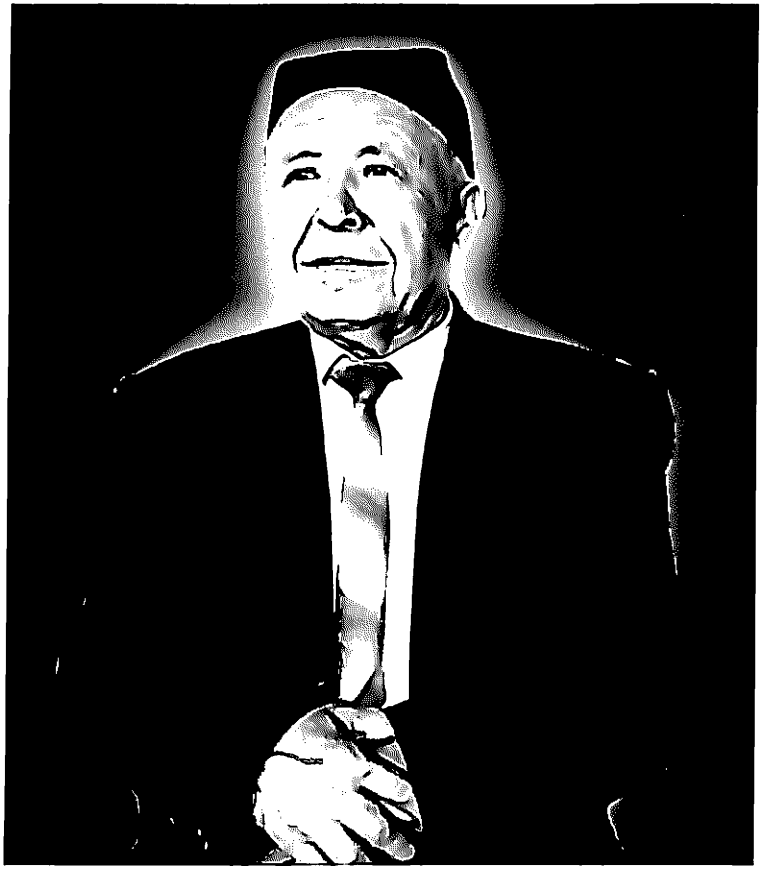
D.Ya.IRGASHEVA

FOYDALANISHNI CHEKLASH USULLARINING SAMARADORLIGINI OSHIRISH

MONOGRAFIYA

Ushbu monografiya otajonim Musayev Yoqubjon Yunusovich xotiralariga bag'ishlanadi



MUSAYEV YOQUBJON YUNUSOVICH

(16.02.1938-14.12.2020)

O‘ZBEKISTON RESPUBLIKASI AXBOROT
TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI
RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI
UNIVERSITETI

IRGASHEVA DURDONA YAKUBDJANOVNA

FOYDALANISHNI CHEKLASH USULLARINING SAMARADORLIGINI OSHIRISH

(MONOGRAFIYA)

«ZEBO PRINT»
TOSHKENT – 2022

UDK. 004.056.052
KBK: 35ya73

D.Ya.Irgasheva. Foydalanishni cheklash usullarining samaradorligini oshirish: Monografiya. –T.: «ZEBO PRINT» nashriyoti, 2022 yil. – 144 bet.

Monografiyada kompyuter tizimlarini samarali himoyalash uchun foydalanishni cheklash vositalarini qurish, vakolatlarni nazoratlash modellari, usullari va algortimlarini ishlab chiqish va takomillashtirishga qaratilgan. Foydalanishni cheklash tizimiga tahdidlarning ta'siri va ushbu tizimning fosh etilishi ehtimolliklarini hisoblashga imkon beruvchi tahdidlar modelining tavsifi, moslanuvchanlikni, ma'murga yuklamaning pasayishini ta'minlash va dinamik faoliyat muammosini hal etishga imkon beruvchi foydalanishni rolli cheklash tizimi dinamik modelining tahlili, dinamik modeldagi rasmiy spetsifikatsiya va algoritmlari hamda ishlab chiqilgan foydalanishni rolli cheklash tizimi modeli algoritmining tavsifiga va ma'lumotlardan foydalanishni boshqarishni detallashtirishni amalga oshirish uchun, atributlar asosida rolli bazani foydalanishni boshqarish bilan birlashtiruvchi foydalanishni cheklashga bag'ishlangan.

Ushbu monografiya kompyuter tizimlarini samarali himoyalash uchun foydalanishni cheklash tizimlarini qurish doirasida ilmiy izlanish olib borayotgan mutaxassislar uchun tavsiya etiladi, hamda mazkur sohada oliy ta'lim muassasalari talabalari, magistrlari va tadqiqotchilari ham foydalanishi mumkin.

Monografiya Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Ilmiy texnik kengashning qarori bilan chop etishga tavsiya etiladi (2022 yil 29 sentyabr № 6-22-sonli bayonnoma).

UDK. 004.056.052
KBK: 35ya73

Taqrizchilar:

Sagatov Miraziz Varisovich	Islom Karimov nomidagi Toshkent davlat texnika universitetining «Axborot texnologiyalari» kafedrasi mudiri, t.f.d., professor.
Kerimov Kamil Fikratovich	Muhammad al-Xorazmiy nomidagi TATU "Tizimli va amaliy dasturlashtirish" kafedrasi mudiri, t.f.d., dotsent.

ISBN 978-9943-8611-2-1

KIRISH

Umumjahon axborot globallashuvi jarayoni kompyuter tizimlarini (KT) inson faoliyatining barcha sohalariga nafaqat joriy etishni, balki axborot tizimi xavfsizligini ta'minlash sharoitlarining zaruratini ko'zda tutadi. Kompyuter tizimida kechayotgan axborot jarayonining o'ziga xos xususiyati ishlanayotgan axborot xavfsizligiga yuqori talablarning ta'minlanishi zarurati hisoblanadi. Bu, bir tomondan KTda ishlanayotgan axborotning qiymati orqali, ikkinchi tomondan esa kompyuter tizimidagi axborot xavfsizligiga tahdidlarning katta sonining mavjudligi orqali aniqlanadi. Shu bilan birga ta'kidlash lozimki, turli tahdidlarni soni vaqt o'tishi bilan doimo ortadi. Rivojlangan mamlakatlarda, jumladan, AQSh, Rossiya Federatsiyasi, Yaponiya, Fransiya, Janubiy Koreya va boshqa davlatlarda kompyuter tizimlarida axborot yaxlitligi va konfidensialligini ta'minlash imkoniyatini beruvchi foydalanishlarni cheklash va nazorat qilish vositalarni ishlab chiqish muhim ahamiyat kasb etmoqda.

Jahonda ruxsatsiz foydalanishlarni bartaraf etishga va ulardan himoyalashga qaratilgan model, usul va algoritmlarni ishlab chiqishga, shuningdek mavjudlarini takomillashtirishga yo'naltirilgan ilmiy-tadqiqot ishlari olib borilmoqda. Bu borada, hozirgi kunda kompyuter tizimlarida foydalanishni cheklash tizimini qurishda shakllangan yondashish, odatda statik xarakterga ega bo'lib, bunday yondashish ishlanuvchi axborotning konfidensialligini kafolatli ta'minlash bo'yicha talablarning qondirilishiga mo'ljallangan usullarini va algoritmlarni ishlab chiqish muhim vazifalardan biri hisoblanmoqda. Shu bilan birga foydalanishni cheklash tizimlarida yuritiladigan axborot xavfsizligi siyosatini dinamik o'zgarishi va vazifalarni taqsimlash texnologiyasi orqali foydalanuvchilarning vakolalatlarini nizolashishi jarayonlarini boshqarishni usullarini takomillashtirishni ilmiy asoslash zarur bo'l-moqda. Dunyoda rolga asoslangan foydalanishni cheklash tizimlarida vakolatlarning sirqib chiqishi xavfini baholashning iyerarxik usullarini ishlab chiqishning ustuvor yo'nalishlari, shuningdek foydalanishni huquqini cheklash modellarida rollar iyerarxiyasi asosida vakolat modellarini ishlab chiqish va atributlarga asoslangan foydalanishni cheklash usullarini takomillashtirish bo'yicha tadqiqotlar olib borilmoqda. Ammo, kompyuter tizimlaridan foydalanishni cheklash tizimini qurishda muayyan formal modellarni tanlash va qo'llash

masalalari yetarlicha o'rganilmagan. Undan tashqari, foydalanishni boshqarishning mavjud modellarining birortasida ham KT foydalanuvchilarning rolli strukturasi, o'zaro ta'sirdagi funksional modullarga muvofiq, hisobga olinmaydi.

Ushbu monografiyaning asosiy mazmuni kompyuter tizimlarini samarali himoyalash uchun foydalanishni cheklash vositalarini qurish, vakolatlarni nazoratlash modellari, usullari va algortimlarini ishlab chiqish va takomillashtirishga qaratilgan.

Birirnchi bobda kompyuter tizimlarini himoyalash muammolarining hamda foydalanishni cheklash modellarining tahlili asosida himoyalangan kompyuter tizimlarini loyihalashga asosiy talablarni shakllantirish masalasiga bag'ishlangan. Kompyuter tizimlarida foydalanishni cheklash tahdidlarining tahlili ham ushbu bobdan o'rin olgan.

Monografiyaning ikkinchi bobi foydalanishni cheklash tizimiga tahdidlarning ta'siri va ushbu tizimning fosh etilishi ehtimolliklarini hisoblashga imkon beruvchi tahdidlar modelining tavsifiga bag'ishlangan. Foydalanishni cheklash tizimi va uning konseptual modeli, hamda foydalanishni cheklash tizimining samaradorligi ko'rsatkichlarining bayoni ham ushbu bobdan o'rin olgan.

Uchinchi bob, moslanuvchanlikni, ma'murga yuklamaning pasayishini ta'minlash va dinamik faoliyat muammosini hal etishga imkon beruvchi foydalanishni rolli cheklash tizimi dinamik modelining tavsifiga bag'ishlangan. Atributlarga asoslangan siyosatning, normativ talablarining murakkabligini pasaytirish evaziga, foydalanishni boshqarish samaradorligini oshirish masalasi ham shu bobdan o'rin olgan.

To'rtinchi bob rollar asosida foydalanishni boshqarishning dinamik modelining tahlili, dinamik modeldagi rasmiy spetsifikatsiya va algoritmlari hamda ishlab chiqilgan foydalanishni rolli cheklash tizimi modeli algoritmining tavsifiga bag'ishlangan.

I-BOB. KOMPYUTER TIZIMLARIDA AXBOROT XAVFSIZLIGINING ZAMONAVIY HOLATI

1.1. Kompyuter tizimlarini himoyalash muammolari

Tashkilotning axborot-hisoblash tarmoqlari yoki kompyuter tarmoqlari ma'lumotlarni uzatish kanallari vositasida birlashtirilgan KT hisoblanadi. Axborot-hisoblash tarmog'i uchun yana bir nom, ya'ni hisoblash tarmog'i nomi bo'lishi mumkin, ammo bu uning asosiy vazifasini-axborotli xizmat ko'rsatishni ifodalamaydi. Kompyuter tizimlarini loyihalashda ikkita yetarlicha ziddiyatli masalalarni yechish lozim.

Birinchi masala-minimal narxli tizimni yaratish. Bunday tizimlarni yaratish narxi jamoaviy resurslardan foydalanish darajasiga mutanosib. Bu degani, tizim narxini minimallashtirish maqsadida tizimdan foydalanuvchilarning barchasi uchun jamoaviy resurslarni, jumladan axborotning saqlanishini madadlovchi vositalarni, axborotni ishlovchi va boshqa vositalardan va tizimlardan foydalanishning dasturiy va apparat vositalarini yaratish maqsadga muvofiq hisoblanadi. Foydalanishni tashkil etishning muvaffaqiyatli tanlanishi va jamoaviy resurslarning imkoniyati tizimni, uning ishlashiga qo'yilgan talablarning amalga oshirilishida, yaratish va ekspluatatsiya narxini yetarlicha pasaytiradi.

Jamoaviy resurs imkoniyatlaridan foydalanib axborotni ishlash, bu imkoniyatlardan har bir foydalanuvchi foydalana olishi shart degani emas. Foydalanuvchanlik tizim yaratilishida ifodalangan qoidalar (talablar) orqali aniqlanadi. Tizimdan foydalanuvchilarni alohida sinflarga ajratishda aynan ushbu qoidalarga rioya qilish *ikkinchi masalani* yechish lozimligini oldindan belgilaydi, ya'ni axborotni uzatish va ishlash jarayonini shunday tashkil etish kerakki, har bir foydalanuvchi faqat unga ruxsat etilgan axborotni olsin. Ravshanki, har bir tizimdan foydalanuvchi uchun resursni individuallashtirish ikkinchi masalaning optimal yechimi hisoblanadi, ammo axborotni ishlash tizimini yaratish va ekspluatatsiya narxi yetarlicha oshadi. Aynan, shu nuqtai nazardan birinchi va ikkinchi masalalar maqsadida ziddiyat mavjud.

Axborotni ishlovchi kompyuter tizimlarining xavfsizligi deganda tizim bilan muloqot jarayonida axborot resurslariga zarar yetkazish urinishlariga qarshilik qilish qobiliyati tushuniladi. Bunday xavfsizlikka ishlanuvchi axborot konfidensialligini hamda o'rnatilgan qoidalarga

muvofiq tizim komponentlari va resurslarining yaxlitligini va foydalanuvchanligini ta'minlash evaziga erishiladi.

Kompyuter tizimlarining tashqi va ichki xavfsizligi farqlanadi. Tashqi xavfsizlik tizimni tabiiy ofatdan, niyati buzuqning tizimning alohida komponentini o'g'irlash, axborot eltuvchilardan foydalanish yoki tizimni ishdan chiqarish maqsadida, tashqaridan suqilib kirishidan himoyalashni ko'zda tutadi. Ichki xavfsizlikning maqsadi tizimning ishonchli va to'g'ri ishlashini, uning dasturlari va ma'lumotlari yaxlitligini ta'minlash hisoblanadi. Hozirda kompyuter tizimlarining ichki xavfsizligini taminlashda ikkita yondashish ma'lum-fragmentar va kompleks.

Fragmentar yondashish ma'lum sharoitlarda ma'lum tahdidlarga qarshi turishni ko'zda tutadi. Bunday yondashishga misol sifatida ixtisoslashtirilgan antivirus vositalarini, qaydlash va boshqarishning alohida tadbirlarini, shifrlashning avtonom vositalarini va h. ko'rsatish mumkin. Fragmentar yondashishning asosiy xususiyati (bir vaqtning o'zida asosiy kamchiligi)-axborotni ishlashning yagona himoyalangan muhitining mavjud emasligi. Fragmentar yondashishning afzalligi uning muayan tahdidga nisbatan yuqori tanlash xususiyati va berilgan yo'nalishdagi harakatlarning samaradorligi. Ammo tahdidning hatto ozgina o'zgarishi himoya samaradorligining yo'qolishiga olib keladi. Lokal tadbirlar ta'sirini butun tizimga darhol tarqatish amaliy jihatdan mumkin emas.

*Kompleks yondashish*ning xususiyati-tarkibida tahdidlarga qarshi turuvchi huquqiy, tashkiliy, dasturiy-apparat tadbirlar mavjud axborotni ishlashning himoyalangan muhitini yaratish. Axborotni ishlashning himoyalangan muhiti axborotni ishlash jarayonining reglamenti asosida shakllantiriladi. Himoyalangan muhitni tashkil etish, qabul qilingan xavfsizlik siyosati doirasida, tizimni himoyalashning zaruriy darajasini kafolatlash imkonini beradi. Kompleks yondashishdan ko'pchilik foydalanuvchi davlat yoki tijorat tizimlarda ham, muhim iqtisodiy, siyosiy va harbiy axborotni ishlovchi nisbatan katta bo'lmagan tizimlarda ham foydalaniladi.

Ruxsatsiz foydalanilishdan himoyalangan kompyuter tizimi loyihalanuvchi ob'ekt sifatida murakkab tizim hisoblanadi. U quyidagi murakkab tizimga xos muhim xususiyatlarga ega:

- boshqarishning yagona maqsadi - kompyuter tizimining axborot xavfsizligi rejimida ishlashini ta'minlash;

- ko‘pgina avtonom qismtizimlarga dekompozitsiyalanish imkoniyati;

- qismtizimlarning guruhlanishi va tobelikning bir necha sathlariga ega iyerarxik qurilishi;

- markazlashtirilishining yuqoriligi;

- tashqi ta’sirlarning tasodifiy xarakterligi bilan bog‘liq tizim ishlashining murakkabligi.

Ushbu kompyuter tizimlarining o‘ziga xos xususiyatlarini nazarda tutgan holda, axborotni himoyalash tizimini loyhalash jarayoni strukturasini 1.1-rasmda keltirilganidek ifodalash mumkin.

Himoya tizimini loyihalash-iteratsion muolaja, umumiy holda, quyidagi muolajalarni o‘tkazishni ko‘zda tutadi:

- himoyalanuvchi kompyuter tizimi funksional xarakteristikalarini tahlillash;

- bo‘lishi mumkin bo‘lgan buzilishlar modelini shakllantirish;

- bo‘lishi mumkin bo‘lgan ruxsatsiz foydalanish kanallarini aniqlash va tahlillash; axborotni himoyalashning dasturiy ta’minotini tanlash yoki ishlab chiqish uchun talablarni shakllantirish;

- axborotni himoyalash tizimini tanlash; axborotni himoyalash tizimi (AHT) samaradorligini baholash; himoyalanganlikni baholash asosida oldingi bosqichlarda shakllantirilgan talablarga aniqlik kiritish [90, 91, 93].

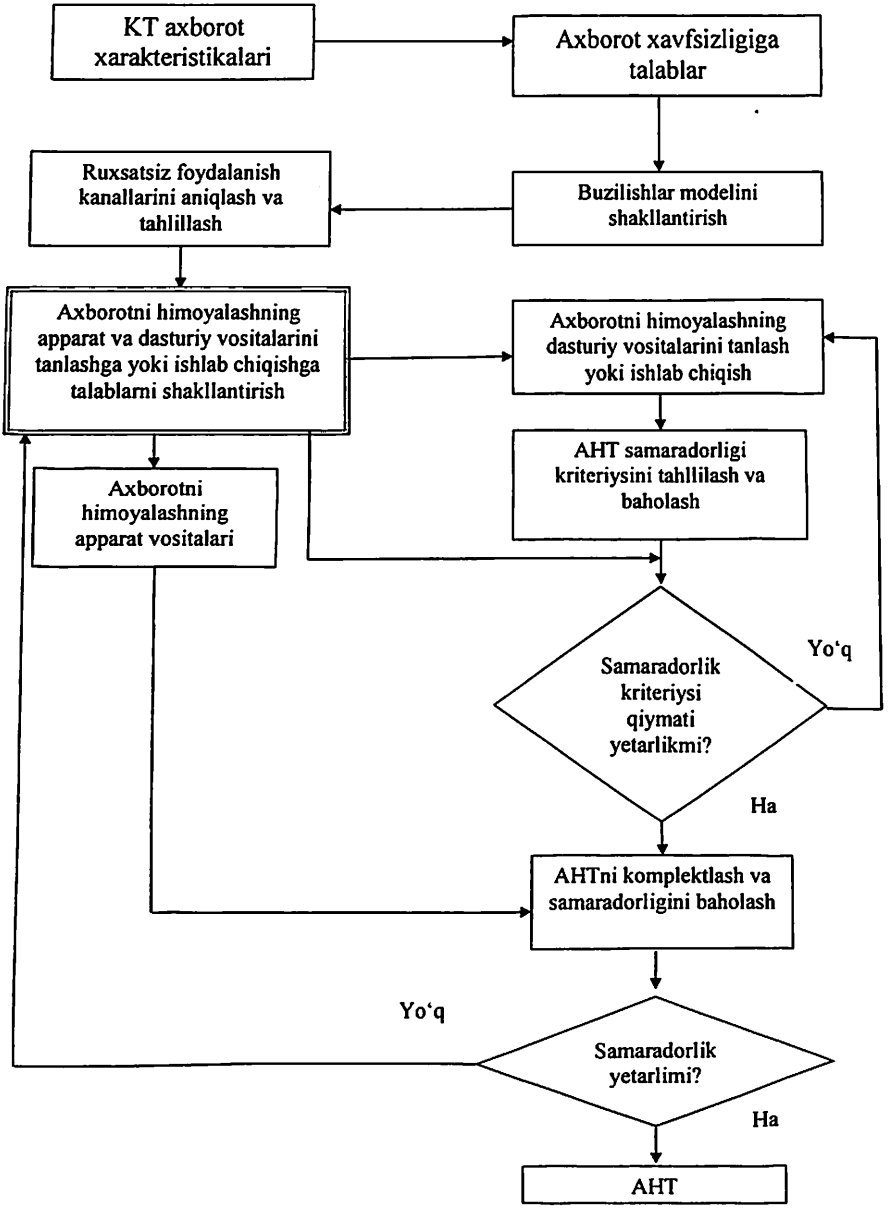
Loyihalash muolajalarining har bir iteratsiyasi ichida bajariluvchi talablarni shakllantirish axborot xavfsizligi tizimini loyihalashning muhim bosqichi hisoblanadi [110, 112, 116]. Bu axborotni himoyalash tizimi sifatining ko‘p jihatdan talablarning asosligiga, hamda ularning tizimda bajarilishi darajasiga bog‘liqligi bilan izohlanadi.

Axborotni ishlash texnologiyasi, tarkibida himoyalashning dasturiy-apparat vositalari va axborotni himoyalash bo‘yicha umumiy talablarning bajarilishini ta’minlovchi tashkiliy tadbirlar mavjud bo‘lsa, himoyalangan hisoblanadi.

Umumiy talablar quyidagilarni ko‘zda tutadi [110, 112, 116]:

- avtomatlashtirilgan tarzda ishlanishi lozim bo‘lgan konfidensial axborotlar ro‘yxatining mavjudligi;

- ma’lum (yaratilgan) javobgar qismbo‘limning mavjudligi. Ushbu qismbo‘limga axborotni ximoyalash texnologiyasini joriy etish, axborotning himoyalanganligi darajasini nazoratlash buyicha vakolatlar taqdim etiladi;



1.1-rasm. Axborotni himoyalash tizimini loyihalash jarayonining strukturasi

- kompyuter tizimining ishlashi mobaynida axborotni himoyalashni ta'minlashga mo'ljallangan tashkiliy va injener-texnik tadbirlar, dasturiy-apparat vositalari majmui hisoblanuvchi AHTni yaratish;

- kompyuter tizimidagi AHTning axborotni himoyalash bo'yicha me'yoriy hujjatlarga mosligi attestatining mavjudligi;

- AHT vositalari yordamida foydalanuvchilar vakolatlarining bir necha iyerarxik sathlarini va axborotning bir necha tasnifiy sathlarini aniqlash imkoniyati;

- kompyuter tizimidagi barcha foydalanuvchilar va ularning konfidensial axborotga nisbatan harakatlari qaydlanishi shart;

- foydalanuvchilarga kompyuter tizimida ishlanuvchi konfidensial axborotdan, faqat xizmat zaruriyati sharoitida, ruxsatli va nazoratlanuvchi foydalanishni taqdim etish imkoniyati;

- kompyuter tizimidagi konfidensial axborotning ruxsatsiz va nazoratsiz modifikatsiyalanishi taqiqlanadi;

- AHT yordamida funksional masalaning yechilishi natijasidagi ma'lumotlarni, tarkibida amal qilinuvchi hujjatlarga muvofiq konfidensial axborot bo'lgan, chop etilgan hujjat shaklida hisobga olishni amalga oshirish;

- konfidensial axborotni ruxsatsiz nusxalash, ko'paytirish, elektron shaklda tarqatish taqiqlanadi;

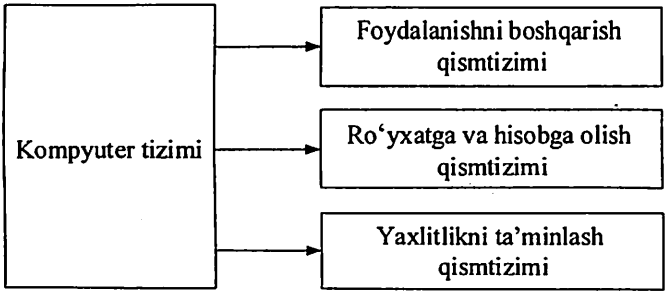
- AHT yordamida konfidensial informatsiyaning ruxsatli nusxalanishini, ko'paytirilishini, elektron shaklda tarqatilishini nazoratlash;

- har bir ro'yxatga olingan foydalanuvchini bir ma'noli identifikatsiyalashni va autentifikatsiyalashni amalga oshirish imkoniyati;

- AHTning ro'yxatga olingan kompyuter tizimlaridan foydalanuvchilarining konfidensial axborotdan o'z vaqtida foydalanishlari imkoniyatini ta'minlash.

Yuqorida keltirilgan talablar bazaviy hisoblanadi va turli xil kompyuter tizimlarida axborotni ruxsatsiz foydalanishdan himoyalashda ishlatiladi [80].

Kompyuter tizimini shartli ravishda axborotni himoyalashni ta'minlovchi muhim qismtizimlarga ajratib, har bir alohida qismtizimlarga kompyuter axborotini ruxsatsiz foydalanishdan himoyalashga qo'yiladigan talablarni belgilash mumkin [112, 116] (1.2-rasm).



1.2-rasm. Kompyuter tizimlarida axborotni himoyalashni ta'minlash qismtizimlari

Foydalanishni boshqarish qismtizimi quyidagi talablarni qondirishi lozim:

- tizimga kirishda foydalanuvchi sub'ektlarni identifikatsiyalash va ularning xaqiqiyligini tekshirish;
- terminallarni, kompyuter tarmog'i uzellarini, aloqa kanallarini, tashqi qurilmalarni, ularning mantiqiy adresi (nomeri) bo'yicha identifikatsiyalash;
- dasturlarni, tomlarni, kataloglarni, fayllarni, yozuvlarni va yozuv hoshiyalarini ularning nomi bo'yicha identifikatsiyalash;
- foydalanish matritsasiga muvofiq sub'ektlarning himoyalanuvchi resurslardan foydalanishlarini nazoratlashni amalga oshirish.

Ro'yxatga va hisobga olish qismtizimi quyidagi talablarni qondirishi lozim:

- foydalanuvchi sub'ektlarning tizimga kirishini (tizimdan chiqishini) yoki operatsion tizimni yuklash va ishga tushishini va uning dasturiy to'xtatilishini ro'yxatga olish;
- chop etilgan hujjatlarning "qattiq" nusxaga o'tkazilishini ro'yxatga olish;
- himoyalanuvchi faylarni ishlashga mo'ljallangan dasturlarni va jarayonlarni ishga tushirilishini (tugallanganligini) ro'yxatga olish;
- dasturiy vositalarning (dasturlar, jarayonlar, topshiriqlar, masallalar) himoyalanuvchi fayllardan foydalanishga urinishlarini ro'yxatga olish;
- dasturiy vositalarning foydalanuvchi qo'shimcha himoyalanuvchi ob'ektlardan, (terminllardan, tarmoq uzellaridan, aloqa kanal-

laridan, tashqi qurilmalardan, dasturlardan, fayllardan va h.) foydalanishga urinishlarini ro'yxatga olish;

- barcha himoyalanuvchi axborot eltuvchilarni, ularning belgilari yordamida jurnallarda qaydlash yo'li bilan hisobga olish;

- himoyalanuvchi axborot eltuvchilarni taqdim etishda ro'yxatga olish;

- asosiy xotira va tashqi to'plagichlarda bo'shagan zonalarni tozalashni amalga oshirish.

Yaxlitlikni ta'minlash qismtizimi quyidagi talablarni qondirishi lozim:

- AHT dasturiy vositalarining yaxlitligini, ishlanuvchi axborotni ruxsatsiz foydalanishdan himoyalash, hamda dasturiy muhitning o'zgarmasligini ta'minlash;

- dasturiy muhit va kompyuter tizimi xodimi o'zgarganida AHT funksiyalarini, ruxsatsiz foydalanishini imitatsiyalovchi test-dasturlar yordamida, davriy testlash;

- ruxsatsiz foydalanishdan himoyalash tizimlarini tiklash vositalarining mavjudligi. Bunda ruxsatsiz foydalanishdan himoyalashning dasturiy vositalarining ikkita nusxasini yuritish, hamda ularni davriy yangilash va ishga layoqatligini nazoratlash ko'zda tutiladi.

Yuqorida keltirilgan barcha mexanizmlar eng muhim hisoblanadi [110, 112, 116]. Ular quyidagicha o'zaro bog'langan: resurslardan foydalanishning barcha huquqlari (resurslardan foydalanishning cheklangan siyosati) foydalanishning muayyan sub'ektiga beriladi. Shu sababli, sub'ekt tizimga kirishida identifikatsiyalanishi va uning xaqiqiyligi nazoratlanishi lozim.

1.2. Kompyuter tizimlarida foydalanishni cheklash modellarining tahlili

Aksariyat foydalanishni cheklash modellari kompyuter tizimini foydalanishning sub'ektlari va ob'ektlari majmui sifatida tasavvur etishga va quyidagi asosiy tushunchalarga asoslanadi.

Foydalanish sub'ekti-ob'ektdan ob'ektga boradigan axborot oqimiga yoki tizim holatining o'zgarishiga sababchi bo'lishi mumkin bo'lgan, odatda foydalanuvchi, jarayon yoki qurilma ko'rinishida ifodalangan tizimning faol komponenti.

Foydalanish ob'ekti -shtatda ko'rsatilgan, texnik vositalar yordamida foydalaniladigan axborot resurs birligi.

Sub'ektlar va ob'ektlar va ular orasidagi munosabatlar majmui tizim holatini belgilaydi. Tizimning har bir holati, modelda taklif etilgan xavfsizlik kriteriylariga muvofiq, xavfsiz yoki xavfli bo'lishi mumkin. Xavfsizlik modelining asosiy qoidasi-xavfsiz holatdagi tizimning, o'rnatilgan barcha qoida va cheklashlarga rioya qilinganida, xavfli holatga o'tmasligi fikrining tasdiqi [110, 114, 118].

Mavjud foydalanish modellarini tahlillash va axborot xavfsizligini t'minlash nuqtai nazaridan, samarali modellarni aniqlash dolzarb muammolardan hisoblanadi.

Tahlillash uchun kriteriylar sifatida qo'yidagilar tavsiya etiladi:

-amalga oshirilishining oddiyligi;

-ma'murlanishining oddiyligi;

-foydalanish huquqlarining ortiqchaligi;

-sozlanishining moslashuvchanligi;

-axborot konfidensialligini himoyalash nazorati;

-axborot yaxlitligini himoyalash nazorati;

-axborot foydalanuvchanligini himoyalash nazorati.

