayllarni, boshqariluvchi fayllarni va h.) ruxsatsiz foydalanishdan himoyalashga imkon beruvchi foydalanishni boshqarish mexanizmlarini ta'minlashi lozim.

O.I&A.ENV – MBBT yordamida foydalanuvchilar haqiqiyligini ishonchli tasdiqlash talab qilinganida bazaviy operatsion tizim foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash vositalarini taqdim etishi lozim.

O.SEP – bazaviy operatsion tizim MBBT xavfsizligi funksiyalarini yakkalash uchun vositalarni va ushbu funksiyalar komponentlarining buzilmasligiga ishonchni taqdim etishi lozim. Ushbu komponentlarga ma'lumotlar bazasini saqlash maqsadida MBBT foydalanuvchi fayllar va ma'lumotlar bazasini boshqaruvchi MBBT jarayonlari taalluqli.

Axborot texnologiyasi bilan bog'liq bo'lmagan, xavfsizlik maqsadlari MBBT doirasida ko'rilgan muolajaviy va boshqa choralar orqali qoniqtirilgan bo'lishi lozim.

O.INSTALL – MBBTga javobgarlar quyidagilarni ta'minlashlari lozim:

- MBBT eksplutatsiya hujjatlariga muvofiq yetkazib berilishi, o'rnatilishi, boshqarilishi va ishlatilishi lozim;

- bazaviy tizim eksplutatsiya hujjatlariga muvofiq o'rnatilishi va ishlatilishi lozim. Agar tizim elementlari sertifikatsiyalangan bo'lsa, ular sertifikatsiyaning kerakli hujjatlariga muvofiq o'rnatilishi va ishlatilishi lozim.

O.PHYSICAL – MBBTga javobgar uning xavfsizlik siyosatiga kritik bo'lgan qismlarining fizik tajovuzdan himoyalanishini ta'minlashi lozim.

O.AUDITLOG – ma'lumotlar bazasi ma'murlari audit vositalarining samarali ishlatilishini ta'minlashlari lozim. Ushbu muolajalar ma'lumotlar bazasi auditi jurnalida va/yoki bazaviy operatsion

tizim auditi jurnalida va/yoki xavfsizlikning tarmoq servislari jurnalida o'z aksini topishi lozim. Ayniqsa:

- auditning davomli ishlashini ta'minlash, masalan, audit jurnalini muntazam arxivlash uchun yetarli band bo'lmagan xotirani ta'minlash uchun kerakli harakatlar qilinishi lozim;
- audit hodisalarini ro'yxatga olish jurnallari muntazam ko'zdan kechirilishi lozim va keyinchalik xavfsizlikning buzilishiga olib kelishi mumkin bo'lgan harakatlar va hodisalarni aniqlash lozim;
- tizim soatlari ruxsatsiz modifikatsiyalanishidan muhofazalanishi lozim (auditning vaqt belgisining yaxlitligi obro'sizlanmasligi uchun).

O.RECOVERY – MBBTga javobgar tizimli yanglishish yoki boshqa uzilishlardan so'ng ishlashni tiklash muolajalari va/yoki mexanizmlari uchun imkoniyatni taqdim etishi lozim.

O.QUOTA – ma'lumotlar bazasi ma'murlari MBBTdan foydalanuvchilarning har birining quyidagi kerakli kvotalarga egaliklarini ta'minlashlari lozim:

- foydalanuvchi foydalana oladigan amallarni boshqarishga yetarli kvotalar;
- foydalanuvchining ekspluatatsiya rejimini, resurslardan foydalanishni buzmasligi va resurslarni monopoliyalashtirmasligi uchun yetarli cheklangan kvotalar.

O.TRUST – MBBTga javobgar faqat ishonch darajasi yuqori bo'lgan foydalanuvchilarning quyidagilarga imkon beruvchi imtiyozlarga egaliklarini ta'minlashi lozim:

- ma'lumotlar bazasi uchun audit jurnalini o'rnatish yoki uning konfiguratsiyasini o'zgartirish;
- ma'lumotlar bazasi auditi jurnalida har qanday yozuvlarni o'zgartirish yoki yo'q qilish;
- foydalanuvchining har qanday hisob yozuvini yaratish yoki foydalanuvchi xavfsizligining har qanday atributini o'zgartirish;
- ma'muriy imtiyozlardan foydalanishga vakolat taqdim etish.

O.AUTHDATA – MBBTga javobgar baholash obyektidan foydalanuvchilarning hamda bazaviy tizimning har qanday hisob yozuvi uchun autentifikatsiya ma'lumotlarining ishonchli madadlanishini va ushbu hisob yozuvidan foydalanishga vakolati bo'lmagan shaxslarga fosh etilmasligini ta'minlashi lozim. Ayniqsa:

- bazaviy operatsion tizim va/yoki xavfsizlikning tarmoq servislari uchun autentifikatsiya ma'lumotlari saqlanuvchi eltuvchilar bazaviy platformadan ruxsatga ega bo'lmagan foydalanuvchilar tomonidan fizik yo'q qilinmasligi lozim;

- foydalanuvchilar o'zlarining parollarini boshqa shaxslarga bildirmasliklari lozim;

- tizim ma'muri tomonidan generatsiyalangan parollar xavfsiz tarqatilishi lozim.

O.MEDIA – MBBTga javobgar ma'lumot eltuvchisida saqlanuvchi ma'lumotlarning konfidensialligining, yaxlitligining va foydalanuvchanligining adekvat himoyalanganligini ta'minlashi lozim. Ayniqsa:

- ma'lumotlar bazasi ma'lumotlari va xavfsizlikka bog'liq ma'lumotlar (operatsion tizimning rezerv nusxalari, ma'lumotlar bazasining rezerv nusxalari, tranzaksiya jurnallari va audit jurnallari) joylashgan ma'lumotlarni saqlovchi avtonom qurilmalar foydalanuvchilar tomonidan bazaviy platformadan ruxsatsiz fizik yo'q qilinishi mumkin emas;

- ma'lumotlar saqlanuvchi tarmoq va avtonom qurilmalar munosib saqlanishi, madadlanishi hamda xavfsizlikka bog'liq ma'lumotlarning yaxlitligini va foydalanuvchanligini ta'minlash maqsadida muntazam tekshirilishi lozim;

- ma'lumotlar bazasi bilan bog'liq fayllar (jumladan, ma'lumotlar bazasi fayllari, eksport fayllar, takroran ro'yxatga olish fayllari, boshqarish fayllari, trassirovka fayllari) saqlanuvchi eltuvchilar takroran ma'lumotlar bazasi bilan bog'liq bo'lmagan maqsadlarda ishlatilishidan oldin tozalanadi.

5.2-jadvalda yuqorida keltirilgan maqsadlarning har birining tahdidga qarshi qo'yilganligi, MBBT xavfsizligi maqsadini madadlashi, siyosatni madadlashi yoki xavfsiz foydalanish farazlarida aks ettirilgani tasvirlangan.

Asosiy talablarda belgilanganidek, himoya siyosatiga mos har qanday MBBT xavfsizlikning barcha funksional talablarining bajarilishini ta'minlashi lozim.

Shuningdek, himoya siyosatiga mos har qanday MBBT ko'rsatilgan autentifikatsiya paketlaridan birini identifikatsiyalashi va bajarilishini ta'minlashi lozim. MBBT har bir ma'lum qilingan

autentifikatsiya paketi uchun xavfsizlikning barcha mos funksional talablarining bajarilishini ta'minlashi lozim.

Muhit xavfsizligi maqsadlarining tahdidlarga, MBBT xavfsizligi maqsadlariga xavfsiz foydalanish siyosati va farazlarida aksi.

5.2-jadval

Muhit xavfsizligi maqsadlari	Qarshi turuvchi tahdid	MBBTning madadla-nuvchi maqsadi	Madadla-nuvchi siyosat	Xavfsiz foydalanish xususidagi farazlar-dagi aksi
O.INSTALL	T.OPERATE			A.TOE.CONFIG, A.SYS.CONFIG, A.MANAGE
O.PHYSICAL	T.PHYSICAL			A.ACCESS, A.PEER, A.PHYSICAL
O.AUDITLOG		O.AUDIT	P.ACCONT	A.MANAGE
O.RECOVERY	T.CRASH			A.MANAGE
O.QUOTA		O.RESOURCE		A.MANAGE
O.TRUST			P.ACCESS	A.MANAGE
O.AUTHDATA		O.I&A.TOE	P.ACCESS	A.MANAGE A.PEER A.NETWORK
O.MEDIA	T.CRASH			A.MANAGE
O.ADMIN.ENV		O.ADMIN. TOE		A.MANAGE
O.FILES	T.ACCESS		P.ACCESS	A.MANAGE
O.I&A.ENV	T.ACCESS	O.I&A.TOE	P.ACCESS	A.MANAGE
O.SEP	T.ACCESS		P.ACCESS	A.MANAGE

Nazorat savollari:

1. Ma'lumotlar bazasini boshqarish tizimlarining himoya profillari nima?
2. Autentifikatsiya paketlari va ularni taqdim etadigan vositalar.
3. Ma'lumotlar bazasini boshqarish tizimining konfiguratsiya-lanish usullarini sanab o'ting.

4. MBBT xavfsizligiga tahdidlar va ularga qarshi tura oladigan choralarni sanab o'ting.

5. Ma'lumotlar bazasini boshqarish tizimidagi himoyalash profili buzg'unchilarini sanab o'ting.

6. "Ma'lumotlar bazasini boshqarish tizimining himoya profili" hujjatida keltirilgan masalalarni tushuntiring.

5.4. Ma'lumotlar bazasi xavfsizligini ta'minlashdagi me'yoriy hujjatlar

Hozirda axborot xavfsizligi sohasidagi mutaxassislar mos standartlar va spetsifikatsiyalarni bilmasdan turib, deyarli hech qanday ishni uddalay olmaydilar. Bunga sabab, birinchidan, standartlar va spetsifikatsiyalar – bilimlarni, avvalo axborot xavsizligining muolajaviy va dasturiy-texnik darajalari xususidagi bilimlarni to'plash usullaridan biri. Unda yuqori malakali mutaxassislar tomonidan ishlab chiqilgan, sinalgan, yuqori sifatli yechimlar va metodologiyalar qaydlangan. Ikkinchidan, standartlar va spetsifikatsiyalar apparat-dasturiy vositalar va ularning komponentlarini o'zaro mosligini ta'minlashda asosiy vosita hisoblanadi. Shu bilan birga ushbu vosita Internet-uyushmada, haqiqatan ham, juda samarali ishlaydi.

Standart va spetsifikatsiyaning asosiy tushunchalari:

- *standart* – hujjat bo'lib, unda ixtiyoriy ravishda ko'p marta foydalanish maqsadida mahsulot xarakteristikalari, ishlab chiqarish, ekspluatatsiya qilish, saqlash, tashish, realizatsiya va utilizatsiya qilish, ishlarni bajarish yoki xizmat ko'rsatish jarayonlarini amalga oshirish qoidalari va xarakteristikalari o'rnatiladi. Standart tarkibida terminologiyaga, simvolikaga, joylashga yoki etiketkaga va uni qayd qilishga talablar bo'lishi mumkin.

- *standartlash* – ixtiyoriy ko'p marta foydalanish maqsadida ishlab chiqarish va mahsulotdan foydalanish sohasini tartibga solishga va mahsulot, ishlar yoki xizmatlar raqobatbardoshligiga erishishga yo'naltirilgan qoidalar va xarakteristikalarni o'rnatish bo'yicha faoliyat.

Amaliy nuqtayi nazardan, axborot xavfsizligi sohasidagi standartlar va spetsifikatsiyalar (xalqaro, milliy, sohaviy va h.) soni cheksiz. Axborot xavfsizligining turli jihatlarini va axborot-

kommunikatsiya tizimining turli xili va konfiguratsiyasini qamrab olish, maqsadli auditoriyaning xilma-xil guruhlariga foydali ma'lumotlarni taqdim etish uchun ularni sathlarga ajratish mumkin.

Yuqori sathda bir-biridan jiddiy farqlanuvchi standartlar va spetsifikatsiyalarning ikkita guruhini ajratish mumkin:

- havfsizlik talablari bo'yicha axborot tizimlarini va himoya vositalarini tasniflash va baholashga mo'ljallangan baholash standartlari;

- himoya usullari va vositalarini amalga oshirish va ulardan foydalanishning turli jihatlarini reglamentlovchi spetsifikatsiyalar.

Ushbu guruhlar, ravshanki, ixtilofda bo'lmaydilar, balki bir-birini to'ldiradilar. Baholash standartlari tashkiliy va arxitekturaviy spetsifikatsiyalar rolini o'ynagan holda, axborot xavfsizligi nuqtayi nazaridan muhim bo'lgan axborot tizimi tushunchalari va jihatlarini tavsiflaydi. Boshqa spetsifikatsiyalar arxitektura ko'rsatmalariga asosan axborot-kommunikatsiya tizimini qanday qurish va tashkiliy talablarni qanday bajarish lozimligini belgilaydi.

