1-Mavzu: Ma’lumotlar bazasi xavfsizligini ta’minlash usullari vositalari va mexanizmlarining asosiy harakteristikalari.

Kompyuter axborotini himoyalash muammolari bo`yicha 70- yillarning oxiri 80-yillaming boshida o‘tkazilgan, keyinchalik turli ilovalarda rivojlantirilgan va mos standartlarda qayd etilgan tadqiqotlar axborot xavfsizligi tushunchasining tarkibiy elementlari sifatida quyidagilami belgilaydi:
-konfidensiallik (ruxsatsiz foydalanishdan himoyalash);
-yaxlitlik (axborotni ruxsatsiz o‘zgartirishdan himoyalash);
-foydalanuvchanlik (axborotni va resurslami ushlab qolinishidan himoyalash, buzilishdan himoyalash, ishga layoqatlikni himoyalash).

Axborot xavfsizligi tarkibiy elementlari

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. Tahdidlami axborot xavfsizligini buzuvchi (buzg'unchi) amalga oshiradi yoki amalga oshirishga urinadi.

Axborot xavfsizligiga u yoki bu tahdidlami 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 atamalari

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) – subyektlaming obyektlardan foydalanish huquqini qat’iy belgilovchi qoidalar majmui;
- ruxsatli foydalanish (authorized access to information) – foydalanishni cheklash qoidalarini buzmasdan axborotdan foydalanish;

- **ruxsatsiz foydalan**ish (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;
- **konfxdensialiik belgisi** (sensitivity label) - obyekt konfidensialligini xarakterlovchi axborot birligi;
- **ko‘p sathli himoya** (multilevel secure) - turli sathli konfidensiallikga ega obyektlardan foydalanishning turli huquqlariga ega subyektlaming foydalaxiishlarini cheklashni ta’minlovchi himoya.

Kompyuterning dasturiy ta’minot strukturasi

Kompyuterning dasturiy ta’minot strukturasida tashqi xotirada ma’lumotlami tashkil etishga, joylashtirishga va undan foydalanishga operatsion tizim javob beradi. Uning mos tashkil etuvchisi ko‘pincha “fayl tizimi” deb yuritiladi. Kompyuteming tashqi xotirasidagi ma’lumotlar fayllar deb ataluvchi nomlangan majmua yordamida ifodalanadi. Ko‘p hollarda operatsion (fayl) tizimi fayllardagi ma’lumotlami tashkil etishning ichki mazmunli mantiqini “bilmaydi” va ular bilan baytlaming 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 kompyuteming 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.

Talbiqiy dasturiy ta’minot

Talbiqiy dasturiy ta’minot hisoblanuvchi, ya’ni muayyan tatbiqiy masalalami yechishga mo‘ljallangan MBBT awal boshdan tizimli funksiyalarini bajargan - tizimli dasturiy ta’minotning fayl tizimi imkoniyatlarini kengaytirgan. Umuman MBBT amalga oshiruvchi quyidagi fimksiyalami ajratish mumkin:
- ma’lumotlami mantiqiy strukturasini (ma’lumotlar bazasi sxemalarini) tashkil etish va madadlash;
- tashqi xotiradagi ma’lumotlaming fizik strukturasini tashkil etish va madadlash;

- ma’lumotlardan foydalanishni tashkil etish va ulami asosiy va tashqi xotirada ishlash.

Ma’lumotlaming mantiqiy strukturasini (ma’lumotlar bazasi sxemalarini) tashkil etish va madadlash *ma’lumotlarni tashkil etish modeli* (“ma’lumotlar modeli”) vositaiari yordamida ta’nrmlanadi.

Ma’lumotlar modeli

Ma’lumotlar modeli ma’lumotlami tashkil qilish usuli, yaxlitlikning cheklanishlari va ma’lumotlami tashkil qilish obyektlari ustida joiz amallar to ‘plami orqali aniqlanadi.

Ma’lumotlar modeli uchta tarkibiy qismga
Strukturali
Yaxlitli
Manipulyatsion qismlarga ajratiladi.

Ma’lumotlami tashkil etishning quyidagi uchta asosiy modellari mavjud:
- Ierarxik
- Tarmoqli
- Relyatsion

Ma’lumotiami 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

MBBTning boshqa muhim fimksiyasi - tashqi xotiradagi ma’lumotlaming fizik strukturasini tashkil etish va madadlash. Ushbu fimksiya 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 strukturalami (indekslami, sahifalami) yaratadi va madadlaydi. Ushbu jihatdan bu fimksiya MBBTning uchinchi funksiyasi — ma’lumotlar bazasidan foydalanishni tishkil etish bilan uzviy bog‘langan.