Xarrison- Ruzzo-Ulmanning diskretsion modeli. Xavfsizlikning diskretsion modeli-foydalanishni diskretsion boshqarishga asoslangan modeli. Foydalanishni diskretsion cheklash-nomlangan sub'ektlar va nomlangan ob'ektlar orasida foydalanishni cheklash. Foydalanishni diskretsion cheklash quyidagi qoidalarni hisobga olgan holda amalga oshiriladi:

-har bir foydalanuvchi, ma'lumotlardan foydalanishdan oldin, autentifikatsiyalanishi shart;

-autentifikatsiyalovchi axborotga (autentifikator va parol) muvofiq foydalanuvchiga uning vakolatlari tizimi belgilanadi.

Foydalanuvchi vakolatiga muvofik, faqat ma'lumotlarning va ularni ishlovchi muolajalarning belgilangan naboridan foydalanish mumkin. Bunda foydalanuvchining hech qanday so'rovi u erishib bo'lmaydigan ma'lumotlarning ishlov jarayoniga jalb qilinishiga yo'l qo'yilmaydi.

Vakolatlarni belgilash va tekshirishda sub'ekt-ob'ekt munosabatlarini xavfsizlik matritsasi ko'rinishida ifodalash qulay hisoblanadi. 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 yozib qo'yiladi [88, 92].

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.

Xarrison-Ruzzo-Ulman modelining xavfsizlik kriteriysiga muvofiq, tizimning xavfsiz konfiguratsiyasi uchun, agar sub'ekt ob'ektdan foydalanish huquqiga avvaldan ega bo'lmagan bo'lsa, u xech qachon ob'ektdan foydalana olmaydi. Foydalanish huquqini olishning mumkin emasligi komandalar bajarilishining inkor etilishiga olib keladi, chunki sub'ekt yoki ob'ektning olib tashlanishi matritsaning mos ustuni yoki qatoridan barcha huquqlarning yo'q qilinishiga olib keladi. Ammo, bu ustun yoki qatorning o'zini yo'q qilinishiga va matritsa o'lchamining qisqarilishiga sabab bo'lmaydi. Demak, agar boshlang'ich holatda qandaydir yacheykada foydalanish huquqi mavjud bo'lsa, ushbu huquq tegishli sub'ekt yoki ob'ektning chiqarib tashlanishi natijasida yacheyka tozalanadi. Ammo, keyinchalik ob'ekt yoki sub'ektning vujudga kelishi natijasida yacheyka qaytadan tiklanadi va ushbu yacheykaga, mos komanda yordamida, yana foydalanish huquqi kiritiladi [110, 114]. Bu xavfsizlikning buzilishini anglatmaydi.

Xarrison-Ruzzo-Ulman modeli amalga oshirilishida eng oddiy , boshqarishda samarali hisoblanadi, chunki hech kanday murakkab algoritmlarni talab etmaydi va foydalanuvchilar vakolatlarini ob'ekt ustida amalgacha aniqlik bilan boshqarishga imkon beradi. Shu sababli, ushbu model zamonaviy tizimlarda keng tarqalgan.

Ushbu modelda tavsiya etilgan xavfsizlik kriteriysi, amaliy jihatdan, nihoyatda e'tiborli, chunki avvaldan mos vakolatlar berilmagan foydalanuvchilarning ma'lum axborotdan foydalana olmasliklarini kafolatlashga imkon beradi.

Klark-Vilsonning diskretsion modeli. Model axborot yaxlitligini ta'minlashga mo'ljallangan. Ushbu modelda, tarkibida qo'yidagilar mavjud "yaxlitlikning uchligi" ko'riladi:

-sub'ekt;

- yaxlitlikni buzmaydigan amal;

- ob'ekt.

O'zgartirish muolajalari deb ataluvchi elementar amallarning mantiqiy birlashgan majmui, hamda yaxlitlikka tekshirishni ta'minlovchi muolajalarning qo'shimcha sinfi kiritiladi.

Quyidagi qoidalar joriy qilinadi:

-yaxlitlikni tekshirish muolajalarining to'plami, yaxlitligini nazoratlash talab qilingan, barcha ob'ektlarga qo'llanishi shart;

-o'zgartirishning barcha muolajalari ob'ektlar yaxlitligini buzmaydigan tranzaksiyalar bo'lishi va tizim ma'muri tomonidan o'rnatiluvchi, yaxlitlikni talab qiluvchi faqat ob'ektlar ro'yxatiga qo'llanilishi lozim;

-tizim, oldingi qoidada aniqlangan ro'yxatga muvofiq, ob'ektlarga amallarning qo'llanishligini nazoratlashi lozim;

-tizim tarkibida muayyan foydalanuvchilarga ruxsat etilgan muolajalarning ro'yxati bo'lishi lozim;

-tizim amallarni bajaruvchi barcha foydalanuvchilarni autentifikatsiyalashi lozim;

-har bir o'zgartirish muolajasi qaydlash jurnaliga, ushbu muolajaning qo'llanish sharoitining to'la manzarasini tiklashga yetarli axborotni yozishi lozim;

-ba'zi o'zgartirish muolajalari yaxlitligi nazorat qilinishi talab etilmaydigan ob'ektlarni yaxlitligi talab etiladigan ob'ektlarga aylantirishi mumkin;

-faqat maxsus vakolatli sub'ekt joiz ob'ektlar ro'yxatini va o'zgartirish muolajalarini o'zgartirish huquqiga ega.

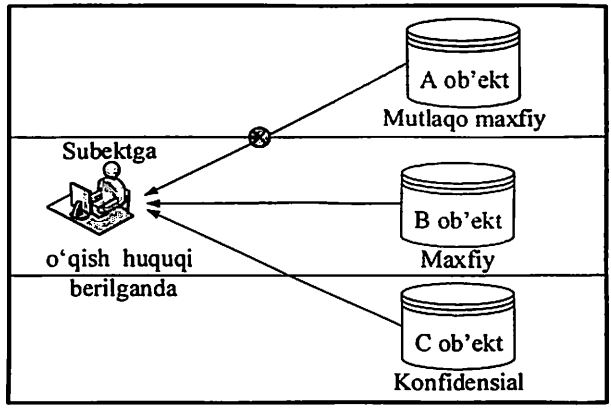
Ushbu modelni amalga oshirish oddiy, ammo u faqat yaxlitlikning buzilishi muammosini hal etadi. Shu sababli, undan, xavfsizlikning muhim kriteriysi-konfidensiallikni himoyalash bo'lgan tizimlarda foydalanish maqsadga muvofiq hisoblanmaydi.

Joiz amallar va ob'ektlar ro'yxatining mavjudligi, ushbu modelga asoslangan tizimni sozlanishda moslashuvchan deb hisoblashga imkon beradi. Ma'murning foydalanuvchilardan izolyatsiyalanganligi sababli, tizimni ma'murlash qulay [88, 92].

Bell-La Padul modeli. Bell-La Padul nomi uni yaratuvchilari Bell va LaPadul ismlari bilan bog'liq. Ushbu model konfidensiallik darajasini hisobga olgan holda, foydalanuvchini mandatli boshqarish mexanizmlarini formallashtirish uchun ishlatiladi. Ma'lumki, foydalanishni cheklashning mandatli prinsipi ob'ektlar konfidensialligining iyerarxik sathlarining va ularga mos konfedensiallik belgilarining mavjudligini ko'zda tutadi [110, 114].

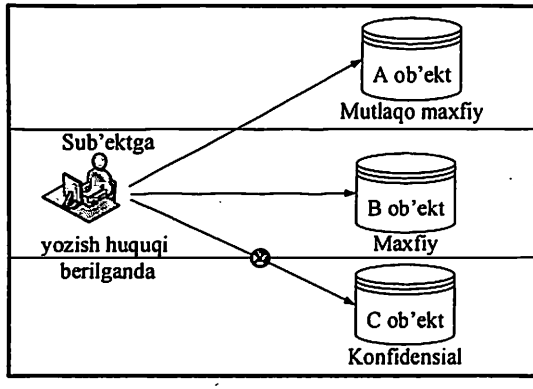
Bell-La Padul modelida tizimdagi sub'ektlar va ob'ektlar maxfiylik grifi bo'yicha taqsimlanadi va quyidagi bazaviy qoidalar bajariladi:

1. *"Xavfsizlikning oddiy qoidasi" (Simple Security).* Ushbu qoidaga binoan sub'ekt faqat xavfsizlik sathi o'zining xavfsizlik sathidan yuqori bo'lmagan hujjatlardan axborotni o'qishga haqli. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 1.3-rasmda keltirilgan.



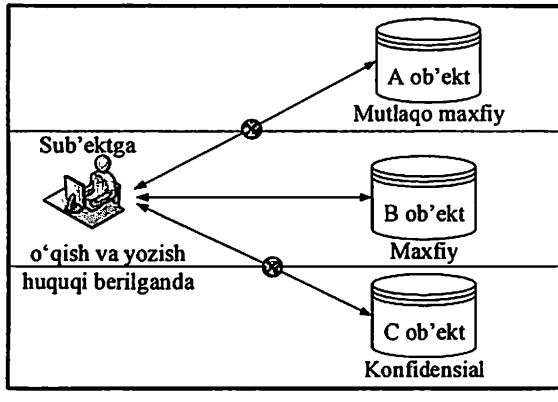
1.3-rasm. "Simple Security" xususiyati uchun axborot oqimlari sxemasi

2. *"-Xususiyat" (-Property).* Ushbu qoidaga binoan sub'ekt xavfsizlik sathi o'zining xavfsizlik sathidan past bo'lmagan hujjatlarga axborot kiritishi mumkin [109]. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 1.4-rasmda keltirilgan.



1.4-rasm. "-Property" xususiyati uchun axborot oqimlari sxemasi

3. *"-Qat'iy xususiyat" (-Strong Property).* Ushbu qoidaga binoan o'qish va yozish huquqiga ega sub'ekt faqat o'zining sathidagi ob'ektlar bilan amallar bajarishi mumkin. Uchta darajali maxfiylikka ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 1.5–rasmda keltirilgan.



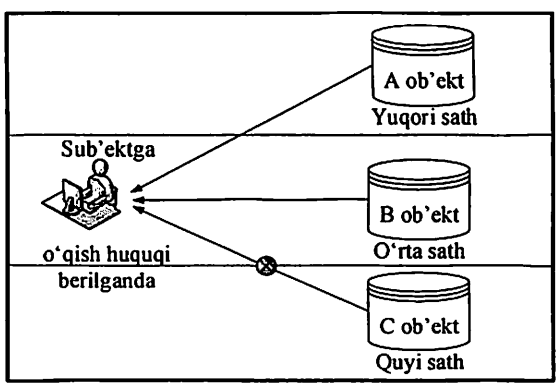
1.5-rasm. "-Strong-property" xususiyati uchun axborot oqimlari sxemasi

Biba modeli. Ushbu model Bell-La Padul modelining modifikatsiyasi bo'lib, ma'lumotlar yaxlitligini ta'minlashga yo'naltirilgan. Biba modelining bazaviy qoidalari quyidagicha ifodalanadi:

1. *"Yaxlitlikning oddiy qoidasi" (Simple Integrity, SI).* Ushbu qoidaga binoan sub'ekt o'zining sathidan past yaxlitlik sathidan axborotni o'qiy olmaydi. Yaxlitlikning uchta sathiga ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 1.6-rasmda keltirilgan.

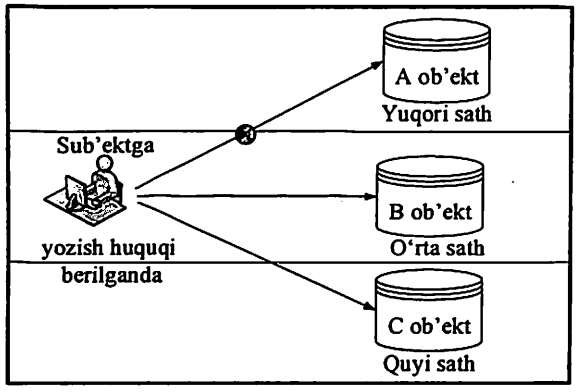
2. *"-Yaxlitlik" (*- integrity).* Ushbu qoidaga binoan sub'ekt o'zining sathidan yuqori yaxlitlik sathiga axborotni yoza olmaydi. Yaxlitlikning uchta sathiga ega tizimda ushbu qoidaning amalga oshirilishiga mos axborot oqimlari sxemasi 1.7-rasmda keltirilgan.

3. *"Chaqiruv xususiyati" (Invocation Property).* Ushbu qoidaga binoan sub'ekt yaxlitlikning yuqori sathidagi sub'ektdan servisni so'ray olmaydi.



1.6-rasm. "Simple integrity" xususiyati uchun axborot oqimlari sxemasi
o'qish

Ta'kidlash lozimki, Biba modelidagi yaxlitlik sathlarini ishonchlilik sathi sifatida qabul qilmoq lozim. Mos axborot oqimlarini esa axborotni ma'lumotlarning yuqori ishonchli majmuidan ishonchligi pastrog'iga va aksincha uzatish kabi qabul qilish lozim [109].



1.7-rasm. "- integrity" xususiyati uchun axborot oqimlari sxemasi*

Millen modeli. Ushbu model axborotning foydalanuvchanligini buzilishidan himoyalashga mo'ljanlangan. Uning asosiy g'oyasi jarayonlar uchun makon va vaqtni taqsimlashga talablarni shakllantirishdan iborat. Modelning asosiy elementlari quyidagilar:

- aktiv jarayonlar to'plami;
- passiv resurslar to'plami;
- barcha xil joiz resurslar birliklarining umumiy maksimal sonini belgilashda foydalaniluvchi qandaydir o'zgarmas chegara;
- qandaydir holatdagi jarayonga ajratilgan har bir resurs uchun resurslar birligi sonini belgilovchi taqsimot vektori;
- jarayonning joriy yoki to'xtab qolganligi xususidagi axborotni shakllantirishga kerakli resurslarning o'zgacha xili;
- qandaydir holatdagi jarayon tomonidan, kerakli vazifani bajarishi uchun, so'ralgan har bir resursning birliklar sonini anglatuvchi makonga oid talablar vektori;
- real vaqtni aks ettirish maqsadida, jarayon uchun oxirgi marta qachon soat o'zgarganligini bildiruvchi funksiya;
- ishni bajarish uchun jarayonning har bir resursiga kerakli vaqt ko'lamini bildiruvchi vaqtli talablar vektori.
- jarayonlarning, ishni tugallashi uchun kerakli resurslar to'plamini hamda muayyan vazifa uchun vaqtiy talablarni, ish boshlanmasidan avval aniqlashi mumkinligi ko'zda tutiladi [109].

Axborot tizimini loyihalashda ushbu modelni amalga oshirish, hamda xavfsizlik tizimini ma'murlash, intuitsiyaga asoslangan

tushunarsiz ko‘p sonli qoidalarning joriy etilishi evaziga, nihoyatda sermehnat jarayon hisoblanadi. Undan tashqari, talablarning aniq berilishi va ularni o‘zgartirish mumkin emasligi sababli, model sozlanishda moslashuvchan emas.

Xavfsizlikning rolli modeli (RBAC). Rolli model xavfsizlik siyosatining mutlaqo o‘zgacha xili hisoblanadiki, bu siyosat diskretsion modelga xos foydalanishni boshqarishdagi moslashuvchanlik bilan mandatli modelga xos foydalanishni nazoratlash qoidalarining kat’iyligi orasidagi murosaga asoslanadi [110, 114].

Rolli modelda “sub’ekt” tushunchasi “foydalanuvchi” va “rol” tushunchalari bilan almashtiriladi. Foydalanuvchi-tizim bilan ishlovchi va ma’lum xizmat vazifalarini bajaruvchi odam. Rol-tizimda faol ishtirok etuvchi abstrakt tushuncha bo‘lib, u bilan ma’lum faoliyatni amalga oshirish uchun zarur vakolatlarning cheklangan, mantiqiy bog‘liq to‘plami.

Rollar tashkilot ichida turli ishchi funksiyalar uchun yaratiladi. Muayyan rollarga, u yoki bu amallarni bajarishlari uchun, vakolatlar beriladi. Tizim foydalanuvchilariga o‘zgarmaydigan rollar berilib, ular orqali foydalanuvchilar o‘zgarmaydigan tizimli funksiyalarni bajarish uchun mos imtiyozlarga ega bo‘ladilar.

Rolli modelning asosiy elementlari quyidagicha:

- U foydalanuvchilar to‘plami;
- R rollar to‘plami;
- P kompyuter tizimi ob’ektlaridan foydalanish huquqlari to‘plami;
- S foydalanuvchilarning tizim bilan ishlash seanslari to‘plami;
- $PA: R \rightarrow 2^R$ har bir rol uchun foydalanish huquqlari to‘plamini belgilovchi funksiya;
- $UA: U \rightarrow 2^R$ har bir foydalanuvchi uchun rollar to‘plamini belgilovchi funksiya;
- bitta sub’ekt bir necha rolga ega bo‘lishi mumkin;
- bitta rol bir necha sub’ektga ega bo‘lishi mumkin;
- bitta rol bir necha vakolatga ega bo‘lishi mumkin;
- bitta vakolat bir necha rolga tegishli bo‘lishi mumkin.

Rolli modelning muhim ijobiy xususiyatlari quyidagilar:

- rollar iyerarxiyasini huquqlar nabori vorisligi bilan qurish imkoniyati. Bu rolli modelni, ayniqsa ko‘p sonli axborot tizimlari ishlatiluvchi tashkilotlarda, xilma-xil infrastrukturalarni soddalashti-

rishga imkon beradi. Iyerarxiya ishlatilganida bir necha o'xshash rollarda huquqlarni qaytadan ko'rsatish zaruriyati bo'lmaydi, ularni har bir rol uchun faqat noyob huquqlarini ko'rsatgan holda, shu'ba sifatida bitta katta rolga joylashtirish kifoya;

- ko'p sonli foydalanuvchilarga bir xil huquqlarni berish oddiy va samarali;

- katta sonli foydalanuvchilar huquqlari naborini o'zgartirish zaruriyati tug'ilganida, roldagi huquqlar naborini o'zgartirish yetarli;

- vakolatlarning bo'linishi prinitsipini amalga oshirish imkoniyati. Bu foydalanuvchilarga ortiqcha vakolatlarning berilishi riskini aytarlicha pasaytiradi. Masalan, bir vaqtning o'zida ikkita rolni bitta foydalanuvchiga berish mumkin emas [65, 81, 82, 88, 92].

Mavjud xavfsizlik modellarining, tavsiya etilgan kriteriylar asosida, tahlillash natijalari 1.1-jadvalda keltirilgan.

Jadvalga binoan xulosa qilish mumkinki, aksariyat modellar axborot xavfsizligining faqat bitta xususiyatini himoyalash muammosini hal etadi.

Axborotning bir necha xususiyatlarini himoyalashni nazoratlashda quyidagi yondashishlardan foydalanish tavsiya etiladi:

-bir necha xavfsizlik modellaridan, ularning qoidalari va elementlarini bitta modelda jamlash yo'li bilan, birgalikda foydalanish;

-bitta kompyuter tizimi doirasida bir necha xavfsizlik modellaridan parallel tarzda birgalikda foydalanish;

-axborotning bir necha xususiyatlarini bir vaqtda himoyalashga mo'ljallangan foydalanish modelini ishlab chiqish.

1.1-jadval

Tahlil natijalarining yig'ma jadvali

Kriteriylar / Xavfsizlik modellari	Amalga oshirining oddiyligi	Ma'murlashning oddiyligi	Foydalanish huquqlarining ortiqchaligi	Moslanuvchanlik	Konfidensiallikni himoyalash	Yaxlitlikni himoyalash	Foydalanuvchanlikni himoyalash

Xarrison-Ruzo-Ulman modeli	+	+	+	+	-	+	-
Klark-Vilson modeli	+	+	+	+	-	+	-
Bella-La Padul model	+	-	+	+	+	-	-
Biba modeli	+	+	-	-	-	+	-
Millen modeli	-	-	+	-	-	-	+
RBAC modeli	-	+	+	+	+	+	+

Xulosa sifatida aytish mumkinki, axborotning uchchala (konfidensiallik, yaxlitlik va foydalanuvchanlik) xususiyatlarini bir vaqtda himoyalash muammosini hal etuvchi modellarni ishlab chiqish imkoniyatlarini o'rganish keyingi tadqiqotlarning ustuvor yo'nalishi hisoblanadi.

1.3. Foydalanishni cheklash tizimlariga tahdidlar

Yuqoridagi aytib o'tilganidek, axborotni himoyalashni ta'minlash kompleks xarakterga ega bo'lishi lozim. U xilma-xil salbiy oqibatlarni teran tahlillashga asoslanishi lozim. Zaifliklarning paydo bo'lishiga va natijada axborot xavfsizligining muhim tahdidlarini aniqlashga imkon beruvchi salbiy oqibatlarni tahlillash tahdidlarning xilma-xil manbalarini so'zsiz identifikatsiyasini ko'zda tutadi [68, 74, 81, 89, 93].

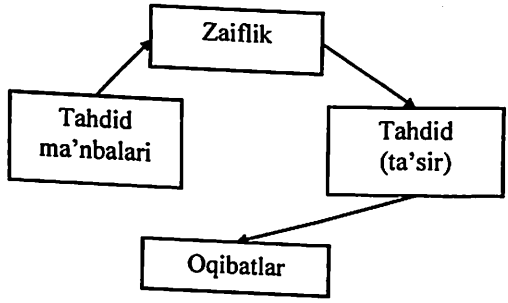
Bo'lishi mumkin bo'lgan tahdidlar manbalari va ularning namoyon bo'lishini tasniflashni 1.8-rasmda keltirilgan mantiqiy zanjirlarning o'zaro bog'lanishi asosida amalga oshirish maqsadga muvofiq xisoblanadi. 1.9-rasmda tahdidlarni amalga oshirilish jarayoni tasvirlangan.

Tahdid manbalari axborot xavfsizligi tahdidlarining eltuvchisi hisoblanadi. Shu bilan birga tahdid manbalari kompyuter tizimining ichida (ichki manbalar) va tashqarisida (tashqi manbalar) bo'lishi mumkin [83, 93].

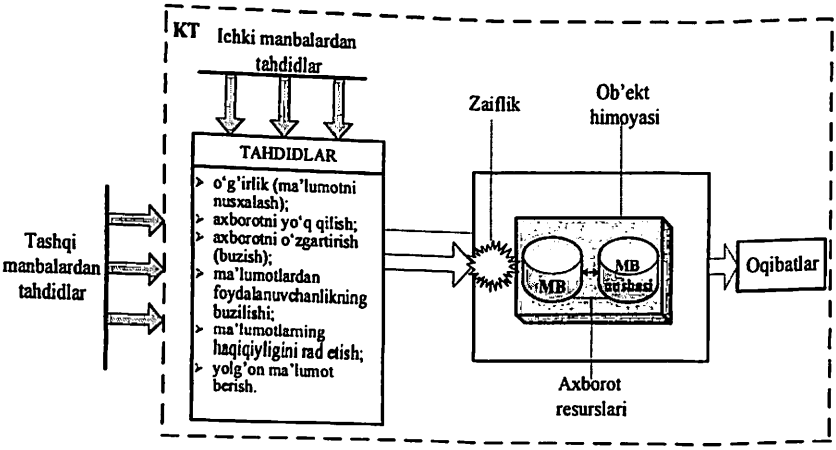
Tashqi tahdidlarni inson faoliyati tug'diradi va tasodifiylariga va qasddan qilinganlariga bo'linadi:

- tasodifiy tahdidlar kompyuter tizimi va uning elementlarini loyihalashdagi, dasturiy ta'minotdagi, xodim harakatlaridagi va h. xatoliklar tufayli sodir bo'ladi.

qasddan qilingan tahdidlar buzg'unchilarning g'arazli, g'oyaviy va boshqa intilishlari bilan bog'liq.



1.8- rasm Tahdid manbalari zanjiri va ularning namoyon bo'lishi



1.9-rasm. Tahdidlarning amalga oshirilishi jarayonlari

Ichki tahdidlar operatsion tizimlarda, tarmoq konfiguratsiyalarida, stol usti tizimlarining pochta mijozlarida, veb-brauzerlarda va xatto, tarmoq xavfsizligining dasturiy ta'minotida doimo sodir bo'ladi. Tahdid resurslariga va, demak tashkilotga zarar yetkazish qobiliyatiga ega.

Ushbu zarar ishlanuvchi axborotga, tizimning o'ziga yoki boshqa resurslarga hujum natijasida ularning avtorizatsiyalanmagan buzilishiga, fosh etilishiga, modifikatsiyalanishiga, ishdan chiqishiga, resurslardan foydalana olmaslikka yoki resurslarning yo'qolishiga olib keladi.

Tahdidlarning sodir bo'lishi tabiiy, tasodifiy yoki maqsadli bo'lgan, inson omiliga bog'liq bo'lishi mumkin. Tahdidlarning aksariyat turlari bo'yicha statistik ma'lumotlar mavjud va tashkilot tomonidan, ularni baholashda, ishlatilishi mumkin [110].

Foydalanishni cheklash tizimi (FChT)-axborotni ruxsatsiz foydalanishdan himoyalashni ta'minlovchi o'zaro bog'langan turli vositalar majmui. *Foydalanishni cheklash-ma'lumotlarni foydalanuvchilarning ruxsatsiz foydalanishlaridan himoyalashni ta'minlovchi usullar, vositalar va tadbirlar majmui* [109]. 1.2- jadvalda ruxsatsiz foydalanishdan himoyalanganligiga ta'sir etuvchi sohalari ko'rsatilgan tahdidlarning turli xillariga misollar keltirilgan.

1.2- jadval

Axborot xavfsizligiga tahdidlar

Konfidensialli k tahdidlari	**Foydalanishni cheklash tahdidlari**	**Yaxlitlik tahdidlari**	**Himoyalangan KT parametlarini fosh etish tahdidlari**
-axborotni ishlash vositalarini, eltuvchilarni va axborotning o'zini o'g'irlash (nusxalash); -axborotni ishlash vositalarini, eltuvchilarni va axborotning o'zini yo'qotish	- axborotni blokirovkalash; - axborotni va uni ishlovchi vositalarni (eltuvchilarni) yo'q qilish; - axborotni uzatish kanallarini va ishlash vositalarini blokirovkalash.	- axborotni modifikatsiyal ash (buzish); - axborot xaqiqiyligini tan olmaslik; - yolg'on axborotni tiqishtirish (aldov); - axborotni yo'q qilish.	- yangi tahdidlarning paydo bo'lishi; - zaifliklarni aniqlash; - risklarning ko'payishi; - hujum muvaffaqiyatlig- ining ko'payishi.

(tasodifiy yo'qotish, sirqib chiqishi); -ruxsatsiz tanishish tarqatish.			

Axborot xavfsizligiga tahdid deganda axborotning asosiy sifatiy xarakteristikalarining (xususiyatlarining) buzilishiga sabab bo'luvchi axborotga salbiy ta'sir ko'rsatishga qodir qasddan yoki tasodifiy tug'dirilgan har qanday hodisa (harakat, vaziyat) tushuniladi.

Axborotdan ruxsatsiz foydalanish holiga quyidagilar taalluqli:

- manfaatdor sub'ektning himoyalanuvchi axborotga, o'rnatilgan huquqiy hujjatlarga rioya qilmay, ega bo'lishi;
- axborotdan yoki uning eltuvchisidan, foydalanish qoidalarini buzib, foydalanish;
- axborot bilan tanishish va uni ishlash, jumladan modifikatsiyalash yoki yo'q qilish.

Foydalanuvchilar uchun o'rnatilgan kompyuter tizimlarining axborot resurslaridan, foydalanish qoidalarini buzib, foydalanish ham axborotdan ruxsatsiz foydalanishga taalluqli. Ruxsatsiz foydalanish-axborot-kompyuter xavfsizligiga qasddan qilinuvchi tahdidning amalga oshirilishi. Shu sababli, ko'pincha uni kompyuter tizimiga hujum deb ham atashadi [83]. Himoyalanuvchi kompyuter tizimlarida axborotdan ruxsatsiz foydalanishning barcha bo'lishi mumkin bo'lgan usullarini quyidagi alomatlari bo'yicha tasniflash mumkin.

Ruxsatsiz foydalanish prinsipi bo'yicha:

- fizik ruxsatsiz foydalanish;
- mantiqiy ruxsatsiz foydalanish.

Ruxsatsiz foydalanish manbaining o'rni bo'yicha:

- lokal tarmoqda joylashgan ruxsatsiz foydalanish manbai;
- lokal tarmoq tashqarisida joylashgan ruxsatsiz foydalanish manbai.

Ruxsatsiz foydalanishni amalga oshirish rejimi bo'yicha:

- insonning bevosita ishtirokida amalga oshiriluvchi hujumlar;
- inson ishtirokisiz, maxsus ishlab chiqilgan dasturlar orqali amalga oshiriluvchi hujumlar.

Axborot-kompyuter tizimi xavfsizligining kamchiligi turi bo'yicha:

- o'rnatilgan xavfsizlik siyosatining kamchiligiga asoslangan hujumlar; kompyuter tizimlarini ma'muriy boshqarishdagi kamchilikka asoslangan hujumlar.

- axborot-kompyuter xavfsizligi vositalarida amalga oshirilgan himoyalash algoritmlarining kamchiligiga asoslangan hujumlar;

- himoya tizimi loyihasini amalga oshirishdagi xatoliklarga asoslangan hujumlar.

Ruxsatsiz foydalanishning marshruti buyicha:

- kompyuter resurslaridan bevosita standart marshrut orqali foydalanishga asoslangan hujumlar;

- kompyuter resurslaridan yashirin marshrut orqali foydalanishga asoslangan hujumlar.

Hujum qilinuvchi ob'ektning joriy o'rnashgan joyi bo'yicha:

- tashqi xotira qurilmalarida saqlanuvchi axborotga hujumlar;

- kompyuter asosiy xotirasida ishlanuvchi axborotga hujumlar.

Bevosita ob'ektga hujumlar bo'yicha:

- himoya tizimining doimiy komponentlariga hujumlar;

- himoya tizimining almashtiriladigan elementlariga hujumlar;

- o'zaro bog'langan protokollarga hujum;

- kompyuter tizimining funksional elementlariga hujum.

Yuqorida keltirilgan tasnif, axborotdan samarali foydalanish faqat himoya tizimining mos zaifliklari mavjudligi asosida amalga oshiriladi deb xulosa qilishga imkon beradi [83].

O'Z Dst ISO/IEC 27033-3:2016 milliy standartda kompyuter tizimlari bilan bog'liq nazoratlash va boshqarish vositalariga daxldor tahdidlar bayon etilgan [5]. Kompyuter tizimlaridagi nazoratlash va boshqarish vositalariga daxldor ruxsatsiz foydalanishdan himoyalanganlikka ta'sir etishi mumkin bo'lgan sohalarning tahlili mos omillarni aniqlashga imkon berdi (1.3-jadval).