Zamonaviy taqsimlangan axborot-kommunikatsiya tizimlarda qo'llaniluvchi texnik spetsifikatsiyalar asosan, "Internet texnologiyalari bo'yicha tematik guruh" (Internet Engineering Take Force, IETF) va uning bo'linmasi - xavfsizlik bo'yicha ishchi guruh tomonidan yaratiladi. Ko'rilayotgan texnik spetsifikatsiyalarning yadrosi sifatida IP- sathdagi (IPsec) xavfsizlik bo'yicha hujjatlar xizmat qiladi. Undan tashqari himoya transport sathida (Transport Lager Security, TLS) hamda ilova sathida (GSS-API, Kerberos spetsifikatsiyalari) tahlillanadi. Ta'kidlash lozimki, Internet - uyushma xavfsizlikning ma'muriy va muolajaviy sathlariga kerakli e'tibor beradi. ("Korxonaning axborot xavfsizligi bo'yicha qo'llanma", "Internet- xizmat" ni ta'minlovchini qanday tanlash lozim?", "Axborot xavfsizligining buzilishiga qanday javob berish kerak?").

Tarmoq xavfsizligi masalalarini quyidagi spetsifikatsiyalarni o'rganmasdan tushunib bo'lmaydi: X800, "Ochiq tizimlarning o'zaro aloqalari uchun xavfsizlik arxitekturasi", X500 "Direktoriya xizmati: konsepsiya, modellar va servislar obzori" va X509 "Direktoriya xizmati: ochiq kalitlar va atributlar sertifikatlarining karkaslari".

Britaniya standarti BS 7799 "Axborot xavfsizligini boshqarish. Amaliy qoidalar" axborot xavfsizligiga javobgar tashkilot rahbarlari va shaxslar uchun foydali. Ushbu standart birozgina bo'lsa-da, jiddiy o'zgarishsiz O'zDSt ISO/IEC 27000-2008 standartda aks ettirilgan.

AQSH Mudofaa vazirligining "Ishonchli kompyuter tizimlarini baholash mezonlari" (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC) standarti xalqaro e'tirofga sazovor bo'lib, axborot xavfsizligi sohasidagi keyingi ishlanmalarga nihoyatda kuchli ta'sir ko'rsatdi. Ushbu standart "To'q sariq kitob" (muqovasining rangi bo'yicha) nomi bilan mashhur.

Mubolag'asiz tasdiqlash mumkinki, "To'q sariq kitob"da axborot xavfsizligining tushuncha asosi solingan. Uning tarkibidagi tushunchalarni sanab o'tish yetarli: xavfsiz va ishonchli tizimlar, xavfsizlik siyosati, kafolatlik darajasi, hisobdorlik, ishonchli hisoblash baza, murojaatlar monitori, xavfsizlik yadrosi va perimetri. Xavsizlik siyosatining foydalanishni ixtiyoriy (diskresion) va majburiy (mandatli) boshqarish, obyektlardan takroran xavfsiz foydalanish kabi jihatlarini ajratib ko'rsatish ham juda muhim. Xavfsizlik siyosatining yana bir muhim jihati – xavfsizlik siyosatiga va kafolatlik darajasiga parallel ravishda talabchanlikni oshirish asosida xavfsizlik talablari bo'yicha tasniflash.

"To'q sariq kitob" dan keyin bir qator "Rang-barang seriya" chop etildi. Konseptual nuqtayi nazaridan undagi eng ahamiyatli hujjat – "Tarmoq konfiguratsiyalari uchun" "To'q sariq kitob"ning sharhi (Trusted Network Interpretation). U ikki qismdan iborat. Birinchi qism sharhlashning o'ziga bag'ishlangan bo'lsa, ikkinchi qismida tarmoq konfiguratsiyalari uchun o'ziga xos xususiyatli yoki ayniqsa muhim xavfsizlik servislari tavsiflanadi.

Birinchi qismga kiritilgan eng muhim tushuncha - ishonchli tarmoq hisoblash bazasi. Boshqa muhim jihat - tarmoq konfiguratsiyalarining dinamikligini nazarda tutish. Himoya mexanizmlari orasidan konfidensiallikni va yaxlitlikni ta'minlashga yordam beruvchi kriptografiya ajratilgan.

Foydalanuvchanlik masalalariga sistematik yondashuv, uni ta'minlashning arxitekturaviy prinsiplarini shakllantirish o'z vaqti uchun yangilik bo'ldi. Obyektga mo'ljallangan uslubda kommuni-

katsiyalarni kriptografik himoyalash bilan birga taqsimlangan axborot tizimini dekompozitsiyalashning nazariy asosi hisoblanuvchi murojaatlar monitorini fragmentlashning yetarlicha korrektlik shartini ham eslash mumkin.

"Evropa mamlakatlarining uyg'unlashgan mezonlari"da axborot tizimi ishlashi lozim bo'lgan shartlarga apriori talablar mavjud emas. Faraz qilinadiki, avvalo baholash maqsadi ta'riflanadi, so'ngra sertifikatsiya organi ushbu maqsadga qancha to'liq erishishligini, ya'ni muayyan vaziyatda xavfsizlik arxitekturasi va mexanizmlarning amalga oshirilishining qanchalik darajada korrektligini va samaraliligini aniqlaydi. Baholash maqsadini ta'riflashni yengillashtirish uchun standart tarkibida hukumat va tijoriy tizimlarga xos funksionallikning o'n nafar namunaviy sinfining tavsifi mavjud.

"Uyg'unlashgan me'zon"larda axborot texnologiyalari tizimlari va mahsulotlarining bir-biridan farqi ta'kidlanadi, ammo talablarni unifikatsiyalash uchun yagona tushuncha - baholanish obyekti kiritiladi.

Xavsizlik funksiyalari (servislari) va ularni amalga oshiruvchi mexanizmlari orasidagi farqni hamda kafolatlanganlikning ikkita jihatini - samaradorligini va xavfsizlik vositalarining korrektligini ko'rsatib o'tish mumkin.

Ushbu yo'nalishdan birinchi diqqatga sazovor chetlanish 1997-yili, xavfsizlikning alohida servisi - tarmoqlararo ekranlar bo'yicha amal qilinadigan hujjat qabul qilinganida yuz berdi. Uning asosiy g'oyasi – tarmoqlararo ekranlarni ma'lumotlar oqimini filtrlashni amalga oshiruvchi yetti sathli etalon modelining sathlari bo'yicha tasniflash. Ushbu g'oya xalqaro e'tirofga sazovor bo'ldi va dolzarbligicha qoldi.

Texnik spetsifikatsiyalar ichida birinchi o'ringa, so'zsiz, X800 "Ochiq tizimlarning o'zaro aloqalari uchun xavfsizlik arxitekturasi" hujjatini qo'yish kerak. Unda xavfsizlikning quyidagi muhim tarmoq servislari ajratilgan: autentifikatsiya, foydalanishni boshqarish, ma'lumotlarning konfidensialligini va/yoki yaxlitligini ta'minlash hamda qilingan harakatdan voz kechishning mumkin emasligi. Servislarni amalga oshirish uchun quyidagi xavfsizlikning tarmoq mexanizmlari va ularning kombinatsiyalari ko'zda tutilgan: shifrlash, elektron raqamli imzo, foydalanishni boshqarish, ma'lu-

motlar yaxlitligining nazorati, autentifikatsiya, trafikni to'ldirish, marshrutlashni boshqarish, notarizatsiyalash. Xavfsizlik servislari va mexanizmlari amalga oshirilishi mumkin bo'lgan yetti sathli etalon model sathlari tanlangan. Nihoyat, taqsimlangan konfiguratsiyalar uchun xavfsizlik vositalarini ma'murlash masalalari batafsil ko'rilgan.

Internet - uyushmaning RFC 1510 "Autentifikatsiyaning tarmoq servisi Kerberos (V5)" xususiyroq, ammo juda muhim va dolzarb muammoga, ya'ni tarmoqqa yagona kirish konsepsiyasini madadlashli xilma-xil taqsimlangan muhitda autentifikatsiyalash muammosiga tegishli. Kerberos autenfikatsiya serveri ishonchli uchinchi tarafni ifodalaydi va xizmat qilinuvchi subyektlarning maxfiy kalitlariga ega va ularga haqiqiylikni juft-juft tekshirishda yordam beradi. Kerberosning mijoz komponentlari aksariyat operatsion tizimlarda mavjud.

"Evropa mamlakatlarining uyg'unlashgan mezonlari" o'z vaqti uchun yetakchi hujjat bo'lgan va ular O'zDSt ISO/IEC 15408:2008 "Axborot texnologiyalari xavfsizligini baholash mezonlari" (Evaluation criteria for LT security) standartining paydo bo'lishiga sababchi bo'ldi. Ushbu standart odatda (unchalik to'g'ri emas) "Umumiy mezonlar" deb ataladi.

Hozirda "Umumiy mezonlar" juda to'liq va zamonaviy baholash standarti hisoblanadi. Aslida ushbu metastandart axborot tizimi xavfsizligini baholash instrumentlarining va ulardan foydalanish tartibini belgilaydi. Unda xavfsizlikning oldindan belgilangan sinflari mavjud emas. Bunday sinflarni qo'yilgan talablarga tayanib tuzish mumkin.

"Umumiy mezonlar"da xavfsizlikka talablarning ikkita asosiy turi mavjud:

- funksional talablar. Ushbu talablar xavfsizlik funksiyalariga (servislariga) va ularni amalga oshiruvchi mexanizmlarga taqdim etiluvchi himoyalashning aktiv jihatiga mos keladi;
- ishonch talablari. Ushbu talablar passiv jihatga mos; ular texnologiyalarga, ishlab chiqarish va ekspluatatsiya jarayonlariga taqdim etiladi.

Xavfsizlik talablari ta'riflanadi va uning bajarilishi ma'lum baholash obyektida, ya'ni apparat-dasturiy mahsulotda yoki axborot tizimida tekshiriladi.

Ta'kidlash lozimki, "Umumiy me'zonlar" amalda ishlatiluvchi me'yoriy hujjatlarning ikkita bazaviy turini, ya'ni himoya profilini va xavfsizlik bo'yicha topshiriqni shakllantirishga yordam beradi.

Himoya profili deganda mahsulotlar va/yoki ma'lum sinf tizimlari qanoatlantirishi shart bo'lgan ma'lumotlarning namunaviy nabori tushuniladi. Xavfsizlik bo'yicha topshiriq tarkibida muayyan ishlanmaga qo'yiladigan talablar majmui bo'lib, ularning bajarilishi xavfsizlikni ta'minlash bo'yicha qo'yilgan masalalarni yechishga imkon beradi.

Kriptografiya – o'ziga xos xususiyatga ega soha. Ammo uning xavfsizlik arxitekturasidagi o'rni va kriptografik komponentlarga qo'yiladigan talablar xususida umumiy tasavvurga ega bo'lish lozim. Buning uchun AQSHning Federal standarti FIPS 140-2 "Kriptografik modullar uchun xavfsizlik talablari" (Security Requirements for Cryptographic Modules) bilan tanishish maqsadga muvofiq hisoblanadi. Ushbu standart kriptografik modulning tashqi interfeysini, bunday modullarga va ular atrofidagi muhitga talablarni tavsiflaydi, ya'ni tashkiliy vazifani bajaradi. Bunday standartning mavjudligi xavfsizlik servislarini va himoya profilini ishlab chiqishni osonlashtiradi.

Kriptografiya xavfsizlik servislarini amalga oshirish vositasi sifatida ikkita jihatga ega: algoritmik va interfeys. Biz uchun qiziqarligi faqat kriptografiyaning interfeys jihati. Shuning uchun FIPS 140-2 standart bilan bir qatorda Internet- uyushma doirasida taklif etilgan "Xavfsizlik xizmatining umumlashgan tatbiqiy dasturiy interfeysi" (Generic Security Service Application Program Interface, GSS-API) texnik spetsifikatsiyani ko'ramiz.

GSS-API xavfsizlik interfeysi mijoz - server arxitekturasida qurilgan dasturiy tizim komponentlari orasidagi kommunikatsiyalarni himoyalashga mo'ljallangan. U muloqotdagi sheriklarni o'zaro autentifikatsiyalash uchun sharoit yaratadi, jo'natiluvchi xabarlar yaxlitligini nazoratlaydi va ularning konfidensialligini kafolatlaydi. Kommunikatsiya protokollari (odatda tatbiqiy sathdagi) yoki mustaqil tarzda ma'lumotlarni jo'natuvchi boshqa

dasturiy tizimlar GSS-API xavfsizlik interfeysining foydalanuvchilari hisoblanadi.

