

12-mavzu.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 imkoniyatlar MBBT himoyasi profilida hisobga olinishi shart. Bu yerda autentifikatsiya tushunchasi kiritiladi va u MBBT uchun foydalanuvchi identifikatorining haqiqiylikini 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 servisleri, va/yoki maxsus dasturiy ta'minot) o'matilgan, konfiguratsiyalangan va xavfsiz boshqariladi.

Bazaviy tizim

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 yakka va MBBT jarayonlarini himoyalash uchun vositalarni taqdim etadi. Aytish mumkinki, boshqarish va yakka 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 muhimligiga 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 (FPURSA.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. Xavfsizlik 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 kecliishga 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).

Ma'muriy imkoniyatlar

Ushbu tizimlar ma'muriy 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 arzlari "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-xataming o'rtacha darajali qandaydir umumlashgan muhiti uchun belgilangan. Ishonchlikka talablar va flinksiyalarning minimal barqarorligi xavfxataming ushbu darajasiga muvofiq tanlangan.

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

Konfiguratsiyalanish usullari

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 sahifalarni shakllantiruvchi Web-server bilan bog‘lanishni madadlovchi Webbrauzer).

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

Pastki bazaviy tizim

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

Autentifikatsiya paketi ma’lumotlar bazasi uchun foydalanuvchining ma’lum qilgan identifikatorining haqiqiylikini 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 haqiqiylikini tasdiqlashni ta’minlaydi. Ma’lumotlar bazasi operatsion tizim tomonidan taqdim etilgan identifikatorni ma’lumotlar bazasi identifikatorini o‘rnatish uchun ishlatadi.

Ma’lumotlar bazasi vositalari yordamida autentifikatsiya

Autentifikatsiyaning ushbu sxemasida ma’lumotlar bazasi o‘zining shaxsiy autentifikatsiyalash mexanizmidan foydalanib, foydalanuvchi bildirgan identifikatorning haqiqiylikini tekshiradi.

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.

MBBT xavfsizligiga tahdidlar

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 choralari).

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.ACCESS — ***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 fribgarlik maqsadida foydalana oluvchi foydalanuvchiga berishi mumkin. Ta'kidlash lozimki, ushbu tahdid ishonchning yuqori darajasiga ega foydalanuvchilarga tarqalmaydi.

Muhit tomonidan bartaraf etiluvchi tahdidlar

T.OPERATE - *xayfli 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.

Ma'lumotlar bazasi obyektlaridan foydalanish

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 ulami 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 obyektidagi amallarga;

- ma'lumotlar bazasi ma'muri tomonidan belgilangan harakatlarga.

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

MBBT bo'yicha taxminlar

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

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 konfiguratsiyalanganiki, tizimdan faqat shaxslarning ruxsatli guruhi foydalanishi mumkin.

A.MANAGE — MBBTni bazaviy tizimini va axborot xavfsizligini boshqarish uchun bir yoki widan 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 haqiqiyiligini ta'minlovchi o'zaro harakatlarning xavfsiz protokollariga asoslanadi. 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 resurslardan foydalanishni boshqarish imkoniyatini ta'minlashi lozim. Buning uchun baholash obyektida quyidagi muayyan maqsadlar mavjud:

O.ACCESS

O.ACCESS.OBJECTS - MBBT ma'lumotlar bazasi 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.RESEDUAL - 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 yordamsiz o'zining foydalanuvchilarini identifikatsiyalash va autentifikatsiyalash vositalarini taqdim etishi lozim.

O.AUDIT

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 objekti 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, ma'lumotlar bazasi fayllarini, eksport

qilinuvchi fayllami, boshqariluvchi fayllarni) ruxsatsiz foydalanishdan himoyalashga imkon beruvchi foydalanishni boshqarish mexanizmlarini ta'minlashi lozim.

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

O.SEP - bazaviy operatsion tizim MBBT xavfsizligi funksiyalarini yakka 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

O.iNSTALL - MBBTga javobgarlar quyidagilarni ta'minlashlari lozim:

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

-bazaviy tizim ekspluatatsiya hujjatlariga muvofiq o'rnatilishi va ishlatilishi lozim.

Agar tizim elementlari sertifikatlangan bo'lsa, ular sertifikatning kerakli hujjatlariga muvofiq o'rnatilishi va ishlatilishi lozim.

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

O.AUDITLOG - ma'lumotlar bazasi ma'murlari audit vositalarining samarali ishlatilishini ta'minlashlari lozim. Ushbu muolajalar ma'lumotlar bazasi audit jomalida va/yoki bazaviy operatsion tizim audit jomalida 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 jumalari 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).