Xavfsizlik tahdidlarining asosiy ob'ektlaridan biri kompyuter tizimining ma'lumotlar bazasida saqlanuvchi operativ axborot hisoblanadi. Ammo, qator hollarda operativ axborotga tahdidlarni amalga oshirishda, axborotdan foydalanish bo'yicha kerakli vakolatlarning mavjudligi ko'zda tutiladi [1, 2, 3, 4, 6, 7]. Ushbu vakolatlarni kompyuter tizimi ma'lumotlar bazasining texnologik axborotiga, jumladan himoya tizimi axborotiga ta'sir etish yo'li bilan olish mumkin.

1.3-jadval

Kompyuter tizimlarida nazoratlash va boshqarish vositalari tahdidlarining turli xil buzish omillari

Barqarorlikni buzish omillari	**Ma'lumotlarning o'g'irlanishi va soxtalashtirilishi**	**Konfidensiallikning buzilishi**	**Yaxlitlikning yo'qotilishi**
Ma'lumotlarning server bazasidan foydalanilganda veb ilovalar uchun ruxsatning soni cheklangan	+		
Foydalanuvchilarning ruxsatsiz foydalanishlarini oldini olish yoki boshqa shaxsning foydalanish huquqlarini ishlatish uchun boshqarish ro'yxatlari	+		+
Bajarilishiga ruxsat berilgan foydalanuvchi funksiyasini cheklash uchun rollarga asoslangan foydalanishni boshqarish	+	+	
Ma'lumotlarning ruxsatsiz o'zgartirilishi yoki nusxalanishi	+		+
Ma'lumotlarning o'g'irlanishi	+	+	
Foydalanish vakolati haqiqiy foydalanuvchilarga berilganligiga ishonchni ta'minlash uchun foydalanuvchini xavfsiz ro'yxatdan o'tkazish	+	+	
Raqamli sertifikatlardan, parollardan, biometriyadan yoki smartkartalardan foydalanib autentifikatsiyalash	+		+
Ilovalardan va boshqa tarmoq resurslaridan foydalanish huquqlarining buzilishi kabi xavfsizlik siyosatining buzilishini aniqlash uchun dasturiy vositalarning monitoringi			+

Kompyuter tizimining ma'lumotlar bazasi uchun ichki tahdidlar muhim hisoblanadi. Xilma-xil tahdidlarning ichida, buzg'unchi ta'siri

natijasida sodir bo‘luvchi, ruxsatsiz foydalanish tahdidlari eng xavfli. Ruxsatsiz foydalanishni amalga oshirish bo‘yicha buzg‘unchining amaliy va nazariy imkoniyatlarining tavsifi ichki buzg‘unchi modeli doirasida amalga oshiriladi. Ichki buzg‘unchining kompyuter tizimi axborot resurslaridan, jumladan ma’lumotlar bazasidan foydalanish bo‘yicha vakolatlarining saviyasi uning asosiy tasnifiy alomati hisoblanadi. Ushbu vakolatlarning to‘rtta sathi ajratiladi [68, 83, 84, 91]. Tasnif iyerarxik, ya’ni har bir keyingi sath oldingi sathning funksional imkoniyatlarini qamrab oladi.

Birinchi sath ma’lumotlar bazasidagi harakat imkoniyatlarining eng past sathini-axborotni ishlash bo‘yicha oldindan ko‘zda tutilgan funksiyalarni amalga oshiruvchi qayd etilgan nabordan so‘rovlarni ishga tushirishni belgilaydi.

Ikkinchi sath axborotni ishlash bo‘yicha yangi funksiyali xususiy so‘rovlarni yaratish va ishga tushirish orqali aniqlanadi.

Uchinchi sath ma’lumotlar bazasini boshqarish imkoniyati, ya’ni bazaviy dasturiy ta’minotga va uskunasining tarkibiga va konfiguratsiyasiga ta’siri orqali aniqlanadi.

To‘rtinchi sath hisoblash texnikasi vositalarini loyihalash, amalga oshirish va ta’mirlash, uning tarkibiga axborotni ishlash bo‘yicha yangi funksiyali xususiy texnik vositalarini kiritishga qadar shaxslar imkoniyatlarining barcha qo‘lami orqali aniqlanadi.

Yuqorida keltirilgan sathlarda ichki buzg‘unchiga ma’lum vakolatlar berilgan va ularning doirasida u ruxsatsiz foydalanishga mo‘ljallangan harakatlarni amalga oshirish bo‘yicha mos imkoniyatlarga ega. Quyida bunday harakatlarga misollar keltirilgan [74]:

- himoyalanuvchi ob’ektdan axborotni nusxalash va uni maxfiylik darajasi bo‘yicha markalanganligiga zid usullar bilan ishlash;
- foydalanish xavfi ostida bo‘lgan resurslarning fosh etilishi yoki ushbu resurlardan boshqa foydalanuvchilarning foydalanishi;
- axborotni o‘rnatilgan qoidalarni buzib ishlash natijasida uning tasodifiy obro‘sizlantirilishi;
- muayyan axborot bilan ishlashga ruxsati yo‘q foydalanuvchilarga axborotni ataylab uzatish;
- qandaydir sub’ektning resurslardan qayta-qayta foydalanishini kuzatish va bunday foydalanish faktini tahlillash yo‘li bilan oldin foydalanib bo‘lmagan axborotni olish;

- ichki buzg'unchi foydalanish huquqiga ega bo'lmagan, himoyalanuvchi foydalanish ob'ektida saqlangan axborotni kuzatish (o'rganish);

- himoyalanuvchi axborot yaxlitligining buzilishiga sabab bo'luvchi noto'g'ri xarakatlarning tasodifiy bajarilishi;

- tizimga zararli dasturiy kodning (viruslarning, "troyan" dasturlarning va h.) tasodifiy yoki qasddan kiritilishi.

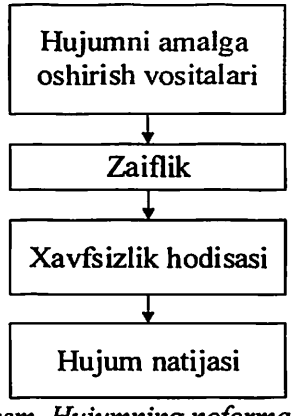
Hujumning har bir xili natijasidagi yo'qotishlar ularning sodir bo'lishi chastotasiga teskari mutanosib. E'tiborsizlik tug'dirgan buzilishlardan minimal dasturiy-apparat harajatlar evaziga himoyalanish talab etiladi. Tizimni zondlashga urinishdan himoyalashda samaraliroq yondashishdan foydalanilsa, suqilib kirishdan himoyalanishda axborotni ko'p sathli himoyalash tizimi ishlatiladi. Himoya tadbirlari tahdidlarning daraja ko'rsatkichiga va amalga oshirilish ehtimoliga adekvat bo'lishi lozim. Faqat tahdidlarning va axborot tizimining himoyalanganlik darajasini kompleks tahlili o'rtamiyona xavfsizlikni ta'minlashi mumkin.

II-BOB. KOMPYUTER TIZIMLARIDA FOYDALANISHNI CHEKLASH TIZIMINI SINTEZLASH

2.1. Kompyuter tizimlarida foydalanishni cheklashda tahdidlar modeli

Monografiyaning birinchi bobida keltirilgan, foydalanishni cheklash tizimiga taalluqli tahdidlar xiliga binoan, buzg'unchi harakati tavsiflanuvchi foydalanishni cheklash tizimiga tahdidlar modelini shakllantirish mumkin. Buzg'unchi sifatida, harakati kompyuter tizimidagi axborotdan ruxsatsiz foydalanishga yo'naltirilgan, axborot tizimidan shtatli vositalar orqali foydalanuvchi sub'ekt ko'rilishi lozim.

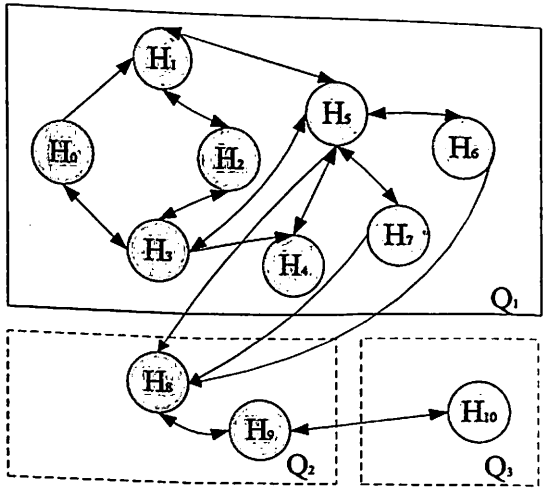
Tahdidlar modelini qurish hujumlarning noformal modelini shakllantirishdan boshlanadi (2.1-rasm).



2.1 – rasm. Hujumning noformal modeli

Hujumni amalga oshirishda niyati buzuq, istalgan natijaga olib keluvchi qandaydir xavfsizlik hodisasini modellaydi [12].

Noformal modeldan tahdidlar modeliga o'tish mumkin. Tahdidlar holatining modelini, har biri tahdidning *i*-holatiga mos keluvchi, bloklar majmui sifatida ko'rish maqsadga muvofiq hisoblanadi [12]. Ushbu model 2.2-rasmda keltirilgan.



2.2-rasm. Tahdidlar holatining modeli

Ushbu xavfsizlik tahdidlari modeli quyidagi holatlarni qamrab oladi:

H_0 – foydalanishni cheklash tizimining dastlabki yoki xavfsiz holati;

H_1 – ruxsatsiz foydalanuvchi xaqiqiyligining tasdiqlanishiga olib keluvchi holat;

H_2 – ma'lumotlarni ruxsatsiz o'zgartirish yoki nusxalash holati;

H_3 – parolni yoki boshqa autentifikatsiyalash vositalarining buzilishi holati;

H_4 – ma'lumotlarning o'g'irlanishi holati;

H_5 – kompyuter tizimida ishlash huquqini ruxsatsiz olish holati;

H_6 – yangi nolegal foydalanuvchini yaratish holati;

H_7 – zararli dasturlarni va kodlarni ruxsatsiz kiritish holati;

H_8 – kompyuter tarmog'i ishlashining ruxsatsiz to'xtatilish holati;

H_9 – foydalanishni madadlashga mos holat;

H_{10} – hujumni yashirishga mos holat;

Q_1 – hujumni tayyorlash holati qismtizimi;

Q_2 – hujumni amalga oshirish holati qismtizimi.

Q_3 – hujumni tugallash holati qismtizimi.

Q_1 da niyati buzuq tomonidan tarmoq batafsil o'rganiladi.

Q_2da tarmoq servislaridan va resurslaridan bevosita foydalaniladi va tarmoq ustidan nazorat o'rnatishga uriniladi.

Q_3 tarmoqdan takroriy foydalanishni va hujumning yashirilishini madadlovchi bosqichlari bilan xarakterlanadi.

Tizimning so'nggi holati aynan H_{10} holati bo'ladi, chunki buzg'unchi tarmoqdan takroran foydalanish uchun o'ziga yo'l qoldirishga doimo urinadi.

Tahdidlar tizimi holati *H(t)* ning vaqt onidagi ehtimolligi, ushbu tizimning H_t holatida bo'lishligining ehtimolliklari majmui sifatida ko'riladi va quyidagicha ifodalanadi:

$$e_i(t) = e(H(t) = h_i). \quad (2.1)$$

Bu yerda $H(t)$ vaqt onidagi tizimning tasodifiy holati.

O'tish ehtimolligi quyidagicha aniqlanadi:

$$e_{ij}(t) = e(H(k) = H_j | H(k-1) = H_j). \quad (2.2)$$

Tahdidlar tizimining *k*-nchi qadamda bo'lishi ehtimolliklari, to'liq ehtimoliklar formulasini qo'llab va $(k-1)$-nchi qadamdan *k*-nchi qadamga o'tish orqali, aniqlanadi va quyidagi rekurrent ko'rinishda ifodalanadi:

$$e_j(k) = \sum_{i=1}^{n} e_i(k-1)e_{ij}. \quad (2.3)$$

Tahdidlar modelining asosiy parametrlari-kompyuter tizimi axborotining himoya tizimiga tahdidlar tizimining ta'siri ehtimolligi va axborot himoya tizimining fosh etilishi ehtimolligi [71].

2.2-rasmda keltirilgan tahdidlar holatining modelidan, 2.3-rasmda himoya tizimi holatining *Di* belgilangan graf ko'rinishidagi modeliga o'tiladi. Buning uchun quyidagi belgilashlar qabul qilinadi:

μ_i - axborot himoyasi tizimini tiklashga yo'naltirilgan intensivlik;

γ_i - himoya tizimining fosh etilishi intensivligi;

e_i - hodisalarning boshlanishi holati ehtimolligi (e_1 - tashqi hujum bo'lmaganligi ehtimolligi; e_2- tashqi hujum bo'lganligi ehtimolligi; e_3- ichki xil (ko'rinishda) hujum bo'lganligi ehtimolligi; e_4- noma'lum hujum bo'lganligi ehtimolligi; e_5 - boshqarish tizimiga hujum bo'lganligi ehtimolligi).

D_i – himoya tizimi holati, bunda:

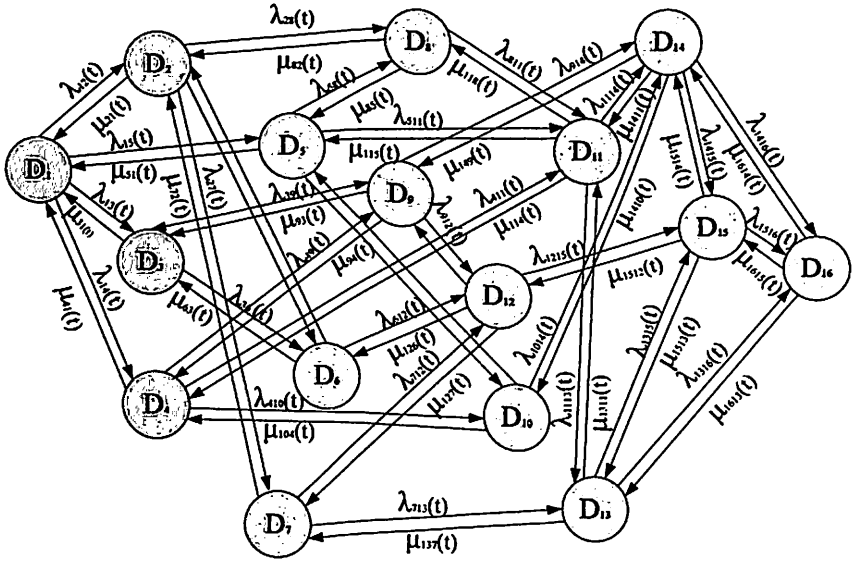
D_1 – himoya tizimining xavfsiz holati (tizim hujumlarga duchor bo'lmagan), ya'ni tizimning dastlabki holati;

D_2 – tashqi hujum bo'lganidagi tizim holati, ya'ni tizim modelining H_1, H_3 holatlari;

D_3 – tashqi hujum bo'lganidagi tizim holati, ya'ni tizim modelining H_1, H_4, H_6 holatlari;

D_4 – boshqarish tizimi orqali hujum bo'lganidagi tizim holati, ya'ni tizim modelining H_5 holati;

D_5 – noma'lum hujum bo'lgan holat, ya'ni tizim modelining H_{10} holati;



2.3-rasm. Himoya tizimi holatining belgilangan grafi

$D_6 - e_1, e_3$ holatlarning bir vaqtda boshlanishi va e_2, e_4, e_5, holatlarning boshlanmasligidagi tizim holati;

$D_7 - e_2, e_4$ holatlarning bir vaqtda boshlanishi va e_1, e_3, e_5 holatlarning boshlanmasligidagi tizim holati;

$D_8 - e_2, e_5$ holatlarning bir vaqtda boshlanishi va e_1, e_3, e_4 holatlarning boshlanmasligidagi tizim holati;

D_9 – e_3, e_4 holatlarning bir vaqtda boshlanishi va e_1, e_2, e_5 holatlarning boshlanmasligidagi tizim holati;

D_{10} – e_3, e_5 holatlarning bir vaqtda boshlanishi va e_1, e_2, e_4 holatlarning boshlanmasligidagi tizim holati;

D_{11} – e_4, e_5 holatlarning bir vaqtda boshlanishi va e, e_2, e_3 holatlarning boshlanmasligidagi tizim holati;

D_{12} – e_2, e_3, e_4 holatlarning bir vaqtda boshlanishi va e_1, e_5 holatlarning boshlanmasligidagi tizim holati;

D_{13} – e_2, e_4, e_5 holatlarning bir vaqtda boshlanishi va e_3 holatlarning boshlanmasligidagi tizim holati;

D_{14} – e_3, e_4, e_5 holatlarning bir vaqtda boshlanishi va e_2 holatining boshlanmasligidagi tizim holati;

D_{15} – e_2, e_3, e_5 holatlarning bir vaqtda boshlanishi va e_4 holatining boshlanmasligidagi tizim holati;

D_{16} – e_2, e_3, e_4, e_5 holatlarning bir vaqtda boshlanishi va e_1 holatining boshlanmasligidagi tizim holati;

2.3-rasmda himoya tizimi holatining belgilangan grafi keltirilgan. Ko'zga tashlanuvchanlikni ta'minlash maqsadida hujumlar oqimi $\lambda_i(t)$ va hujumlarga qarshi ta'sir qiluvchi oqimlar $\mu_i(t)$ strelkalar "⇆" orqali belgilangan [67, 71].

Modelga qator cheklashlar kiritiladi:

- tizimning barcha holatlari $D_1, D_2, \ldots, D_{16}$ mustaqil hodislar hisoblanadi;
- hujumlar oqimi o'zgaruvchi intensivlik $\lambda_i(t)$ bilan Puasson taqsimoti doirasida;
- tahdidlar oqimiga tizim tahdidlarga qarshi ta'sir etuvchi oqimlar bilan javob beradi.

Tizim holati grafi bo'yicha himoya tizimi intensivligi matritsasini tuzish mumkin:

$$\|\lambda_D(t)\| = \begin{vmatrix}
0 & \lambda_{12} & \lambda_{13} & \lambda_{14} & \lambda_{15} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mu_{21} & 0 & 0 & 0 & 0 & \lambda_{26} & \lambda_{27} & \lambda_{28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mu_{31} & 0 & 0 & 0 & 0 & \lambda_{36} & 0 & 0 & \lambda_{39} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mu_{41} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{49} & \lambda_{410} & \lambda_{411} & 0 & 0 & 0 & 0 & 0 \\
\mu_{51} & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{58} & 0 & \lambda_{510} & \lambda_{511} & \lambda_{612} & 0 & 0 & 0 & 0 \\
0 & \mu_{62} & \mu_{63} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{712} & \lambda_{713} & 0 & 0 & 0 \\
0 & \mu_{72} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{811} & 0 & 0 & \lambda_{914} & 0 & 0 \\
0 & \mu_{82} & 0 & 0 & \mu_{85} & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{912} & 0 & \lambda_{1014} & 0 & 0 \\
0 & 0 & \mu_{93} & \mu_{94} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1114} & 0 & 0 \\
0 & 0 & 0 & \mu_{104} & \mu_{105} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1215} & \lambda_{1216} \\
0 & 0 & 0 & \mu_{114} & \mu_{115} & 0 & 0 & \mu_{118} & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1315} & \lambda_{1316} \\
0 & 0 & 0 & 0 & 0 & \mu_{126} & \mu_{127} & 0 & \mu_{129} & 0 & 0 & 0 & 0 & 0 & \lambda_{1415} & \lambda_{1416} \\
0 & 0 & 0 & 0 & 0 & 0 & \mu_{137} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1516} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{149} & \mu_{1410} & \mu_{1411} & 0 & 0 & \lambda_{1415} & \lambda_{1416} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{1512} & \lambda_{1513} & \lambda_{1514} & 0 & \lambda_{1516} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{1612} & \mu_{1613} & \mu_{1614} & \mu_{1615} & 0
\end{vmatrix}$$

Belgilangan grafni yoki intensivlik matritsasini bilgan holda, mnemonik qoidadan foydalanib, axborotni himoyalash tizimi holati ehtimolligi uchun differensial tenglamalar sistemasini yozish mumkin.

$$\frac{de_i(t)}{dt} = \sum_{j=1}^{n} e_j(t)\lambda_{ij}(t) - e_i(t)\sum_{j=1}^{n}\lambda_{ij}(t). \quad (2.4)$$

(2.4) ifoda asosida quyidagi tenglamalar sistemasini olish mumkin:

$$\begin{cases}
e_1 = e_2\mu_{21} + e_3\mu_{31} + e_4\mu_{41} + e_5\mu_{51} - e_1(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15}) \\
e_2 = e_1\lambda_{12} + e_6\mu_{62} + e_7\mu_{72} + e\mu_{82} - e_2(\mu_{21} + \lambda_{26} + \lambda_{27} + \lambda_{28}) \\
e_3 = e_1\lambda_{13} + e_6\mu_{63} + e_9\mu_{93} - e_3(\mu_{31} + \lambda_{36} + \lambda_{39}) \\
e_4 = e_1\lambda_{14} + e_9\mu_{94} + e_{10}\mu_{104} + e_{11}\mu_{114} - e_4(\mu_{41} + \lambda_{49} + \lambda_{410} + \lambda_{411}) \\
e_5 = e_1\lambda_{15} + e_8\mu_{85} + e_{10}\mu_{105} + e_{11}\mu_{115} - e_5(\mu_{51} + \lambda_{58} + \lambda_{510} + \lambda_{511}) \\
e_6 = e\lambda_{26} + e_3\lambda_{36} + e_{12}\mu_{126} - e_6(\mu_{62} + \mu_{63} + \lambda_{612}) \\
e_7 = e_2\lambda_{27} + e_{12}\mu_{127} + e_{13}\mu_{137} - e_7(\mu_{72} + \lambda_{712} + \lambda_{713}) \\
e_8 = e_2\lambda_{28} + e_5\lambda_{58} + e_{11}\mu_{118} - e_8(\mu_{82} + \mu_{85} + \lambda_{812}) \\
e_9 = e_3\lambda_{39} + e\lambda_{49} + e_{12}\mu_{129} + e_{14}\mu_{149} - e_9(\mu_{93} + \mu_{94} + \lambda_{912} + \lambda_{914}) \\
e_{10} = e_4\lambda_{410} + e_5\lambda_{510} + e_{14}\lambda_{1410} - e_{10}(\mu_{104} + \mu_{105} + \lambda_{1014}) \\
e_{11} = e_4\lambda_{411} + e_5\lambda_{511} + e_8\lambda_{811} + e_{14}\mu_{1411} - e_{11}(\mu_{114} + \mu_{115} + \lambda_{1114}) \\
e_{12} = e_6\lambda_{612} + e_7\lambda_{712} + e_9\lambda_{912} + e_{15}\mu_{1512} + e_{16}\mu_{1612} - e_{12}(\mu_{1216} + \mu_{1217} + \mu_{129} + \lambda_{1215} + \lambda_{1216}) \\
e_{13} = e_7\lambda_{713} + e_{15}\mu_{1513} + e_{16}\mu_{1613} - e_{13}(\mu_{137} + \lambda_{1315} + \lambda_{1316}) \\
e_{14} = e_9\lambda_{914} + e_{10}\lambda_{1014} + e_{11}\lambda_{1114} + e_{15}\mu_{1514} + e_{16}\mu_{1614} - e(\mu_{1419} + \mu_{1410} + \mu_{1411} + \lambda_{1415} + \lambda_{1416}) \\
e_{15} = e_{12}\lambda_{1215} + e_{13}\lambda_{1315} + e_{14}\lambda_{1415} + e_{16}\mu_{1615} - e_{15}(\mu_{1512} + \mu_{1513} + \mu_{1514} + \lambda_{1516}) \\
e_{16} = e_{12}\lambda_{1216} + e_{13}\lambda_{1316} + e_{14}\lambda_{1416} + e_{15}\mu_{1516} - e_{16}(\mu_{1612} + \mu_{1613} + \mu_{1614} + \lambda_{1615})
\end{cases}$$

Ushbu tenglamalar sistemasida $e_i = e_i(t), \lambda_y = \lambda_y(t), \mu_y = \mu_y(t)$.

Ushbu tenglamalar sistemasi, vaqtning dastlabki oni $t = 0$ da holatlar ehtimoligini beruvchi boshlang'ich shartlarda, yechiladi. Bunda vaqtning ixtiyoriy onida quyidagi normallangan shartning bajarilishi hisobga olinishi lozim:

$$e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 + e_8 + e_9 + e_{10} + e_{11} + e_{12} + e_{13} + e_{14} + e_{15} + e_{16} = 1.$$

Faraz qilaylik, vaqtning dastlabki onida tizimga hujum qilinmagan hamda $\mu_{ij} = const$ va $\lambda_{ij} = const$.

Unda o'zgarmas koeffitsiyentli bir jinsli differensial tenglamalar sistemasi o'rniga o'zgarmas koeffitsiyentli bir jinsli algebraik tenglamalar sistemasini olish mumkin. Bu algebraik tenglamalar sistemasini, quyidagi normallangan shartni hisobga olgan holda, yechish mumkin:

$$\sum_{i=1}^{16} e_i(t) = 1, (0 \le e_i(t) \le 1; t \ge 0)$$

$$x\pi_i(x) = \sum_{j=1}^{m}\lambda_{ij}\pi_i(x) + e_i(0), \ (i=1,2,\ldots,n). \quad (2.5)$$

(2.5) tenglamadan quyidagi natijani olish mumkin:

$$\pi_i(x) = \frac{\sum_{j=1}^{n} \lambda_{ij}\pi_j(x) + e_i(0)}{x + \lambda_i} = \frac{\sum_{j=1}^{n} \lambda_{ij}\pi_j(x) + e_i(0)}{x + \sum_{j=1}^{n} \lambda_{ij}}. \quad (2.6)$$

Demak, olingan tenglamalar sistemasining bitta tenglamasini va ehtimolik tasvirini $e_i(t)$ oddiyroq ifoda bilan almashtirish mumkin.

$$\sum_{j=1}^{n} \pi_i(x) = \frac{1}{x}. \quad (2.7)$$

(2.7) ifoda normal shartning tasviridir:

$x\pi_1(x) = \mu_{21}\pi_2(x) + \mu_{31}\pi_3(x) + \mu_{41}\pi_4(x) + \mu_{51}\pi_5(x) - \pi_1(x)(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15}) + 1,$

$x\pi_2(x) = \lambda_{12}\pi_1(x) + \mu_{62}\pi_6(x) + \mu_{72}\pi_7(x) + \mu_{82}\pi_8(x) - \pi_2(x)(\mu_{21} + \lambda_{26} + \lambda_{27} + \lambda_{28}),$

$x\pi_3(x) = \lambda_{13}\pi_1(x) + \mu_{63}\pi_6(x) + \mu_{93}\pi_9(x) - \pi_3(x)(\mu_{31} + \lambda_{36} + \lambda_{39}),$

$x\pi_4(x) = \lambda_{14}\pi_1(x) + \mu_{94}\pi_9(x) + \mu_{164}\pi_{10}(x) + \mu_{114}\pi_{11}(x) - \pi_4(x)(\mu_{41} + \lambda_{49} + \lambda_{410} + \lambda_{411}),$

$x\pi_5(x) = \lambda_{15}\pi_1(x) + \mu_{85}\pi_8(x) + \mu_{105}\pi_{10}(x) + \mu_{115}\pi_{11}(x) - \pi_5(x)(\mu_{51} + \lambda_{58} + \lambda_{510} + \lambda_{511}),$

$x\pi_6(x) = \lambda_{26}\pi_2(x) + \lambda_{36}\pi_3(x) + \mu_{126}\pi_{12}(x) - \pi_6(x)(\mu_{62} + \mu_{63} + \lambda_{612}),$

$x\pi_7(x) = \lambda_{27}\pi_2(x) + \mu_{127}\pi_{12}(x) + \mu_{137}\pi_{13}(x) - \pi_7(x)(\mu_{72} + \mu_{74} + \lambda_{712} + \lambda_{713}),$

$x\pi_8(x) = \lambda_{28}\pi_2(x) + \lambda_{58}\pi_5(x) + \mu_{118}\pi_{11}(x) - \pi_8(x)(\mu_{82} + \mu_{85} + \lambda_{812}),$

$x\pi_9(x) = \lambda_{39}\pi_3(x) + \lambda_{49}\pi_4(x) + \mu_{129}\pi_{12}(x) + \mu_{149}\pi_{14}(x) - \pi_9(x)(\mu_{93} + \mu_{94} + \lambda_{912} + \lambda_{914}),$

$x\pi_{10}(x) = \lambda_{410}\pi_4(x) + \lambda_{510}\pi_5(x) + \lambda_{1410}\pi_{14}(x) - \pi_{10}(x)(\mu_{104} + \mu_{105} + \lambda_{1014}),$

$x\pi_{11}(x) = \lambda_{411}\pi_4(x) + \lambda_{511}\pi_5(x) + \lambda_{811}\pi_8(x) + \mu_{1411}\pi_{14}(x) - \pi_{11}(x)(\mu_{114} + \mu_{115} + \lambda_{1114}),$

$x\pi_{12}(x) = \lambda_{612}\pi_6(x) + \lambda_{712}\pi_7(x) + \lambda_{912}\pi_9(x) + \mu_{1512}\pi_{15}(x) + \mu_{1612}\pi_{16}(x) - \pi_{12}(x)(\mu_{1216} + \mu_{1217} + \mu_{129} + \lambda_{1215} + \lambda_{1216}),$

$x\pi_{13}(x) = \lambda_{713}\pi_7(x) + \mu_{1513}\pi_{15}(x) + \mu_{1613}\pi_{16}(x) + \mu_{1613}\pi_{16}(x) - \pi_{13}(x)(\mu_{137} + \lambda_{1315} + \lambda_{1316}),$

$x\pi_{14}(x) = \lambda_{914}\pi_9(x) + \lambda_{1014}\pi_{10}(x) + \lambda_{1114}\pi_{11}(x) + \mu_{1514}\pi_{15}(x) + \mu_{1614}\pi_{16}(x) - \pi_{14}(x)(\mu_{1419} + \mu_{1410} + \mu_{1411} + \lambda_{1415} + \lambda_{1416}),$

$$x\pi_{15}(x) = \lambda_{1215}\pi_{12}(x) + \lambda_{1315}\pi_{13}(x) + \lambda_{1415}\pi_{14}(x) + \mu_{1615}\pi_{16}(x) - \pi_{15}(x)(\mu_{1512} + \mu_{1513} + \lambda_{1514} + \lambda_{1516}),$$

$$x\pi_{16}(x) = \lambda_{1216}\pi_{12}(x) + \lambda_{1316}\pi_{13}(x) + \lambda_{1416}\pi_{14}(x) + \mu_{1516}\pi_{16}(x) - \pi_{16}(x)(\mu_{1612} + \mu_{1613} + \lambda_{1614} + \lambda_{1615}),$$

$$\pi_1(x) + \pi_2(x) + \pi_3(x) + \pi_4(x) + \pi_5(x) - \pi_6(x) + \pi_7(x) + \pi_8(x) + \pi_{10}(x) + \pi_{11}(x) + \pi_{12}(x) + \pi_{13}(x) + \pi_{14}(x) + \pi_{15}(x) + \pi_{16}(x) = \frac{1}{x}.$$

Olingan tenglamalar sistemasini soddalashtirish mumkin. Tizimda ma'lum ehtimollik bilan kechuvchi jarayon boshqa ixtiyoriy holatning yaqinidan o'tadi deb hisoblaymiz. Aytaylik, tizimni bir holatdan ikkinchisiga o'tkazuvchi hodisalarning barcha oqimi o'zgarmas intensivli sodda bo'lsin [71]. Demak, statsionar ishlash rejimida Kolmogorovning differensial tenglamasi o'zgarmas koeffitsiyentli bir jinsli algebraik tenglamalar sistemasiga o'zgartiriladi:

$$e_i = \sum_{j=1}^{n} \lambda_{ij} e_j - e_i \sum_{j=1}^{n} \lambda_{ij}, (i = 1,2 \dots, n). \quad (2.8)$$

(2.8) ifodani quyidagi ko'rinishiga keltirish mumkin:

$$e_i \sum_{j=1}^{n} \lambda_{ij} = \sum_{j=1}^{n} \lambda_{ij}\, e_j, (i = 1,2 \dots, n). \quad (2.9)$$

Yoki yanada sodda ko'rinishi: $e_i = \frac{\sum_{j=1}^{n} \lambda_{ij} e_j}{\lambda_i}, (i = 1,2,3, \dots, n).$

$$Bu\ yerda\ \lambda_i = \sum_{j=1}^{n} \lambda_{ij}.$$

Algebraik tenglamalar sistemasini yechish uchun ushbu tenglamalardan birini normalovchi shart $\sum_{j=1}^{n} e_i = 1$ bilan almashtirish kerak.