IPSning texnik spetsifikatsiyalar mubolag'asiz, fundamental ahamiyatga ega. Ular tarmoq sathida konfidensiallikni va yaxlitlikni ta'minlovchi vositalarning to'liq naborini tavsiflaydi. Hozirda asosiy hisoblanuvchi IP protokolining 4-versiyasi uchun ular fakultativ xarakterga ega; istiqbolli IP protokolining 6-versiyasida ularning amalga oshirilishi shart. IPsec asosida yuqoriroq sath (tatbiqiy sathga qadar) protokollarning himoya mexanizmlari hamda xavfsizlikning tugal vositalari, xususan virtual xususiy tarmoq quriladi. Ravshanki, IPsec jiddiy tarzda kriptografik mexanizmlarga va kalit infrastrukturasiga tayanadi.

Transport sathi xavfsizligi vositalari (Transport Layer Security, TLS) ham xuddi shunday xarakterlanadi. TLS spetsifikatsiyasi turli vazifali ko'p sonli dasturiy mahsulotlarda ishlatiluvchi ommaviy Secure Socket Layer (SSL)) protokolini rivojlantiradi va oydinlashtiradi.

Infrastruktura nuqtayi nazaridan, X500 "Direktoriya xizmati: konsepsiyalar, modellar va servislar obzori (The directory: Overview of concepts, models and services)" va X509 "Direktoriya xizmati: ochiq kalitlar va atributlar sertifikatlarining karkaslari. The directory: Public-key and attribute certificate frameworks)" tavsiyalari juda muhim. X509 tavsiyalarda ochiq kalitlar va atributlar (ochiq kalitlar infrastrukturalarining bazaviy elementlari) sertifikatlarining formati va imtiyozlarni boshqarish tavsiflangan.

Ma'lumki, axborot xavfsizligini ta'minlash kompleks muammo hisoblanadi va qonun chiqarish, ma'muriy, muolajaviy va dasturiy texnik sathlarda kelishilgan choralarni qabul qilishni talab etadi. Ma'muriy sathning bazaviy hujjatini, ya'ni tashkilot havfsizlik siyosatini ishlab chiqishda va amalga oshirishda Internet-uyushmaning "Korxona axborot xavfsizligi bo'yicha qo'llanmasi" (Site Security Handbook) juda yaxshi ko'makdosh bo'lishi mumkin. Unda xavfsizlik siyosati va mulojalarini shakllantirishning amaliy jihatlari yoritiladi, ma'muriy va muolajaviy sathlarning asosiy tushunchalariga izoh beriladi, tavsiya etiluvchi harakatlari asoslanadi, xavf-xatarlarning (risklarning) tahlili, axborot xavsizligining buzilishiga reaksiya va buzilish bartaraf etilganidan so'ngi

harakatlar aks ettiriladi. Oxirgi masalalar "Axborot xavfsizligi buzilishiga qanday javob berish kerak" (Expectations for Computer Security Incident Response) tavsiyasida batafsil ko'rilgan. Ushbu hujjatda foydali axborot resurslariga havolalarni ham, muolajaviy sathning amaliy maslahatlarini ham topish mumkin.

Korporativ axborot tizimlarini rivojida va qayta tashkil etishda "Internet-xizmatni ta'minlovchini qanday tanlash lozim" (Site Security Handbook Addendum for ISPs) tavsiyasi, shubxasiz, foydali bo'ladi. Avvalo ushbu tavsiyaning qoidalariga muolajaviy va dasturiy-texnik sathlarning boshqa choralari asoslanuvchi tashkiliy va arxitekturaviy xavfsizlikni shakllantirish jarayonida rioya qilish lozim.

Ma'muriy va muolojaviy sathlari regulyatorlari yordamida axborot xavfsizligi rejimini amalda yaratish va madadlash uchun Britaniya standarti BS7799 "Axborot xavfsizligini boshqarish. Amaliy qoidalar" (Code of practice for information security management) va uning ikkinchi qismi BS 7799-2:2002 "Axborot xavfsizligini boshqarish tizimlari – foydalanishga qo'llanmali spetsifikatsiya" (Information security management systems- Specification with quidance for use) bilan tanishish kerak bo'ladi. Unda xavfsizlik siyosati, himoyani tashkil etishning asosiy prinsiplari, resurslar tasnifi va ularni boshqarish, xodim xavfsizligi, fizik xavfsizlik, tizimlar va tarmoqlarni ma'murlash prinsiplari, foydalanishni boshqarish, axborot tizimini yaratish va kuzatish, tashkilotning uzluksiz ishlashini rejalashtirish kabi tushunchalar va muolajalar yoritiladi.

Hozirda mamlakatimizda ham bu borada olib borilayotgan ishlar e'tiborga loyiqdir va quyida amal qilayotgan bir necha standartlar va spetsifikatsiyalar keltirilgan:

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

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

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

4. O‘z DSt 1108:2011 – Axborot texnologiyasi. Ochiq tizimlarning o‘zaro bog‘liqligi. ERI ochiq kaliti sertifikati va atribut sertifikatining strukturasi.

5. O‘z DSt 1135:2007 – Axborot texnologiyasi. Ma’lumotlar bazalari va joylardagi davlat boshqaruvi hamda davlat hokimiyati organlari o‘rtasida axborot almashishiga qo‘yiladigan talablar.

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

7. O‘z DSt 1270:2009 – Elektron hujjat aylanishi. Elektron hujjat aylanishi tizimlarining o‘zaro ishlashi.

8. O‘z DSt 2295:2011 – Elektron hujjat. Shakllantirish, qo‘llash va saqlashga qo‘yiladigan talablar.

9. O‘z DSt 2590:2012 – Axborot texnologiyasi. Milliy axborot tizimini shakllantirish doirasida davlat organlari tomonidan foydalanadigan axborot tizimlari integratsiyasiga va o‘zaro faoliyatiga qo‘yiladigan talablar.

10. O‘z DSt 2826:2014 – Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elliptik egri chiziqlarga asoslangan elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.

11. O‘z DSt 2875:2014 – Axborot texnologiyasi. Datamarkazlarga qo‘yiladigan talablar. Infratuzilma va axborot xavfsizligini ta’minlash.

12. O‘z DSt 2927:2015 – Axborot texnologiyasi. Axborot xavfsizligi. Atamalar va ta’riflar.

13. O‘z DSt ISO 7498-2:2011 (ISO 7498-2:1989, MOD) – Axborot texnologiyasi. Ochiq tizimlarning o‘zaro bog‘liqligi. Asosiy etalon model. 2-qism. Xavfsizlik arxitekturasi.

14. O‘z DSt ISO/IEC 15945:2015 – Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Elektron imzolar qo‘llanishini ta’minlash uchun IUT xizmatlari spetsifikatsiyasi.

15. O‘z DSt ISO/IEC 18045:2013 – Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalari xavfsizligini baholash metodologiyasi.

16. O‘z DSt 1986:2010 – Axborot texnologiyasi. Axborot tizimlari. Yaratish bosqichlari.

17. O'z DSt 2863:2014 – Axborot texnologiyasi. Interaktiv davlat xizmatlari. Tasniflash va shakllantirishga asosiy talablar.

18. O'z DSt 2814:2014 – Axborot texnologiyasi. Avtomatlashtirilgan tizimlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo'yicha tasniflash.

19. O'z DSt 2815:2014 – Axborot texnologiyasi. Tarmoqlararo ekranlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo'yicha tasniflash.

20. O'z DSt 2816:2014 – Axborot texnologiyasi. Axborotni muhofaza qilish vositalarining dasturiy ta'minotini deklaratsiya qilinmagan imkoniyatlar yo'qligini nazorat qilish darajasi bo'yicha tasniflash.

21. O'z DSt 2817:2014 – Axborot texnologiyasi. Hisoblash texnikasi vositalari. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo'yicha tasniflash.

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.

Nazorat savollari

1. Standart va spetsifikatsiyaning asosiy tushunchalari.
2. X800 texnik spetsifikatsiya.
3. Umumiy mezonlar xavfsizlikning qanday talablarini qamrab oladi?
4. Axborot xavfsizligini ta'minlash sohasidagi O'zbekiston Respublikasining amaldagi standartlari.

FOYDALANILGAN ADABIYOTLAR

1. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд.4-е –М.: Ленанд, 2015.

2. Tarmoq standarti. Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta'riflar. TSt 45-010:2010.

3. Шаньгин В.Ф. Информационная безопасность. –М.: ДМК Пресс, 2014.

4. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений выс.образования/. –М.: Издательский центр «Академия», 2014.

5. Мельников Д.А. Информационная безопасность открытых систем: учебник/ –М.: Флинта: Наука, 2013.

6. Stamp, Mark. Information security: principles and practice/ Mark Stamp/ -2nd ed. ISBN 978-0-4-470-62639-9(hardback)/ QA76.9.A25S69, USA, 2011.

7. Зрюмов Е.А., Зрюмова А.Г. Базы данных для инженеров: учебное пособие. - Барнаул: Изд-во АлтГТУ, 2010, 131 с.

8. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс. –Гелиос АРВ, 2002, 368 с.

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы 4 издание. –Питер, 2010, 944с.

10. Joel Scambray, Vincent Liu. Hacking exposed. Web Applications 3. Caleb Sima. 2010y.

11. 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. First published 2000. The original version is in print December 2010 with Pearson Education.

12. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. Монография. Издательство Уральского университета, 2003, 328 с.

13. Michael Lee, Gentry Bieker. MASTERING Microsoft SQL Server 2008. Wiley Publishing, Inc. 2009, 723 p.

14. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. учебное пособие. –Екатеринбург, 2008, 212с.

15. G'aniev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. Oliy o'quv yurt talabalari uchun mo'ljallangan. –T.: "Aloqachi", 2008.

16. Аткинсон, Леон. MySQL библиотека профессионала. –М.: Издательство «Вильяме», 2002, 624 с.

17. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. – М.: Радио и связь, 2001.

18. Кузнецов С.Д. Основы баз данных, 2-е издание. Бином. Лаборатория знаний. Интернет-университет информационных технологий, 2007.

19. Кузин А.В., Левонисова С.В. База данных. –Издательство: «Академия», 2012.

20. Itzik Ben-Gan. Training Kit (Exam 70-461): Querying Microsoft SQL Server 2. Izdatelstvo: «Microsoft Press». 2012.

21. Карпова Т.С. База данных: модели, разработка, реализация. –Национальный открытый университет «ИНТУИТ», 2016, 241с.

22. Бессарабов Н. В. Модели и смыслы данных в Cache и Oracle. –Национальный открытый университет «ИНТУИТ», 2016, 617 с.

23. Фейерштейн С., Прибыл Б. Oracle PL/SQL. Для профессионалов. 6-е изд. –Издательство: Питер, 2015, 1024 с.

24. Alfred Basta, Melissa Zgola. Database Security. Paperback – 2014.

25. Ron Ben Natan. Implementing Database Security and Auditing. Digital Press; 1 edition (May 2, 2005). 432 pages.

26. Maria Grazia Fugini, Silvana Castano, Giancarlo Martella. Database Security (Acm Press Books) 1st Edition. Pearson Education Ltd; 1st edition. 456 pages.

27. Josh Shaul, Aaron Ingram. Practical Oracle Security: Your Unauthorized Guide to Relational Database Security 1st Edition. Syngress; 1 edition (November 26, 2007). 288 pages.

28. Нестеров С.А. База данных. –Издательство: СПбГПУ, 2013.

29. Агальцов В.П. Распределенные и удаленные базы данных: учебник. –М.: ид. форум, НИЦ инфра-м, 2013.

30. Крис Фиайли. SQL. Руководство по изучению языка. Серия: Quick Start –Издательство: ДМК Пресс, 2013, 456с.

QISQARTMA SO‘ZLAR RUYXATI

MB – ma’lumotlar bazasi.
MBBT – ma’lumotlar bazasini boshqarish tizimlari.
SQL – (structured query language) strukturalangan so‘rovlar tili.
TCB – (Trusted Computing Base) ishonch qozongan hisoblash bazasi.
NRU – (no read up - NRU) yuqorini o‘qish man etiladi.
NWD – (no write down - NWD) pastga yozish man etiladi.
ANSI – Amerika milliy standartlashtirish instituti.
ISO – Xalqaro standartlashtirish instituti.
DDL – ma’lumotlarni tavsiflash tili DDL (Data Definition Language).
DML – ma’lumotlarni manipulyatsiyalash tili DML (Data Manipulation Language).
DAC – foydalanishni diskresion boshqarishga (Discretionary Acces Control) asoslangan model.
MAC – foydalanishni mandatli cheklashga (Mandatory Access Control) asoslangan model.
RBAC – foydalanishni cheklashning rolli modeli (Role – Based Access Control).
FS – fayl serveri modeli (File Server).
RDA – ma’lumotlardan masofadan foydalanish modeli (Remote Data Access).
DBS – ma’lumotlar bazasi serveri modeli (Data Base Server).
AS – ilovalar serveri modeli (Application Server).
ODBC – Open Database Connectivity – ma’lumotlar bazasidan oshkora foydalanish.
Authorization ID - har bir foydalanuvchi maxsus identifikatsiya nomi yoki nomeri.
SAN – Storage Area Network – Ma’lumotlarni saqlash tarmog‘i.
DCE – OSF konsernining taqsimlangan hisoblash muhiti.
TLS – Transport Layer Security – transport sathi xavfsizligi.
SSL – Security Socket Layer – xavfsiz soket sathi.