Tashqi xotiradagi ma’lumotlaming 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 ulami asosiy va tashqi xotirada ishlashni tashkil etish tranzaksiya deb ataluvchi jarayonlarni amalga oshirish orqali bajariladi.

Tranzaksiya

Tranzaksiya - ma’lumotlar bazasining joriy holatiga nisbatan alohida ma’noli qiymatga ega amallaming ketma-ket majmui. Masalan, ma’lumotlar bazasidagi alohida yozuvni olib tashlash tranzaksiyasi quyidagilami 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’lumotlami 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).

Tranzaksiya monitori

MBBTning tranzaksiyalami tashkil etish va boshqarish bo‘yicha funksiyalarining majmui *tranzaksiya monitori* deb ataladi. Ma’liimotlar bazasiga nisbatan tranzaksiyalar ma’lumotlar banki foydalanuvchilari harakatlariga tenglashtiriluvchi tashqi jarayonlar bilan ishtirok etadi. Bunda tranzaksiyalaming 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 tranzaksiyalami monitorlashning asosiy vazifasi - birdaniga bir nechta foydalanuvchilaming umumiy ma’lumotlar ustida tranzaksiyalaming birgalikda samarali bajarishlarini ta’minlash.

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

MBBTning ma’lumotlardan foydalanish

MBBTning ma’lumotlardan foydalanish va ulami ishlashini tashkil etish bo‘yicha funksiyasining yana bir muhim tarkibiy qismi ma’lumotlar bazasining barcha joriy o‘zgarishlarini jumallashtirish hisoblanadi. *Jumallashtirish* ma’lumotlaming bo‘lishi mumkin bo‘lgan yanglishishlar va buzilishlarda but saqlanishini ta’minlovchi asosiy vosita hisoblanadi. Aksariyat MBBTlarda bunday tahdidlami neytrallash uchun saqlash va joylashtirishning o‘zgacha rejimli ma’lumotlar bazasining o‘zgarishlari jumali tashkil etiladi. Ma’lumotlar bazasining o‘zgarishlar jumalining zaxirali nusxasi, odatda, ma’lumotlar bazasining asosiy faylidan alohida eltuvchilarda joylashtiriladi.

Ma’lumotlar bazasi strukturasi

Ma’lumotlar bazasi strukturasini tavsiflash va madadlash protsessor MBBTning yadrosi hisoblanadi. U ma’lumotlami 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 strukturasini o‘matishni hamda ma’lumotlar bazasi strukturasini ma’lumotlar bazasining ichki sxemasiga (ma’lumotlaming 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.'

Ma’lumotlami kiritish interfeysi

MBBTning ma’lumotlami kiritish interfeysi abonentlami — axborot yetkazib beruvchilami 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 qoilash 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 anketalaming electron 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 ulami ma’lumotlar bazasining mantiqiy strukturasini tavsiflash atamalarida sharxlash vositalarini ta’minlaydi.

So‘rovlar interfeysi

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‘rovlami shakllantirishning maxsus “konstruktorlar” yoki qadamba- qadam “masterlar” ko‘rinishidagi dialog-ko‘rgazmali vositalaridan foydalanishdan iborat.

So'rovlar protsessor

So'rovlar protsessor shakllantirilgan so‘rovlami ma’lumotlami manipulyatsiyalovchi til atamalarida sharxlaydi va ma’lumotlar ball zasi strukturasini tavsiflash va madadlash prosessor bilan birgalikda so‘rovlarni bajaradi. Relyatsion MBBTlarda so‘rovlar prosessoming asosini SQL tilining asosiy qismi hisoblanuvchi ma’lumotlami matt ipulyatsiyalovchi 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. Malu`motlar mashinasining funksiyalaidan va imkoniyatlaridan MBBTning tartibi yuqoriroq komponentlari foydalanadi. Bu MBBT komponentalarini va ma’lumotlar bankini uchta sathga - mantiqiy sathga, ma’lumotlar mashinasiga va ma’lumotlaming o‘ziga ajratishga va standartlashga imkon beradi.

Tranzaksiyalar monitori

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’lumotlaming yaxlitligini va kompyuter tizimi predmet sohasi qoidalari orqali aniqlanuvchi cheklashlami ta’minlash hisoblanadi.