Normalovchi shartni inobatga olib quyidagi algebraik tenglamalar sistemasini yozish mumkin:

$$e_1 = \frac{(\mu_{21}e_2 + \mu_{31}e_3 + \mu_{41}e_4 + \mu_{51}e_5)}{(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15})},$$

$$e_2 = \frac{(\lambda_{12}e_1 + \mu_{62}e_6 + \mu_{72}e_7 + \mu_{82}e_8)}{(\mu_{21} + \lambda_{26} + \lambda_{27} + \lambda_{28})},$$

$$e_3 = \frac{(\lambda_{13}e_1 + \mu_{63}e_6 + \mu_{93}e_9)}{(\mu_{31} + \lambda_{36} + \lambda_{39})},$$

$$e_4 = \frac{(\lambda_{14}e_1 + \mu_{94}e_9 + \mu_{104}e_{10} + \mu_{114}e_{11})}{(\mu_{41} + \lambda_{49} + \lambda_{410} + \lambda_{411})},$$

$$e_5 = \frac{(\lambda_{15}e_1 + \mu_{85}e_8 + \mu_{105}e_{10} + \mu_{115}e_{11})}{(\mu_{51} + \lambda_{58} + \lambda_{510} + \lambda_{511})},$$

$$e_6 = \frac{(\lambda_{26}e_2+\lambda_{36}e_3+\mu_{126}e_{12})}{(\mu_{62}+\mu_{63}+\lambda_{612})},$$

$$e_7 = \frac{(\lambda_{27}e_2+\mu_{127}e_{12}+\mu_{137}e_{13})}{(\mu_{72}+\lambda_{712}+\lambda_{713})},$$

$$e_8 = \frac{(\lambda_{28}e_2+\lambda_{58}e_5+\mu_{118}e_{11})}{(\mu_{82}+\mu_{85}+\lambda_{812})},$$

$$e_9 = \frac{(\lambda_{39}e_3+\lambda_{49}e_4+\mu_{129}e_{12}+\mu_{149}e_{14})}{(\mu_{93}+\mu_{94}+\lambda_{912}+\lambda_{914})},$$

$$e_{10} = \frac{(\lambda_{410}e_4+\lambda_{510}e_5+\lambda_{1410}e_{14})}{(\mu_{104}+\mu_{105}+\lambda_{1014})},$$

$$e_{11} = \frac{(\lambda_{411}e_4+\lambda_{511}e_5+\lambda_{811}e_8+\mu_{1411}e_{14})}{(\mu_{114}+\mu_{115}+\lambda_{1114})},$$

$$e_{12} = \frac{(\lambda_{612}e_6+\lambda_{712}e_7+\lambda_{912}e_9+\mu_{1512}e_{15}+\mu_{1612}e_{16})}{(\mu_{1216}+\mu_{1217}+\mu_{129}+\lambda_{1215}+\lambda_{1216})},$$

$$e_{13} = \frac{(\lambda_{713}e_7+\mu_{1513}e_{15}+\mu_{1613}e_{16})}{(\mu_{137}+\lambda_{1315}+\lambda_{1316})},$$

$$e_{14} = \frac{(\lambda_{914}e_9+\lambda_{1014}e_{10}+\lambda_{1114}e_{11}+\mu_{1514}e_{15}+\mu_{1614}e_{16})}{(\mu_{1419}+\mu_{1410}+\mu_{1411}+\lambda_{1415}+\lambda_{1416})},$$

$$e_{15} = \frac{(\lambda_{1215}e_{12}+\lambda_{1315}e_{13}+\lambda_{1415}e_{14}+\mu_{1615}e_{16})}{(\mu_{1512}+\mu_{1513}+\mu_{1514}+\lambda_{1516})},$$

$$e_{16} = \frac{(\lambda_{1216}e_{12}+\lambda_{1316}e_{13}+\lambda_{1416}e_{14}+\mu_{1516}e_{15})}{(\mu_{612}+\mu_{1613}+\mu_{1614}+\lambda_{1615})},$$

$e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 + e_8 + e_9 + e_{10} + e_{11} + e_{12} + e_{13} + e_{14} + e_{15} + e_{16} = 1.$

O'tish rejimining vaqti boshlang'ich shartlar vektoriga bog'liq bo'lgani sababli, ya'ni $t=0$ onida $e_i(0)(i = 1,2 \ldots, n)$ ehtimolliklari oxirgi ehtimolliklarga teng bo'lsa, o'tish rejimining vaqti nolga teng bo'ladi.

Quyida himoya tizimiga hujumlarning turli intensivligida va hujumlarga qayta ta'sir qilishga yo'naltirilgan himoya tizimi intensivligida himoya tizimining o'tishlari ehtimolliklari hisoblangan.

Hujum oqimlari λ va hujumga qarshi himoya koeffitsiyent μ larning yig'indisi 1 ga teng deb olinadi. Bu holda, λ va μ bir-biriga teskari mutanosib.

$\lambda = 0{,}5. e_1 - e_{16} = 0{,}0625;$

$\lambda = 0.25. \mu = 0.75. e_1 = 0{,}3116;\ e_2, e_3, e_4, e_5 = 0{,}105;$

$e_6, e_7, e_8, e_9, e_{10}, e_{11} = 0{,}035;\ e_{12}, e_{13}, e_{14}, e_{15} = 0{,}011;\ e_{16} = 0{,}004;$

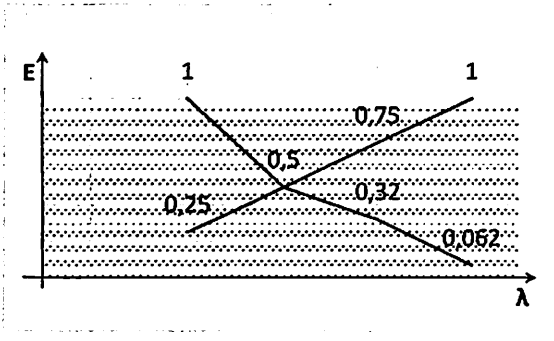
$\lambda = 0.75.\ \mu = 0.25. E_1 = 0{,}004;\ e_2, e_3, e_4, e_5 = 0{,}012;$

$e_6, e_7, e_8, e_9, e_{10}, e_{11} = 0{,}035;\ e_{12}, e_{13}, e_{14}, e_{15} = 0{,}105;\ e_{16} = 0{,}316;$

$\lambda = 1.\mu = 0;\ e_1 - e_{15} = 0;\ e_{16} = 1;$

$\lambda = 1.\mu = 1;\ e_1 = 1; e_2 - e_{16} = 0.$

Hisoblash natijalari asosida himoya tizimining bir holatdan ikkinchisiga o'tish ehtimolliklarining λ va μ lar ta'siriga bog'liqlik grafigi quriladi (2.4 - rasm).



2.4-rasm. Himoya tizimining bir holatdan ikkinchisiga o'tishi ehtimolliklarining λ va μlar ta'siriga bog'liqligi

Ishlab chiqilgan model asosida quyidagi xulosalarga kelish mumkin:

- himoya tizimiga hujumlarning maksimal oqimi ta'sirida va ushbu hujumlarga ushbu tizim tarafidan har qanday qarshi ta'sirning yo'qligida tizimning fosh etilishi ehtimolligi 1ga teng;
- hujumlarning va hujumlarga qarshi ta'sir oqimlarining tengligida himoya tizimining to'liq fosh etilishi ehtimolligi 0.0625 ga teng;
- $\lambda = 0.75$ va $\mu = 0.25$ holida himoya tizimining to'liq fosh etilishi ehtimolligi 0.3 ga teng.

Demak, himoya tizimiga ta'sir etuvchi hujumlar oqimi λga samarali qarshi ta'sir etish uchun $\mu = 0.3 - 0.5$ ga teng intensivlik bilan ishlovchi qarshi ta'sir tizimi zarur. Intensivlikning oshishi himoya tizimining qimmatlashiga olib keladi.

Ta'kidlash lozimki, hujumlar oqimiga tegishlicha intensivlik bilan qarshi turish uchun, nafaqat hujum o'tkazish bosqichida, balki razvedka bosqichida ishlovchi himoya elementlarini boshqarishning samarali tizimi zarur.

2.2. Kompyuter tizimlarida foydalanishni cheklash tizimi

Foydalanishni boshqarish tizimini amalga oshirish uchun axborot tizimining modeli yaratiladi. U axborot tizimining barcha holatlarini, bir holatdan boshqa holatga o'tishlarini modellashi, hamda qaysi holatni xavfsiz deb hisoblashni ko'rsatishi mumkin. Axborot tizimini, tanlangan xavfsizlik siyosatiga asosan, himoyalash tizimini sintezlash masalasini formallashtirishning turli yondashuvlari mavjud. Himoya usullarini ishlab chiqishdagi harajatlarni, ekspluatatsiyasini va xavfsiz vaqtni ularning asosiy xarakteristikalariga oid deb hisoblash mumkin. Xavfsiz vaqt deganda suqilib kirishlarning joiz variantlari to'plamini sinash yo'li bilan himoya usulining fosh etilishining matematik kutilmasi tushuniladi [73, 75].

Xavfsiz vaqt himoya usullarining samaradorligini baholashga xizmat qilishi mumkin. Masalan, dasturiy amalga oshiriluvchi har qanday himoya muolajasi kompyuterning asosiy xotirasi, protsessor vaqti va (yoki) axborotning tashqi eltuvchilari bilan almashishi kabi resurslarning harajatlari bilan bog'liq. Ravshanki, foydalanishni nazoratlash muolajalari qanchalik murakkab bo'lsa, hamda kompyuter ishlashida ularning amalga oshirilishi chastotasi qanchalik yuqori bo'lsa, himoya tizimining ekspluatatsiyasiga hisoblash tizim resurslarning harajatlari shunchalik katta bo'ladi.

Foydalanishni nazoratlashning bittagina muolajasini turli usullar bilan amalga oshirish turli harajatlarga olib kelishi mumkin. Ta'kidlash lozimki, himoya usullarining yuqorida keltirilgan xarakteristikalari o'zaro to'g'ri mutanosiblik bilan bog'langan. Masalan, foydalanishni boshqarish uchun ishlatiladigan parol qanchalik uzun bo'lsa, himoyaning ushbu usulini amalga oshirishdagi harajatlar shunchalik yuqori bo'ladi. Chunki, parol variantlarining bo'lishi mumkin bo'lgan saralash soni oshishi bilan xavfsiz vaqt qiymati oshadi.

Ravshanki, niyati buzuq tomonidan himoya usulini yengish ehtimoli uning imkoniyatlarining sarflanishi orqali aniqlanadi. Kompyuter tizimini himoyalash usulini buzish uchun niyati buzuq tomonidan sarflangan resurslar, ko'rilayotgan usulni yaratish harajatlaridan oshgani sari, ruxsatsiz foydalanish ehtimoli oshadi. Kompyuter tizimini himoya tizimini sintezlashda loyihalash masalasining yechilishiga ta'sir etuvchi omillar sifatida, tizimni ishlab chiqishga va ekspluatatsiyasiga, hamda ishlab chiqaruvchilar tarkibi va malakasiga ajratilgan mablag'larga bog'liq, cheklashlar ishtirok etadi.

Demak, sintezlanuvchi tizim kompyuter tizimining axborot resurslarini ruxsatsiz foydalanishdan himoyalash funksiyalarining, yuqorida keltirilgan loyihalash va ekspluatatsiya vositalariga ma'lum cheklashlar sharoitida, bajarilishini ta'minlashi lozim [73, 75].

Kompyuter tizimining kanonik, mantiqiy va fizik strukturalarini himoyalash mexanizmlarini shakllantirish usullarini ko'raylik. Umumiy holda, himoya mexanizmlari axborotdan faqat mos vakolatlarga ega foydalanuvchilarning foydalana olishlarini ta'minlashga mo'ljallangan. Himoya mexanizmi bitta yoki bir nechta himoya vositalaridan (tashkiliy, muolajaviy, strukturaviy, apparat yoki dasturiy) foydalanish yo'li bilan amalga oshiriladi.

Kompyuter tizimini himoyalash mexanizmi, kompyuter tizimi axborotidan va tatbiqiy dasturlardan atayin yoki tasodifan ruxsatsiz foydalanishning istisno etilishini ta'minlash bo'yicha, unga qo'yilgan talablar ro'yxati orqali, aniqlanadi. Himoyalash mexanizmi qonuniy va noqonuniy foydalanuvchilarni farqlashga va ular harakatlarining qonuniyligini identifikatsiyalashga hamda foydalanuvchilarning noqonuniy harakatlarini bartaraf etishga imkon beradi.

Faraz qilaylik $Z = (z_m : m = 1, \mathcal{M}\}$-axborot tizimi foydalanuvchilari to'plami, $\mathcal{Y} = \{y_i : i = 1, \mathcal{J}_y\}$-loyihalanuvchi axborot tizimi; $\mathcal{X} = \{x_j : j = 1, \mathcal{J}_x\}$- tatbiqiy dasturiy ta'minot, bu yerda y_i yoki p_j– mos holda loyihalanuvchi axborot tizimi va dasturiy ta'minotining komponentlari. U holda, kompyuter tizimini himoyalash mexanizimini quyidagi akslantirish $\mathcal{L}$ orqali ifodalash mumkin:

$$\{(z_m, y_i, x_j)\} \to \mathcal{L} \to (0,1). \qquad (2.10)$$

bu yerda "1" foydalanuvchi $z_m \in Z$ ning $y_i \in \mathcal{Y}$ yoki $x_j \in \mathcal{X}$ elementlaridan foydalanishning qonuniyligiga mos kelsa, "0" bunday foydalanishning taqiqiga mos keladi. Demak, axborot tizimini himoyalash mexanizmi foydalanuvchining u yoki bu axborot va dastur elementlardan foydalanishni amalga oshirish ruxsatiga egaligini aniqlashga imkon beradi.

Himoya tizimi $S = \{S_i := 1, I\}$ himoya usullarining majmuidan iborat, bu yerda S_i i-chi usul, I – esa usullarning umumiy soni.

Kompyuter tizimini himoyalashning optimal tizimi deganda, uning ishlashidagi, strukturaviy va foydalanuvchilar tomonidan funksional cheklashlarga quyilgan talablarga rioya qilingan shartida, qandaydir samaradorlik kriteriysining ekstremal qiymatini ta'minlovchi usullar majmui tushuniladi [75].

Optimallash kriteriysi sifatida ishlatilishi mumkin bo'lgan kompyuter tizimini himoyalash tizimi xarakteristikalariga quyidagilar taalluqli:

- buzg'unchilar tomonidan himoyani "buzish" ehtimoli: xavfsiz vaqt;
- himoya tizimini ishlab chiqish muddati, narxi va ekspluatatsiya harajatlari;
- foydalanuvchilarning ma'lumotlar bazasining himoyalangan turli resurslariga ruxsatsiz murojaatlarining minimal soni va h.

Hozirda kompyuter tizimida foydalanishni cheklash tizimini shakllantirish, odatda, xavfsizlik ma'muri tomonidan evristik usuli bilan amalga oshiriladi. Ammo samarali foydalanishni cheklash tizimini qurish ushbu jarayonni so'zsiz formallashtirish zaruriyatini taqozo etadi. Bunda birinchi qadam masala qo'yilishini formallashtirish hisoblanadi [75].

Umumiy holda, foydalanishni cheklash tizimi, bir birini to'ldiruvchi va sub'ektlarning ob'ektlardan foydalanishini cheklash jarayoniga turlicha ta'sir etuvchi, har xil himoyalash vositalaridan tarkib topgan. Foydalanishni cheklash tizimidagi himoyaning turli vositalarida ishlatiluvchi texnologiyaning tub ma'nosidan abstraksiyalanib, foydalanishni cheklash masalasining qo'yilishini formallashtirish bajarilsa, bunday qo'yilish turli muayyan hollarda kompyuter tizimida yaratiluvchi muayyan foydalanishni cheklash tizimiga nisbatan invariant bo'ladi. Bunday qo'yilish *foydalanishni cheklash masalasining kanonik quyilishi (bayonnomasi)* deb ataladi. Ushbu quyilishi (bayonnomasi) asosida har qanday boshqa xususiy foydalanishni cheklash tizimini qurish masalasini qo'yish mumkin. Foydalanishni cheklash masalasining kanonik qo'yilishi quyidagi ko'rinishga ega. Berilgan:

- $A = \{a_i\}, i = 1, ..., I$- foydalanish ob'ektlar (himoyalanuvchi resurslar) to'plami;
- $B = \{b_j\}, j = 1, ..., J$ - foydalanish sub'ektlar (foydalanuvchilar, dasturlar)to'plami;
- $P=\{p_k\}$ – vakolat turlarining to'plami;
- foydalanishni cheklash tizimlarida tashkil etilgan foydalanishni cheklash vositalarining to'plami-cheklash vositalari sifatida tarmoqlararo ekran (TE), operatsion tizimlar (OT), ma'lumotlar bazasini boshqarish tizimlari (MBBT) ko'riladi: $\Phi_{FChT} = \{\Phi_{TE}, \Phi_{OT}, \Phi_{MBBT}\}$.

- $S_{talab} \subseteq B \times A \times P$-sub'ektlarning ob'ektlardan foydalanishni cheklashda talab etiluvchi sxema.

2.6-rasmda foydalanishni cheklash masalasining kanonik quyilishi(bayoni)dagi dastlabki ma'lumotlarning grafik ifodalanishi keltirilgan.

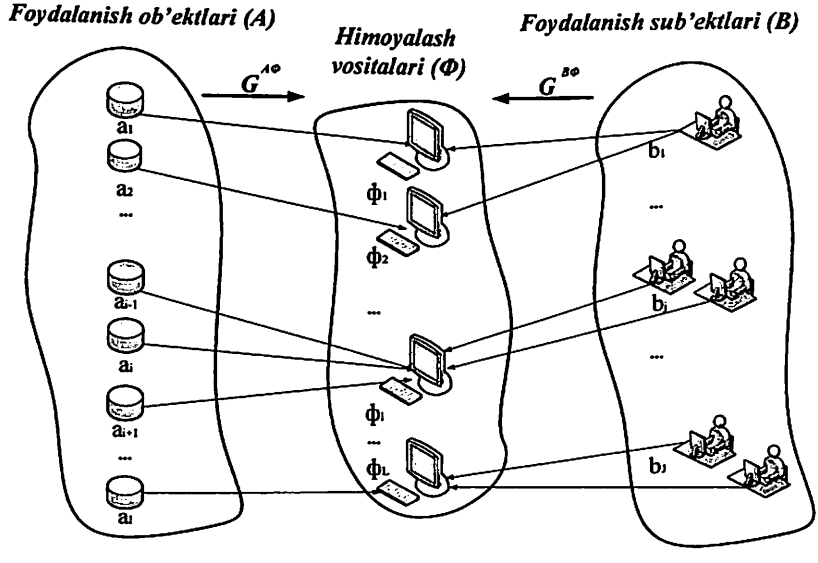
2.6-rasmdan ko'rinib turibdiki, dastlabki ma'lumotlar orasida quyidagi akslantirishlar mavjud:

- $G^{A\Phi}: A \to \Phi$, foydalanish ob'ektlari to'plamini himoya vositalari to'plamiga akslantirish;
- $G^{B\Phi}: B \to \Phi$, foydalanish sub'ektlari to'plamini himoya vositalari to'plamiga akslantirish.

$G^{A\Phi}$ va $G^{B\Phi}$ akslantirishlarning ko'rinishi Φ_{FChT} ning strukturasiga va tashkil etilishining parametrlariga bog'liq va, o'z navbatida, cheklashning real sxemasi $S_{real} \subseteq B \times A \times P$ ni belgilaydi.

Cheklashning real sxemasini, umumiy holda, quyidagi funktsional ko'rinishda ifodalash mumkin:

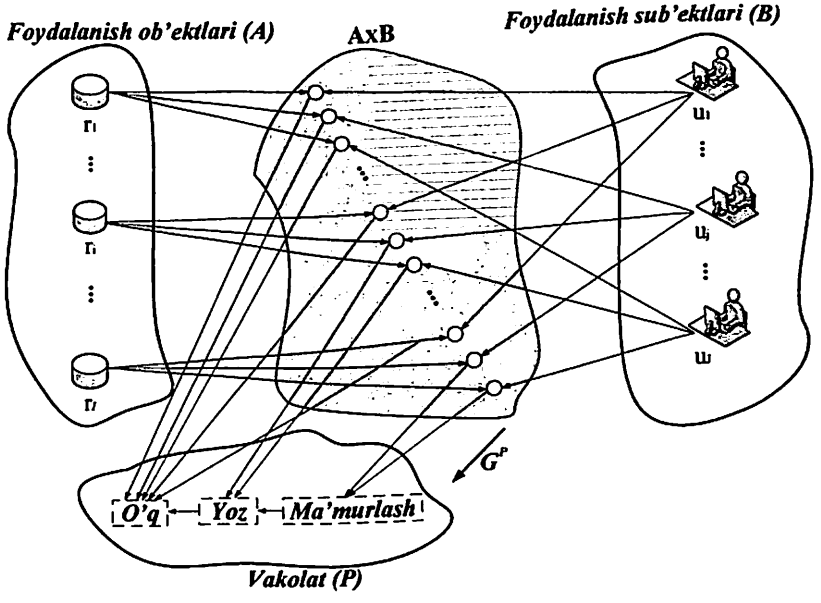
$$S_{real} = F(B, A, P, \Phi_{FChT}) \quad . \qquad (2.11)$$



2.6-rasm. Foydalanishni cheklash masalasining kanonik qo'yilishi(bayoni)dagi dastlabki ma'lumotlarning grafik ifodalanishi

2.7-rasmda keltirilgan misolda quyidagi munosabatlar mavjud: *O'q < Yoz < Ma'murlash*. Masalan, *O'q* - faqat "o'qish uchun foydalanish" vakolati, *Yoz* - "o'qish uchun yozish" vakolati va *Ma'murlash*-"ma'muriyatning foydalanishi" vakolati. Agar ba'zi bir b_j sub'ekti *Ma'murlash* vakolatiga ega bo'lgan a_i ob'ektidan foydalanish munosabatiga ega bo'lsa, demak, *O'q* vakolati bo'yicha foydalanish, va agar *Ma'murlash* vakolati bilan foydalanish mavjud bo'lsa, demak, bu *Yoz* va *O'q* vakolatiga ham ruxsat berilganligini anglatadi [75].

2.7-rasmda tasvirlangan foydalanishni cheklash sxemasi, jadval shaklida ham taqdim etilishi mumkin (2.1-jadval).



2.7-rasm. Foydalanishni cheklashda akslantirishlar sxemasining ko'rinishi

Foydalanishni cheklash sxemasini jadvalda aks ettirish, uni B × A × P dekart mahsulotining to'plami sifatida qabul qilishga imkon beradi. 2.1-jadvaldan ko'rinib turibdiki, b_1 foydalanuvchi barcha ob'ektlardan faqat *O'q* minimal vakolati bilan foydalanishga ega. b_j foydalanuvchi a_1 ob'ektidan *O'q* minimal vakolati bilan foydalanishga, qolganlariga esa - *Yoz* vakolati bilan foydalanishga ega. Shuningdek, b_j

foydalanuvchi ham a_1 ob'ekti uchun ham *O'q* minimal vakolati bilan foydalanishga ega, va qolganlariga - *Ma'murlash* vakolati bilan foydalanish huquqi beriladi [75].

Agar talab qilinuvchi va haqiqiy foydalanishni cheklash sxemasi to'plamlar ko'rinishida namoyish etilishi mumkin bo'lsa, unda ularning qiyosiy tahlilini o'tkazishda ularga an'anaviy nazariy-to'plam muolajalari, xususan, "\" muolajasini - "ayirish" nazariy-to'plami qo'llanilishi mumkin.

2.1-jadval

Foydalanishni cheklash sxemasining jadval ko'rinishi

Tartib raqami	Akslanuvchi to'plam		
	A	*B*	*P*
1.	a_1	b_1	*O'q*
2.	a_i	b_1	*O'q*
3.	a_1	b_1	*O'q*
4.	a_1	b_j	*O'q*
5.	a_i	b_j	*O'q*
6.	a_i	b_j	*Yoz*
7.	a_1	b_j	*O'q*
8.	a_1	b_j	*Yoz*
9.	a_1	b_J	*O'q*
10.	a_i	b_J	*O'q*
11.	a_i	b_J	*Yoz*
12.	a_i	b_J	*Ma'murlash*
13.	a_1	b_J	*O'q*
14.	a_1	b_J	*Yoz*
15.	a_1	b_J	*Ma'murlash*

$\Delta S_{talab} = S_{talab} \setminus S_{real}$ va $\Delta S_{real} = S_{real} \setminus S_{talab}$ belgisi kiritiladi. "Ayirish" nazariy-to'plamining ta'rifi bo'yicha, ΔS_{talab} tarkibiga faqatgina ΔS_{real} tarkibiga kirmagan S_{talab} to'plami elementlari kiradi, ΔS_{real} tarkibiga esa aksincha, S_{talab} tarkibiga kirmagan S_{real} to'plami elementlari kiradi [12] (2.8-rasm).

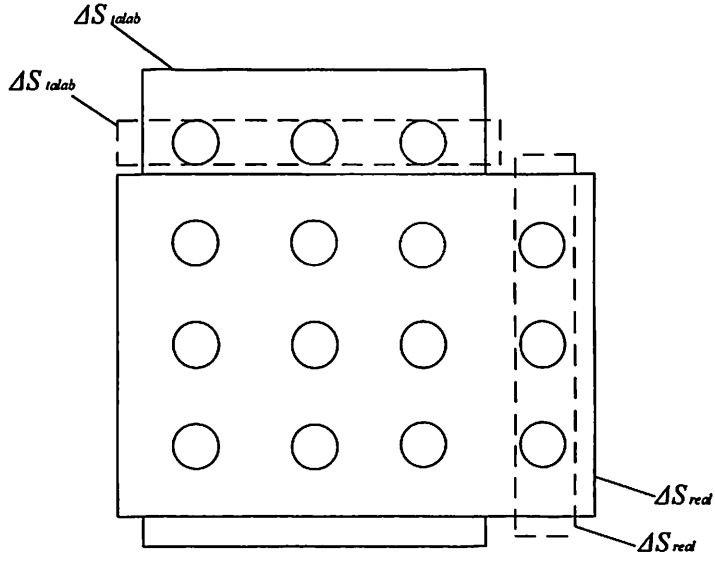
Agar S_{real} bilan S_{talab} mos kelsa, unda bir vaqtning o'zida quyidagi shart bajariladi

$$\Delta S_{talab} = 0. \quad (2.13)$$

$$\Delta S_{real}=0. \quad (2.14)$$

Bunday holda, FChTni qurishda axborot xavfsizligi talablari to'liq qondiriladi. Biroq, amalyotda, odatda yoki (2.13) bajarilmaydi, yoki (2.14) bajarilmaydi, yoki (2.13) va (2.14) birgalikda bajarilmaydi. Bunday holda FChT axborot xavfsizligi talablarini qisman qondiradi.

(2.13) shartning bajarilmaganligi, talab qilinuvchi S_{talab} sxemasi, ΔS_{real} real sxemasida mavjud bo'lmagan elementlarni o'z ichiga olganligini anglatadi. Natijada, real sxema tomonidan ba'zi talablar ta'minlanmagan hisoblanadi. Bu esa, axborot *konfidensialligining* buzilishi xususiyati mavjudligini anglatadi.



2.8-rasm. ΔS_{talab} *va* ΔS_{real} *ning izohlanishi*

(2.14) shartning bajarilmaganligi, aksincha, foydalanuvchilarning ma'lumotlarga cheklashda haddan tashqari cheklovlar mavjudligini bildiradi, ular talablar bilan madadlanmaydi, chunki S_{real} real sxemasi, S_{talab} sxemasida mavjud bo'lmagan elementlarni o'z ichiga oladi. Aslida, bu *foydalanuvchanlik* xususiyatining buzilishini anglatadi [12, 73, 75].

Konfidensiallik va foydalanuvchanlik axborot xavfsizligining yuqori darajadagi ma'lum xususiy sifatlarini belgilovchi xususiyatlari hisoblanganligi sababli, ushbu xususiyatlarning har qanday buzilishi, umuman axborot xavfsizligini buzilishini anglatadi. Shuning uchun,

foydalanishning cheklash masalasining kanonik bayonining qidiruv mezonlarini yaratish uchun FChT tomonidan konfidensiallik va foydalanuvchanlikga bo'lgan talablarning bajarilishini tavsiflovchi ko'rsatkichlardan foydalanish kerak.

Konfidensiallik ko'rsatkichi W_{konf} va foydalanuvchanlik ko'rsatkichi W_{foyd} tegishli funksionallar tomonidan o'rnatiladi

$$W_{konf} = W_{konf}(\Delta S_{talab}). \quad (2.15)$$

$$W_{foyd} = W_{foyd}(\Delta S_{real}). \quad (2.16)$$

Umumiy holda, xavfsizlik ko'rsatkichi W_{umum} quyidagi funksional ko'rinishida beriladi:

$$W_{umum} = W_{umum}(\Delta S_{talab}, \Delta S_{real}). \quad (2.17)$$

Xususiy holda, qachonki W_{konf} va W_{foyd} mustaqil bo'lganida, (2.16) o'rniga quyidagi iborani ishlatish mumkin:

$$W_{umum} = W_{umum}(W_{konf}, W_{foyd}) \quad . \quad (2.18)$$

(2.15), (2.16), (2.17) va (2.18) funksional shakllari FChT o'ziga xos tarkibi va tuzilishi bilan belgilanadi.