ATAMALAR LUG‘ATI

Algoritm – amallarning cheklangan soni yordamida masala yechimini belgilovchi buyruqlarning cheklangan to‘plami.

Алгоритм – упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Algorithm – an ordered finite set of clearly defined rules for solving a finite number of steps.

Asliga to‘g‘rilik – 1. Haqiqiylik 2. Subyekt yoki resursning so‘ralganiga muvofiqligini kafolatlanuvchi xususiyat.

Аутентичность – 1. Подлинность. 2. Свойство гарантирующее, что субъект или ресурс идентичны заявленным. Аутентичность применяется к таким субъектам, как пользователи, процессы, системы и информация.

Authenticity – 1. Authenticity. 2. Feature ensures that the subject or resource identical stated. Authenticity applies to entities such as people, processes, systems and information.

Autentifikatsiya axboroti – foydalanuvchining haqiqatdan aynan o‘zi ekanligiga ishonch hosil qilishda foydalaniladigan axborot.

Информация аутентификации – информация, используемая для установления подлинности личности, за которую выдает себя пользователь.

Authenfication information – information used for establishment of authenticity of the personality for which the user gives out himself.

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.

Аутентификатор – средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Authenticator – authentication means representing the hallmark of the user. Means of user.

Autentifikatsiya ma'lumotlari – taqdim etilgan foydalanuvchi identifikatorini tasdiqlash uchun ishlatiladigan axborot.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора пользователя.

Authentication data – information used to verify the presented user ID.

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.

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.

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.

Autentifikatsiya kodi – axborotni imitohimoyalovchi kodlash algoritmining turi. Odatda, autentifikatsiya kodi xabarni uning haqiqiyligi kodi bilan taqqoslaydi. Axborotning haqiqiyligi xususida qarab qabul qilish algoritmi xabar haqiqiyligi kodi qiymatini tekshirishga asoslangan.

Код аутентификации – вид алгоритма кодирования имитозащищающего информации. Как правило, к. а. сопоставляет сообщению его код аутентичности сообщения. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения.

Authentication code – type of coding algorithm simulation protected information. As a rule, it is post code authenticity of the message. Decision algorithm authentication information is based on checking the authenticity of the message code value.

Avtomatlashtirilgan axborot tizimi – ma'lumotlarni va axborotni yaratish, uzatish, ishlash, tarqatish, saqlash va/yoki boshqarishga va hisoblashlarni amalga oshirishga mo'ljallangan dasturiy va apparat vositalar.

Автоматизированная информационная система – совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.

Automated Information System – a set of software and hardware designed for the creation, transmission, processing, distribution, storage and/or data and information management and production calculations.

Avtorizatsiya – tizimda foydalanuvchiga uning ijobiy autenfikatsiyasiga asosan ma'lum foydalanish huquqlarini taqdim etish.

Авторизация – представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.

Authorization – View user specific access rights on the basis of a positive result in its authentication system.

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 foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalanish sathi holati.

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.

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.

Axborot xavfsizligi – ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifan, ichki va tashqi informatsion ta'sirlarga qarshi tizimning tura olish xususiyati.

Информационная безопасность – способность системы противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение.

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.

Axborot tizimi xavfsizligi – axborot tizimining ruxsatsiz foydalanishiga urinishga qarshi tura olishi xususiyati. Kompyuter tizimining adekvat himoyalanishini ta'minlashga zaruriy elementlar majmui: apparat va/yoki dasturiy funksiyalar, xarakteristikalar va vositalar, amaliy va qaydlash muolajalari; markaziy kompyuterdan, masofadagi kompyuterlardan va telekommunikatsiya vositalaridan foydalanishni boshqarish vositalari; ma'muriy tadbirlar, fizik konstruksiyalar va qurilmalar; xodimlarni va kommunikatsiyalarni boshqarish.

Безопасность информационной системы – свойство информационной системы противостоять попыткам несанкционированного доступа. Совокупность элементов, необходимых для обеспечения адекватной защиты компьютерной системы: аппаратные и/или программные функции, характеристики и

средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удаленных компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.

Information system security – property information system to resist attempts of unauthorized access. Assembly of components necessary to ensure adequate protection of the computer system; comprises hardware and / or software functions, characteristics, and means; operating and accounting procedures, controls access to the central computer, remote computers and telecommunication facilities; administrative measures, physical structures and devices; personnel management and communications.

Axborot – kommunikatsiya texnologiyalari xavfsizligi (AKT xavsizligi) – axborot - telekommunikatsiya texnologiyalarining konfidensialligini, yaxlitligini, foydalanuvchanligini, bosh tortmasligini, hisobdorligini, asliga to'g'riligini va ishonchliligini aniqlash, ularga erishish va ularni madadlash bilan bog'liq barcha jihatlar.

Безопасность информационно – коммуникационных технологий (безопасность ИКТ) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информационно – телекоммуникационных технологий.

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.

Axborot xavfsizligi doktrinasi – axborot xavfsizligini ta'minlash maqsadlariga, masalalariga, prinsiplariga va asosiy yo'nalishlariga rasmiy qarashlar majmui.

Доктрина информационной безопасности – совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности.

Information Security Doctrine -totality of official views on the goals, objectives, principles and guidelines ensuring the information security.

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.

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.

Information reliability – 1. Ability of algorithm 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.

Axborot tizimi – hujjatlarning (hujjatlar massivining) va axborot texnologiyalarining, xususan, axborot jarayonlarini amalga

oshiruvchi hisoblash texnikasi va aloqa vositalaridan foydalanib, tashkiliy tartibga solingan majmui.

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Information system – organizationally ordered set of documents (document files) and information technologies, including with use of computer aids and the communications, realizing information processes.

Axborot texnologiyasi – axborotni ishlash usullari va texnik vositalari tizimi.

Информационная технология – система технических средств и способов обработки информации.

Information technology – system of technical means and ways of information processing.

Axborotdan foydalanish – shtatga oid texnik vositalardan foydalanib, axborot bilan tanishish, uni hujjatlash, nusxalash, modifikatsiyalash yoki axborotni yo'q qilish jarayoni.

Доступ к информации – процесс ознакомления с информацией, ее документирование, модификация или уничтожение, осуществляемые с использованием штатных технических средств.

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.

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'lish.

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.

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.

Axborotni himoyalash konsepsiyasi – axborotni himoyalash bo'yicha qarashlar va umumiy texnik talablar tizimi.

Концепция защиты информации – система взглядов и общих технических требований по защите информации.

The concept of information security – frame of reference and the general technical requirements on information security.

Axborot himoyasi sohasidagi litsenziya – axborot xavfsizligi sohasida u yoki bu ishlarni bajarish huquqiga litsenzion bitim (shartnoma) bilan rasmiylashtirilgan ruxsatnoma.

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации, оформленное лицензионным соглашением (договором).

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/.

Axborot yaxlitligining buzilishi – axborotni texnik vositalari yordamida ishlanishida uning yo'qotilishi, ruxsatsiz modifikasiyalanishi yoki yo'q qilinishi natijasida yaxlitlik xususiyatining yo'qolishi.

Нарушение целостности информации – утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения.

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.

Axborotni soxtalash – axborotning texnik vositalarda ishlanishida raqibning oldida muayyan foyda (afzallik) olish maqsadida axborotni atayin ruxsatsiz modifikatsiyalash.

Подделка информации – умышленная несанкционированная модификация информации при ее обработке техническими средствами с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

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.

Axborotning muhimligi – axborotning insonning maqsadli faoliyatining turli sohalarida amaliy foydalanishga yaroqliligi orqali aniqlanuvchi xususiyati.

Ценность информации – свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности человека.

Information value - property information, determine its applicability to practical use in various fields of purposeful human activity.

Axborotni himoyalash – axborot xavfsizligini ta'minlashga yo'naltirilgan tadbirlar kompleksi. Amalda axborotni himoyalash deganda ma'lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligi, foydalanuvchanligini, shuningdek, agar kerak bo'lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

Защита информации – включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности, а также если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Information protection - includes a complex of the actions aimed at providing information security. In practice it 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.

Axborot yaxlitligi – tasodifan va/yoki atayin buzilish hollarida hisoblash texnikasi vositalarining yoki avtomatlashtirilgan tizimning axborotni o'zgartirmasligini ta'minlovchi xususiyati.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспе-

чивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Information Integrity – the ability of computers and automated systems to provide consistent information in a casual and / or intentional distortion (destruction).

Brandmauer – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli. Yana bir necha komponentlardan (masalan, brandmauer dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan himoya to'sig'i hisoblanadi.

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. Он еще - является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).

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).

Bir taraflama autentifikatsiya – taraflarning autentifikatsiyasi bo'lib, taraflarning biri u bilan o'zaro harakatdagi tarafning haqiqatan ham o'zi ekanligini tekshiradi. Bir taraflama autentifikatsiya ikkita ishtirokchi: isbotlovchi va tekshiruvchi bilan autentifikatsiyalash protokoli orqali amalga oshiriladi.

Односторонняя аутентификация – аутентификация сторон, при которой одна из сторон проверяет, что взаимодействующая с ней сторона именно та, за которую себя выдает. О. а. реализуется протоколом идентификации с двумя участниками: доказывающим и проверяющим.

One-way authentication – authentication of the parties, in which one of the parties to check that it interacts with the side - namely that for which he is. Identification protocol is implemented with two participants: proving and inspection.

Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko'z pardasining to'ri va h.) asosidagi autentifikatsiyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo'lmasligi. Ularni esdan chiqarishning, yo'qotishning yoki boshqa foydalanuvchiga berishning iloji yuq.

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.

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 cannot be forgotten, lost or transferred to another user.

Buzilish – ma'lumotlar signali parametrlari qiymatlarining o'rnatilgan talablardan chetlanishi. Aloqa liniyasi bo'yicha uzatiluvchi xabar tarkibining o'zgarishi.

Искажение – отклонение значений параметров сигнала данных от установленных требований. Изменение содержимого сообщения, передаваемого по линии связи.

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.

Buzilmaslik – tizimning unga yuklatilgan vazifalarni berilgan sharoitda istalgan vaqt onida bajarish qobiliyati.

Безотказность – способность системы выполнять возложенные на нее функции в требуемый момент времени в задаваемых условиях.

Reliability – the ability of the system to fulfill its function in the desired time in the given conditions.

Buzg'unchi – harakatlari ko'rilayotgan kompyuter tizimida axborot xavfsizligini buzadigan subyekt.

Нарушитель – субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Attacker – a subject whose actions violate the information security in a computer system under consideration.

Davlat siri – davlat tomonidan muhofaza qilinuvchi, fosh qilinishi davlatning harbiy-iqtisodiy potensialining sifatli holatiga salbiy ta'sir etuvchi yoki uning mudofaa imkoniyati, davlat xavfsizligi, iqtisodiy va siyosiy manfaatlari uchun boshqa og'ir oqi-

batlarga olib kelishi mumkin bo'lgan ma'lumotlar. Davlat siriga "juda muhim" va "mutlaqo maxfiy" grifli axborot taalluqli.

Государственная тайна – сведения, охраняемые государством, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь за собой другие тяжкие последствия для ее обороноспособности, государственной безопасности, экономических и политических интересов. К государственной тайне относится секретная информация с грифами «особой важности» и «совершенно секретно».

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".

Dezinformatsiya – foydalanuvchi shaxslarga yolg'on tasavvurni shakllantirish maqsadida ularga uzatiluvchi xabarni atayin buzib ko'rsatish; yolg'on axborotni uzatish.

Дезинформация – сознательное искажение передаваемых сведений с целью ложного представления у лиц, использующих эти сведения; передача ложной информации.

Misinformation – deliberate distortion of transmitted data with the purpose of the false representations in individuals using this information; transmission of false information.

«Dushman o'rtada» hujumi – kripttografik protokolga hujum bulib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni

ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman C ishtirokchi A dan ishtirokchi B ga va aksincha, xabarni uzgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o'rtada» hujumining muvaffaqiyatli amalga oshirilishini dushmanga ishtirokchi B uchun o'zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi. «Dushman o'rtada» hujumini amalga oshirish uchun protokolning ikkita seansining sinxronlanishini ta'minlash lozim.

Атака «противник в середине» – атака на криптографический протокол, в которой противник С выполняет этот протокол как с участником А, так и с участником В. Противник С выполняет сеанс с участником А от имени В, а с участником В от имени А. В процессе выполнения сеанса противник пересылает сообщения от А к В и обратно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для В под именем А. Для осуществления атаки «противник в середине» необходимо обеспечивать синхронизацию двух сеансов протокола.

Man-in-the-middle attack - attack on a cryptographic protocol in which the enemy With this protocol performs as a party A and party B. with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During Runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack "in the middle of the enemy" allows authenticate itself to the enemy in the name of A.

To carry out the attack "in the middle of the enemy" is necessary to ensure the synchronization of the two sessions of the protocol.