RECOVERY

RECOVERY - MBBTga javobgar tizimli yangilash 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 jumalini o'zgartirish yoki uning konfiguratsiyasini o'zgartirish;
- ma'lumotlar bazasi auditi jumalida 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

O.AUTHDATA - MBBTga javobgar baholash obyektidan foydalanuvchilarning hamda bazaviy tizimning har qanday hisob yozuvi uchun autentifikatsiya ma'lumotlarining ishonchli madadlanishini va ushbu hisob yozuidan 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.IWEDIA

O.IWEDIA - 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 jumallari va audit jumallari) 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.

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.

Obyektli yondashuvda talablar tahlili va dasturiy ta'minot spetsifikatsiyalarini baholash

Ishlab chiqiluvchi dasturiy ta'minotning obyektli yondashuvdagi model lari real dunyo predmetlari va hodisalariga asoslangan. Shuningdek, ushbu modellar asosida ishlab chiqiluvchi dasturiy ta'minlashning talab qilinuvchi xatti-harakati, ya'ni uning funkcionalligi bayoni turadi, biroq bu xatti-harakat muayyan predmetli soha elementlari (obyektlari)ning holatlari bilan bog'liq bo'ladi.

Shunday qilib, tahlil bosqichida ikki vazifa qo'yiladi:

- ishlab chiqiluvchi dasturiy ta'minotning talab qilinuvchi xatti-harakatini aniqlashtirish;
- qo'yilgan vazifalar nuqtayi nazaridan uning predmetli sohasi konseptual modelini ishlab chiqish.

UML standart tili

UML — dasturiy mahsulotlar ishlab chiqishning obyektli yondashuv bilan birgalikdagi standart tili

Dasturiy ta'minotni ishlab chiqishga obyektli yondashuv asosida obyektli dekompozitsiya, ya'ni ishlab chiquvchi dasturiy ta'minotni obyektlar jamlanmasi tarzida taqdim etish turadiki, ushbu obyektarning o'zaro harakati jarayonida axborotlarni berish orqali talab qilinuvchi funksiyalarni bajarish yuz beradi. Biroq xuddi tuzilmaviy yondashuvdagi kabi obyektli yondashuvda ham faqat juda oddiy dasturiy ta'minot dekompozitsiyasini darhol bajarish mumkin.

Shu boisdan obyektli, mo'ljalli dasturlash davri ibtidosida dasturiy ta'minotni obyektli yondashuv doirasida tahlil qilish va loyihalashning har xil modellar hamda notatsiyalardan foydalanilgan turlicha usullari taklif qilingandi.

Mazkur usullar va modellarning afzalliklari hamda kamchiliklari xususida uzoq bahslashish mumkin edi. Ushbu vaziyat «usullar urushi» nomini olgandi.

«Usullar urushi»ga 1995-yilda UML (Unified Modeling Language — modellashtirishning unifikatsiyalangan tili) tili birinchi versiyasining paydo bo'lishi yakun yasadi. Ushbu til hozirgi paytda obyektga — mo'ljallangan yondashuv bilan yaratiluvchi loyihalar bayonining standart vositasi deb amalda tan olingan. Ushbu sohalaridagi yetakchi mutaxassislar Gradi Buch, Ivar Yakobson va Jeyms Rombo mazkur tilning yaratuvchilari bo'lib, ular «usullar urushi» vaqtida ushbu mualliflarning yondashuvlarida paydo bo'lgan barcha yaxshi narsalardan o'z tilida foydalanishgan.

UML dan foydalanish

UML dan foydalanishda ishlab chiqiluvchi dasturiy ta'minot spetsifikatsiyasi bir necha modellarni: foydalanish, mantiqiy, amalga oshirish, jarayonlar, yoyish

modellarini birlashtiradi. Foydalanish modeli foydalanuvchi nuqtayi nazaridan dasturiy ta'minlash funktsionalligi bayonini o'zida ifoda etadi. Mantiqiy model dasturiy ta'minotning kalit abstraksiyalarihi (sinflar, interfeyslar va h.k.), ya'ni talab qilinuvchi funktsiyalarni ta'minlovchi vositalarni bayon etadi.

Amalga oshirish modeli ishlab chiqish muhitida dasturiy modellarning real tashkillantirilishini belgilaydi.