Agar (2.15) va (2.16) dan aniq foydalanish mavjud bo'lsa, u holda foydalanishning cheklash masalasining kanonik bayonidagi sintez mezonlari quyidagi variantlarda shakllanadi

$$W_{konf} \geq W_{konf}^{talab}, W_{foyd} \Rightarrow \max; \quad (2.19)$$

$$W_{foyd} \geq W_{foyd}^{talab}, W_{konf} \Rightarrow \max; \quad (2.20)$$

$$W_{konf} \geq W_{konf}^{talab}, W_{foyd} \geq W_{foyd}^{talab}. \quad (2.21)$$

bu yerda W_{konf}^{talab} va W_{foyd}^{talab} - mos ravishda, konfidensiallik va foydalanuvchanlik ko'rsatkichlarining talab etilgan qiymatlari hisoblanib, konfidensiallik va foydalanuvchanlik kriteriylari bo'yicha axborot xavfsizligining to'liq ta'minlanganlik (max) xususiyatlari hisoblanadi.

Agar (2.17) yoki (2.18) dan foydalanilgan o'rni bo'lsa, u holda foydalanishning cheklash masalasining kanonik bayonidagi sintez mezonlari quyidagi turlardan biriga ega bo'ladi:

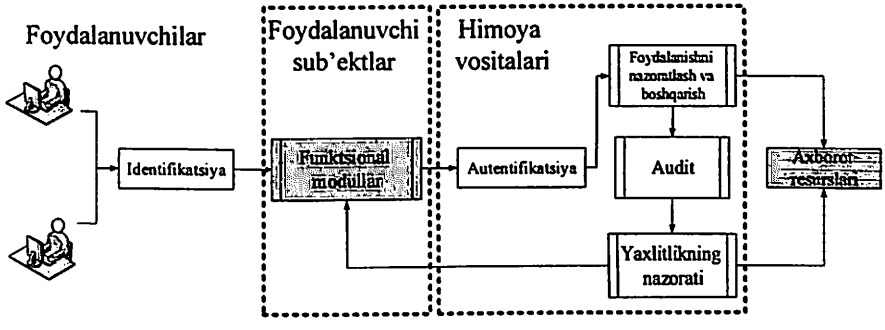
$$W_{umum} \geq W_{umum}^{talab}, \quad (2.22)$$

$$W_{umum} \Rightarrow \max. \quad (2.23)$$

bu yerda W_{umum}^{talab} - axborot xavfsizligini ta'minlash uchun FChTga qo'yiladigan talablar.

2.3. Foydalanishni cheklash tizimining konseptual modeli

90-chi yillarda dasturiy hujumlardan himoyalash tizimi vositalarini ishlab chiqaruvchilari tomonidan taklif etilgan xavfsizlikni adaptiv boshqarish (Adaptive Network Security) modeliga muvofiq, foydalanishni cheklash tizimi tarkibiga "passiv" komponent bilan bir qatorda, himoyalanganlikni va sezuvchanlikni tahlillash vositalari kompleksidan iborat "aktiv" komponent ham kiritiladi [8]. Axborot resurslari va funksional modullar tushunchalariga asoslangan kompyuter tizimi ishlashining strukturasi kompyuter tizimini himoyalash vositalari ishlashining umumlashtirilgan sxemasini belgilaydi (2.9 - rasm) [75].



2.9-rasm. Kompyuter tizimini himoyalash vositalari ishlashining umumlashtirilgan sxemasi

Autentifikatsiya vositalari faqat avtorizatsiyalangan foydalanuvchilarning tizimdan foydalanishlarini ta'minlaydi. Foydalanuvchi nomidan bajariluvchi va uning vakolatlariga ega jarayon kompyuter tizimi resurslaridan foydalanishni, unga mos foydalanish sub'ektini belgilovchi, autentifikatsiya vositalarining so'zsiz nazorati ostida amalga oshiradi.

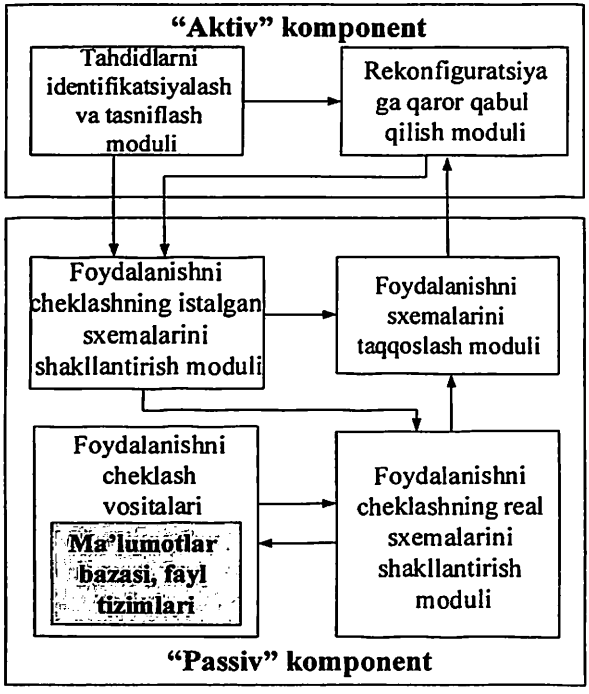
Axborot resurslariga barcha murojaatlar ob'ektlar hisoblanuvchi axborot resurslaridan foydalanishda xavfsizlik siyosati qoidalarining bajarilishini ta'minlovchi, foydalanishni boshqarish vositalari nazorati ostida amalga oshiriladi.

Resurslardan foydalanish amallarining barchasi (muvaffaqiyatli yoki muvaffaqiyatsiz) audit protokoliga kiritiladi. Yaxlitlikni nazorat-

lash vositalari himoya vositalarining va axborot resurslarining yaxlitligini tiklashni amalga oshiradi.

Natijada, foydalanishni cheklash tizimining an'anaviy funksional komponentlariga, axborotdan foydalanishni va tahdidlarni aniqlash va ularning paydo bo'lishini sezuvchi resurslarni operativ nazoratlash funksiyalarini amalga oshiruvchi qo'shimcha modullar qo'shiladi.

Foydalanishni cheklash tizimi tarkibiga, yuqorida keltirilgan funksiyalarni amalga oshiruvchi, mos holda loyihalangan va boshqaruvchi vositalar qo'shilishining shartligi ko'zda tutiladi (2.10-rasm).



2.10 - rasm. Foydalanishni cheklash tizimining umumlashtirilgan sxemasi

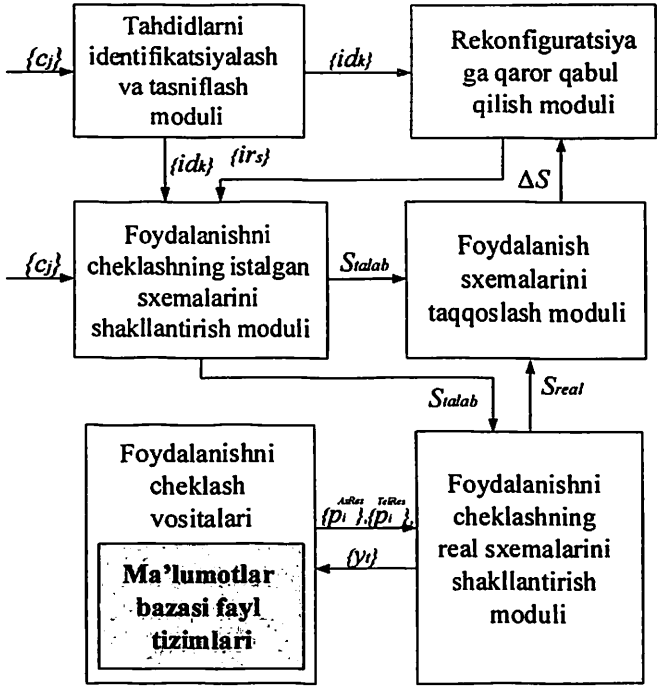
Foydalanishni cheklash tizimining an'anaviy funksional komponentlariga, axborotdan foydalanishni va tahdidlarni aniqlash va ularning

paydo bo'lishini sezuvchi resurslarni operativ nazoratlash funksiyalarini amalga oshiruvchi qo'shimcha modullar qo'shiladi.

Foydalanishni cheklash tizimi tarkibiga, yuqorida keltirilgan funksiyalarni amalga oshiruvchi, mos holda loyihalangan va boshqaruvchi vositalar qo'shilishining shartligi ko'zda tutiladi. Foydalanishni cheklash tizimining konseptual modeli 2.11-rasmda keltirilganidek ifodalash mumkin [75].

Bu holda, foydalanishning cheklash tizimi ishlashi jarayonini quyidagi ifoda orqali tavsiflash mumkin:

$$y(t_2) = Y\left(S_{talab}(t_1), \vec{V}^{AxRes}(t_1), \vec{V}^{TelRes}(t_1)\right). \qquad (2.24)$$



2.11-rasm. Foydalanishni cheklash tizimining konseptual modeli

Bu yerda:

$S_{talab}(t_1)$ -t_1 vaqt onida foydalanishni cheklash tizimining istalgan sxemasi;

$\vec{V}^{AxRes}(t_1) = \{v_i^{AxRes}\}$ -t_1 vaqt onida kompyuter tizimining axborot resurslaridan (ma'lumotlar bazasidan, fayl tizimlaridan) foydalanishni cheklash vositalari xarakteristikalarining vektori;

$\vec{V}^{TelRes}(t_1) = \{v_i^{TelRes}\}$ -t_1 vaqt onida kompyuter tizimining telekommunikatsiya resurslaridan (virtual tarmoqlardan) foydalanishni cheklash vositalari xarakteristikalarining vektori;

$y(t_2)$- t_2 vaqt onida foydalanishni cheklash tizimi tomonidan shakllantirilgan foydalanishni cheklash buyicha yechim, $t_2 > t_1$.

Foydalanishni cheklashning istalgan sxemasi t_2 vaqt onida foydalanishni cheklashning istalgan sxemalarini shakllantirish modulida yaratiladi:

$$S_{talab}(t_2) = F(\vec{C}(t_1), \vec{Id}(t_1), \vec{Ir}(t_1)) \ . \quad (2.25)$$

Bu yerda:

$\vec{C}(t_1) = \{c_j\}$-t_1 vaqt onida kompyuter tizimi axborot va telekommunikatsiya resurslarining ichki parametrlarining vektori;

$\vec{Id}(t_1) = \{id_k\}$-identifikatsiyalash va tasniflash modulida t_1 vaqtida aniqlangan tahdidlar vektori;

$\vec{Ir}(t_1) = \{ir_s\}$-rekonfiguratsiyalash lozimligini belgilovchi modulda t_1 vaqt onida shakllantirilgan yechimlar vektori.

Foydalanishni cheklashning real sxemasi t_2 vaqt onida foydalanishni cheklashning real sxemalarini shaklantirish modulida yaratiladi [75, 101]:

$$S_{real}(t_2) = \Pi(S_{talab}(t_1), \vec{V}^{AxRes}(t_1), \vec{V}^{TelRes}(t_1)). \quad (2.26)$$

Foydalanishni cheklashning istalgan va real sxemalarini taqqoslash bahosi foydalanish sxemalarini taqqoslash modulida, quyidagi ifodaga binoan shakllantiriladi:

$$\Delta S(t_2) = \Phi\ (S_{talab}(t_1), S_{real}\ (t_1)). \quad (2.27)$$

Foydalanishni cheklash tizimini rekonfiguratsiyalash zaruriyati xususidagi yechim rekonfiguratsiyalash lozimligini belgilovchi modulda t_2 vaqt onida quyidagi ifodaga binoan shakllantiriladi:

$$Ir(t_2) = Ir(\vec{Ir}(t_1), \Delta S(t_1)). \quad (2.28)$$

Identifikatsiyalash va tasniflash modulida tahdidlar vektori t_2 vaqt onida quyidagi ifodaga binoan aniqlanadi:

$$\vec{Id}(t_2) = Id\left(\vec{C}(t_1)\right). \quad (2.29)$$

Yuqorida tavsiflangan foydalanishni cheklash tizimining konseptual modelining strukturasi bo'yicha quyidagi xulosalar qilish mumkin:

- foydalanishni cheklash tizimi ishlashi jarayonini amalga oshirish uchun uning tarkibiga tahdidlarni identifikatsiyalash va tasniflash bilan bog'liq foydalanishni cheklashni boshqarish funksiyalarini bajaruvchi vositalar kiritilishi lozim.

- funksional jihatdan foydalanishni cheklash tizimini, tarkibida foydalanishni cheklashning an'anaviy "passiv" komponenti bilan bir qatorda "aktiv" komponentining mavjudligi sifatida tasavvur etish mumkin.

2.4. Foydalanishni cheklash tizimini sintezlash samaradorligini baholash ko'rsatkichlari

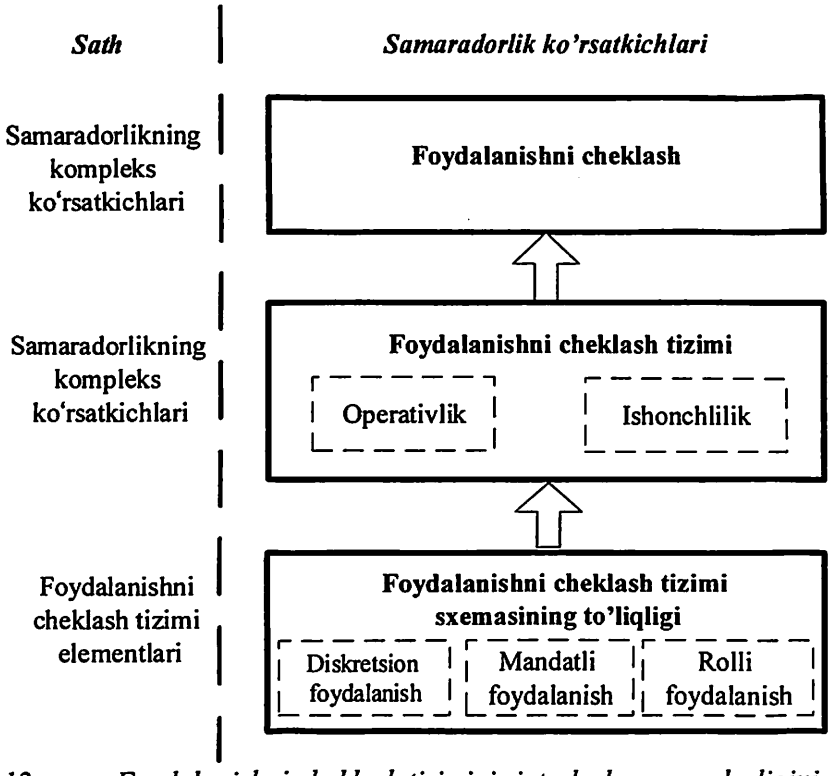
Maqsadga yo'naltirilgan jarayonlar samaradorligini baholashning ma'lum metodologiyasi, ko'rsatkichlar tizimini shakllantirishda, uning tarkibiga baholanuvchi jarayonni tavsiflovchi natijaliligi, resurslar ko'lami, operativlik va ishonchlilik kabi ko'rsatkichlarning so'zsiz kiritilishini ko'zda tutadi. Ushbu ko'rsatkichlar birgalikda ko'p sathli tizimni hosil qiladi (2.12-rasm).

Sintezlash jarayonining natijaliligini quyidagi *kompleks ko'rsatkichlari* orqali baholash mumkin:

E_{RFSH} - axborotni ruxsatsiz foydalanishdan statik himoyalanganligini tavsiflovchi axborotdan ruxsatsiz foydalanish ehtimolligi;

E_{RFDH}-axborotni ruxsatsiz foydalanishdan dinamik himoyalanganligini tavsiflovchi, berilgan vaqt mobaynida axborotni ruxsatsiz foydalanishdan himoyalashni ta'minlash ehtimolligi.

E_{RF} qiymati foydalanishni cheklash tizimining ruxsatsiz foydalanishga urinishlarini bartaraf etish qobiliyatini ifodalaydi. Bu axborotni ruxsatsiz foydalanishdan himoyalash tizimi samaradorligini baholashning an'anaviy yondashishiga mos keladi. E_{RFH} ning ehtimolligi, aksincha, ruxsatsiz foydalanishga urinishlar va dasturiy hujumlar mavjudligida, foydalanishni cheklash tizimining axborotni ruxsatsiz foydalanishdan himoyalash qobiliyatini aks ettiradi [75].



2.12- rasm.Foydalanishni cheklash tizimini sintezlash samaradorligini baholash ko'rsatkichlari

Yuqorida keltirilgan ko'rsatkichlar kompleks sathining samaradorlik ko'rsatkichlari hisoblanadi [45, 61, 98]. Ulardan tashqari, ushbu sathga kuyidagilar tegishli:

K_F^{HR}-hisoblash resurslarining ishlatilish koeffitsiyenti;

K_F^{TR}-tarmoq resurslarining ishlatilish koeffitsiyenti;

N - narxi.

Ushbu ko'rsatkichlar, foydalanishni cheklash ehtiyoji nuqtai nazaridan, axborotni himoyalash tizimining hisoblash va tarmoq quvvatlarining qanchalik yuklanganligini ko'rsatadi. Ushbu ko'rsatkichlar o'lchamsiz kattaliklar hisoblanadi.

Samaradorlikning *xususiy ko'rsatkichlari* sathiga ikkita ko'rsatkich-operativlik va ishonchlilik tegishli. Operativlik ko'rsatkichi quyidagicha:

$E\ (t_I <= T^{ishonch})$- xavfsizlik tahdidlarini o'z vaqtida identifikatsiyalash va tasniflash ehtimolligi;

$E\ (t_Q <= T^{ishonch})$- foydalanishni cheklash tizimini boshqarish variantlarini o'z vaqtida qidirish ehtimolligi;

$E\ (t_{Sh} <= T^{ishonch})$- foydalanishni cheklash sxemasini o'z vaqtida shakllantirish ehtimolligi.

Ishonchlilik ko'rsatkichlariga quyidagilar tegishli:

E_{IX} - tahdidlarni identifikatsiyalash xatoliklari ehtimolligi;

E_{BX} - boshqarish xatoliklari ehtimolligi;

E_{ShX} - foydalanishni cheklash sxemalarini shakllantirish xatoliklari ehtimolligi.

Foydalanishni cheklash tizimi *elementlari ko'rsatkichlari* sathi, ya'ni kompyuter tizimida ishlatiluvchi foydalanishning diskretsion, mandatli va rolli usullari sxemalarida quyidagi ko'rsatkichlardan foydalaniladi:

K_{konf}-konfidensiallik bo'yicha talablarning amalga oshirilishining to'liqlik koeffitsiyenti;

K_{foyd}-foydalanuvchanlik bo'yicha talablarning amalga oshirilishining to'liqlik koeffitsiyenti.

Yuqorida keltirilgan ko'rsatkichlarni foydalanishni cheklashning mavjud modellariga, taklif etilgan foydalanishni cheklashning konseptual modelini hisobga olgan holda, qo'llash orqali foydalanishni cheklash tizimlarining qiyosiy bahosiga ega bo'lish mumkin.

Monografiyaning 2.1 bo'limida bayon etilganidek, foydalanishni cheklash tizimiga tahdidlar ta'siri ehtimolligini hisoblashga imkon beruvchi diskretsion modellar (DAC) "Troyan ot" yordamidagi hujumga nisbatan zaif, chunki ularda faqat sub'ektlarning ob'ektlardan foydalanish amallari nazoratlanadi, ular orasidagi axborot oqimi nazoratlanmaydi. Foydalanishning diskretsion siyosatining yana bir kamchiligi tizimning barcha resurslari tizim foydalanuvchilariga tegishli. Demak, resurslardan foydalanish nazorati foydalanuvchi zimmasida qoladi. Bunday tizimlar, asosan, kam sonli foydalanuvchilarga mo'ljallangan. Foydalanuvchilar soni oshganda, tizimni ma'murlash vazifalari bir necha bor ortadi.

Mandatli cheklashga (MAC) binoan barcha foydalanish ob'ektlari maxfiylikning ma'lum sathiga ega, barcha sub'ektlar esa axborotdan foydalanish huquqi darajasiga binoan iyerarxiyani hosil qiluvchi

guruhlarga ajratiladi. Demak, real tizimda mandatli modelni qo'llash uchun o'qish, yozish va muayyan tizimda amalga oshirilgan amallar orasida munosib muvofiqlikni o'rnatish zarur. Ushbu masalani yechish oson emas, chunki, real xayotda sub'ektdan ob'ektga yoki aksincha qat'iy o'tuvchi, bir tarafga yo'nalgan axborot oqimi bilan chegaralanish mumkin emas. Axir, masalan, o'qish amalini bajarish uchun sub'ekt, avvalo, u qiziqayotgan ob'ektdan foydalanishni amalga oshiruvchi xizmatga so'rov yuborishi lozim.

Agar tizim ishlashiga shu nuqtai nazardan qaralsa, mandatli siyosatni qo'llash mumkin bo'lmay qoladi, chunki mandatli modelni nazoratlanuvchi o'zaro harakatni amalga oshiruvchi past darajali mexanizmlarga tatbiq etishga urinishlar, ushbu siyosatning avtomatik tarzda buzilishiga olib keladi.

Shunday qilib, diskretsion modellarda foydalanishni boshqarish foydalanuvchilarga ma'lum ob'ektlar ustida ma'lum amallarni bajarish vakolatini berish yo'li bilan amalga oshirilsa, mandatli modellar foydalanishni xufiya holda tizimning barcha sub'ekt va ob'ektlariga xavfsizlik sathlarini belgilash orqali boshqaradi. Ushbu xavfsizlik sathlari sub'ektlar va ob'ektlar orasidagi joiz o'zaro harakatlarni aniqlaydi va o'zaro harakatlarga cheklashlar mavjud emas.

Xavfsizlikning rolli modelining (RBAC) qo'llanishi kompyuter tizimlarida foydalanishni cheklash tizimini loyihalashni va ma'murlashni jiddiy soddalashtiradi.

Foydalanishni rolli boshqarish tizimini, murakkab iyerarxiyali va ko'p sonli taqsimlanuvchi amallar mavjud yirik tashkilotlarda ishlatish maqsadga muvofiq hisoblanadi. Bunday tizimda ma'lumotlar, odatdi, foydalanuvchilarga emas, tizimga tegishli bo'ladi. Xattoki, resurslardan, foydalanishni boshqarish resurslarning tegishligiga emas, balki tashkilotdagi foydalanuvchi funksiyalariga asoslanadi. Ta'kidlash lozimki, RBAC ob'ektlarni o'ziga emas, balki ob'ektlar ustidagi amallardan foydalanishni boshqarish bilan ko'proq bog'langan [75, 81].

Foydalanishni nazoratlashning diskretsion va mandatli modellarining rolli modeldan bitta muhim farqi mavjud. Ushbu modellarda tizim xavfsizlik siyosati oldindan aniqlanadi va uni har bir muayyan vaziyat uchun sozlash imkoni mavjud.

Rolli model xavfsizlik siyosatini aslo oldindan aniqlamaydi, balki uni tashkilotga zarur ko'rinishda sozlashga imkon beradi. Boshqacha aytganda, foydalanishni rolli cheklash foydalanishni cheklash tizimining

ishlashi modeliga ishonchlik darajasini oshirish imkoniyatini taqdim etadi. 2.2 - jadvalda foydalanishni cheklash tizimi elementlari darajalari ko'rsatkichilarini taqqoslash natijalari keltirilgan.

Rolli siyosatning o'ziga xos xususiyatlari foydalanuvchilar va ob'ektlar soni ko'p, murakkab tizimlarda yaxshigina boshqaruvchanlikka ega foydalanishni cheklash tizimini qurishga imkon beradi va shuning uchun, amaliy tizimlarda keng qo'llaniladi.

2.2 - jadval

Foydalanishni cheklash tizimi elementlari darajalari ko'rsatkichlarini taqqoslash

FChT elementlari darajalari / Foydalanishni cheklash tizimlari	**Amalga oshirilishning soddaligi**	**Ma'murlashning soddaligi**	K_{konf}	K_{foyd}	**Rekonfiguratsiyaga qaror qabul qilish**
DAC	+	-	-	-	-
MAC	-	-	+	-	-
RBAC	-	+	+	+	+

Xulosa qilib aytganda, RBAC modeli foydalanuvchilarni bitta katalogda yoki bir xil huquqlarga ega bo'lgan katta guruhlarni boshqarish kabi aniq muammolar uchun foydali yechim hisoblanadi. Ammo, RBAC, foydalanuvchanlikga ruxsat beruvchi yagona model sifatida, ko'p sonli taqsimlanuvchi amallar mavjud yirik tashkilotlarda ishlashida foydalanuvchilar huquqlarini boshqarish va dinamik foydalanuvchilarga ruxsat berish muammolariga mos kelmaydi. Shunday qilib, ushbu tadqiqotning maqsadiga erishish uchun, zamonaviy KT xususiyatlarini hisobga olgan holda, takomillashtirilgan foydalanishni cheklash modellarining kombinatsiyalangan modelini ishlab chiqish zarur.

III-BOB. FOYDALANISHNI ROLLI CHEKLASH TIZIMI MODELINING SAMARADORLIGINI OSHIRISH

3.1. Foydalanishni rolli cheklashning bazaviy modeli

Rollarning kiritilishi foydalanishni cheklash tizimining ikki bosqichli tashkil etilishiga olib keladi:

1. Rollarni yaratish va ular vakolatlarini aniqlash, ob'ektlardan foydalanish huquqlari;

2. Tizim foydalanuvchilariga rollarni tayinlash.

Mos holda rolli modellarning formal spetsifikatsiyalari u yoki bu tarzda, aniqrog'i ma'lum bir siyosat chegarasida, rollarga vakolatlarni va foydalanuvchilarga rollarni tayinlashni reglamentlashi lozim. Foydalanishni boshqarish ikki bosqichda amalga oshiriladi: dastlab, har bir rol uchun ob'ektlarga, foydalanish huquqlari to'plamini ifodalovchi, vakolatlar nabori ko'rsatiladi, so'ngra har bir foydalanuvchiga unga tushunarli rollar ro'yxati tayinlanadi.

Foydalanishni cheklashning rolli modelining rasmiy spetsifikatsiyasi:

1. RBAC-rolli modeli tizimni quyidagi to'plamlar shaklida tavsiflaydi:

U - foydalanuvchilar to'plami;

R - rollar to'plami;

P - ob'ektlardan foydalanish uchun vakolatlar to'plami;

S - foydalanuvchining tizim bilan ishlash seanslari to'plami [18, 27, 28, 31, 32, 33, 34, 70, 81, 87].

Umumiy qoida vakolatlar to'plami R, foydalanish amallari va foydalanish ob'ektlarini birlashtiruvchi maxsus mexanizmlar tomonidan o'rnatiladi.

2. Rol munosabatlari tizim mohiyatlari to'plamlarining quyidagi akslantirishlari orqali o'rnatiladi.

$FPR \subseteq P \times R$-har bir rolga berilgan vakolatlar naborini belgilash orqali, vakolatlar to'plamini rollar to'plamiga akslantiradi;

$FUR \subseteq U \times R$-har bir foydalanuvchiga tushunarli rollar naborini belgilash orqali, foydalanuvchilar to'plamini rollar to'plamiga akslantiradi.

FPR va FUR akslantirilishlari, rolli foydalanish tizimini tashkil etishning birinchi va ikkinchi bosqich jarayonlarini ta'minlashini ko'rish qiyin emas. Bunda FUR akslanishi, foydalanishni cheklashning bazaviy

siyosatlaridan biri - "foydalanuvchilar - rollar" matritsasi mexanizmlari yoki foydalanuvchilarning foydalanish darajalari yoki rollarning konfidensiallik griflari nisbati asosida amalga oshirish mumkin.

3. Roli xavfsizlik siyosatidan foydalanishni boshqarish qoidalari quyidagi funksiyalar orqali belgilanadi:

$fuser: S \rightarrow U$- U=fuser(s) funksiya qiymati, tizim bilan ishlash seansini amalga oshiruvchi foydalanuvchi $u \in U$ hisoblanadi;

$froles: S \rightarrow R$- R=froles(s) funksiya qiymati, berilgan seansda foydalanuvchi foydalanishni amalga oshirishda ishlatuvchi foydalanuvchi uchun tushunarli rollar nabori hisoblanadi;

$fpermissions: S \rightarrow P$- P=fpermissions(s) funksiya qiymati, vakolatlar nabori $P \subseteq P$ hisoblanib, ushbu $s \in S$ seansda foydalanuvchi tomonidan ishlatilgan barcha rollar uchun tushunarli.

4. Rolli modelning xavfsizlik kriteriylari quyidagicha aniqlanadi: agar tizimning har qanday foydalanuvchisi $u \in U$ seans $s \in S$, vakolat $p \in P$ doirasidagi ta'sirlarni bajarishi mumkin bo'lsa, faqat $P = fpermissions(s)$ shartida, tizim xavfsiz ishlaydi.

Rolli siyosat asosida foydalanishni tashkil etish va boshqarish jarayonlarida asosiy e'tibor foydalanuvchilar to'plamining rollar to'plami FURga akslantirish xususiyatlariga va ushbu seansdagi foydalanuvchini avtorizatsiyalash funksiyasi froles(s)ga qo'yilgan cheklashlarga qaratilishini anglash qiyin emas [69].

3.1-rasmda strukturasi tasvirlangan foydalanishni cheklashning rolli modelini qo'llash, murakkab tashkiliy-texnologik va tashkiliy-boshqaruv sxemalarni va jarayonlarni amalga oshiruvchi KTda foydalanishni cheklash tizimlarini loyihalashni va ma'murlashni sezilarli darajada soddalashtirishga imkon beradi. Shuning uchun rolli siyosat, tizimning samarali xavfsizligini ta'minlashga imkon beruvchi rollar va foydalanuvchilar vakolatlarini boshqarish mexanizmi sifatida ishlatilishi mumkin [81].

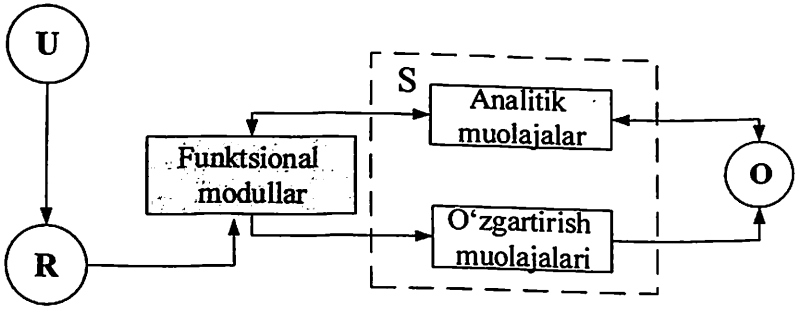
Rollarga asoslangan foydalanishni boshqarish bir qator muhim ijobiy xususiyatlarga ega. Masalan:

Huquqlar naborining vorisligi bilan rollar iyerarxiyasini yaratish qobiliyati. Bu, ayniqsa, ko'plab axborot tizimlari qo'llaniladigan, turli xil infratuzilmali tashkilotlarda rolli modelning tatbiqini soddalashtiradi. Iyerarxiyadan foydalangan holda, bir necha bunday rollarda huquqlarni qayta belgilashga hojat yo'q, ularni, har bir rol uchun faqat noyob

huquqlarni ko‘rsatib, ularni bitta katta rolga, sho‘‘ba sifatida joylashtirish kifoya.