Fishing – foydalanish paroli, bank va identifikatsiya kartalari ma'lumotlari va h. kabi shaxsiy konfidensial ma'lumotlarni o'g'rilashdan iborat internet-firibgarlik texnologiyasi.

Фишинг – технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д.

Phishing – Internet-fraud technique, is used for stealing personal confidential data such as passwords, bank and identification cards, etc.

Foydalanish ma'muri – ma'lumotlar bazasidan foydalanishni tashkil etishga javobgar, ma'lumotlar banki ma'muriyati tarkibidagi lavozimli shaxslardan biri.

Администратор доступа – один из должностных лиц в составе администрации банка данных, отвечающий за организацию доступа пользователей к базам данных.

Administrator access – one of the officials in the administration part of the data bank, the organization responsible for user access to databases.

Foydalanuvchining autentifikatsiyasi – foydalanuvchi taqdim etgan identifikatori yordamida uning haqiqiyligini tasdiqlash. Foydalanuvchining u taqdim etgan identifikatorga mosligini taqqoslash.

Аутентификация пользователя – подтверждение подлинности пользователя с помощью предъявляемого им аутенти-

фикатора. Проверка соответствия пользователя предъявляемому им идентификатору.

User Authentication – User authentication using against them authenticator. Also, to check compliance against them user ID.

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.

Доступ – предоставление данных системе обработки данных или получение их из нее путем выполнения операций поиска, чтения и (или) записи данных.

Access – providing data processing system or getting them out of it by doing a search, read and (or) data record.

Foydalanuvchanlik – avtorizatsiyalangan foydalanuvchi so'rovi bo'yicha mantiqiy obyektning tayyorlik va foydalanuvchanlik holatida bo'lishi xususiyati.

Доступность – свойство логического объекта находиться в состоянии готовности и используемости по запросу авторизованного пользователя.

Availability, accessibitity – property of an object in a state of readiness and usage upon request authorized entity.

Foydalanish identifikatori – foydalanuvchi subyekt yoki obyektning noyob alomati.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Access identifier - unique sign of the subject or object of access.

Foydalanuvchi identifikatori – hisoblash tizimi resurslaridan foydalanish uchun alohida shaxsga yoki shaxslar guruhiga beriladigan ramziy ism.

Идентификатор пользователя – символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы.

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.

Foydalanishni tanlab boshqarish – foydalanuvchini, jarayonni va/yoki u tegishli guruhni identifikatsiyalashga va tanishga asoslangan tizim subyektlarining obyektlardan foydalanishni boshqarish usuli. Bunda ma'lum huquqli subyekt huquqlarni har qanday obyektga o'rnatilgan cheklashlarga bog'liq bo'lmagan holda uzatishni amalga oshirishi mumkin.

Избирательное управление доступом – метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Управление является избирательным в том смысле, что субъект с определенными правами может осуществлять передачу прав любому объекту независимо от установленных ограничений.

Discretionary access control – method of control over access of subjects of system to. To the objects, based on identification and an identification of the user, process and/or group to which it belongs. Management is selective in the sense that the subject with certain rights can carry out transfer of rights to any object

irrespective of the set restrictions (access can be provided and not directly).

Foydalanish nazorati – foydalanuvchilarning, dasturlarning yoki jarayonlarning hisoblash tizimlari qurilmalaridan, dasturlaridan va ma'lumotlaridan foydalanishlarini aniqlash va cheklash.

Контроль доступа – определение и ограничение доступа пользователей, программ или процессов к устройствам, программам и данным вычислительной системы.

Assess control – definition and restriction of access of users, programs or processes to devices, programs and data of the computing system.

Foydalanishni mandatli boshqarish – maxfiylik (konfidensiallik) belgisi orqali aniqlanuvchi maxfiylik grifi buyicha axborotdan foydalanishga ruxsat etilgan subyektlarning axborot resurslaridan foydalanish konsepsiyasi (modeli).

Мандатное управление доступом – концепция (модель) доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности (конфиденциальности).

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/.

Foydalanish matritsasi – xususidagi ma'lumotlar foydalanish dispetcherida saqlanuvchi axborot resurslaridan subyektlarning foydalanish qoidalarini aks ettiruvchi jadvallar; foydalanishni cheklash qoidalarini aks ettiruvchi jadval.

Матрица доступа – таблица, отображающая правила доступа субъектов к информационным ресурсам, данные о которых храняться в диспетчере доступа. Таблица, отображающая правила разграничения доступа.

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.

Foydalanishni vakolatli boshqarish – obyektlar tarkibidagi axborotning konfidensialligini xarakterlovchi belgiga va subyektlarning bunday konfidensiallik darajasiga ega informatsiyaga murojaat etishlariga rasmiy ruxsatga asoslangan subyektlarning obyektlardan foydalanishlarini cheklash.

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.

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.

Foydalanish huquqini taqdim etish – muayyan dasturlar va ma'lumotlardan foydalanishga ruxsat (sanksiya) berish.

Предоставление права на доступ – выдача разрешения (санкции) на использование определенных программ и данных.

Authorization – authorization (approval) to use certain programs and data.

Foydalanishni boshqarish – foydalanuvchilarning, dasturlarning va jarayonlarning ma'lumotlardan, hisoblash texnikasi dasturlari va qurilmalaridan foydalanishlarini belgilash va cheklash.

Управление доступом – определение и ограничение доступа пользователей, программ и процессов к данным, программам и устройствам вычислительной системы.

Access control – definition and limitation of access users, programs, and processes the data, programs, and devices of a computer system.

Frod – inglizcha fraud - 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.

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.

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.

Foydalanish turi — ma'lum qurilmadan, dasturdan, fayldan va h. foydalanish huquqining ma'nosi (odatda read, write, execute, append, modify, delete).

Тип доступа – сущность права доступа к определенному устройству, программе, файлу и т.д. (обычно 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).

Foydalanishni boshqarish kaliti – jarayon tomonidan ma'lumotlar bazasini boshqarish tizimiga beriluvchi va ma'lumotlardan ruxsatsiz foydalanishni bartaraf etish maqsadida mos qulf bilan taqqoslanuvchi qiymat.

Ключ управления доступом – значение, предъявляемое процессом системе управления базой данных и сравниваемое ею с соответствующим замком с целью предотвращения несанкционированного доступа к данным.

Access control key – the value shown by process to a database management system and compared by it to the corresponding lock for the purpose of prevention of unauthorized access to data.

Foydalanishni cheklash – ma'lumotlarni foydalanuvchilarning ruxsatsiz foydalanishlaridan himoyalashni ta'minlovchi usullar, vositalar va tadbirlar majmui.

Разграничение доступа – совокупность методов, средств и мероприятий, обеспечивающих защиту данных от несанкционированного доступа пользователей.

Access control – a set of methods, tools and measures to ensure the protection of data from unauthorized users.

Himoya ma'muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Администратор защиты – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Security administrator – access entity responsible for the protection of the automated system from unauthorized access to information.

Himoyaning apparat vositalari – axborotni ruxsatsiz foydalanishdan, modifikatsiyalanishidan, nusxalashdan, o'g'irlanishidan himoyalashga mo'ljallangan mexanik, elektromexanik, elektron, optik, lazer, radio, radiotexnik, radiolokatsion va boshqa qurilmalar, tizimlar va inshooatlar.

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.

Hardware protection – mechanical, electromechanical, electronic, optical, laser, radio, radio, radar and other devices, systems and structures designed to protect the information from unauthorized access, copying, modification or theft.

Himoya mexanizmlari turlari – himoya mexanizmlarining ba'zi turlari - shifrlash, kalitlarni ma'muriy boshqarish jihatlari, raqamli imzo mexanizmlari, foydalanishni boshqarish mexanizmlari, ma'lumotlar yaxlitligi mexanizmlari, autentifikatsiya axborotini almashish mexanizmlari, trafikni to'ldirish mexanizmlari, marshrutlashni boshqarish mexanizmi, notarizatsiya mexanizmi, fizik yoki shaxsiy himoya, ishonchli apparat dasturiy ta'minot.

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.

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.

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.

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.

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.

Himoyalash – hisoblash tizimidan yoki uning qismidan foydalanishni cheklash vositasi; apparaturadan, dasturdan va ma'lu-

motlardan ruxsatsiz foydalanishni bartaraf etuvchi tashkiliy va texnik, jumladan, dasturiy choralar.

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.

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.

Himoyalangan dastur – nusxalashdan himoyalangan dastur.

Защищенная программа – программа, защищенная от копирования.

Copy protected software – the program protected from copying.

Himoyalangan tizim – kirish uchun parol talab qilinadigan tizim.

Защищенная система – система, вход в которую требует ввода пароля.

Protected system – system, an entrance in which demands password input.

Himoyalanganlik – hisoblash texnikasida tizimning dasturlardan va ma'lumotlardan ruxsatsiz foydalanishiga (xavsizlik, maxfiylik) hamda ularni tasodifan buzilishiga (yaxlitlik) yoki o'zgartirilishiga qarshi tura olish xususiyati.

Защищенность – системы в вычислительной технике способность противостоять несанкционированному доступу к

программам и данным (безопасность, секретность), а также их случайному искажению или разрушению (целостность).

Security, immunity – in computer facilities ability of system to resist to unauthorized access to programs and data (safety, privacy), and also to their casual distortion or destruction (integrity).

Himoyalangan fayl – yozuvlaridan foydalanish uchun parol talab qilinadigan fayl.

Защищенный файл – файл, для доступа к записям которого необходимо ввести пароль.

Protected file – the file, for access to which records it is necessary to enter the password.

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.

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.

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.

Himoyalash strategiyasi – tizimning ma'lum tahdidlardan himoyalashni ta'minlashda amal qilinishi lozim bo'lgan mezonlarni, ayniqsa, operativ mezonlarni rasmiy aniqlash.

Стратегия защиты — формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

Security strategy – a formal definition of the criteria, particularly operational, to be followed while protecting the system against known threats.

Himoya profili – axborotni himoyalash masalalarini funksional talablar va kafolatlanish talablari atamalarida tavsiflovchi hujjat.

Профиль защиты — документ, описывающий задачи обеспечения защиты информации в терминах функциональных требований и требований гарантированности.

Protection Profile – document describing the task of ensuring the protection of information in terms of the functional requirements and the requirements of the warranty.

Hujjat – axborotning ixtiyoriy usullarda amalga oshirilgan matnli va grafik materiallar ko'rinishida hamda perforatsiyalangan va magnit eltuvchilarda, foto va kinoplyonka ko'rinishida mavjudlik shakli. Matnli va grafik materiallar qo'lda yozilishi, tasvirlanishi, chizilishi, mashinkada yozilishi yoki tipografik usul orqali bajarilishi mumkin.

Документ – форма существования информации в виде текстовых и графических материалов, выполненных любыми способами, а также в виде перфорированных и магнитных носителей, фото и кинопленок. Текстовые и графические материалы могут быть написаны от руки, нарисованы, выграви-

рованы, начерчены, напечатаны на машинке или исполнены типографским способом.

Document – existence form information in the form of test and graphics made by any means, as well as perforated and magnetic carriers, the photo - and films. Text and graphics can be written by hand, painted, engraved, drawn, typed or filled in hard copy.

Hujjatlangan axborot – rekvizitlari identifikatsiyalanishiga imkon beruvchi, material eltuvchida qaydlangan axborot.

Документированная информация – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Documented information – fixed in a tangible medium with requisites allowing its identification.

Identifikatsiya – foydalanish subyektlari va obektlariga identifikator berish va/yoki taqdim etilgan identifikatorni berilganlari ro'yxati bilan taqqoslash.

Идентификация – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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.

Identifikatsiya va autentifikatsiya – tizim foydalanuvchisining resurslardan foydalanish huquqini qo'lga kiritish uchun bajariladigan o'z nomini tanishtirish va haqiqiyligini (aynan o'zi ekanligini) tasdiqlash jarayonini belgilovchi umumiy atama.

Идентификация и аутентификация – общий термин для обозначения процесса представления своего имени и подтверж-

дения подлинности (идентичности) пользователя системы, который выполняется им для получения права доступа к ресурсам.

Identification and Authentication (I&A) – the general term for designation of process of representation of the name and confirmation of authenticity (identity) of the user of system who is carried out by it for receiving right of access to resources.

Identifikatsiya so'rovi – boshqaruvchi stansiyaning boshqariluvchi stansiyaga uni identifikatsiyalash yoki holatini aniqlash uchun bergan so'rovi.

Запрос идентификации (опознания) – запрос, заданный ведущей станцией ведомой станции для ее идентификации или определения ее состояния.

Request identification – query specified slave master station to identify it or determine its status.

Identifikator – subyekt yoki obyektning farqlanuvchi alomatidan iborat foydalanishning identifikatsiya vositasi. Foydalanuvchilar uchun asosiy identifikatsiya vositasi parol hisoblanadi.

Идентификатор – средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

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.

Identifikatsiya ma'lumotlari – tizimda bir ma'noli identifikatsiyalanishiga imkon beruvchi, muayyan qatnashchiga tegishli noyob identifikatsiya ma'lumotlari majmui.