Jarayonlar modeli hisoblashlar tashkillashtirilishini aks ettiradi va <<jarayonlar>> va <<iplar>> tushunchalari bilan ish yuritadi.

Ushbu model dasturiy ta'minlash mahsuldorligini, miqyoslanuvchanligini va ishonchliligini baholashga imkon beradi.

Nihoyat, yoyish modeli muayyan uskunada dasturiy komponentalarni joylashtirishning xususiyatlarini ko'rsatadi. Shunday qilib, ko'rsatilgan modellarning har biri loyihalanuvchi tizimning muayyan aspektini tavsiflaydi, ularning hammasi esa birgalikda ishlab chiqiluvchi dasturiy ta'minlashning nisbatan to'liq modelini tarkib toptiradi.

UML diagrammasi

Umuman UML turli modellarga mansub va bir-birini toldiruvchi to'qqizta diagrammani taklif etadi:

- foydalanish variantlari diagrammalari;
- sinflar diagrammalari;
- paketlar diagrammalari;
- amallar bosqichliliklari diagrammalari;
- kooperatsiya diagrammalari;
- faoliyatlar diagrammalari;
- obyektlar holatlari diagrammalari;
- komponentalar diagrammalari;
- joylashtirish diagrammalari.

Ko'rsatilgan barcha diagrammalar imkon boricha yagona grafikli notatsiyadan foydalanadi, bu ularni tushunishni yengillashtiradi.

Ko'rsatilgan diagrammalar bilan birga, tuzilmaviy yondashuvdagi kabi, spetsifikatsiya amallar lug'atini, shuningdek turli xil bayonlarni va matnli spetsifikatsiyalarni muqarrar qamrab oladi.

Hujjatlarning muayyan majmui ishlab chiquvchi tomonidan belgilanadi. UML hamda o'sha mualliflar taklif etgan Rational Unified Process metodikasi Rational Software Corporation firmasining Rational Rose paketi bilan quvvatlanadi. UML ning qator diagrammalarini, shuningdek Microsoft Visual Modeler dasturi vositalari hamda boshqa CASE vositalar bilan ham qurish mumkin hozirgi paytda <<USA Today>> ma'lumotlariga ko'ra, 50 ta yetakchi kompyuter kompaniyalaridan 49 tasi dasturiy ta'minotni obyektli yondashuv bilan birgalikda ishlab chiqishda UML dan foydalanishadi, bu esa bugun UML amalda bunday ishlab chiqishlar bayonining standarti bo'lib qolganligi haqida gapirishga imkon beradi.

«Foydalanish variantlarini»

Dasturiy ta'minot spetsifikatsiyasining ishlab chiqilishi texnik topshiriqda ko'rsatilgan funkcionallikka talablar tahlilidan boshlanadi. Tahlil jarayonida ishlab chiqaruvchi dasturiy ta'minotning tashqi foydalanuvchilar va muayyan foydalanuvchilar bilan o'zaro harakatlanish jarayonida uning xatti-harakatlari alohida aspektlari sanoqnomasi aniqlanadi. Dasturiy ta'minotning xatti-harakati aspektlari «foydalanish variantlari» yoki «presedentlar» (USE CASES) deb nomlangandi.

Eslatma. Foydalanish variantlari ko'pchilik dasturiy ta'minot ishlab chiquvchilar tomonidan 1980—1990-yillarda qo'llanilgan loyihalanuvchi dasturiy tizimlar funktsiya bajarishi ssenariylarining norasmiy bayoniga asoslangan.

Foydalanish varianti muayyan harakatlanuvchi shaxs tomonidan ishlab chiqiluvchi tizim qo'llanishining xarakterli protsedurasini o'zida ifoda etdiki, bunday shaxs sifatida nafaqat odamlar, balki boshqa tizimlar yoki qurilmalar ham namoyon bo'lishi mumkin.

Foydalanish variantini bo'lg'usi tizimning muayyan operatsiyalari bilan adashtirmaslik lozim. Har bir foydalanish variant mustaqil ahamiyatga ega ayrim maqsad bilan bog'liq, masalan matniy muharrir uchun sarlavhani shakllantirish bu foydalanish varianti, sarlavhalarni maxsus uslublar bilan bogiash esa sarlavhalashni avtomatik ravishda tuzish mumkin bo'lishi uchun bajarilishi zarur operatsiyadir.