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

Chiqarish shakllari “hisobot’ni shakllantirish asosida ham yotadi. Hisobot chiqarilgan ma’lumotlami 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 bazasiniyaratish va foydalanishning* instrumental muhiti va MBBT tili (ma’lumotlami tavsiflash tili, ma’lumotlami manipulyatsiyalash tili, interfeysni yaratish tili va vositalari) majmui hisoblanadi.

MBBTdan foydalanuvchilami uch guruhi

MBBTdan foydalanuvchilami uchta guruhga ajratish mumkin:

- **tatbiqiy dasturchilar** - ma’lumotlar bazasi asosida dastur yaratilishiga javobgar. Ma’lumotlari himoyalash ma’nosida dasturchi ma’lumot obyektlarini yaratish va ulami manipulyatsiyalash imtiyoziga yoki faqat ma’lumotlami manipulyatsiyalash imtiyoziga ega foydalanuvchi bolishi mumkin;

- **ma’lumotlar bazasidan oxirgi foydalanuvchilar** - ma’lumotlar bazasi bilan bevosita terminal yoki ishchi stansiya orqali ishlashadi. Odatda, ular ma’lumotlami manipulyatsiyalash bo‘yicha imtiyozlaming 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 boisa) 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 foydalanuvchilami kerakli ma’lumotlardan foydalanishlarini ta’minlash hamda foydalanuvchilarga kerakli ma’lumotlaming tashqi tasawurini yozish kiradi. Ma’mur xavfsizlik qoidasini va ma’lumotlar yaxlitligini belgilaydi.

Ma’lumotlar xavfsizligi modellari.

Xavfsizlik modeli quyidagilami 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 tizimtarini subyekt-obyekt modeli yotadi, xususan, avtomatlashtirilgan axborot tizimlarining yadrosi sifatidarci 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.

Axborot tizimlari ishlashi xavfsizligining ikkita eng muhim prinsipi ma’lum:
-Obyektga nisbatan barcha subyektlar va jarayonlaming identifikatsiyasi va autentiflkatsiyasi;
- Obyektga nisbatan subyektlar vakolatlarini cheklash va ma’lumotlar ustidagi har qanday vakolatlami tekshirish shartligi. Mos holda MBBT yadrosi strukturasida ma’lumotlami ishlashningnbarcha jarayonlarida belgilangan xavfsizlik siyosatini amalga oshiruvchi, xavfsizlik monitori (serveri, menedjeri, yadrosi) deb ataluvchi qo‘shimcha komponent ajratiladi (Trusted Computing Base - TCB). Ushbu komponent ma’lumotlami 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 funksiyalami amalga oshiruvchi ustqurmani o‘z ichiga oluvchi yadro majmui sifatida tasawur etilsa, xavfsizlik monitorining roli va o‘mini sxema orqali izohlash mumkin.

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

Foydalanish matritsasi

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‘matadi.

Foydalanishni boshqarish xavfsizlik modelinmg 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.

Bunday yondashishda ma’lumotlar bazasida foydalanishni cheklash tizimini foydalanuvchilar va resurslaming 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’lumotlar bazasida maxsus ishonchli subyekt (ma’mur) ajratiladi va u ma’lumotlar bazasi obyektlaridan foydalanuvchi barcha qolgan subyektlami 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 foydalanuvchilaming ehtiyojlari va vakolatlariga, foydalanishni cheklash tizimini sozlash nuqtayi nazaridan, moslashuvchanligi kamroq, aniqligi pastroq, chunki obyektlar (resurslar) tarkibi va konfidensialligi xususidagi eng to‘liq tasavurga olaming egalari ega boladilar.

Amalda foydalanishni boshqarishning kombinatsiyalangan usuli qoilanishi mumkin. Unga binoan obyektlardan foydalanish vakolatining ma’lum qismi ma’mur tomonidan, boshqa qismi esa obyekt egalari tomonidan o‘matiladi. An’anaviy

sohalarda (kompyuter sohasida emas) va texnologiyalarda axborot xavfsizligini ta’minlashga yondashishlaming tadqiqi ko‘rsatadiki, ma’lumotlar xavfsizligining bir sathli modeli real ishlab chiqarish va tashkiliy sxemalami adekvat akslantirishga yetarli emas. Xususan, an’anaviy yondashishlar axborot resurslarini konfidensiallik darajasi bo‘yicha kategoriyalashdan foydalanadi. Mos holda axborot resurslaridan foydalanuvchi subyektlar ham mos ishonch darajasi bo‘yicha kategoriyalanadi. Ularga 1-darajali dopusk, 2-darajali dopusk beriladi. Dopusk tushunchasi axborotdan foydalanishni cheklashning mandatli (vakolatli) prinsipini belgilaydi.