Идентификационные данные – совокупность уникальных идентификационных данных, соответствующая конкретному участнику, позволяющая осуществить однозначную его идентификацию в системе.

Data identification – a set of unique identification data corresponding to a specific party, it allows an unambiguous identification of the system.

Ijtimoiy injeneriya – xizmatchi xodimlar va foydalanuvchilar bilan turli hiyla-nayrang, aldov orqali chalg'itish asosidagi muloqotdan olinadigan axborot yordamida axborot tizimining xavfsizlik tizimini chetlab o'tish.

Социальная инженерия – обход системы безопасности информационной системы с помощью информации, получаемой из контактов с обслуживающим персоналом и пользователями на основе введения их в заблуждение за счет различных уловок, обмана и пр.

Social engineering – round of system of safety of system information by means of information received from contacts with the service personnel and users on the basis of their introduction in delusion at the expense of various tricks, deception and so forth.

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

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).

Two-factor authentication – user authentication based on two different factors are usually based on what the user knows, and what he owns (ex. password-based and physical identifier).

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/IPning aniq xizmatlari generatsiyalaydigan axborotni shlyuz orqali uzatilishini ta'minlaydi.

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.

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.

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.

Разделение привилегий – принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

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).

Insayder – guruhga tegishli yashirin axborotdan foydalanish huquqiga ega guruh a'zosi. Odatda, axborot sirqib chiqish bilan bog'liq mojoroda muhim shaxs hisoblanadi. Shu nuqtayi nazardan insayderlarning quyidagi xillari farqlanadi: beparvolar; manipulyatsiyalanuvchilar, ranjiganlar, qo'shimcha pul ishlovchilar va x.

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.

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.

Ishonch – axborot texnologiyalari mahsulotining yoki tizimining xavfsizlik maqsadlariga javob berishiga ishonish uchun asos.

Доверие – основа для уверенности в том, что продукт или система информационных технологий отвечают целям безопасности.

Assurance – basis for confidence that the product or system information technology meet the security objectives.

Ishonchlilik – xavfsizlikning qandaydir mezonlarga moslik xususiyati.

Доверительность – свойство соответствия безопасности некоторым критериям.

Trusted functionality – compliance with safety properties of some criteria.

Ishonchlilik – axborotninig to'g'ri o'zlashtirilish xususiyati; xatolik yo'qligining ehtimolligi.

Достоверность — свойство информации быть правильно воспринятой; вероятность отсутствия ошибок.

Validity, adequacy – property information to be correctly perceived; the probability of no errors.

Ishonchlilik – ma'lum sharoitlarda berilgan vaqt oralig'ida funksional uzelning, qurilmaning, tizimning o'ziga topshirilgan vazifalarni bajarish qobiliyatining xarakteristikasi.

Надежность – характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени.

Reliability – the ability of the functional characteristics of node devices, the system under certain circumstances to carry out the desired function during a certain

Java tili – Sun Microsystems, Inc. tomonidan ishlab chiqilgan yangi dasturlash tili. U oddiy til sifatida tarmoq ilovalarini ishlab chiqish uchun qo'llanilishi mumkin. Undan tashqari u applet deb ataluvchi katta bo'lmagan ilovalarni yozishda qo'llaniladi.

Язык Java – новый язык программирования, разработанный Sun Microsystems, Inc. Он может использоваться как обычный язык программирования для разработки сетевых приложений. Кроме того, он используется для написания небольших приложений, называемых апплетами.

Language Java – a new programming language developed by Sun Microsystems, Inc. It can be used as a conventional programming language for development of network applications. In addition, it is used for writing small applications called applets.

Jurnal – statistik axborotni, turli xabarlarni va boshqa ma'lumotlarni yig'ish va hisobga olish uchun operatsion yoki boshqa tizim foydalanadigan hisoblash texnikasidagi ma'lumotlar nabori (fayl).

Журнал – набор данных (файл), в вычислительной технике, используемый операционной или иной системой для сбора и учета статистической информации, различных сообщений и других данных.

Journal, log – in computing the data set (file) used by the operating system or another for collection and recording of statistical information, different messages and other data.

Jurnallashtirish – tizimli jurnalga xabarlar, so'rovlar, bajarilgan dasturlar, ishlatilgan ma'lumotlar nabori va boshqa ma'lumotlar xususida axborotni yozish jarayoni.

Журнализация – процесс записи в системный журнал информации о сообщениях, запросах, выполнявшихся программах, использованных наборах данных и других сведений.

Journalizing – process the system log information about messages, queries, execute programs, use a set of data and other information.

Konseptual model – muammoli sohaning tushuncha sathidagi rasman ifodasi.

Концептуальная модель – формальное представление проблемной области на понятийном уровне.

Conceptual model – formal representation of problem area at conceptual level.

Kod – 1. Simvolni ikkilik kod orqali ifodalash. 2. Matnni kodlangan shaklga o'zgartirishda ixtiyoriy jadvaldan yoki kodlash kitobidan foydalanuvchi kriptografik usul.

Код – 1. Представление символа двоичным кодом. 2. Криптографический прием, в котором используется произвольная таблица или кодировочная книга для преобразования текста в закодированную форму.

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.

Kirib olish kanali – niyati buzuqdan to konfidensial axborot manbaigacha bo'lgan yo'l. U orqali himoyalanuvchi ma'lumotlardan ruxsatsiz foydalanishi mumkin.

Канал проникновения – путь от злоумышленника к источнику конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям.

Insecurity channel – actual path from the malefactor to a source of confidential information by means of which unauthorized access to protected data is possible.

Kiberjinoyatchilik – g'arazli yoki bezorilik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o'g'irlashga yoki buzishga yo'naltirilgan alohida shaxslarning yoki guruhning harakatlari.

Киберпреступность – действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях.

Cybercrime – 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.

Konfidensial axborotdan foydalanish – muayyan shaxsga tarkibida konfidensial xarakterli ma'lumot bo'lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati.

Доступ к конфиденциальной информации – санкционированное полномочным должностным лицом ознакомление конкретного лица с информацией, содержащей сведения конфиденциального характера.

Access to confidential information – authorized authorized official introduction of a particular person with the information containing confidential information.

Kompyuter tizim xavfsizligi – kompyuter tizimining destruktiv harakatlarga va yolg'on axborotni zo'rlab qabul qilinishiga olib keluvchi ishlanuvchi va saqlanuvchi axborotdan ruxsatsiz foydalanishga urinishlarga qarshi tura olish xususiyati.

Безопасность компьютерных систем – свойство компьютерных систем противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям и навязыванию ложной информации.

Security of computer systems – property computer systems to resist attempts of unauthorized access to information processed and stored, the input of information, leading to destructive actions, and the imposition of false information.

Ko'p faktorli autentifikatsiya – bir necha mustaqil faktorlar asosida foydalanish nazoratini amalga oshirish. Autentifikatsiyaning turli usullari asosida foydalanishni boshqarishning barqaror tizimini amalga oshirishni tashkil etish imkoniyatiga ega moslanuvchan yondashish hisoblanadi. Ko'p faktorli autentifikatsiya texnologiyasi tarkibiga bir martali parollar, sertifikatlar asosidagi autentifikatsiya, kontekst asosidagi autentifikatsiya va h. kiradi.

Многофакторная аутентификация – реализация контроля доступа, представляющая собой идентификацию пользователя на основе нескольких независимых факторов. Представляет гибкий подход, позволяющий организации реализовать устойчивую систему управления доступом на основе использования различных методов аутентификации. Технологии м.а. включают: одноразовые пароли, аутентификацию на основе сертификатов, аутентификацию на основе контекста и др.

Multifactor Authentication – implementing access control, which is a user identification based on several independent factors. A flexible approach allows organizations to implement robust

access control system based on the use of different authentication methods.

Litsenziya – sotish yoki xizmat ko'rsatish huquqiga ruxsatnoma. .

Лицензия – разрешение на право продажи или предоставления услуг.

License – permission to the right of sale or service.

Lug'atga asoslangan hujum – kriptotizimga ochiq matn elementlari lug'atidan foydalanishga asoslangan hujum.

Атака со словарем – атака на криптосистему, использующая словарь элементов открытого текста.

With a dictionary Attack – attack on the cryptosystem that uses a dictionary of text elements open.

Ma'lumotlarning shajara modeli – shajara strukturasi ma'lumotlarini ifodalovchi ma'lumotlar modeli.

Иерархическая модель данных – модель данных для представления данных иерархической структуры.

Hierarchical model – model given for data presentation of hierarchical structure.

Ma'lumotlarning shajara strukturasi – qisman tartibga solingan to'plamdan iborat ma'lumotlar strukturasi. Bunda ushbu to'plamning oldingi elementlariga ega bo'lmagan faqat bitta elementi mavjud, boshqa barcha elementlari esa faqat bitta oldingi elementga ega.

Иерархическая структура данных – структура данных, представляющая собой множество, частично упорядоченное таким образом, что существует только один элемент этого мно-

жества, не имеющий предыдущего, а все другие элементы имеют только один предыдущий.

Hierarchical data structure – the structure of data representing a set, partially ordered in such a way that exists only one element of this set which doesn't have previous, and all other elements have only one previous.

Ma'lumotlar avtorizatsiyasi – ma'lumotlarning ma'lumotlar bazasiga tegishli darajasini aniqlash va belgilash.

Авторизация данных – определение и установление степени приватности данных в базе данных.

Data authorization – identification and degree of privacy data in the database.

Ma'lumotlar bazasi ma'muri – ma'lumotlar bazasi xususida to'liq tasavvurga ega va undan foydalanish va rivojlantirish uchun javobgar maxsus lavozimli shaxs (shaxslar guruhi). Ma'lumotlar banki ma'muriyati tarkibiga kiradi.

Администратор базы данных – специальное должностное лицо (группа лиц), имеющее(ие) полное представление о базе данных и отвечающее за ее ведение, использование и развитие. Входит в состав администрации банка данных.

Database Administrator – special officer (group of persons) having (s) a complete picture of the database and is responsible for its maintenance, use and development. Included in the administration of the bank data.

Ma'lumotlar banki ma'muriyati – ma'lumotlar bankining ekspluatatsiyasiga javobgar shaxslar guruhi (bo'linma): ma'lumotlar bazasini yuritish, undan tashqari kollektiv foydalanishni tashkil etish va tizimni rivojlantirish.

Администрация банка данных – группа лиц (подразделение), отвечающих за эксплуатацию банка данных: ведение баз данных, организацию коллективного доступа к ним пользователей и развитие системы.

Administration Data Bank – a group of persons (unit), responsible for the operation of a data bank: maintenance of databases, the collective access to users and system development.

Ma'lumotlar bazasini ma'murlash – bazadagi ma'lumotlarni aniqlash, tashkil etish, boshqarish va himoyalash vazifalarini bajarish.

Администрирование базы данных – выполнение функций определения, организации, управления и защиты данных в базе.

Database Administration – acting as determining the organization, management and protection of data in the database.

Ma'lumotlar autentifikatsiyasi (raqamli imzo) – elektron shaklda taqdim etilgan ixtiyoriy ma'lumotlarninng haqiqiyligini (soxtalashtirishning yoki buzilishning yo'qligini) tasdiqlash jarayoni. Ma'lumotlar, xabarlar, fayl, ma'lumotlar bazasi (dastur) elementlari, foydalanuvchining identifikatori (autentifikatori), tarmoq abonenti manzili va h. ko'rinishida bo'lishi mumkin.

Аутентификация данных (цифровая подпись) – процесс подтверждения подлинности (отсутствия фальсификации или искажения) произвольных данных, предъявленных в электронной форме. Данные могут представлять собой: сообщения, файл, элементы базы данных (программы), идентификатор (аутентификатор) пользователя, адрес сетевого абонента и т.п.

Authentication data (digital signature) – authentication process (lack of falsification or distortion) of arbitrary data, presented in electronic form. These may be: the message file, the database item (program), an identifier (an authenticator) the user is connected to a network address, etc.

Ma'lumotlar manbaining autentifikatsiyasi – olingan ma'lumotlar manbaining haqiqiyligini tasdiqlash.

Аутентификация источника данных – подтверждение подлинности источника полученных данных.

Data origin authentication – confirmation of the authenticity of the source of the data obtained.

Ma'lumotlar bazasi – tatbiqiy dasturlarga bog'liq bo'lmagan holda ma'lumotlarni tavsiflash, saqlash va manipulyatsiyalashning umumiy prinsiplarini ko'zda tutuvchi, ma'lum qoidalar bo'yicha tashkil etilgan ma'lumotlar majmui. Predmet sohasining informatsion modeli hisoblanadi. Ma'lumotlar bazasi odatda abstraksiyaning tashqi, konseptual va ichki sathlari orqali ifodalanadi.

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информационной моделью предметной области. БД, как правило, представляется тремя уровнями абстракции: внешним, концептуальным и внутренним.

Database – a set of data organized according to certain rules, general principles providing descriptions, storing and manipulating data, regardless of the application. Information is the domain model.