Foydalanish variantlari

Muayyan protseduraning bajarilish maqsadiga bog'liq ravishda quyidagi foydalanish variantlari farqlanadi:

- asosiy — ishlab chiqiluvchi dasturiy ta'minlashning talab qiluvchi funkcionalligini ta'minlaydi;
- ko'makchi — tizimning zaruriy sozlanishi va«unga xizmat ko'rsatilishi (masalan, axborotni arxivlashtirish va h.k) bajarilishini ta'minlaydi;
- qo'shimcha — foydalanuvchi uchun qo'shimcha qulayliklarni ta'minlaydi (odatda, ishlab chiqishda ham, tasarrufda ham qandaydir resurslarning jiddiy sarflanishini talab qilmagan holatda amalga oshiriladi).

Foydalanish variantini qisqacha yoki batafsil bayon etish mumkin. Qisqacha bayon shakli quyidagilarni qamrab oladi: foydalanish varianti nomi, uning maqsadi, harakatlanuvchi shaxslar nomi, foydalanish varianti tipi (asosiy, ikkinchi darajali yoki qo'shimcha) va uning qisqacha bayoni.

Kombinatorik — optimallashtiruvchi masalalarni hal etish tizimi topshirig'ni bajarish foydalanish variantini quyidagicha tarzda taqdim etishi mumkin:

Asosiy foydalanish variantlari odatda ishlab chiqiluvchi dasturiy ta'minot predmeti sohasini aks ettirishga intilgan holda batafsil bayon ettiriladi. Batafsil shakl yuqorida ko'rsatilgan axborotdan tashqari hodisalar tipik bajarishning va mumkin bo'lgan muqobilliklarning bayonini ham qamrab oladi.

Hodisalarning tipik borishi ketma-ket raqamlagan holda foydalanuvchi bilan tizim

o'rtasidagi muloqot tarzida taqdim etiladi. Agar foydalanuvchi variantlarni tanlashi mumkin bo'lsa, ular alohida jadvalda bayon etiladi. Shuningdek, hodisalarning tipik borishi buzilishi bilan bog'liq muqobilliklar ham keltiriladi. Quyida topshiriqni bajarish foydalanish variantining batafsil bayoni taqdim etiladi:

Harakatlanuvchi shaxs

Harakatlanuvchi shaxs — ishlab chiqiluvchi dasturiy ta'minotga munosabat bo'yicha tashqi mavjudod bo'lib, u bilan qandaydir axborotni olish yoki taqdim etish maqsadida o'zaro harakatlanadi. Yuqorida eslatib o'tilganidek, ishlab chiqiluvchi dasturiy ta'minot bilan o'zaro harakatlanuvchi foydalanuvchilar, boshqa dasturiy ta'minotlar yoki qandaydir texnik vositalar harakatlanuvchi shaxslar bo'la olishlari mumkin.

Foydalanish varianti — harakatlanuvchi shaxs uchun uning muayyan topshirig'ini hal etuvchi ayrim ravshan protsedura. Barcha foydalanish variantlari u yoki bu darajada ishlab chiqiluvchi tizim funktsionalligiga bog'liq va bajariluvchi ish hajmi bo'yicha kuchli farqlanishi mumkin.

Aloqa

Aloqa — harakatlanuvchi shaxslar va tegishli foydalanish variantlarining o'zaro harakatlanishi.

Foydalanish variantlari, shuningdek o'zaro bog'liq bo'lishi ham mumkin. Bundan foydalanish va kengayish aloqalari qayd etiladi.

Foydalanish ishlab chiqiluvchi dasturiy ta'minot xatti-harakatining bir necha foydalanish variantlarida takrorlanadigan ayrim ragmenti mavjudligini e'tiborda tutadi. Mazkur fragment alohida foydalanish varianti sifatida rasmiylashtiriladi va u bilan «foydalanish» tipidagi aloqa ko'rsatiladi.

Kengayish birida ayrim qo'shimcha amallar mavjudligi bilan farqlanadigan ikkita o'xshash foydalanish varianti bor bo'lgan taqdirda qo'llaniladi. Mazkur holatda qo'shimcha amallar alohida foydalanish varianti sifatida belgilanadi va u asosiy variant bilan bog'liq bo'ladi.