Ko‘p sonli foydalanuvchilarga bir xil huquqlarni berish oddiy va samarali-foydalanuvchilarga esa bitta rolni tayinlash kifoya. Ko‘p sonli foydalanuvchilar uchun huquqlar naborini o‘zgartirish zaruriyati tug‘ilsa, rolda huquqlar naborini o‘zgartirish kifoya.

Vakolatlarni taqsimlash prinsipini amalga oshirish imkoniyati (SOD – Segregation Of Duties). Bu foydalanuvchilarga ortiqcha vakolat berish xavfini sezilarli darajada kamaytiradi, masalan, bitta foydalanuvchiga bir vaqtning o‘zida ikkita rolni berib bo‘lmaganday [21].



3.1-rasm. Foydalanishni cheklashning rolli modelining strukturasi

Foydalanishni boshqarishning rolli modelini loyihalashda, tatbiq etishda va foydalanishda vaqt va mablag‘ isrofining katta bo‘lishiga olib keladigan omillarni hisobga olish lozim.

Birinchidan, ***“foydalanuvchilarning xilma-xilligi”***: amalda yirik tashkilotlarda noyob huquqlarga ega juda ko‘p sonli foydalanuvchilar bo‘lishi mumkin, ularning ba’zilari bir xil lavozimda yoki hattoki bitta bo‘limda bo‘lishi mumkin. Bu rolli modelni tuzishni murakkablashtiradi va har bir foydalanuvchi o‘zining noyob roliga muhtoj bo‘lgan vaziyatga olib kelishi mumkin. Bunday holatlar, agar xodim o‘z lavozimi doirasida “o‘sgan” bo‘lsa yoki u o‘z bo‘limida noyob funksiyalarga ega bo‘lsa, paydo bo‘lishi mumkin. Bu foydalanishni boshqarish tizimi uchun jiddiy muammo bo‘lishi mumkin.

Ikkinchidan, ***“juda ko‘p rollar”*** mavjud: bu har doim ham shunday emas, ammo shunday vaziyat yuzaga kelishi mumkinki, foydalanishni

boshqarish tizimiga yana bir boshqariluvchi tizim ulanganida, oldin ulangan tizimlarga belgilangan rollarni, yangi tizim bilan birgalikda ishlatilishining barcha mumkin bo'lgan variantlarini hisobga olgan holda, bir necha boshqa rollarga aylantirish lozim. Agar bunday yangi tizimlar bir nechta bo'lsa, unda foydalanuvchilarga nisbatan rollar sonining ko'proq bo'lishi vaziyati yuzaga kelishi mumkin.

Uchinchidan, ***"foydalanuvchi mas'uliyatini o'zgartirish va biznesni qayta tashkil etish"***: hatto rolli model tashkilotdagi joriy vaziyatni aks ettirsa ham, uni doimo dolzarb holda madadlash, foydalanuvchi majburiyatidagi o'zgarishlarni kuzatib borish va zudlik bilan rolli modelga o'zgartirishlar kiritilishi kerak.

To'rtinchidan, ***"narx"***: shuni yodda tutish kerakki, rolli modelni ishlab chiqish va madadlash, oxir-oqibat qo'lda ma'murlashga qaraganda qimmatga tushadi. Bundan tashqari, rolli modelni boshqarish, boshqarish huquqini beradigan ma'murga qaraganda, ko'proq malakali mutaxassislarni talab qiladi [10, 16].

Rolli siyosat qo'llanilganda foydalanishni boshqarish ikkita bosqichda amalga oshiriladi: avval har bir rol uchun ob'ektlardan foydalanish huquqlar naboridan iborat vakolatlar nabori ko'rsatiladi, so'ngra har bir foydalanuvchiga unga mumkin bo'lgan rollar ro'yxati belgilanadi.

Rolli modelning kamchiliklaridan biri foydalanuvchi vazifalarining cheklangan to'liqligining yo'qligi hisoblanadi. Shu sababli foydalanuvchiga berilgan vakolatlarning ta'sir doirasini cheklash, ya'ni ob'ektdan foydalanish sxemasini soddalashtirish zaruriyati mavjud. Shu maqsadda monografiya ishida ikki tomonlama ishonchlikni o'rnatishga imkon beradi, foydalanishni cheklashning zona siyosatili funksional - rolli modeli taklif etilgan [69,70].

Foydalanishni zonali cheklashli rolli modelida "sohib" R roli kiritilgan bo'lib, ushbu rol foydalanuvchilarga ular egalik qiladigan ob'ektlar doirasida belgilanadi. Zonali siyosat qo'llanilganida tizimning fizik ob'ektlar to'plamini $V(v_1, v_2, \ldots, v_l)$ - hisoblash qurilmalari (ishchi stansiyalar, serverlar,) printerlar, kommunikatsion uskunalar va h., hamda tizim zonalari to'plamini $Z(z_1, z_2, \ldots, z_k)$ kiritish lozim.

Xavfsizlikning ichki zonali siyosati xavfsizlik vazifalarining to'la naborini ta'minlovchi *xavfsizlikning ichki zonali monitoringi* yordamida amalga oshiriladi. Xavfsizlikning ichki zonali monitoringi (3.2-rasm) – tizim sub'ekt (jarayon) zona ob'ektlariga nisbatan ruxsat etilgan

foydalanishlar to'plamini ichki zona siyosati belgilagan qoidalar yordamida amalga oshirsa, zona foydalanuvchilarining boshqa zona ob'ektlaridan masofadan foydalanishi xavfsizlikning zonalararo siyosati yordamida amalga oshiriladi: ya'ni

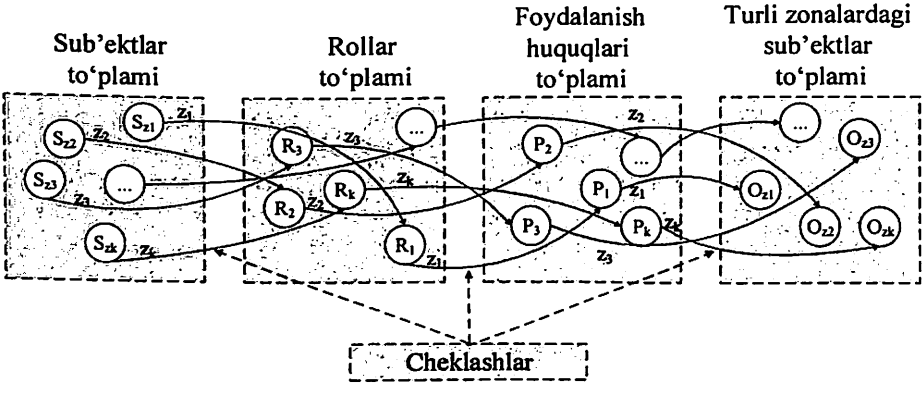
$$P_L(z) = P_L^{in}(z) \cup P_L^{out}(z), \qquad (3.1)$$

Bu yerda: $P_L^{in}(z)$ – xavfsiz ichki zonali foydalanishlar to'plami;
$P_L^{out}(z)$ – xavfsiz masofadan foydalanishlar to'plami.

Taklif etilgan foydalanishning zonali cheklashli rolli modelida har qanday zona o'ziga ishonadi, ya'ni ichki zonali foydalanish man etilmagan. Zonalararo foydalanishni formallashtirish maqsadida quyidagi akslantirish kiritilgan: $f_{UZ}^{out}: U \times Z'$ - foydalanuvchi to'plamini "begona" zonalar $z' \in Z'$ ga akslantirish (bu yerda $Z' = (Z \backslash f_{user}(u))$ foydalanuvchi $(z' \leq f_{user}(u))$ zonasiga ishonadi). Ushbu zonalarda masofadagi foydalanuvchi sub'ektini hosil qilib, mos zonalar ob'ektidan masofaviy foydalanishi mumkin.

Shunday qilib, xavfsizlikning umumtizim siyosati ichki zonali foydalanish siyosati va foydalanishni zonalararo cheklash siyosatidan tashkil topgan bo'lib, kompyuter tarmog'idan ruxsatli foydalanishlar to'plamini belgilaydi ya'ni

$$P_L^{out}(z_l) = \bigcup_{\substack{i \neq k \\ k=1}}^{K} P_L^{out}(z_l \rightarrow z_k) \cup \bigcup_{\substack{l \neq k \\ k=1}}^{K} P_L^{out}(z_l \leftarrow z_k), \qquad (3.2)$$



3.2-rasm. Xavfsizlikni ichki zonali monitoringining modeli

Ushbu model, tarkibida rollarni va foydalanuvchilar vakolatlarini boshqarishda ma'lum foydalanuvchilar uchun ma'lum amallarni bajarish

qoidalari nabori bo'lgan, ikki tomonlama ishonch munosabatlarini o'rnatishga imkon beradi.

Ammo RBAC tizimidagi ixtiloflar bitta foydalanuvchiga, tarkibida bir xil imtiyozlar uchun qarama-qarshi belgili qoidalar bo'lgan rollarni tayinlanishidan kelib chiqadi. Bunday ixtiloflarni hal etish yoki oldini olish uchun quyidagi yondashuvlar mavjud.

Ixtiloflarga yo'l qo'ymaslik. RBAC tizimidagi rollar ixtiloflari, agar barcha rollar bir xil belgili qoidalar ya'ni faqat ruxsat berish yoki faqat ruxsat bermaslik qoidalari asosida ko'rilsa, umuman sodir bo'lmaydi. Faqat ruxsat etilgan qoidalardan tashkil topgan rollarning qismto'plamida foydalanuvchiga boshqa rolni berish, uning foydalanish huquqlarini oshiradi va mavjudlariga cheklovlar qo'ymaydi.

Ixtiloflarni hal qilishda statik va dinamik usullarni qo'llash mumkin:

Statik:

- foydalanuvchilarni mustaqil loginlari va nizolashmaydigan rollar naborili bir necha sub'ektlarga taqsimlash;
- nizolashuvchi qoidalardan birini bekor qilishning statik muolajasini joriy etish.

Dinamik:

- ma'lum foydalanuvchi uchun tayinlangan rollarning faqat bir-biriga zid bo'lmagan to'plamini bitta seans doirasida aktivlashtirish;
- seanslar orasida o'zgartirish. Avval aktivlashtirilgan rollarning Aktiv rollardan biri bilan ziddiyatda bo'lgan rolni joriy seans aktivlashtirishda tugallanadi, ziddiyatli rol undan chiqarib tashlanadi, yangi rol qo'shiladi va hosil bo'lgan rollar nabori uchun RBAC ning yangi versiyasi yaratiladi [76].

Dinamik usul vaqtning har bir lahzasida bir holat to'g'ridan-to'g'ri yoki bilvosita boshqasiga yoki bir nechtasiga bog'liqligi ma'nosida dinamikdir. Har bir holatning o'zgarishi unda belgilangan qonunlar va qoidalarga mos keladi. Biroq, simulyatsiyadan foydalanishda bir qator cheklovlar mavjud. Birinchidan, turli xil tizimlardagi o'zgarishlar har xil tezlikda sodir bo'ladi, agar bu ko'rsatkichlar bir-biriga joylashtirilsa, idroksh muammolari paydo bo'ladi. Masalan, ma'lumotlar bazasini ruxsatsiz nusxalash ma'lum vaqtni oladi, ammo ulanishlarni tahlil qilish bir lahzani oladi. Ikkinchidan, tizimning bir elementtidagi o'zgarishlar odatda boshqa elementlarda bashorat qilish qiyin bo'lgan o'zgarishlarni keltirib chiqaradi, tizim yangi holatga o'tadi va uning harakati o'zgaradi.

Uchinchidan, ko'plab jarayonlarning chiziqli bo'lmaganligi sababli, uning o'tmishdagi xatti-harakatlar tendensiyasining ekstrapolyatsiyasi foydalangan holda tizimning xatti-harakatlarini oldindan aytib bo'lmaydi.

RBAC modeli foydalanuvchi va vakolatlar orasiga rolni kiritadi. Natijada, foydalanishni nazoratlashni boshqarish ikki qismga bo'linadi: foydalanuvchi-rol qiyoslanishi va rol-vakolat qiyoslanishi, bu esa foydalanishni nazoratlashni boshqarishni soddalashtiradi. Bir tomondan, model rollar o'rtasidagi munosabatlarning vorisligini belgilash orqali foydalanishni nazoratlashni boshqarishni yanada soddalashtirishi mumkin, boshqa tomondan cheklovlarni kiritish orqali boshqaruv xavfsizligini amalga oshirishi mumkin. Ammo RBAC modeli joylashgan muhit foydalanuvchi-vakolat qiyoslanishini dinamik boshqarishga mos emas.

Yuqorida keltirilganlardan xulosa qilish mumkinki, RBAC ba'zi bir muayyan muammolar uchun foydali yechim hisoblanadi: foydalanuvchilarni bitta katalogda boshqarish yoki bir xil huquqlarga ega foydalanuvchilarning katta guruhlarini boshqarish. Ammo, RBAC, foydalanishni taqdim etuvchi yagona model sifatida, xilma-xil foydalanuvchilar huquqlarini boshqarish muammolari va aksariyat tizimlarda foydalanuvchilarning dinamik foydalanishi uchun munosib emas. Resurslar va foydalanuvchilar ko'pincha turli domenlarda joylashganligi sababli, bunday tizimlarda sub'ektlar va ob'ektlar o'rtasidagi munosabatlar juda murakkab va dinamik xarakterga ega. Ushbu muammolarni hal qilish uchun atributli foydalanishni cheklash (Attribute Based Access Control - ABAC) usuli taklif qilingan [11, 14, 15, 17]. Uning maqsadi sub'ektlar va ob'ektlarni atributlar to'plami bilan belgilash va ushbu usul foydalanishni boshqarish bo'yicha qarorlarni, sub'ektlar yoki ularga xizmat ko'rsatuvchi provayder bilan munosabatlari xususida oldindan bilmasdan, qabul qilishga imkon beradi. Atributlarga asoslangan siyosatning normativ talablarning murakkabligini pasaytirishi evaziga, foydalanishni boshqarish samaradorligi oshadi [76].

3.2. Rol va atribut asosida foydalanishni boshqarish modeli

Foydalanishni atributli cheklash (ABAC) usuliga binoan sub'ektning ob'ekt ustida ma'lum amallarni bajarish so'rovlari, ularga yozilgan atributlar, bajarish muhiti sharoitlari va ushbu sharoitlar va

atributlarni hisobga olgan holda ifodalangan siyosatlar nabori asosida, qanoatlantiriladi yoki qanoatlantirilmaydi. Rollarga asoslangan foydalanishni boshqarish (RBAC)da oldindan belgilangan rollar ishlatiladi. Bu rollar o'zlari bilan bog'langan va sub'ektlarga tayinlangan imtiyozlarning ma'lum naborini eltadi. Foydalanishni atributli cheklash (ABAC) esa turli atributlar to'plamini baholovchi mantiqiy qoidalarning murakkab naborini ifodalovchi siyosatlar konsepsiyasi hisoblanadi [11, 14]. ABAC konsepsiyasi "keyingi avlod" avtorizatsiya modeli hisoblanadi, chunki u resurslardan foydalanishning dinamik, kontekst-bog'liqliq va intellektual nazoratini ta'minlaydi. Bu esa ko'pgina turli axborot tizimlaridan ma'lum atributlarni o'z ichiga oluvchi foydalanishni nazoratlash siyosatidan foydalanishga imkon beradi.

ABAC rollarni, mulkka egalik huquqini yoki tizim ma'muri tomonidan xavfsiz belgisini tayinlamaydi, balki foydalanuvchilar va ob'ektlar atributlari asosida foydalanish siyosatini yaratish imkonini beradi. Bu ABACning afzalligi hisoblanadi va foydalanuvchilar soni ko'p murakkab tizimlarda ma'murlashni soddalashtiradi, ya'ni ma'lum rollar yoki xavfsizlik darajasi uchun foydalanishni avtorizatsiyalashda shaxsning aralashishini bartaraf etadi. Undan tashqari, masofadagi foydalanuvchilar uchun foydalanishni boshqarish bo'yicha yechimni avtomatlashtirish imkoniyati yaratiladi.

Atributlar odatda, argumentlari vazifasini sub'ektlar va ob'ektlar bajaruvchi funksiyalar, natija esa ularning atributlari sifatida ifodalanadi. Avtorizatsiya siyosati foydalanuvchilar guruhiga berilgan ob'ektlardan, ular atributlarining qiymatlarini baholash asosida, foydalanishning ma'lum xilini (masalan, o'qish va yozish) taqdim etadi.

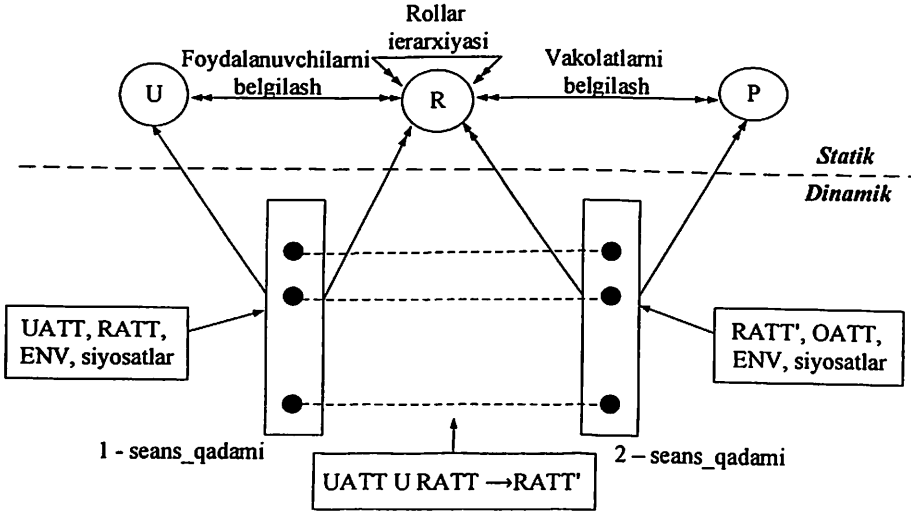
Foydalanishni boshqarish bo'yicha yechimlar ko'p darajada foydalanishni boshqarish so'rovlari va atributlar, sub'ektlar va ob'ektlar xavfsizligi o'rin olgan kontekstga bog'liq [76].

Yuqorida aytilganidek, RBAC va ABAClar o'zlarining afzalliklariga va kamchiliklariga ega va ularning afzalliklari bir-birini to'ldiradi. Shu sababli, rollar asosidagi soddalikni va xavfsizlikni, hamda ABAC moslashuvchanligini saqlash maqsadida RBAC\ABAC gibrid yondashuvni (RABAC modelini) taqdim etilgan [24, 26, 39]. RABAC modeli RBACdan foydalanuvchilar va ma'murlar orasidagi munosabatlarni, xavfsizlik nuqtai nazaridan, boshqarishda foydalansa, ABACdan foydalanuvchilar va vakolatlar orasidagi dinamik munosabatlarni boshqarishda foydalanadi.

Turli tadqiqotchilar RBAC va ABAClarni birlashtirishning bir necha yondashuvlarini taklif etganlar. RBAC modeliga atributlarni qo'shish bu sohadagi muhim hissa hisoblanadi. Qiziqtiradigan yondashuvlardan biri-foydalanuvchilarni rollar buyicha dinamik taqsimlash. Dinamik taqsimlash foydalanuvchilar va rollar atributlariga asoslangan. Tadqiqotchilar an'anaviy RBAC modelidagi foydalanuvchilar va rollar atributlari tushunchalarini berishdi [44]. Ammo, model, foydalanuvchilarning va rollarning atributlar yordamida avtomatik tarzda tayinlanishlari sababli, cheklangan edi. Atributlar tushunchasi faqat foydalanuvchilar va rollar orasiga kiritilgan edi.

Qo'shilishda uchta usul ishlatilishi mumkin: dinamik rolli, atributga mo'ljallangan va rolli. Ammo RBAC bilan ABACni qo'shishda dinamik rollar yagona qulay yondashish hisoblanadi [26].

3.3-rasmda foydalanishni boshqarish modelining strukturasi keltirilgan. Model yuqori va pastki qismlarga ajratilgan.



3.3-rasm. Rol va atribut asosida foydalanishni cheklash modelining strukturasi

Yuqori qismida, foydalanuvchilar va vakolatlar orasidagi statik munosabatlardan iborat, foydalanishni boshqarish uchun RBAC modeli

ishlatiladi. Pastki qismida foydalanishni boshqarishning dinamik qismini boshqarish uchun ABAC modeli ishlatiladi. Bu atributlar asosida foydalanishni nazoratlash qoidalari bo'yicha foydalanuvchilarga bog'liq vakolatlar sonini kamaytiradi.

Modelning statik qismida RBAC modelining aksariyat elementlari, jumladan, foydalanuvchilar, rollar, vakolatlar saqlanadi. Vakolatlarni amallarga (OPS) va ob'ektlarga (OBS) ajratish mumkin. Bunda $Permissions \subseteq OPS \times OBS$. Ob'ektlar amallar atributi kabi quriladi, ya'ni $Permissions=OPS$, foydalanuv-rol munosabatlari (UR), rol-vakolatlar munosabatlari (RR), rollarning vorislik munosabatlari. Undan tashqari, foydalanuvchi uchun foydalanuvchilar atributi (UATT), rol uchun rollar atributi (RATT), vakolatlar uchun ob'ekt atributlari (OATT) aniqlanadi. Ushbu atributlar, vakolatlarni filtrlash maqsadida, modelning dinamik qismiga kiritiladi. Bu foydalanuvchilarning foydalanish huquqlarining kamayishiga sabab bo'ladi.

Mazkur ishda seanslarni o'rnatish jarayoni ikkita bosqichga ajratilgan: *Sessions_Step1* va *Sessions_Step2*. Foydalanuvchilar va rollarning statik o'zaro bog'liqlari o'rnatilganidan so'ng *Sessions_Step1*, foydalanuvchiga tamomila mumkin bo'lgan rollarni dinamik tarzda aniqlash uchun, UATT, RATT va muhit atributlari ENV orqali aniqlangan, foydalanishni boshqarish siyosatini ishga soladi. Foydalanuvchiga tamomila mumkin bo'lgan rollarni dinamik tarzda aniqlash uchun, oldingi bosqichda aniqlangan rollar va mos vakolatlar asosida, *Sessions_Step2*, RATT', OATT va ENV lar orqali aniqlangan, siyosatni ishga solish mumkin.

RBAC va ABAC integratsiyasi ishlab chiqilganligiga ko'p bo'lmaganligiga qaramay, tadqiqotning muhim yo'nalishi sifatida rivojlanmoqda. Ko'p tadqiqot ishlarida [24, 30] ikkata modelni afzalliklarini birlashtirish uchun yangi usulda birlashtirgan foydalanishni boshqarish modeli taklif qilingan. Bu tadqiqot ishlarida foydalanishni boshqarish bo'yicha qarorlar qabul qilishda nafaqat kontekstual ma'lumotlarni hisobga oladigan, tizim elementlari tarkibidan foydalanish orqali ilovalar uchun ham mos bo'lgan resurslardan foydalanishni boshqarishning nozik mexanizmini taqdim etadi. Tadqiqot ishlarida [24, 30] keltirilgan foydalanishni nazoratlash modeliga nisbatan, monografiyada taklif etilayotgan model foydalanishning moslanuvchanroq nazoratini madadlaydi. Tadqiqot ishlarida [24, 30] tavsiflangan, atributlar asosidagi foydalanishni boshqarish siyosatlari faqat foydala-

nuvchi-vakolatlar munosabatlariga qo'llaniladi. Monografuyada taklif etilgan siyosatlar nafaqat foydalanuvchi-vakolatlar munosabatlariga (*Sessions_Step2*), balki foydalanuvchi-rol munosabatlariga (*Sessions_Step1*) ham qo'llanilishi mumkin.

Shunungdek ba'zi bir manbalarda [105] tavsiflangan foydalanishni nazoratlash modeliga nisbatan taklif etilayotgan model teran detallashtirilgan. Ushbu manbada rol-foydalanuvchi va rol-vakolatlar atributlari asosida foydalanishni boshqarish siyosati qo'llaniladi, ammo rol-vakolatlar munosabatlariga siyosat qo'llanganida rolning oddiy atributlari (RATT) ishlatiladi. Mazkur monografiyada RATT va UATT birgalikda ishlatiladi. Bunda, *Sessions_Step1* dan *Sessions_Step2* ga o'tish vaqtida yangi RATT'ni shakllantirish uchun RATTga UATT kiritiladi. RATT' tarkibida foydalaniluvchi atributlarning mavjudligi rol-vakolatlar munosabatlarini aniq nazoratlashga imkon beradi. 3.3-rasmda modelning statik tavsifini akslantiruvchi umumiy strukturasi keltirilgan. Qo'yida modelning dinamik tavsifi, ya'ni foydalanishni nazoratlash xususida yechim qabul qilish jarayonida model komponentlarining qanday ishtirok etganliklarining tavsifi keltirilgan. Mazkur monografiyada ushbu jarayon foydalanishni nazoratlashning ishchi jarayoni deb ataladi va qo'ydagicha tavsiflanadi:

1. Foydalaniluvchi rollarning qiyoslanishini aniqlashda RBAC modelidan foydalanish, ya'ni $U \rightarrow R$;
2. Foydalanishni boshqarish qoidalarini buzuvchi qiyoslanishlarni $U \rightarrow R$dan chiqarib tashlash.
3. Rollar va vakolatlar qiyoslanishlarini ($R \rightarrow P$) aniqlashda RBAC modelidan foydalanish va rollarning yangi atributlarini yaratish uchun UATT va RATTni birlashtirish.
4. RATT, UATT, ENVlarga muvofiq $R' \rightarrow P$dan foydalanish qoidalarini buzuvchi qiyoslanishlarni shunday chiqarib tashlash kerakki, natijada rol uchun yangi qiyoslanishlar tuzilsin.

Yuqorida tavsiflangan harakatlar bajarilganidan keyin, so'nggi foydalanuvchi-vakolatlar qiyoslanishi $U \rightarrow P'$ olinadi. Ushbu qiyoslanish RBAC modeli tomonidan aniqlanuvchi foydalaniluvchi vakolati qismtizimi hisoblanadi, ya'ni $U - P' \subseteq U \rightarrow P$. $U \rightarrow P$ning xavfsizligi RBAC modeli tomonidan kafolatlanganligi sababli, foydalanishni boshqarish modeli faqat ba'zi nojoiz qiyoslanishlarni U→P dan chiqarib tashlaydi. Bu taklif etilayotgan model doirasida qabul qilingan strategiya hisoblanadi [76].

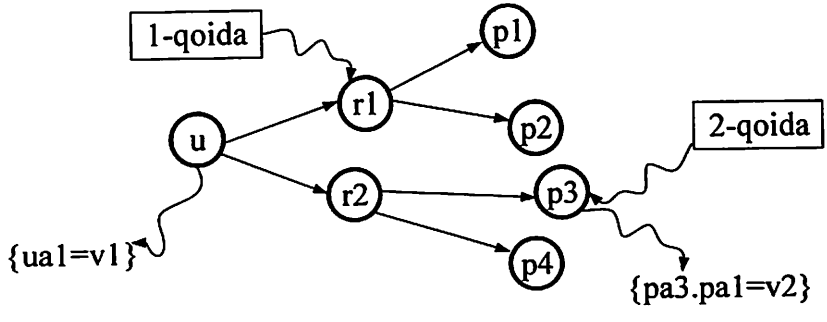
Foydalanishni boshqarishning ishchi jarayoni, aslida tashkilot seansi jarayoni hisoblanadi. RBAC modelida, sessiya faqat foydalanuvchi-rol qiyoslanishini o'rnatadi, seans esa foydalanuvchi-rol qiyoslanishiga qo'shimcha ravishda rollar vakolatlarining qiyoslanishlarini o'rnatadi. Ta'kidlash lozimki, seans vaqtida nafaqat foydalanuvchi-rol va rol-foydalanuvchi munosabatlari aniqlanadi, balki ushbu munosabatlarni filtrlash uchun atributlar asosidagi siyosat qo'llaniladi.

Misol. Faraz qilaylik, foydalanuvchi *u*, qiymati *v1*ga teng *ua1* atributiga ega. *U* foydalanuvchi *r1* va *r2* rollar bilan bog'langan. *R1* - *r1* va *r2* vakolatlari bilan bog'langan. *R2* - *p3* va *p4* vakolatlar bilan bog'langan. *P3*ning qiymati *v2* ga teng, *ra1* atributiga ega. Quyidagi ikkita qoida mavjud:

1-qoida: Agar $u.ua1=v1$ bo'lsa, $u \rightarrow r1$ aktiv emas.

2-qoida: Agar $u.ua1=v1$ va $p3.pa1=v2$ bo'lsa, $r2 \rightarrow p3$ aktiv emas.

Foydalanuvchilar, rollar va foydalanishni boshqarish orasidagi munosabatlarni 3.4-rasmda keltirilganidek tasvirlash mumkin.



3.4-rasm. Foydalanuvchilar, rollar va foydalanishni boshqarish orasidagi elementlarning o'zaro bog'liqligi

1-qoidani qo'llash natijasida *r1* rollar nabori *{R1,R2}* dan chiqarib tashlanadi. So'ngra rollar va vakolatlar munosabatlari aniqlanadi va rol-vakolatlar munosabatlari asosida foydalanishni boshqarish qoidasi olinadi.

2-qoidani qo'llash natijasida *r3* vakolati chiqarib tashlanadi. Axir foydalanuvchi *u* da *p4* vakolati mavjud.

Taklif etilayotgan yondashuv asl model RBACga nisbatan moslanuvchan, chunki sub'ekt atributlari ABAC asosida foydalanish

modelini qurishga imkon beradi. Alohida rollarni yaratish zaruriyati bo'lmaydi, qoidalar atributlarini o'zgartirish kifoya.

Asl model RBACdan foydalanish qoidalarini osongina ma'murlashga imkon beradi, ammo modelning o'zini ishlab chiqish ko'p vaqtni talab etadi. ABAC modelini sozlash oddiy, ammo foydalanuvchilar huquqlarini tahlillash va o'zgartirish muammoli bo'lishi mumkin.

3.1-jadvalda RBAC va ABAC modellarining bo'lishi mumkin bo'lgan kombinatsiyalari keltirilgan.