Database, usually represented by three levels of abstraction: external, conceptual and internal.

Ma'lumotlar banki – ma'lumotlarni markazlashgan saqlash va kollektiv foydalanishning avtomatlashtirilgan informatsion tizimi. Bank tarkibiga bir yoki bir necha bazasi, ma'lumotlar bazasining boshqarish tizimi hamda so'rovlar va tatbiqiy dasturlar bibliotekasi kiradi. Foydlanuvchilarning ma'lum guruhiga ma'lum tematika bo'yicha ma'lumotlarni saqlash va qidirish xizmatlarini taqdim etish.

Банк данных – автоматизированная информационная система централизованного хранения и коллективного использования данных. В состав банка данных входят одна или несколько баз данных, справочник баз данных, система управления базами данных, а также библиотека запросов и прикладных программ. Система, предоставляющая услуги по хранению и поиску данных определенной группе пользователей по определенной тематике.

Databank – automated information system for centralized storage and sharing of data. The structure of the data bank includes one or more databases, reference databases, database management system, as well as libraries of queries and applications. More - a system that provides services for data storage and retrieval specific group of users on a particular topic.

Ma'lumotlar xavfsizligi – ma'lumotlarni ruxsatsiz (atayin yoki tasodifan) modifikatsiyalanishidan, buzilishidan, fosh etilishidan himoyalash. Kompyuter tizimining ishlanadigan va saqlanadigan axborotdan ruxsatsiz foydalanishga qarshi tura olishi xususiyati.

Безопасность данных – защита данных от несанкционированной (случайной или намеренной) модификации, разрушения или раскрытия. Свойство компьютерной системы противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации.

Data security – protection of data against unauthorized (accidental or intentional) modification, destruction or disclosure. Also, property of a computer system to resist the attempts of unauthorized access to information stored and processed.

Ma'lumotlar bazasini yuritish – ma'lumotlar bazasini yangilash va tiklash hamda uning strukturasini qayta qurishga yo'naltirilgan faoliyat.

Ведение базы данных – деятельность, направленная на обновление и восстановление базы данных, а также на перестройку ее структуры.

Maintaining a database – activities aimed at updating and restoring the database, as well as the restructuring of its structure.

Ma'lumotlar bazasining tashqi sxemasi – ma'lumotlarning muayyan modeliga muvofiq ma'lumotlar bazasining tashqi sathdagi rasmiy tavfsifi.

Внешняя схема базы данных – формальное описание базы данных на внешнем уровне в соответствии с конкретной моделью данных.

External scheme database – the formal description of the database at the external level, in accordance with a specific data model.

Ma'lumotlar bazasining ichki sxemasi – ma'lumotlarning muayyan modeliga muvofiq ma'lumotlar bazasining ichki sathidagi rasmiy tavsifi.

Внутренняя схема базы данных – формальное описание базы данных на внутреннем уровне в соответствии с конкретной моделью данных.

Internal schema database – formal description of the database at the domestic level in accordance with a specific data model.

Ma'lumotlar bazasini tiklash – 1) Ma'lumotlar bazasini to'liq yoki qisman qayta yuklash. 2) Mashina yanglishishi yoki dasturiy xatolik holida ma'lumotlar yaxlitligini madadlash maqsadida ma'lumotlar bazasi tarkibini rezerv nusxa bo'yicha asliga keltirish.

Восстановление базы данных – 1) Полная или частичная повторная загрузка базы данных. 2) Воссоздание содержимого базы данных по резервной копии, выполняемое в случае машинных сбоев или программных ошибок для поддержания целостности данных.

Database recovery – 1) Complete or partial reload database. 2) Restoration of the database contents from a backup performed in the case of machine failures or software errors to maintain data integrity.

Ma'lumotlarni tiklash – eltuvchining asl nusxasida ma'lumotlar yaxlitligi buzilganida unga ma'lumotlarning himoya nusxasi bo'lgan eltuvchidan nushalash jarayoni.

Восстановление данных – процесс копирования данных с носителя, содержащего защитную копию данных, на носитель оригинал в случае нарушения на нем целостности данных.

Data recovery – the process of copying data from one media containing protecting your data on original carrier in case of violation of the integrity of the data on it.

Ma'lumotlar – odam ishtiroki bilan yoki avtomatik tarzda uzatishga, izohlashga yoki ishlashga yaroqli, formallashgan ko'rinishda ifodalangan axborot.

Данные – информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека либо автоматическими средствами.

Data – information presented in a formalized manner suitable for communication, interpretation or processing involving human or automated means.

Maxfiy hujjat – maxfiy axborotli har qanday eltuvchidan foydalanish cheklangan hujjat.

Конфиденциальный документ – документ ограниченного доступа на любом носителе, содержащий конфиденциальную информацию.

Confidential document – document restricted in any medium, containing confidential information.

Ma'lumotlarni himoyalash – ma'lumotlarni ruxsatsiz, atayin yoki tasodifan ochilishidan, modifikatsiyalanishidan yoki yo'q qilinishidan qo'riqlash.

Защита данных – охрана данных от несанкционированного, умышленного или случайного их раскрытия, модификации или уничтожения.

Data protection – protection of data from unauthorized, deliberate or their casual disclosure, modification or destruction.

Mojaro – ruxsatsiz foydalanish huquqiga ega bo'lishga yoki kompyuter tizimiga hujum o'tkazishga urinishning qayd etilgan holi.

Инцидент – зафиксированный случай попытки получения несанкционированного доступа или проведения атаки на компьютерную систему.

Incident – the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.

Ma'lumotlarni uzatuvchi kanal – fizik muhit, u orqali axborot bir qurilmadan ikkinchisiga uzatiladi.

Канал передачи данных – физическая среда, по которой передается информация из одного устройства в другое.

Data transmission channel – the physical environment on which information from one device is transferred to another.

Ma'lumotlar bazasi kaliti – ma'lumotlar bazasini boshqarish tizimi tomonidan berilgan va ma'lumotlar bazasidagi yozuvni bir ma'noda identifikatsiyalovchi kalit.

Ключ базы данных – ключ, присвоенный системой управления базой данных и однозначно идентифицирующий запись базы данных.

Database key – the key which is appropriated by a database management system and unambiguously identifying record of a database.

Mandat – obyektdan foydalanish va uning ustida ruxsat etilgan amallarni bajarish yo'lini aniqlovchi ko'rsatkich turi.

Мандат – разновидность указателя, определяющий путь доступа к объекту и разрешенные над ним операции.

Sarability, Mandate — kind of the index defining a way of access to object and operations allowed over it.

Ma'lumotlarni ishlash – ma'lumotlar ustida amallarning muntazam bajarilishi.

Обработка данных — систематическое выполнение операций над данными.

Data processing – manipulation of data by a computer.

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.

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.

Data error – a condition in which data on a digital medium has been altered erroneously. The error can manifest as several incorrect bits or even a single bit that is 0 when it should be 1 or vice versa.

Ma'lumotlar bazasini ma'murlash tili – ma'lumotlar bazasini ma'murlash bilan bog'liq harakatlarni tavsiflash uchun qo'llaniladigan sun'iy til.

Язык администрирования базы данных – искусственный язык для описания действий, связанных с администрированием базы данных.

Database administration language – artificial language to describe actions related to database administration.

Ma'lumotlar bazasi tili – ma'lumotlar bazasini yaratish, yuritish va qo'llash jarayonlarini tavsiflash uchun qo'llaniladigan sun'iy til.

Язык базы данных – искусственный язык для описания процессов создания, ведения и использования баз данных.

Database language – artificial language to describe the creation, maintenance and use of databases.

Mualliflik huquqi – fan, adabiyot va san'at asarlarini yaratish, foydalanish va huquqiy himoyalashda vujudga keladigan munosabatlarni tartibga soluvchi huquqiy normalar majmui.

Авторское право – совокупность правовых норм (раздел гражданского права), которые регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства.

Copyright – the body of law (Civil Law Section), which regulate the relations arising in connection with the creation and use of scientific, literary and artistic works (copyright.

Niyati buzuq – dasturlardan yoki ma'lumotlardan ruxsatsiz foydalanishdan manfaatdor, bunday foydalanishga uringan yoki amalga oshirgan shaxs yoki tashkilot.

Злоумышленник – лицо или организация, заинтересованные в получении несанкционированного доступа к программам или данным, предпринимающие попытку такого доступа или совершившие его.

Intruder – the person or the organization interested in receiving unauthorized access to programs or data, making an attempt of such access or made it.

Ortiqchalik – tizim ishonchliligini oshirish maqsadida unga keragidan ortiq qo'shimcha komponentlarning kiritilishi. Apparat, algoritm, informatsion ortiqchaliklar farqlanadi.

Избыточность – введение в систему дополнительных компонентов сверх минимально необходимого их числа с целью повышения надежности системы. Различают избыточность аппаратную, информационную, алгоритмическую.

Redudancu - introducing additional components into the system in excess of the minimum required number of them in order to increase system reliability. There are redundant hardware, information, algorithmic.

Obro'sizlantirish – jiddiy axborotni yo'qotish yoki uni avtorizatsiyalanmagan subyektlar (shaxslar, dasturlar, jarayonlar va h.k.) tomonidan o'zlashtirilishi.

Компрометация – утеря значительной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т.д.)

Compromising - loss of critical information or receiving it the subjects not authorized for this purpose (persons, programs, processes, etc.)

Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan hujum.

Атака со словарем паролей – атака на криптосистему, основанная на переборе значений пароля.

Attack with a dictionary of passwords – an attack on a cryptosystem based on iterating values password.

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'irlashga urinib ko'radi.

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.

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.

Parollarni fosh qiluvchi – parollarni tanlashni yoki o'g'irlashni amalga oshiruvchi kompyuter dasturi.

Вскрыватель паролей – компьютерная программа, которая осуществляет подбор или похищение паролей.

Password cracker – computer program that carries out the selection or stealing passwords.

Parol – tizimdan, dasturdan yoki ma'lumotlardan foydalanishga ruxsat olish uchun kompyuter so'rovi bo'yicha kiritiladigan simvollarning noyob ketma-ketligi.

Пароль – уникальная последовательность символов, которую необходимо ввести по запросу компьютера, чтобы получить доступ к системе, программе или данным.

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.

Ruyxatga olingan foydalanuvchi – berilgan kollektiv foydalanuvchi tizimda ustuvor nomerli foydalanuvchi.

Зарегистрированный пользователь – пользователь, имеющий приоритетный номер в данной системе коллективного пользования.

Authorized user – a user with a priority number in the system of collective use.

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. Himoyalashning eng keng tarqalgan dasturiy usuli parollar tizimi hisoblanadi.

Защита от несанкционированного доступа – предотвращение или существенное затруднение несанкционированного доступа к программам и данным путем использования аппаратных, программных и криптографических методов и средств защиты, а также проведение организационных мероприятий. Наиболее распространенным программным методом защиты является система паролей.

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.

Rezident – asosiy xotirada doimo mavjud.

Резидентный – постоянно присутствующий в оперативной памяти.

Resident – constantly present in memory.

Samaradorlik – berilgan miqdordagi xarakteristikalari bilan xizmat ko'rsatishga bo'lgan talablarni qondiruvchi obyektning xususiyati.

Эффективность – свойство объекта удовлетворять требованиям к услуге с заданными количественными характеристиками.

Efficiency – object property to satisfy the requirements of the service with the given quantitative characteristics.

Soxtalashtirish – boshqa tizim IP-adresidan foydalanib, unga o'xshab niqoblanish yordamida IP-adreslar asosida foydalanishni boshqarish tizimini chetlab o'tish uchun turli texnologiyalardan foydalanish.

Фальсификация – использование различных технологий для обхода систем управления доступом на основе IP-адресов с помощью маскирования под другую систему, используя ее IP-адрес.

Spoofing – the use of different technologies to bypass access control systems, IP-based addresses using masking under another system using its IP-address.

Server-vositachi – brandmauer bo'lib, unda barcha avtorizatsiyalangan mijozlarning IP-adreslarini brandmauer bilan bog'liq IP-adreslarga o'zgartirish uchun adreslarni translyatsiyalash (adress translation) deb ataluvchi jarayondan foydalaniladi.

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).

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).

Seans sathi shlyuzi – avtorizatsiyadan o'tgan mijoz va tashqi xost o'rtasidagi to'g'ridan-to'g'ri o'zar aloqa amalga oshishiga yo'l

qo'ymaydi. Shlyuz ishonchli mijozdan so'rov qabul qiladi va so'ralgan seansga ruxsat etilganligini tekshiruvidan so'ng tashqi xost bilan aloqani o'rnatadi. Shundan so'ng ikkala yo'nalishda tarmoq paketlarini filtrlamasdan nusxa oladi.

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.

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.

So'rovlar tili – ma'lumotlar bazasida ma'lumotlarni qidirish so'rovlari va ular ustida amallar bajarishni tavsiflashda qo'llaniladigan sun'iy til.

Язык запросов – искусственный язык для описания запросов, поиска данных в базах данных и действий над запросами.