Predmetli soha konseptual modelini tuzish

Sinflar diagrammalari dasturiy ta'minot ishlab chiqish obyektli mo'ljalli usullarning markaziy bo'g'inidir, shu bois barcha mavjud usullar mashhur notatsiyalardan birida sinflar diagrammalaridan foydalanadi. Biroq ushbu usullarda sinflar diagrammalarini asosan loyihalash bosqichida qo'llaniladiki, bu muayyan sinflar tuzilishining xususiyatlarini ko'rsatish uchun amalga oshiriladi. Avval mavjud bo'lgan notatsiyalardan farqli o'laroq,

UML sinflar diagrammalarining uch darajasidan ularni detallashtirish pog'onasiga bog'liqlikda foydalanishni taklif etadi:

- konseptual daraja, bunda mazkur holatda kontekstli deb nomlanuvchi sinflar diagrammalari predmetli sohaning asosiy tushunchalari o'rtasidagi aloqani namoyish etadi;

- spetsifikatsiyalar darajasi, bunda sinflar diagrammalari predmetli soha sinflarining interfeyslarini, ya'ni ushbu sinflar obyektlarining aloqalarini aks ettiradi;

- amalga oshirish darajasi, bunda sinflar diagrammalari bevosita muayyan sinflarning maydonlari va operatsiyalarini ko'rsatadi.

Amalda bular uchta turli model bo'lib, ular o'rtasidagi aloqa bir xil emas. Xususan, agar konseptual model predmetli sohaning ayrim tushunchasini sinf sifatida belgilash, bu mazkur tushunchani amalga oshirish uchun alohida sinfdan foydalanilishini anglatmaydi. Biroq barcha uch modelda va ularning statik nisbati qiziqtiradi, bu esa yagona notatsiyadan foydalanishga imkon beradi.

Sanab o'tilgan modellarning har biridan dasturiy ta'minot ishlab chiqishning muayyan bosqichida foydalaniladi:

- konseptual modeldan — tahlil bosqichida;

- spetsifikatsiya darajasi sinflar diagrammalaridan — loyihalash bosqichida;

- amalga oshirish darajasi sinflar diagrammalaridan — amalga oshirish bosqichida.

Konseptual model ta'rifiga muvofiq ravishda predmetli soha tushunchalari, ushbu tushunchalarning atributlari va ular o'rtasidagi munosabatlar bilan operatsiyalarni bajaradi. Ishlab chiqiluvchi dasturiy ta'minot predmetli sohasining tushunchasiga moddiy predmetlar ham, predmetli soha mutaxassisleri qo'llaydigan abstraksiyalar ham to'g'ri kelishi mumkin.

Modeldagi asosiy tushunchalarga muvofiq ravishda sinflar qo'yiladi. Bunda sinf deyilganda predmetli sohaning topshirilgan obyektlari guruhiga xos umumiy alamatlar jamlanmasi tushuniladi.

Rol

Sinflar nusxalari o'rtasidagi aloqa tegishli obyektlar bir-biriga munosabat bo'yicha o'ynaydigan ayrim rollarni e'tiborda tutadi.

Rol assotsiatsiya yo'nalishi bilan bog'liq.

Rol, shuningdek har bir tomondan bir aloqada qancha obyekt qatnashishi mumkinligini ko'rsatuvchi ko'plik tavsifga ham ega. Ko'plikni quyidagicha ko'rsatishga ruxsat etiladi:

* — 0 dan cheksizlikkacha;

<yaxlit>.. * — topshirilgan miqdordan cheksizlikkacha;

<yaxlit> — obyektlarning aniq belgilangan miqdori;

<yaxlit1>, <yaxlit2> — obyektlar aniq miqdorining bir necha variantlari;

<yaxlit1>..<yaxlit2> — obyektlar diapazonlari.

Nazariy nuqtayi nazardan atribut ham nusxalari ko'rilayotgan sinf bilan qat'iy assotsiatsiyalanuvchi sinfdir. Konseptual modelda tegishli munosabatlarni aks ettirish uchun assotsiatsiyalar ham qo'llanishi mumkin.

Xatti-harakat bayoni

Tizimiy hodisalar va operatsiyalar Konseptual model ishlab chiqiluvchi dasturiy ta'minotning statik xossalarini xarakterlaydi. Uning xatti-harakati xususiyatlarini,

ya'ni tizimning mumkin bo'lgan amallarini bayon etish uchun tizim ketma-ketliklari diagrammalaridan, tizimiy hodisalar, tizimiy operatsiyalar, faoliyatlar diagrammalaridan, zaruriyat bo'lganda obyektlar holatlari diagrammalaridan ham foydalanish maqsadga muvofiqdir.

Tizim ketma-ketliklari diagrammasi.