3.1-jadval

RBAC va ABAC modellarining kombinatsiyalari

U	R	At	Model	Foydalanish huquqlarining akslantirilishi
0	0	0	Aniqlanmagan	----------
0	0	1	Asosiy ABAC	$At_1At_2,...At_n \rightarrow permissions$
0	1	0	Aniqlanmagan	----------
0	1	1	Kombinatsiyalangan RABAC	$R, At_1,At_2,...At_n \rightarrow permissions$
1	0	0	Foydalanish ro'yxati	$U \rightarrow permissions$
1	0	1	ABAC-ID	$U, At_1,At_2,...At_n \rightarrow permissions$
1	1	0	Asosiy RBAC	$U \rightarrow R \rightarrow permissions$
1	1	1	Dinamik rolli RABAC	$U, At_1,At_2,...At_n \rightarrow R \rightarrow permissions$
1	1	1	Atribut asosidagi RABAC	$U, R, At_1,At_2,...At_n \rightarrow permissions$
1	1	1	Rol asosidagi RABAC	$U \rightarrow R \rightarrow At_1,At_2,...At_n \rightarrow permissions$

Jadvaldagi faqat quyidagi uchta kombinatsiya e'tiborga loyiq.

RABAC-dinamik rollar. Rolning an'anaviy strukturasi saqlanadi, ammo rollar atributlarini dinamik tarzda o'zgartirishi imkoni mavjud. Masalan, roldan foydalanishga vaqt bo'yicha yoki bir vaqtda faoliyat ko'rsatuchi tizim ma'murlar soniga cheklov kiritish.

RABAC–atributlar asosida. Ushbu modelda atributlarning biri rol nomi hisoblanadi. Asl RBAC modelidan farqi-rol cheklovlar nabori emas, balki atributlar nomi ekanligi. Ma'murlanishining murakkabligi ushbu modelning kamchiligi hisoblanadi.

RABAC–rollar asosida. Ushbu modelda RBACdagi cheklovlarga sub'ekt atributlari ko'shiladi. Atributlardan foydalanuvchi qoidalar rollar ta'sirini toraytiradi. Ammo, foydalaniluvchi vakolatlarning aniq sozlanishi imkoniyati paydo bo'ladi [76].

RBAC bilan ABACning qo'shilishi, ya'ni kombinatsiyalangan foydalanishni boshqarishda ma'murlashni soddalashtirish va RBACdagi muammolarni bartaraf etish imkoniyatlarini beradi. Ikkala modelning qo'shilishi ichki xavfsizlik tahdidlaridan himoyalamaydi. Mazkur ishda, ichki tahdidlardan xavfsiz sxemani yaratish uchun vakolatlar sathida (rollar sathida emas) vazifalarni taqsimlash-SODni amalga oshirish taklif etiladi. Shunday qilib, foydalanuvchilarning vakolatlari ilgaridek qoladi va tizim taklif etilayotgan modeldagi SODni buzmaydi. SOD, bitta odam nazoratidan qutilish va firibgarliklarning o'sishi yo'llarini kamaytirish uchun, amalga oshiriladi. Ilgari vakolatlar asosidagi SOD statik RBAC modelida amalga oshirilgan edi [21,41].

3.3. Foydalanishni boshqarishning dinamik modelida rollar va vakolatlar asosidagi vazifalar taqsimoti

Vazifalar taqsimoti (SOD) RBAC va ABACdagi ustuvorliklar konsepsiyasiga amal qilinishni ta'minlashda ishlatiladi. Undan tashqari, SOD - masala yechilishida bittadan ortiq inson ishtiroki talab qilinadigan konsepsiya bo'lib, tashkilotni ichki xavfsizlik hujumlari va tahdidlaridan himoyalashda ishlatiluvchi kuchli vosita hisoblanadi. Mohiyatan, SOD alohida shaxs faoliyatiga nisbatan to'xtalishlar va qarshiliklarning mos darajasini amalga oshiradi [21,41]. SOD konsepsiyasiga binoan biznes uchun kritik muhim vazifalarni funksiyalarning to'rtta xiliga ajratish mumkin: avtorizatsiya, saqlash, qaydlash, va muvofiqlashtirish. Ideal tizimda hech kim bittadan ortiq funksiyani bajarishi mumkin emas.

RBAC standartida SOD nizolashuvchi rollar soniga bog'liq. Bunda, tarkibida bitta yoki bir necha nizolashuvchi vakolatlar bo'lgan rol nizolashuvchi rol deb ataladi. Boshqa rollar bilan nizolashuvchi rollar ham bir-birini inkor qiluvchi rollar (Mutually Exclusive Roles-MER) deb yuritiladi. Uning ustiga, MERga tegishli barcha vakolatlar ham bir-birini inkor qilish holatida (Mutually Exclusive -ME) bo'ladi. Foydalanishni boshqarishga atalgan vakolatlar va rollar o'z ichida manfaatlar ixtilofini (Conflict Of Interest-COI) boshlab bermaydi, ammo vakolatlar va rollar orasida COIning mavjudligi joiz hisoblanadi. Aslida,

MER vakolatlari boshqa MERlarning barcha vakolatlari bilan COIni yaratmaydi. Odatda, boshqa MERlar tomonidan juz'iy rozilik bo'lganida, COIni yaratuvchi MERdagi vakolatlarning juz'iy soni mavjud bo'ladi.

Agar vakolatda boshqa vakolat bilan COI bo'lsa, ikkala vakolat bir-birini inkor etuvchi vakolatlar (Mutually Exclusive Permissions-MEP) deb yuritiladi. Masalan, birinchi vakolat-talabnoma yuborish, ikkinchisi-talabnomani maqullash. Birinchi va ikkinchi vakolatlar bir-biri bilan COIga ega, chunki bitta foydalanuvchi bir vaqtda ikkala vakolatni faollashtira olmaydi. Sababi, xodim qanday qilib bir vaqtda "talabnoma"ni yuborishi va o'zining talabnomasini tasdiqlashi mumkin. Tipik SODda yagona nizolashuvchi vakolatning paydo bo'lishi barcha rollarni nizolashuvchi rolga aylantiradi. Undan tashqari, MERdagi barcha vakolatlar MEda bo'lishi lozim. Demak, amalga oshirish SODdagi rollar sathida emas, balki vakolatlar sathida bajarilishi lozim. Agar SOD rollar sathida amalga oshirilsa, boshqa muammolar paydo bo'lishi mumkin.

Rol, SODni qo'llash uchun, MER kabi ma'lum qilinsa, barcha vakolatlar ta'sirlanadi, chunki ular, RBAC standartida ko'rsatilganidek, MEP bo'lib qoladi [9,10]. Shu tariqa, MERdagi nizolashmaydigan vakolatlar ham nizolashuvchi vakolatlar kabi ish tutishni boshlaydi. Natijada, bir-birini inkor qilmaydigan vakolatlar tomonidan avtorizatsiya uchun tasdiqlangan foydalanuvchilarga ushbu vakolatlardan foydalanishlariga ruxsat berilmaydi, chunki ular MER a'zolari hisoblanadi. Shunday qilib, ziddiyat paydo bo'ladi va foydalanuvchilar avtorizatsiyalangan vakolatlardan foydalana olmaydilar. Avval vakolatlardan foydalanuvchilar foydalanar edilar, ammo rol MER bo'lib qolganida, barcha vakolatlar MEP bo'lib qoladi va foydalanuvchi obro'siga putur yetadi.

RBAC standarti [9,10] SODni rollar sathida amalga oshirishi sababli, xavfsizlik ma'muri, ziddiyatli vakolatlarni nazoratlash maqsadida barcha MERlarni kuzatadi. Undan tashqari nizolashuvchi vakolatlar xususidagi axborotni saqlash mexanizmi mavjud emas.

Yuqorida keltirilganlar nuqtai nazaridan, nizolashuvchi vakolatlar xususida yetarlicha axborotning mavjud emasligi sababli, xavfsizlik ma'muri tasodifan bitta rolga ikkita nizolashuvchi vakolatni tayinlashi ehtimoli bor. Bunday rol tayinlangan foydalanuvchilar, ikkita MEPni faollashtirib va ulardan foydalanish huquqini olib, SODni buzishlari

mumkin. Demak, SOD xavfsizlik ma'muri va foydalanuvchilar tomonidan tasodifan buzilishi mumkin.

Rollar asosidagi SOD. Mazkur monografiyada RBAC dinamik modelida vakolatlar sathida SODning samarali amalga oshirilishining tadqiqiga bag'ishlangan. Avval SOD rollar sathida emas, balki vakolatlar sathida amalga oshirilar edi, ammo amalga oshirish RBACning statik modelida bajarilgan [21]. Undan tashqari RBACning atributiv modeli taklif etilgan, ammo model faqat RBACning bazaviy modeli uchun yaroqli edi [21].

RBACning tub ma'nosi-tarkibida atributlar mavjud ob'ektlar, rollar va foydalanuvchilar, ya'ni ma'mur ob'ektlarni, rollarni va foydalanuvchilarni yaratgan vaqtida, ularga atributlarni ham tayinlaydi. Natijada orttirilgan ob'ekt, orttirilgan rol va orttirilgan foydalanuvchi hosil bo'ladi.

Quyida RBAC dinamik modelining, vakolatlarning yaratilishi vaqtidan to rollarga vakolatlarni va foydalanuvchilarga rollarni tayinlash vaqtigacha tavsifi keltirilgan. Dastlab atributlar taqdim etilgan ob'ektlar yaratiladi. Masalan, time= 9:00dan 18:00gacha, IP=192.168.0.1, kun=dushanbadan jumagacha atributli ob'ekt yaratiladi. Ushbu ob'ektdan, faqat foydalanuvchi atributlari atributlar nabori va ularning qiymatlariga mos kelgandagina, foydalanish mumkin. Undan tashqari, ob'ektlar kategoriyalarning konteynerlari orqali tayinladi. Masalan, ma'mur moliya bo'limi uchun, axborot xavfsizligi fakulteti o'qituvchilari va talabalar uchun ob'ektlarni yaratadi. Shu tariqa, ma'mur kategoriyalashning uchta turli konteynerini yaratishi mumkin.

RBAC dinamik modeli tipik RBAC modeliga va atributli RBAC modellariga nisbatan moslashuvchan. Moslashuvchanlikning sababi-vakolatlarni to'rtta turli usullar yordamida yaratish jarayoni:

1. Ma'mur tipik RBACda amalga oshirilganidek, vakolatlarni yaratish uchun ob'ektlarga ta'sirni qo'llashi mumkin.

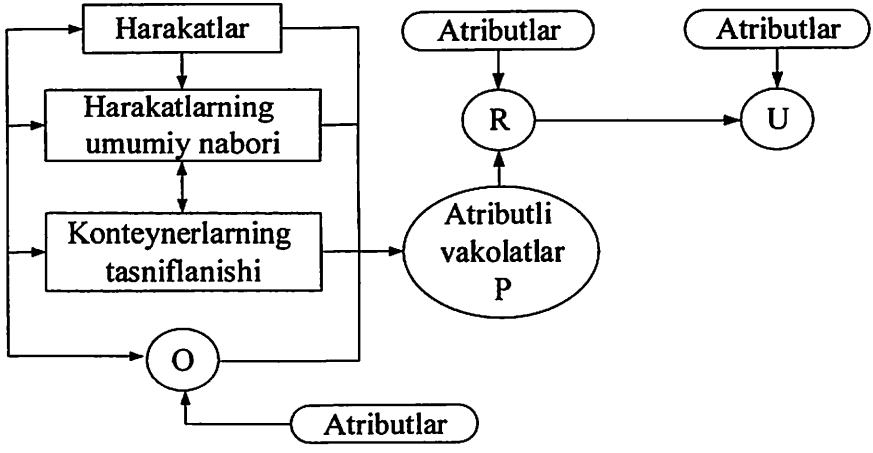
2. Ma'mur bir necha vakolatlarni yaratish uchun kategoriyalar konteynerlariga ta'sirni qo'llashi mumkin.

3. Ma'mur bir necha vakolatlarni yaratish uchun ob'ektlarga ta'sirlarning umumiy naborini qo'llashi mumkin.

4. Ma'mur bir necha vakolatlarni bir vaqtda yaratish uchun kategoriyalash konteynerlariga ta'sirlarning umumiy naborini qo'llashi mumkin. Masalan, agar ta'sirlarning umumiy nabori to'rtta ta'sirdan,

kategoriyalash konteyneri esa beshta ob'ektdan iborat bo'lsa, ushbu konteynerlarning qo'shilishi 20ta vakolatni (4x5 =20) yaratadi.

Ma'mur vakolatlarni, vaziyatga bog'liq holda, turlicha yaratishi mumkin. Agar bitta ob'ekt mavjud bo'lsa, vakolatlarni yaratish uchun esa bir necha ta'sir talab etilsa, ma'mur ob'ektga ta'sirlarning umumiy naborini qo'llashi mumkin. Agar ob'ektlar soni bittadan ko'p bo'lsa va ma'mur barcha ob'ektlarga bir xil ta'sirni qo'llashni istasa, ma'mur umumiy ta'sirli bir necha vakolatlarni yaratish uchun kategoriyalash konteynerlariga ta'sirni qo'llashi mumkin. Shu tariqa ma'mur turli vakolatlarni, tipik RBAC modeliga nisbatan, kam vaqt sarfi evaziga yaratishi mumkin. RBACning dinamik modeli 3.5- rasmda keltirilgan.



3.5-rasm. Atributlar qo'shilgan rollar orasidagi foydalanishni dinamik nazoratlash modeli

Vakolat atributlari ob'ekt atributlari kabi, chunki vakolat-ob'ekt va ta'sir kombinatsiyasi. Shunday qilib, orttirilgan ob'ektlar orttirilgan vakolatlarni yaratadi. Orttirilgan vakolatlar orttirilgan rollarga avtomatik tarzda tayinlanadi.

Agar vakolat atributlari rol atributlari bilan bir xil bo'lsa, vakolatlar ushbu rollarga atributlar yordamida, avtomatik tarzda tayinlanadi. Masalan, *P1, P2* va *P3* vakolatlar atributlari: time=9:00dan

18:00gacha va IP=192.168.0.1. Xuddi shunday ikkita *R1* va *R2.R1* vakolatlar atributlari: time=9:00dan 18:00gacha va IP=192.168.0.0.

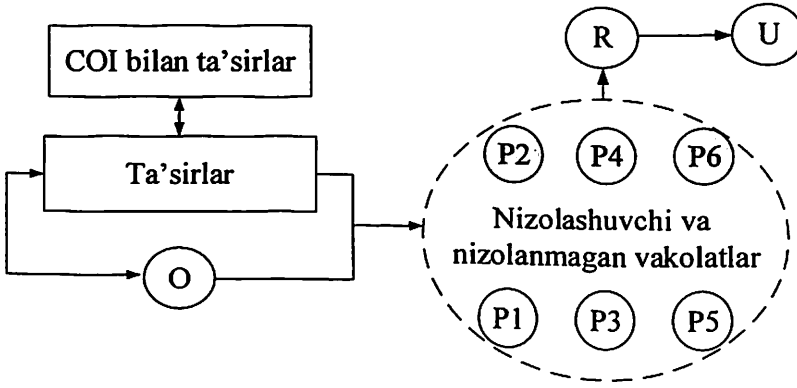
Boshqa tomondan, *R2*da time=9:00dan 17:00gacha va IP=192.168.0.1 atribut mavjud. Tizim *R1* ga *P1, P2, P3* vakolatlarni avtomatik tarzda tayinlaydi, chunki vakolatlar atributlari faqat *R1*ga mos. Foydalanuvchilarga rollarni tayinlash atributlar asosida ham amalga oshiriladi. Foydalanuvchilar va rollar orasidagi moslik kriteriylari ham rollar va foydalanuvchilar atributlari bo'ladi. Tizim foydalanuvchilar va rollar atributlarini qiyoslaydi. Bu, foydalanuvchilarga rollar tayinlanganida, ular atributlarining mosligini ta'minlash uchun zarur (3.4-rasm). Masalan *U1* va *U2* foydalanuvchilar atributlari: time=10:00dan 14:00gacha va IP=192.168.1.10. Yana ikkita qo'shimcha *R4* va *R5.R4* rollarning atributlari: time=9:00dan 18:00gacha va IP=192.168.0.1. Undan tashqari *R5*ning atributlari: time=10:00dan 14:00gacha va IP=192.168.1.10. Demak, tizim *U1* va *U2* foydalanuvchilarga, *R5* rol asosida, foydalanish huquqini taqdim etadi, chunki ularning atributlari va atributlar qiymatlari mos. *U1* va *U2* foydalanuvchilarga *R4* dan foydalanish huquqi berilmaydi, chunki ularning atributlari va atributlar qiymatlari mos emas.

Vakolatlar asosidagi SOD. Vakolatlar asosidagi RBACda foydalanuvchi bir necha nizolashuvchi rollardan foydalanish huquqini olishi mumkin, ammo bir-biri bilan nizolashuvchi vakolatlardan foydalanish huquqini ola olmaydi. Modelning ushbu qismida jarayon yana ta'sirni va ob'ektni yaratishdan boshlanadi. Undan tashqari, ta'sirlar boshqa ta'sirlar manfaatlari (COI)ni hisobga olgan holda yaratiladi. Masalan, "yozish" ta'siri "baholash" ta'siri bilan nizolashadi, "jo'natish" ta'siri "maqullash" ta'siri bilan nizolashadi. Ya'ni, agar xodim ta'til uchun ariza bersa, u o'zining arizasini maqullashi yoki rad etishi mumkin emas. Agar talaba topshiriqni yoki imtihon ishini bajarsa, u o'zining topshirig'ini yoki imtihon ishini baholay olmaydi. Shunday qilib, ma'mur ta'sirlarni yaratadi va ularning boshqa ta'sirlar bilan COI sini aniqlaydi. Foydalanuvchi bitta ob'ekt ustida ikkita nizolashuvchi ta'sirlarni bajarishga urina olmaydi. Ikkita ta'sir va ikkita vakolat orasidagi COI konsepsiyasini bilish talab etiladi. Agar, bir-biri bilan COIga ega ikkita ta'sir bitta ob'ektga qo'llanilsa, ular, bir-biri bilan COIga ega nizolashuvchi vakolatlarni yaratadi [76]. Shu tariqa, foydalanuvchi ikkala vakolatdan bir vaqtda foydalanish huquqini ola olmaydi. Taklif etilayotgan modelga binoan, ta'sirlarning ob'ektlarga

qo'llanilishi natijasida, nizolashuvchi va nizolashmaydigan hisoblanuvchi, ikki kategoriyali vakolatlar yaratiladi (3.6-rasm).

Rasmda P1, P3 va P5 nomli rangsiz ajratilgan vakolatlar nizolashmaydigan vakolatlar, P2, P4 va P6 nomli kulrang bilan ajratilgan vakolatlar esa nizolashuvchi vakolatlar hisoblanadi.

Vakolatlar turli rollarga tayinlanadi, rollar esa foydalanuvchilarga belgilanadi. Foydalanuvchilar, foydalanuvchi vakolatlari domeniga muvofiq, turli rollardan va ularning ichidagi vakolatlardan foydalanish huquqini olishlari mumkin.



3.6-rasm. Nizolashuvchi va nizolanmagan ta'sirli vakolatlar asosidagi SOD

Faraz qilaylik, *R1*-, *R2*-, *R3*- va *R4*-rollari mavjud. Ushbu rollar, odatda, ularga vakolatlar tayinlanganidan so'ng, foydalanuvchiga tayinlanadi. Masalan, *R1*-rol talabalarga, *R2*-rol o'qituvchilarga, *R3*-rol menedjerlarga va ma'muriyat xodimlariga, *R4*-rol dekanlarga atalgan. Ma'mur ushbu rollarni yaratganidan so'ng, ularni muayyan foydalanuvchilarga tayinlaydi. *R1*-rol tarkibida beshta nizolashmaydigan vakolatlar R1,R3,R5, R7 va R9 mavjud. *R2*-rol tarkibida ham beshta vakolat mavjud, ammo ulardan uchtasi R2, R4 va R6 nizolashuvchi, ikkitasi R11 va R13 nizolashmaydigan vakolatlar. *R3*-rol tarkibida beshta vakolat mavjud, ammo ulardan to'rttasi R8, R10, R12 va R14 nizolashuvchi, bittasi R15 nizolashmaydigan vakolat. *R4*-rol tarkibida,

to'rtta nizolashuvchi vakolatlar R16, R18, R20 va R22 mavjud (3.2 - jadval).

3.2 - jadval

Foydalanuvchilarga rol orqali vakolatlarni nizolashli va nizolashsiz tayinlash

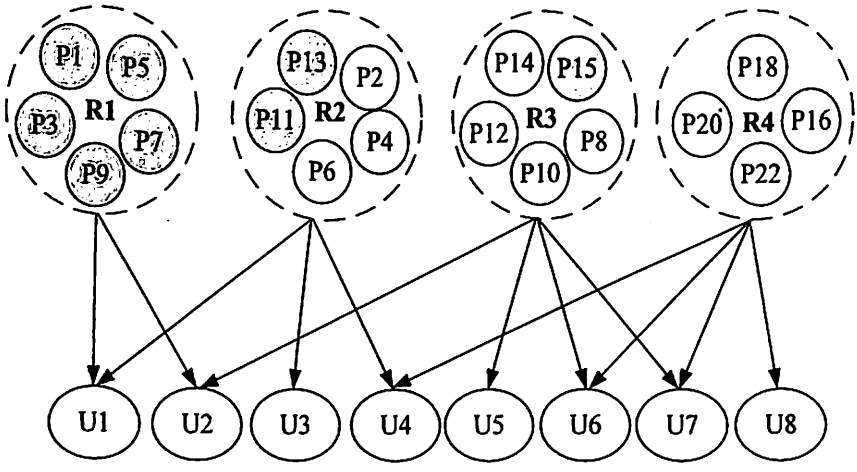
Rol nomi	Barcha vakolatlar	Nizoli vakolat	Nizosiz vakolat	Belgilangan foydalanuvchilar
R1	Beshta	Hech kim	P1, P3, P5, P7, P9	U1, U2
R2	Beshta	P2, P4, P6	P11, P13	U1, U3, U4
R3	Beshta	P8, P10, P12, P14	P15	U2, U5, U6,U7
R4	To'rtta	P16, P18, P20, P22	Hech kim	U4, U6, U7,U8

3.7-rasmda foydalanuvchilarga, tarkibida nizolashuvchi va nizolashmaydigan vakolatlar bo'lgan, rollarni tayinlash sxemasi keltirilgan. Nizolashuvchi vakolatlar nursiz rangga va juft raqamlarga, nizolashmaydigan vakolatlar kulrangga va toq raqamlarga ega.

Rollarni foydalanuvchilarga tayinlash sxemasi 3.2-jadvaldagi ma'lumotlar asosida shakllantirilgan.

Masalan, P2 vakolat P12 va R22 vakolatlar bilan COIga ega. Xuddi shunday, *R2*-roldagi R4 vakolat *R3* dagi R14 vakolat bilan COIga ega va h.

Agar server, jadvalga binoan, nizolashuvchi vakolatga murojaat etsa, ushbu foydalanuvchi avvalroq foydalanilgan, COIga ega boshqa vakolatdan foydalanishi huquqini ola olmaydi. Bu degani, agar foydalanuvchi R8 vakolatga murojaat etsa, u 18 vakolatdan foydalanish huquqini ola olmaydi, chunki ikkala vakolat bir-biri bilan COIga ega.



3.7-rasm. Foydalanuvchilarga, tarkibida nizolashuvchi va nizolashmaydigan vakolatlar bo'lgan, rollarni tayinlash

Nizolashuvchi vakolatlar bilan boshqa nizolashuvchi vakolatlar orasidagi COI 3.3- jadvalda keltirilgan.

3.3-jadval

Nizolashuvchi vakolatlar bilan boshqa nizolashuvchi vakolatlar orasidagi COI

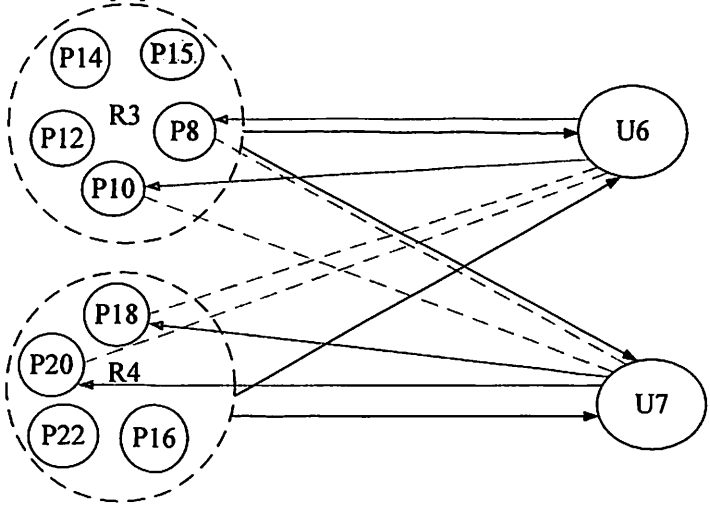
Rollar nomi	**Vakolatlar nomi**	**Vakolatli COI**	**Vakolatga ega rol COI**
R2	P2	P12, P22	R3,R4
R2	P4	P14	R3
R2	P6	P16	R4
R3	P8	P18	R4
R3	P10	P20	R4
R3	P12	P2	R2
R3	P14	P4	R2
R4	P16	P6	R2
R4	P18	P8	R3
R4	P20	P10	R3
R4	P22	P2	R2

Taklif etilayotgan modelga binoan foydalanuvchi ikkita nizolashuvchi vakolatlardan bir vaqtda foydalanish huquqini ola olmaydi. 3.8 - rasmda foydalanuvchilarning bir necha nizolashuvchi vakolatlardan foydalanish sxemasi keltirilgan.

Masalan, *U6*-foydalanuvchi *R3*- va *R4*-rollardan foydalanish huquqini olishi mumkin, ammo u, bir-biri bilan COI ga ega ikkita vakolatdan, faqat bitta nizolashuvchi vakolatdan foydalana oladi.

Ushbu ssenariyga muvofiq *U6*-foydalanuvchi R8 va R10 nizolashuvchi vakolatlardan foydalanish huquqini oladi, ammo u R18 va R20 nizolashuvchi vakolatlardan foydalanishga urinsa, "foydalanish taqiqlangan" xabarini oladi, chunki R8 va R10 vakolatlari bilan R18 va R20 vakolatlari orasida COI mavjud. Xuddi shunday vaziyat *U7*-foydalanuvchiga nisbatan ham sodir bo'ladi.

Shu asnoda, nizolashmaydigan vakolatlarga hech qanday cheklash mavjud emas. Foydalanuvchilar barcha nizolashmaydigan vakolatlardan foydalanish huquqini bemalol olishlari mumkin.



3.8-rasm. Foydalanuvchilarning bir nechta nizolashuvchi vakolatlardan foydalanishi

Shunday qilib, foydalanuvchi vakolatlari doirasi avvalgidek qoladi va SOD ham samarali amalga oshiriladi. Uning ustiga, ma'mur

tomonidan buzilishlar sodir bo'lmaydi, chunki SOD rollar sathida emas, balki vakolatlar sathida amalga oshiriladi.

3.4. Rollarga asoslangan dinamik modelda vakolatlar asosida vazifalarni taqsimlashning amalga oshirilish usullari

Oldingi paragraflarda modelning ikkala qismi batafsil tushuntirilgan edi. Qo'yida modelning ushbu qismlarini, vakolatlar asosida SODni amalga oshiruvchi, to'liq dinamik model RBAC sifatida birlashtirish masalasi, hamda dinamik model RBACning foydalanishni nazoratlashning mavjud modellari bilan qiyosiy tahlili ko'rilgan. Ushbu modelni qurish jarayoni ob'ektlar va ta'sirlarni yaratishdan boshlanadi. Ob'ektlar (ortirilgan ob'ektlar) va ta'sirlar (nizolashuvchi ta'sirlar) yaratilganidan, hamda ularni konteynerlarga tayinlanganidan so'ng, vakolatlarni yaratish jarayoni harakatga keltiriladi.

Ma'mur vakolatlarni to'rtta usul asosida yaratishi mumkin.

1-usul. Ma'mur vakolatlarni yaratish uchun orttirilgan ob'ektlarga ta'sirni COI bilan birga yoki usiz bevosita qo'llashi mumkin. Ushbu usul tipik RBAC modelidagi vakolatlar yaratish usuliga o'xshash, ya'ni ma'mur bir martada bitta vakolatni yaratishi mumkin.

2-usul. Ma'mur bir xil nomli ta'sirli bittadan ko'p vakolatni yaratish uchun konteynerlarni kategoriyalashda ta'sirni COI bilan yoki usiz qo'llashi mumkin. Ushbu usul oldin taklif etilgan usullardan farqlanadi.

3-usul. Ma'mur bitta ob'ekt va turli ta'sirlar uchun bir necha vakolatlarni yaratishda orttirilgan ob'ektlarga ta'sirlarning umumiy naborini qo'llashi mumkin. Ushbu usulni avval taklif etilgan modellarda amalga oshirib bo'lmaydi.

4-usul. Ma'mur bir necha vakolatlarni yaratish uchun kategoriyalash konteynerlariga ta'sirlarning umumiy naborini qo'llashi mumkin.

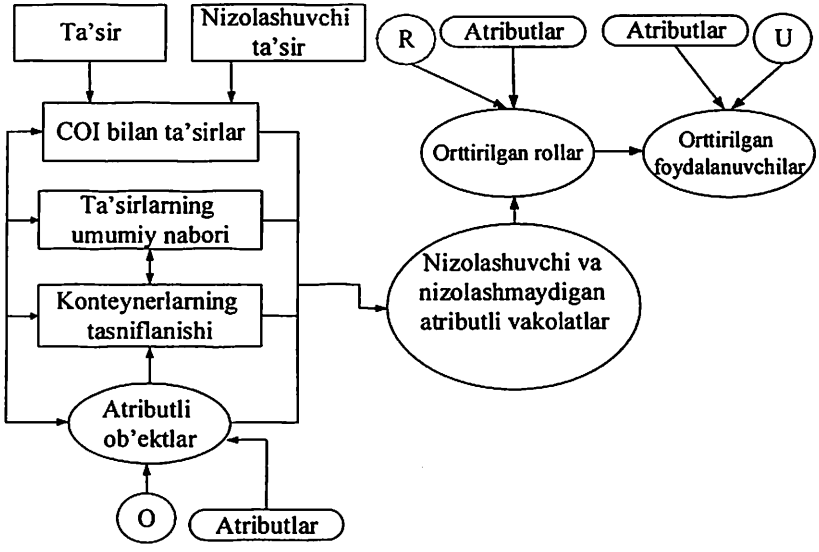
Yuqorida keltirilgan usullar asosida yaratilgan vakolatlar, nizoli – atributli vakolatlar va nizosiz-atributli vakolatlar hisoblanadi (3.9-rasm).

Ushbu sozlanuvchi vakolatlar ilgari amalga kiritilmagan edi. Ma'mur rollarni va foydalanuvchilarni turli atributlar bilan yaratadi. So'ngra atributlangan nizoli va nizosiz vakolatlar avtomatik tarzda atributlangan rollarga (orttirilgan rollarga) tayinlanadi. Barcha vakolatlar, nizoli va nizosiz vakolatlarga o'xshab, bir xil atributlarga ega

rollarga avtomatik tarzda o'tkaziladi. Va nihoyat, orttirilgan rollar orttirilgan foydalanuvchilarga tayinlanadi. Ushbu jarayon ham avtomatik tarzda, ma'mur tomonidan aralashuvsiz, bajariladi (3.9-rasm).