Query language – artificial language to describe the query, retrieval of data in databases and actions on requests.

Tizim ma'muri – tizimni ekspluatatsiyasiga va uning ishga layoqatligini ta'minlashga javobgar shaxs.

Администратор системы – лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.

The system administrator – the person responsible for the operation of the system and maintaining it in working condition.

Texnik razvedka apparaturasi – razvedka axborotini òlishga mo'ljallangan aniqlash, qabul qilish, qaydlash, o'lchash va tahlillash texnik qurilmalari majmui.

Аппаратура технической разведки – совокупность технических устройств обнаружения, приема, регистрации, измерения и анализа, предназначенная для получения разведывательной информации.

Equipment and technical intelligence – a set of technical detection devices, receiving, recording, measurement and analysis, designed for intelligence.

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.

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, данных.

Network Security – measures that protect the network information from unauthorized access,. accidental or intentional inter-

ference with normal activities or attempts to destroy its components. Includes the protection of hardware, software, data.

Tizim xavfsizligi – tizimning uning resurslaridan va funksional imkoniyatlaridan ruxsatsiz foydalanishdan hamda tizim ishlashida turli bashorat qilinadigan yoki qilinmaydigan holatlar sabab bo'luvchi bo'lishi mumkin bo'lgan buzilishlardan himoyalanishi.

Безопасность системы – защищенность системы от несанкционированного использования ее ресурсов и функциональных возможностей, а также от возможных нарушений ее функционирования, вызванных различными предсказуемыми и непредсказуемыми обстоятельствами.

System Security – the security of the system from unauthorized use of its resources and capabilities, as well as possible violations of its functioning caused by various predictable and unpredictable circumstances.

Tahdid turlari - tahdidlarni tasodifanlariga va atayinlariga, aktivlariga va passivlariga tasniflash mumkin.

Виды угроз – угрозы могут классифицироваться на случайные и преднамеренные и могут быть активными и пассивными.

Types of Threats – threats can be classified into random and deliberate and can be active or passive.

Tiklanuvchanlik – yuklanuvchi modulning bajarilishi jarayonida modifikatsiyalanishidan o'zi yoki ixtiyoriy boshqa modul tomonidan himoyalash mumkinligi xususiyati. Tiklash dasturi bunday modulni ishlash tartibiga, yakuniy natijaga ta'sir etmasdan, yangi nusxa bilan almashtirishi mumkin.

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.

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.

Tiklanish – 1) Dastlabki qiymatiga yoki me'yoriy ishlashiga qaytish. 2) Jarayon bo'lib, uning yordamida ma'lumotlarni uzatish stansiyasi ixtilofni hal etadi yoki ma'lumotlarni uzatishda paydo bo'luvchi xatolikni tuzatadi.

Восстановление – 1) Возврат к исходному значению или к нормальному функционированию. 2) Процесс, с помощью которого станция передачи данных разрешает конфликт или исправляет ошибки, возникающие при передаче данных.

Recovery (regeneration) – 1) Return to the initial value or to normal functioning. 2) The process by which data transmission station resolves the conflict or corrects errors. Arising in / data transmission.

Tizimning tayyorligi – tizimning ishlash holatida o'z vazifalarini bajarish qobiliyatining o'lchovi. Miqdoran, tayyorgarlikni tayyorlik koeffitsienti yordamida baholash mumkin.

Готовность системы – мера способности системы выполнять свои функции при нахождении в рабочем состоянии. Ко-

личественно готовность можно оценивать с помощью коэффициента готовности.

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.

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.

Журнал восстановления – журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в БД (файле) с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

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.

Tahdid (axborot xavfsizligiga tahdid) – axborot xavfsizligini buzuvchi potentsial yoki real mavjud xavfni tug'diruvchi sharoitlar va omillar majmui.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Threat – set of conditions and factors that create potential or actual violations of the existing danger of information security.

Tashqi buzg'unchi – dushman atamasidan foydalanish tavsiya etiladi.

Внешний нарушитель – рекомендуется использовать термин противник.

External violator – it is recommended to use the term enemy.

Vakolatlar – himoyalangan ma'lumotlar ustida u yoki bu muolajani bajarishi bo'yicha foydalanuvchining (terminalning, dasturning, tizimning) huquqi.

Полномочия – право пользователя (терминала, программы, системы) осуществлять те или иные процедуры над защищенными данными.

Privileges – the right of the user (terminal program, system) to implement certain procedures over the protected data.

Vakolatlar matritsasi – elementlari muayyan obyektning himoyalanuvchi ma'lumotlarga nisbatan huquqlarini (vakolatlarini, imtiyozlarini) belgilovchi jadval.

Матрица полномочий – таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта относительно защищаемых данных.

Privilege matrix – table, elements which determine the right (powers and privileges) with respect to a certain object protected data.

Vakolatlarning buzilishi – foydalanuvchining yoki dasturning ruxsat etilmagan amalni bajarishga urinishi.

Нарушение полномочий – попытка пользователя или программы выполнить неразрешенную операцию.

Privilege violation – user or program attempts to perform an unauthorized operation.

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.

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.

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.

Xavfsizlik xizmati ma'muri – xavfsizlikni ta'minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs (yoki shaxslar guruxi).

Администратор службы безопасности – человек (или группа людей), имеющий(ие) полное представление об одной или нескольких системах обеспечения безопасности и контролирующий(ие) проектирование и их использование.

Administrator security – person (or group of people) having (s) complete understanding of one or more security systems and controls (s) design and use.

Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab buluvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanishi anchagina qiyinlashadi.

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.

Denial-of-Service attack (DoS attack) – attack to cause failure of the system, that is to create the conditions under which legitimate users cannot get access to the resources provided by the system, or that access will be significantly hampered.

Himoya obyektining attestatsiyasi – himoya obyektida axborotni himoyalashda belgilangan talablar va samaradorlik me'yorlarining bajarilishini ta'minlovchi zaruriy va yetarli sharoitlar borligi xususida sertifikatsiya beruvchi organning yoki boshqa maxsus vakolatli organning rasmiy tasdig'i.

Аттестация объекта защиты – официальное подтверждение органом по сертификации или другим специально уполномоченным органом наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований и норм эффективности защиты информации.

Attestation object protection – official confirmation by the certification body or other specially authorized presence in the facility protection necessary and sufficient conditions for fulfilling specified requirements and performance standards of information security.

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.

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.

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 safety.

Xavfsiz operatsion tizim – ma'lumotlar va resurslar mazmuniga mos himoyalash darajasini ta'minlash maqsadida apparat va dasturiy vositalarni samarali boshqaruvchi operatsion tizim.

Безопасная операционная система – операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

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.

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 dasturlaming ishlatilishi, ko'rib chiqilishi va avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan modifikatsiyalanishi mumkin bo'lmagan holat.

Безопасность – свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифици-

рованы неавторизованными лицами (включая персонала системы), компьютерами или программами.

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.

Xavfsizlik domeni – xavfsizlikning bitta ma'muri tomonidan xavfsizlikning bir xil usuli qo'llaniladigan xavfsizlik subyektlari va obyektlarining cheklangan guruhi.

Домен безопасности – ограниченная группа объектов и субъектов безопасности, к которым применяется одна методика безопасности со стороны одного и того же администратора безопасности.

Security domain – limited group of objects and subjects of security, to which the one method of security from the same security administrator.

Xatoliklar jurnali – tizim tomonidan adashishlar xususidagi axborot yoziladigan fayl.

Журнал ошибок – файл, в который система записывает информацию о сбоях.

Error Log – file in which the system records information about failures.

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.

Менеджмент риска – полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.

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.

Hujumchi – harakati ko'rilayotgan kompyuter tizimida axborot xavfsizligini buzadigan subyekt.

Нападающий – субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Attacker – a subject whose actions violate the information security in a under consideration computer system.

Xavfsizlik tizimining buzilishi – tizimga suqilib kirish bilan tugallanadigan xavfsizlikni boshqarish vositalarining shikastlanishi.

Нарушение системы безопасности – успешное поражение средства управления безопасностью, которое завершается проникновением в систему.

Security system violation – the successful defeat security controls, which concludes with penetration into the system.

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.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практи-

ческих приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Security policy – set of documented policies, procedures, practical methods or guidelines in the field of information security used by the organization in its activities.

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.

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.

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.

Xufiya dasturiy ta'minot – foydalanuvchilarni ruxsatisiz kompyuter konfiguratsiyalari, foydalanuvchilar faoliyati va har qanday boshqa konfidensial axborotni yig'ish bo'yicha faoliyat olib boradigan zararli dasturiy ta'minot turi.

Шпионское программное обеспечение – вид вредоносного программного обеспечения, осуществляющего деятельность по сбору информации о конфигурации компьютера, дея-

тельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

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.

Yolg'on axborot – xarakteristikalarni va alomatlarni noto'g'ri akslantiruvchi hamda real mavjud bo'lmagan obyekt xususidagi axborot.

Ложная информация – информация, ошибочно отражающая характеристики и признаки, а также информация о не существующем реально объекте.

False information – information which is mistakenly reflecting characteristics and signs, and also information on object not existing really.

Yashovchanlik – tizimning tashqi ta'sirlar sharoitida ishga layoqatli qolishi xususiyati.

Живучесть – свойство системы оставаться работоспособной в условиях внешних воздействий.

Viability – property of the system to remain operational under external influences.

Yaxlitlikning buzilishi – fayl yoki ma'lumotlar bazasi ichidagi yozuvlarning buzilishi. Mashinaning yanglishishi, dasturiy xatoliklar hamda foydalanuvchilarning noto'g'ri harakatlari natijasida ro'y beradi.

Нарушение целостности – искажение содержимого записей файла или базы данных. Происходит вследствие машинных

сбоев, программных ошибок, а также ошибочных действий пользователей.

Integrity violation – the distortion of the contents of the recorded files or database. This is due to machine failures, software errors and erroneous actions of users.

Cheklangan foydalanish – axborot resursidan, ushbu resursga faqat mos vakolatlarga ega shaxslarning ma'lum doirasiga o'rnatilgan foydalanish qoidalari bo'yicha ruxsatli foydalanish.

Ограниченный доступ – доступ к информационному ресурсу, разрешаемый установленными для данного ресурса правилами доступа только определенному кругу лиц, обладающих соответствующими полномочиями.

Restricted access – access to the resources of the information allowed by the established rules for the resource access only certain persons with appropriate authority.

Shaxsiy ma'lumotlar xavfsizligi – bunga natijasi shaxsiy ma'lumotlarni yo'q qilish, o'zgartirish, blokirovka qilish, nusxalash, tarqatish bo'lishi mumkin bo'lgan ruxsatsiz, xususan, tasodifiy foydalanishni hamda boshqa ruxsatsiz harakatlarni istisno qilish yo'li bilan erishiladi.

Безопасность персональных данных – достигается путем исключения несанкционированного доступа, в том числе случайного, к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Personal Data Security – is achieved by eliminating unauthorized access, including random, personal data, which may

result in destruction, alteration, blocking, copying, distribution of personal data, as well as other illegal actions.

Shaxsiy ma'lumotlar – bunday axborot asosida aniq yoki aniqlanuvchi fizik shaxsga (shaxsiy ma'lumotlar subyektiga) tegishli har qanday axborot, jumladan, uning ismi-sharifi, tug'ilgan yili, oyi, kuni va manzili, oilaviy, ijtimoiy, mulkiy holati, ma'lumoti, kasbi, daromadi, boshqa axborot.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Personal data – any information relating to an identified or identifiable on the basis of such information to an individual (the subject of personal data), including its name, first name, year, month, date and place of birth, address, marital, social, property status, education, occupation, income, other information.

MUNDARIJA

4-bob. XAVFSIZLIK AUDITI VA MA'LUMOTLAR BAZASINI REZERVLI NUSXALASH

5-bob. MA'LUMOTLAR BAZASI XAVFSIZLIGINI TA'MINLASH BO'YICHA STANDARTLAR VA SPETSIFIKATSIYALAR

СОДЕРЖАНИЕ

CONTENT

Chapter 4. SECURITY AUDIT AND DATABASE BACKUP

Chapter 5. STANDARTS AND SPECIFICATIONS ON PROVIDING DATABASE SECURITY

QAYDLAR UCHUN

S.K. GANIYEV, A.A. GANIYEV, D.Y. IRGASHEVA

MA'LUMOTLAR BAZASI XAVFSIZLIGI

Toshkent – «Fan va texnologiya» – 2016

Muharrir:	Sh.Aliyeva
Tex. muharrir:	M.Xolmuhamedov
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: 28.12.2016.
Bichimi 60x84 $^{1}/_{16}$. «Timez Uz» garniturasi. Ofset bosma usulida bosildi.
Shartli bosma tabog'i 13,75. Nashriyot bosma tabog'i 14,0.
Tiraji 100. Buyurtma №293.

«Fan va texnologiyalar» Markazining
bosmaxonasida chop etildi.
100066, Toshkent sh., Olmazor ko'chasi, 171-uy.