Mandatli prinsip

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.

Bell-La Padula modeli

Bell-La Padula modelida obyektlar va subyektlar foydalanishning ierarxik mandatli prinsipi bo‘yicha kategoriyalanadi. 1- (eng yuqori) darajali dopuskga ftga. - ≪subyekt konfidensialliknine 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.

Bell-LaPadula modelida xavfsizlik siyosatining ikkita asosiy cheklashlari o‘matiladi va madadlanadi:
- yuqorini o‘qish man etiladi (no read up - NRU);
- pastga yozish man etiladi (no write down - NWD).

NRU cheklash foydalanish

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, obyektlaming konfidensiallik sathini faqat obyekt egalari belgilaydi va o‘zgartiradi).

Ma’lumotlar bazasini boshqarish tizimlarining turlari

Muloqot tillari bo‘yicha ochiq, yopiq va aralash MBBTlari farqlanadi. Ochiq tizimlarda ma’lumotlar bazasiga murojaat uchun dasturlaming 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, sathlaming katta sonini ajratish mumkin. MBBTning arxitekturaviy sathi deganda mexanizmlari ma’lumotlar abstraktsiyasining qandaydir sathini madadlashga xizmat qiluvchi funksional komponent tushuniladi.

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‘rsatkichlami avtomatik tarzda olishga imkon beradi, ishlash algoritmini o‘zgartirishi mumkin.

Universal va Ixtisoslashtirilgan MBBTlari

Qo‘llanishi mumkin boigan soha bo‘yicha universal va ixtisoslashtirilgan (muammoga yo‘naltirilgan) MBBTlari farqlanadi. Turli MBBTdagi joiz ma’lumotlaming turlar nabori har xil. Undan tashqari, qator MBBTlar ishlab chiqaruvchiga ma’lumotlaming yangi turlarini va bu ma’lumotlar ustida bajariluvchi yangi amallami qo‘shishga imkon beradi. Bunday tizimlar ma’ lumotlar bazasining kengayuvchi tizimlari deb yuritiladi.

Ma’lumotlar bazasining kengayuvchi tizimlari konsepsiyasining keyingi rivoji - murakkab obyektlami bevosita modellashda yetarlicha *quvvatli ifodalash* imkoniyatlariga ega boigan mal`umotlar 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 talablaming yuqori emasligi, oxirgi foydalanuvchiga mo`ljallanganligi, narxining pastligi bilan xarakterlanadi.

Korporativ MBBTlar

Korporativ MBBTlar taqsimlangan muhitda ishlashni, yuqori unumdorlikni, tizimni loyihalashdajamoa ishining madadini ta’minlaydi, rivojlangan ma’murlash vositasiga va yaxlitlikni madadlashning keng imkoniyatlariga ega. Ushbu tizimlar murakkab, qimmat, ko‘pgina hisoblash resurslarini talab etadi. Ikkala sinf tizimlari jadallik bilan rivojlanmoqda, uning ustiga rivojning ba’zi tendensiyalari ushbu sinflarning har biriga taalluqli. Birinchi navbatda, ilovalami ishlab chiqishda yuqori sathli vositalardan foydalanish unumdorliging va funksional imkoniyatlaming o‘sishi, lokal va global tarmoqlarda ishlashi. 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 tizimlami 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‘riqlaming intellektual modullarining maviudligi, bexosdan qilingan xatolardan himoyaning yuqoriligi.

MBBTlami avlodlar bo‘yicha ajratish

MBBTlami avlodlar bo‘yicha ajratish mavjud. Birinchi avlod MBBTlari (XX asming 60-70-yillari) ierarxik va tarmoqli modellarga asoslangan, ikkinchi avlod MBBTlariga relyatsion tizimlar taalluqli. Uchinchi avlod MBBTlari ma’lumotlaming murakkab strukturalarini va ma’lumotlar yaxlitligini ta’minlovchi rivojlangan vositalami madadlashi, ochiq tizimlarga qo‘yiladigan talablami qondirishi lozim.