Tizim ketma-ketliklari diagrammasi — grafik model bo'lib, foydalanish variantining belgilangan ssenariysi uchun harakatlanuvchi shaxslar bo'laklaydigan hodisalarni va ularning tartibini ko'rsatadi. Bunda tizim yagona yaxlitlik sifatida qaraladi. Tizim ketma-ketliklari diagrammasi tizimi uchun quyidagilar zarur:

- tizimni «qora quti» sifatida tasavvur etish va uning uchun hayot chizig'ini blokka pastdan boruvchi vertikal punktir chiziqni tasvirlash lozim;
- har bir harakatlanuvchi shaxsni identifikatsiyalash va uning uchun hayot chizig'ini tasvirlash kerak (dasturiy ta'minlashdan birgalikda foydalanish variantlarida ko'plab harakatlanuvchi shaxslar bo'ladi);
- foydalanish varianti bayonidan tizimiy hodisalar ko'pligini va ularning ketma-ketligini belgilash darkor;
- tizimiy hodisalarni oxirida strelkani chiziqlar tarzida harakatlanuvchi shaxslar va tizimlar hayot chiziqlari o'rtasida tasvirlash, hamda hodisalarning nomlarini va beriluvchi ifodalar ro'yxatlarini ko'rsatish shart.

Ichki hodisalardan farqli o'laroq, tizim uchun harakatlanuvchi shaxslar tomonidan bo'laklanadigan hodisalar tizimiy hodisalar deyiladi. Tizimli hodisalar tegishli ko'plab operatsiyalar (ular ham tizimiy deyiladi) bajarilishini boshlaydi. Har bir tizimiy operatsiyani tegishli xabar nomi bo'yicha nomlanadi.

Barcha tizimli operatsiyalarning ko'pligini barcha foydalanish variantlarining tizimiy hodisalarni identifikatsiyalagan holda belgilanadi. Ko'rgazmalilik uchun tizimiy operatsiyalarni

System abstrakt sinfi (tipi) operatsiyalari tarzida tasvirlanadi.

Agar operatsiyalar ko'pligini turli foydalanuvchilar boshlanuvchi tagko'pliklarga ajratish zarur bo'lsa, u holda bir necha System 1, System 2 va h.k. abstrakt sinflardan foydalaniladi.

Tizimiy hodisalar va operatsiyalar

Har bir tizimli operatsiyalarni bayon etish zarur. Odatda tizimli operatsiya bayoni quyidagilarni qamrab oladi:

- operatsiya nomi va uning parametrlari;
- majburiyat bayoni;
- tip ko'rsatmasi;
- u foydalaniladigan foydalanish variantlari nomlari;
- algoritmlar ishlab chiquvchilari uchun eslatmalar va h.k.lar;
- mumkin bo'lgan istisnolarga ishlov berish bayoni;
- nointerfeys xabarlarini chiqarish bayoni;
- operatsiya bajarilgunga qadar tizim holati haqida taxmin

(old shart);

- operatsiya bajarilgandan so‘ng tizim holati o‘zgarishining bayoni (so‘ng shart).

Foydalanilgan adabiyotlar

1. Ramez Elmasri, Shamkant B.Navathe. Fundamentals of Database Systems (7th Edition). Pearson. USA, 2015.
2. M.T.Azimjanova, Muradova, M.Pazilova. Informatika va axborot texnologiyalari. O'quv qo'llanma. T.: “O'zbekiston faylasuflari milliy jamiyati”, 2013 y.
3. Holmatov T.X., N.I.Tayloqov. Amaliy matematika, dasturlash va kompyuteming dasturiy ta'minoti. O'quv qo'llanma. T.: “Mehnat”, 2000 y.
4. S.S.Qosimov Axborot texnologiyalar O'quv qo'llanma. T.:“Aloqachi”, 2006 y.
5. M Aripov, B.Begalov va boshqalar. Axborot texnologiyalari. O'quv qo'llanma. T.:, “Noshir”, 2009 y.
6. A.Sattorov. Ma'lumotlar bazasini boshqarish sistemasi Access (Windows 9x/2006) O'quv qo'llanma. T.: “Fan Va texnologiya”, 2006 y.
7. Axborot xavfsizligi asoslari, i.M.Karimov tashkent, 2019
8. S.K.Ganiyev, a.A. Ganiyev, d.Y. Irgasheva Ma'lumotlar bazasi Xavfsizligi
9. Sh.A. Nazirov, g.S. Ivanova, s.M. Gaynazarov Dasturlash texnologiyalari
10. Зегжда Д.П. Основы безопасности информационных систем: Учеб. пособие для студ. вузов. – М.: Горячая линия – Телеком, 2016.