Orttirilgan foydalanuvchilar, o'zlaridagi atributlarga ega rollardan foydalana oladilar. Foydalanuvchilar rollardan, hamda ulardagi vakolatlardan foydalana oladilar. Foydalanuvchi tayinlangan rollardagi nizosiz vakolatlarning barchasidan foydalanish huquqini takroran olishi va tashkilotdagi kundalik vazifalarni bajarishi mumkin.

Undan tashqari, foydalanuvchi nizolashuvchi vakolat Aga murojaat etganida, u nizolashuvchi vakolat Vdan foydalanish huquqini ola olmaydi, chunki A va V vakolatlar bir-birlari bilan COIga ega. Agar, u dastlab vakolat Vga murojaat etsa, u COI tufayli, vakolat Adan foydalanish huquqini ola olmaydi. Taklif etilayotgan model SODni vakolatlar sathida amalga oshiradi.



3.9-rasm. Dinamik modelida vakolatlar asosidagi SODning amalga oshirilishi

Foydalanuvchi turli nizolashmaydigan vakolatlardan, ammo bitta nizolashuvchi vakolatdan foydalanish huquqini olishi mumkin. Shunday qilib taklif etilayotgan modelda SOD hamda foydalanuvchi domeni

buzilmaydi. Undan tashqari taklif etilayotgan model, nizolashuvchi va nizolanmagan vakolatlarni rollarga dinamik taqdim etish evaziga ma'murga yuklamani pasaytiradi. Undan tashqari, rollarni taqsimlash ham dinamik hisoblanadi.

Monografiyada taklif etilayotgan modelning foydalanishni nazoratlashning mavjud modellari bilan qiyosiy tahlili. Qiyosiy tahlil taklif etilayotgan modelning tipik RBAC modeliga nisbatan samaradorligi, hamda taklif etilayotgan model xarakteristikalarini mavjud bo'lgan modellar xarakteristikalari bilan taqqoslash bo'yicha amalga oshirilgan.

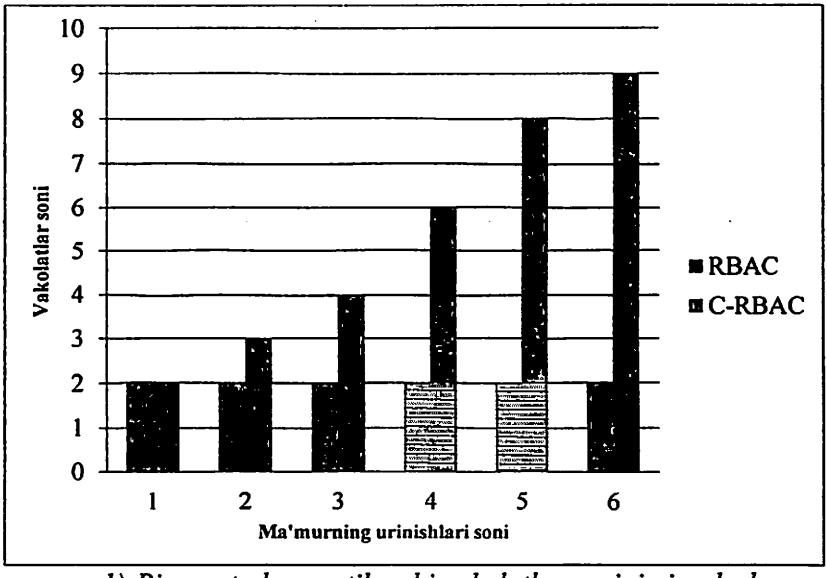
Monografiyada taklif etilayotgan, vakolatlar asosidagi, dinamik RBAC modeli C-RBACning foydalanishni boshqarishning turli modellari bilan taqqoslash 3.10 (1,2)-rasmda grafik ko'rinishda keltirilgan.

Monografiyada taklif etilayotgan model C-RBAC bir vaqtning o'zida bir necha vakolatlarni yaratadi, bu uning, faqat bitta vakolat yaratuvchi RBAC modelidan afzalligini ko'rsatadi.

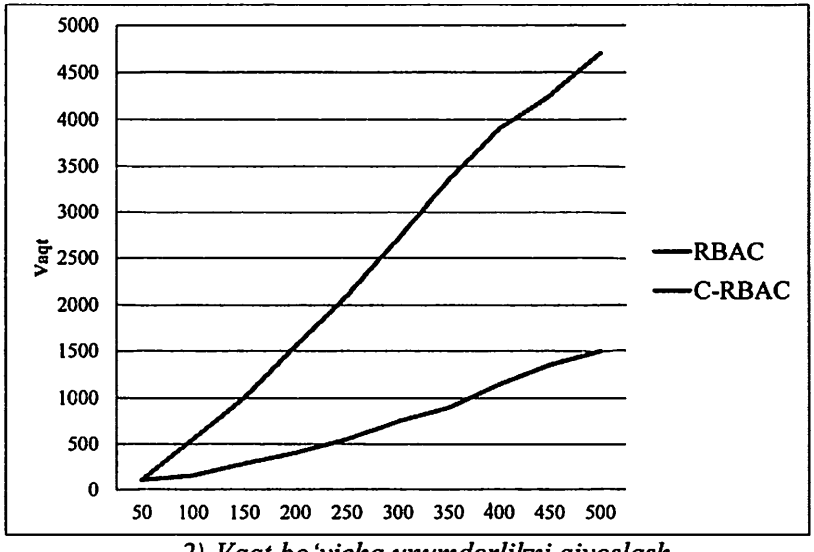
Ma'mur ham bitta vakolatni yaratishi mumkin. Shu tarzda, ushbu ish, ma'murning har bir urinishiga nisbatan vakolatlarning katta sonining yaratilishi evaziga, anchagina yaxshilanadi.(3.9 (1)-rasm).

3.9 (2)-rasmda C-RBAC modelining tipik RBAC modeliga nisbatan vaqt bo'yicha samaradorligi grafik ko'rinishda aks ettirilgan. Ko'k chiziq tipik model RBAC unumdorligini ko'rsatasa, qizil chiziq C-RBAC modeli unumdorligini ko'rsatadi.

Tizim unumdorligida muhim rol o'ynaydigan ikkita omil mavjud. Birinchisi-ma'murning birdaniga bir necha vakolatni yarata olishi jarayoni. Tipik RBAC modelida ma'mur vakolatlarni ketma-ket yarata olishi mumkin. Demak, RBAC modelida vakolatlarni yaratish uchun ko'p vaqt talab etiladi. Taklif etilayotgan modelda esa bir necha vakolatning bir vaqtda yaratilishi evaziga vaqt tejaladi. Ikkinchisi-vakolatlarning rollarga, rollarning foydalanuvchilarga tayinlash jarayoni. RBAC modelida ushbu jarayon qo'lda amalga oshiriladi. Bu butun diqqat-e'tiborni talab qiladigan, sermehnat ish.



1) Bir martada yaratiluvchi vakolatlar sonini qiyoslash



2) Vaqt bo'yicha unumdorlikni qiyoslash

3.10-rasm. RBAC a C-RBAC modellarining qiyoslash grafiklari

Monografiyada taklif etilayotgan modelda vakolatlarni rollarga, rollarning foydalanuvchilarga tayinlash avtomatik tarzda amalga oshiriladi. 3.4-jadvalda foydalanishni nazoratlash modellari xarakteristikalarining tahlili keltirilgan.

3.4-jadval

Foydalanishni nazoratlash modellari xarakteristikalarining tahlili

Modellar / Xarak-teristikalari	RBAC	ABAC	RABAC	Taklif etilayotgan C-RBAC
Dinamikligi	-	+	+	+
Eng kam vakolatlar	+	-	+	+
Oddiylik	+	-	+	+
Moslashuvchanlik	-	+	-	+
SODning samarali amalga oshirilishi	-	-	-	+
Siyosatni aniqlash va texnik xizmat ko'rsatish	+	-	+	+
Ma'murga ish jarayonining yangilligi	-	+	+	+

SOD ni vakolatlar sathida ko'rib chiqadigan dinamik RBAC modeli atributlar qo'shilishi bilan-moslashuvchanlikni ta'minlash, yuklamani kamaytirish va dinamik xatti-harakatlarga murojaat qilish uchun amalga oshirildi. SODni vakolatlar asosida amalga oshirishning kombinatsiyalangan foydalanishni boshqarish C-RBAC modeli taklif etildi. Bunda foydalanuvchilarning vakolatlari ilgaridek qoladi va tizim taklif etilayotgan C-RBAC model doirasida SODni buzmaydi. SOD alohida shaxs faoliyatiga nisbatan to'xtalishlar va qarshiliklarning mos darajasini amalga oshiradi.

C-RBAC modeli dinamik xarakterga ega va SODni samarali amalga oshiradi. Uning ustiga, vakolatlarni to'rtta usul asosida yaratish jarayoni ma'mur uchun tashvish tug'dirmaydi, chunki u ma'murlashning oddiyligini va vaqtning tejamligini ta'minlash uchun ko'zda tutilgan.

C-RBAC modelining bazaviy strukturasi RBAC modeliga asoslanganligi sababli, C-RBAC modeli oddiylikni, eng kam imtiyozlikni va xizmat ko'rsatishda yengillikni ta'minlaydi. SODning samarali amalga

oshirilishi-taklif etilayotgan modelning ajoyib xususiyatlaridan biri. Monografiyada taklif etilayotgan model ma'murlashning oddiyligini, faoliyatning dinamikligini, qat'iy xavfsizlikni va SODning samarali amalga oshirilishini ta'minlaydi.

Monografiyada taklif etilayotgan C-RBAC modeli dinamik xarakterga ega va SODni samarali amalga oshiradi. Uning ustiga, vakolatlarni to'rtta usul asosida yaratish jarayoni ma'mur uchun tashvish tug'dirmaydi, chunki u ma'murlashning oddiyligini va vaqtning tejamligini ta'minlash uchun ko'zda tutilgan. C-RBAC modelining bazaviy strukturasi RBAC modeliga asoslanganligi sababli, C-RBAC modeli oddiylikni, eng kam imtiyozlikni va xizmat ko'rsatishda yengillikni ta'minlaydi. SODning samarali amalga oshirilishi-taklif etilayotgan modelning ajoyib xususiyatlaridan biri. Monografiyada taklif etilayotgan model ma'murlashning oddiyligini, faoliyatning dinamikligini, qat'iy xavfsizlikni va SODning samarali amalga oshirilishini ta'minlaydi.

IV-BOB. FOYDALANISHNI ROLLI CHEKLASH TIZIMINI QURISH USULLARI VA ALGORITMLARI

4.1. Rollar asosida foydalanishni boshqarishning dinamik modelining tahlili

Foydalanishni boshqarish modellarini tahlillash, ayniqsa formal tahlillash, juda muhim va murakkab masala hisoblanadi. RBAC modelidan boshlab, ko'pdan ko'p formal modellar o'rganilgan, hamda ushbu modellarning tahlillash usullari taklif qilingan [21, 23]. RBAC modelini o'rganish bo'yicha juda kam manba mavjud. Masalan, [24, 30, 105] manbalardagi modellar rasman sinovdan o'tkazilmagan. [9] manbada foydalanishni boshqarish modelida ikkita xususiyat-to'lalik va monotonlik aniqlanadi. Bu ikki xususiyat, foydalanishni boshqarish bo'yicha yechim qabul qilish qoidalariga taalluqli, qaror qabul qilish jarayonining o'ziga xos xususiyatlari, modelda hisobga olinmaydi. Monografiyaning 2.3-bo'limida ta'kidlanganidek, foydalanishni rolli cheklash uchun qaror qabul qilish, strukturasi o'zgartiriluvchi modelga ishlash ishonchligini oshirish imkoniyatini taqdim etadi. Quyida RBAC modeliga mos uchta xususiyat-foydalanishni boshqarish, moslashuvchanlik va qaror qabul qilishning samaradorligi muhokama qilinib, modelning ushbu uchta xususiyat nuqtai nazaridan, [24, 30, 105] manbalardagi modellardan afzalligi isbotlanadi.

Foydalanishni boshqarishni detallashtirish. RBAC, RABAC yoki kombinatsiyalangan model bo'lishidan qat'i nazar, modelning maqsadi-foydalanuvchilar va vakolatlar orasidagi o'zaro bog'liqlikni, ya'ni joriy seansda foydalanuvchi olishi mumkin bo'lgan vakolatlarni aniqlash. Ushbu maqsadga erishish uchun RBAC modeli foydalanuvchilarni rollarga asoslangan vakolatlar bilan statik tarzda bog'laydi. RABAC foydalanuvchi-vakolatlar dinamik munosabatlarini aniqlash uchun atributlar asosida foydalanishni boshqarish qoidalarini ishlatadi; kombinatsiyalangan model C-RBAC avval foydalanuvchilar va vakolatlar orasidagi statik munosabatlarni aniqlash uchun RBACdan foydalanadi, so'ngra foydalanuvchi-vakolatlar munosabatlarini dinamik pasaytirish uchun RABACdan foydalanadi.

Monografiyada taklif etilayotgan model ham, [24,30,105] manbadagi modellar ham kombinatsiyalangan model yondashuvidan foydalanadi, ya'ni avval statik munosabatlarni aniqlanadi, so'ngra bu munosabatlarni dinamik pasaytirish uchun atributlardan foydalaniladi.

Foydalanuvchilar va vakolatlar orasidagi bog'lanishlarni qisqartirish ushbu modellarning o'ziga xos xususiyati hisoblanadi. Foydalanuvchilar va vakolatlar orasidagi bog'lanishlarni qisqartirish jarayoni turli atributlarni talab qilinadi. Shunday qilib, ushbu tadqiqot ishida atributlardan foydalanishni boshqarishni detallashtirish o'lchovi sifatida foydalaniladi.

RBAC modelida foydalanishni boshqarishni detallashtirish darajasi, foydalanuvchi-vakolatlar munosabatlarini qisqartirish jarayonida, foydalaniluvchi atributlarning maksimal soniga bog'liq.

Yuqorida keltirigan o'lchov asosida, turli RABAC modellarining foydalanishni detallashtirish darajalarini taqqoslash mumkin. Avvalo foydalanuvchilar va vakolatlar orasidagi munosabatlarni qisqartirishda qanday atributlar ishlatilishini aniqlash lozim. Rasmiy tahlil ko'rsatadiki, [24, 30] manbalardagi model dastlab, foydalanuvchilar va vakolatlardan tarkib topgan tartiblangan juftlikni (UP, $UP \subseteq USERS \times PERMS$) generatsiyalash uchun RBACdan foydalanildi, so'ngra UPdagi har bir juftlik (U, P) aktiv yoki aktiv emasligini aniqlash uchun atributlarga asoslangan siyosatdan foydalanadi, bu aslida {T, F} to'plamiga UPdan akslantirishni o'rnatadi. Qiyoslanishni qurishda model foydalanuvchi atributlaridan, rollar atributlaridan va vakolat atributlaridan foydalanishi lozim. Akslantirishni quyidagicha ifodalash mumkin:

$$up\_tf: UP \times 2^{UATT} \times 2^{RATT} \times 2^{OATT} \times 2^{ENV} \rightarrow \{T, F\}. \quad (4.1)$$

up_tf akslanishda *dom (up_tf)* o'z ichiga $2^{UATT} \times 2^{OATT} \times 2^{ENV}$ larni oladi, bu yerda UATT-foydalanuvchi atributlari, RATT-rol atributlari, OATT- ob'ekt atributlari, ularni vakolat atributlari sifatida ko'rish mumkin, ENV-esa muhit atributlari. *dom (up_tf)* strukturasidan quyidagi xulosa qilish mumkin: *UP* va *{T, F}* orasidagi munosabatni aniqlashda foydalanuvchi atributlarining maksimal soni $|UATT|+|RATT|+|OATT|+|ENV|$ ga teng bo'ladi. Yuqorida keltirilgan tahlil jarayonining imkoniyati-UPni {T, F}ga qiyoslash strukturasiga aniqlik kiritish, so'ngra atributlarni qo'llash asosida modelning foydalanishni boshqarishni detallashtirish darajasini hisoblash.

Ushbu tahlil usulini [105] manbadagi modelga qo'llab, ushbu modelning foydalanishni boshqarishning detallashtirish darajasini hisoblash mumkin. Modellarning o'ziga xos xususiyati shundaki, foydalanishni boshqarish bo'yicha qaror qabul qilishdagi jarayon ikki bosqichga bo'linadi. Birinchi bosqichda foydalanuvchilar va rollardan

tarkib topgan tartiblangan juftliklar naborini (UR, $UR \subseteq USERS \times ROLES$) qurish uchun RBAC modeli ishlatiladi, so'ngra URni $\{T, F\}$ga akslantirish o'rnatiladi. Rolning vakolatlar naboriga mosligi sabablı, qiyoslanish har bir U, P juftligining aktiv yoki aktiv emasligini aniqlay olmaydi. Demak, birinchi bosqich modeldan foydalanishni boshqarishni detallashtirishni ko'zda tutmaydi. Ikkinchi bosqichda, RBACdan foydalanib, rollar va vakolatlardan tarkib topgan (RP, $RP \subseteq ROLES \times PERMS$) tartiblangan juftliklar naborini o'rnatiladi. Rolni foydalanuvchi agent sifatida ko'rilishi mumkinligi sababli, yaratilgan RP nabori o'rnatilgani UP naborining o'rnatilganini ko'zda tutadi va atributlar asosidagi keyingi siyosatlar UPga ham taalluqli. [105] manba tavsifiga ko'ra, UPni $\{T,F\}$ga akslantirishni o'rnatishning ikkinchi bosqichini quyidagicha ifodalash mumkin:

$$up\_tf: UP \times 2^{RATT} \times 2^{OATT} \times 2^{ENV} \rightarrow \{T, F\}. \quad (4.2)$$

(4.2) ifodadan ko'rinib turibdiki, $|RATT|+|OATT|+|ENV|$ atributlar $|UATT|+|RATT|+|OATT|+|ENV|$ atributlardan shubhasiz kam. (4.1) ifodada RATT atributi UATT atributi tarkibida, ya'ni $RATT \subseteq UATT$, ma'lumki $|RATT| \leq |UATT|$. Demak, [24, 30] manbadagi model, [105] manbadagi modelga nisbatan detallanishi yuqori.

Mazkur monografiya ishida taklif etilayotgan modelning foydalanishni boshqarishni detallashtirish jarayoni ham ikki bosqichga bo'lingan. Birinchi bosqich [105] manbadagi modeldagidek farqi ikkinchi bosqichda. Ushbu bosqichga binoan (4.2) ifoda strukturasi quyidagiga o'zgartiriladi:

$$up\_tf: UP \times 2^{RATT'} \times 2^{OATT} \times 2^{ENV} \rightarrow \{T, F\}. \quad (4.3)$$

(4.3) ifodada $RATT' = UATT \cup RATT$. Demak, (4.3) quyidagiga ekvivalent:

$$up\_tf: UP \times 2^{UATT} \times 2^{RATT} \times 2^{OATT} \times 2^{ENV} \rightarrow \{T, F\}. \quad (4.4)$$

(4.4) ifoda strukturasidan ko'rinib turibdiki, monografiya ishida taklif etilayotgan modelning foydalanishni boshqarishning detallashtirish darajasi [24, 30] manbalardagi modeldagidek, ammo [105] manbadagi modeldan yaxshiroq.

3.2-bo'limida keltirilgan misolni ko'raylik. Faraz qilaylik, $u.ua1=v1$ va $p3.\ pa1=v2$ bo'lganida ma'mur u foydalanuvchining $p3$ vakolatiga ega bo'lmasligini xohlaydi. Agar [105] manbadagi modeldan foydalanilsa, ushbu talab qondirilmaydi, chunki, rol-vakolat munosabatlarini aniqlashda, foydalanuvchi atributlari foydalanuvchi hisoblanmaydi. Shu vaqtda monografiya ishida taklif etilayotgan model ushbu

talabni madadlaydi, chunki rol-vakolat munosabatlarini aniqlashda foydalanuvchi atributlar tarkibida foydalanuvchi atributlari, rol atributlari, muhit atributlari va ob'ekt atributlari (vakolat atributlari) mavjud. Turli foydalanuvchi atributlar modelning foydalanishni boshqarishini turli darajali detallashtirilishiga olib keladi. Taklif etilayotgan model, foydalanuvchilar va vakolatlar atributlariga muvofiq, rollar va vakolatlar orasidagi munosabatlarni boshqarishni yetarlicha detallashtirishi mumkin.

Moslashuvchanlik. Moslashuvchanlik nisbiy tushuncha: odatda, model boshqasiga nisbatan moslashuvchan deb aytiladi. [24, 30] manbalardagi modelni monografiya ishida taklif etilayotgan model bilan taqqoslab, monografiya ishidagi modelning nafaqat (4.1) kabi akslanishga, balki *UR*ni *{T,F}*ga akslanishga ega ekanligini aniqlash mumkin:

$$ur\_tf: UR \times 2^{UATT} \times 2^{RATT} \times 2^{ENV} \rightarrow \{T, F\}. \qquad (4.5)$$

Ushbu atributlar va muhit e'tiborga olinmaganida, ishdagi model tarkibida $UR \rightarrow \{T, F\}$ va $UP \rightarrow \{T, F\}$ mavjud bo'ladi. Bu ikkita akslanishni quyidagicha qayta yozish mumkin: $U \times R \rightarrow \{T, F\}$ va $U \times P \rightarrow \{T, F\}$, bu yerda U-*USERS*ni, R- *ROLES*ni va R- *PERMS*ni ifodalaydi. *R*ning *R* to'plamiga tegishli ekanligi ushbu ikkita akslanishlarni quyidagi akslanishga birlashtirishga imkon beradi:

$$upp\_tf: U \times 2^{P} \rightarrow \{T, F\}. \qquad (4.6)$$

Shunday qilib, moslashuvchanlik o'lchoviga ta'rif berish mumkin. Moslashuvchanlik o'lchovi- *dom(upp_tf)* komplektining maksimal sig'imi *(upp_tf)*, ya'ni $|dom(upp\_tf)|$ qiymati. [24, 30] manbalardagi model moslashuvchan, chunki $|U \times 2^{P}| > |U \times P|$. Bunga asosan aytish mumkinki, monografiya ishida taklif etilayotgan model ham moslashuvchan, chunki ular teng.

3.2-§da keltirilgan misolni ko'raylik. Taklif etilayotgan model *U* va *P1* va *P2* oralaridagi munosabatlarni bir vaqtda boshqarish qoidalarini ishlatishi mumkin, bunga rollarni boshqarish evaziga erishiladi. Ammo, [24,30] manbalardagi modelda, agar rol vakolatning atributi hisoblanmasa, bunday boshqarishga erishish oson emas. Taklif etilayotgan model *U* to'plami va 2^{P} orasidagi munosabatlarni boshqarish mumkin, [24, 30] manbalardagi model esa *U* to'plam va *P* to'plam orasidagi o'zaro bog'liqlikni nazoratlaydi. Demak, taklif etilayotgan modelning moslashuvchanligi yuqori.

Qaror qabul qilish samaradorligi. Monografiyada modelning

qaror qabul qilish samaradorligi uning bajarilishi tezligini aks ettiradi. RABAC modeli uchun qaror qabul qilish samaradorligi, asosan, foydalanishni nazoratlash siyosatining bajarish tezligi orqali belgilanadi. Chunki, foydalanishni boshqarish bo'yicha qaror qabul qilish jarayonida, RABACning har bir modelida foydalanuvchi-rol va rol-vakolat munosabatlarini aniqlash uchun RBAC dan foydalanish jarayoni bir xil. Ushbu modellar orasidagi farq atributlarga asoslangan siyosatlarda. Monografiyada va [105] manbada bayon etilgan siyosat (4.1) akslanishga va (4.5) munosabatga taalluqli. [24,30] manbada bayon etilgan siyosat faqat (4.1) akslanishga taalluqli.

Foydalanishni nazoratlash siyosatini amalga oshirishda avval siyosatni aniqlash, so'ngra uni tahlillash kerak. Siyosatni amalga oshirish samaradorligi, asosan, siyosatni aniqlash usuliga va uni tahlillash algoritmiga bog'liq. Siyosatni aniqlash samaradorligini oshirish uchun, rollarga va vakolatlarga bog'lash lozim, chunki foydalanishni boshqarish tizimlarida rollar va vakolatlar barqaror va odatda, ularning soni foydalanuvchilar soniga nisbatan kam.

Har bir rol va vakolat foydalanishni nazoratlashning mos siyosatiga ega deb faraz qilinsa, siyosatni aniqlash vaqtining murakkabligi, birinchi navbatda, rollar va vakolatlarning soniga bog'liq bo'ladi.

Monografiyada taklif etilayotgan modelda va [29] manbadagi modelda siyosatni aniqlashning vaqtiy murakkabligi-$|R|+|P|$ning funksiyasi, ya'ni $f(|R|+|P|)$, [24, 30] manbalardagi model uchun vaqtiy murakkablik-$|P|$ funksiyasi, ya'ni g $(|P|)$. Agar rol va vakolatning ikkalasi iyerarxik strukturada saqlansa, f va g logarifmik funksiyalar bo'lishi mumkin. Aksariyat ilovalarda rollar sonining, odatda, vakolatlar sonidan kamligini hisobga olgan holda, quyidagini yozish mumkin:

$$f(|R|+|P|) \leq f(2|P|) = log2 + log(|P|) = log2 + g(|P|) \qquad (4.7)$$

(4.7) ifodadan ko'rinib turibdiki, tavsiya etilayotgan model va [24, 30, 105] manbalardagi modellar, foydalanishni boshqarish siyosatini aniqlashning vaqtiy murakkabligi bo'yicha ziddiyatli emas va, shu sababli, rekonfiguratsiyalashga qaror qabul qilishda samaradorligi bo'yicha umuman, bir xil [72, 77].

4.2. Foydalanishni rolli boshqarishning dinamik modelidagi rasmiy spetsifikatsiya va algoritmlar

An'anaviy RBACda foydalanuvchilar, ishlash muhitini amalga oshirmasdan, rollar va mos amallar bo'yicha muayyan vakolatga ega, bu xavfsizlikning yashirin muammolarini osongina vujudga keltiradi. Dinamik RBAC ushbu oqimda bajarilishi lozim bo'lgan joriy vakolatni tekshiradi va vakolatning bajarilishi mumkinligini yoki mumkin emasligini aniqlaydi.

RBACning ichki muvofiqligini va ba'zi algebraik xususiyatlarini tekshirishda soddalashtirilgan modellash tizimi Alloydan foydalaniladi. Alloy-birinchi tartibli mantiqiy modellash tili [23]. Modelda Java singari, ob'ektga yo'naltirilgan dasturlash tillari sinfiga ekvivalent bo'lgan, *sig Name {}* tilining konstruksiyasi ishlatiladi. Uning tarkibida sinfning barcha ob'ektlari va ushbu ob'ektlar orasidagi munosabatlar mavjud. RBAC modelidagi asosiy naborlar va funksiyalar 4.1-jadvalda keltirilgan. Ushbu naborlar va funksiyalar RABACga ham qo'llaniladi. Monografiyada, atributlar asosida foydalanish siyosatini yaratish uchun, naborlar va funksiyalar qo'shiladi (4.2-jadval):

4.1-jadval

RBAC modelidagi asosiy naborlar va funksiyalar

- USERS, ROLES, OPS i OBS (foydalanuvchilar, rollar, amallar va ob'ektlar);
- $PERMS \in 2^{(OPS \times OBS)}$, vakolatlar nabori;
- SESSIONS, seans (sessiya)lar nabori;
- user sessions (u:USERS)$\rightarrow 2^{SESSIONS}$, foydalanuvchi *u*-ni seanslar naboriga akslantirish;
- avail_sessiya_roles (u:USERS)$\rightarrow 2^{ROLES}$, foydalanuvchi *u*-ni rollar naboriga akslantirish;
- avail_session_perms (rs:2^{ROLES}) $\rightarrow$ 2^{PERMS}, rollar naborini, vakolatlar to'plamiga akslantirish;
- $UA \subseteq USERS \times ROLES$ foydalanuvchilar va rollarning qiyoslash;
- $PA \subseteq ROLES \times PERMS$ rol bilan vakolatni qiyoslash.

-avail_session_roles: ushbu funksiya seans o'rnatilishining birinchi fazasida ishlatiluvchi, foydalanuvchilar va rollar orasidagi munosabatlarni ifodalaydi, ya'ni *Sessions_Step1*;

-avail_session_perms: ushbu funksiya senas o'rnatilishining ikkinchi fazasida, ishlatiluvchi rollar va vakolatlar orasidagi munosabatlarni ifodalaydi, ya'ni *Sessions_Step2*;

- Set ENV: ushbu nabor dinamik nabor bo'lib, uning elementlari muhit atributlariga mos keluvchi joriy qiymatlarni ifodalaydi.

-filter_r: ushbu funksiya rolga asoslanib, ushbu rol uchun ishlatilishi mumkin bo'lgan barcha foydalanishni boshqarish siyosatini tanlab oladi. Har bir foydalanishni boshqarish siyosati foydalanuvchi atributlarga, rol atributlarga va muhit qiymatlariga asoslangan. Funksiya qiymati Tga teng bo'lsa, bu foydalanuvchilar va rollar o'rtasidagi munosabatlarning amalga kirishini bildiradi, aks holda munosabatlar yaroqsiz hisoblanadi. Ushbu funksiya *Sessions_Step2*da foydalanuvchilar rollarining qiyoslanishlarini dinamik aniqlash uchun ishlatiladi.

-filter_p: ushbu funksiya vakolatlarga muvofiq barcha foydalanuvchi foydalanishni boshqarish siyosatlarini tanlab oladi. Har bir foydalanishni nazoratlash siyosati yangi rol atributlariga (RATT), ob'ekt atributlariga va muhit qiymatlariga asoslangan. Ushbu funksiya *Sessions_Step2*da rollar vakolatlari qiyoslanishlarini dinamik aniqlash uchun ishlatiladi.

4.2-jadval

RABAC uchun qo'shimcha naborlar va funksiyalar

- ENV vaqt, harorat va namlik kabi atrof-muhit xususiyatlarining joriy qiymatlarini ifodalaydi.
- *UATT, RATT* va *OATT,* mos ravishda, foydalanuvchi, rol va ob'ekt atributlari funksiyalarining cheklangan naborini ifodalaydi.
- *UATT∪RATT∪OATT* dagi har bir atribut uchun *Range (att)* atributning diapazonini, elementar qiymatlarining cheklangan naboriini ifodalaydi.
- *attType:UATT∪RATT∪OATT→{set, atomic}*. Atributlarni belgilangan qiymatlar bo'yicha o'rnatadi.
- Har bir atribut funksiyasi USERS va OBSdagi elementlarni berilgan qiymatlarga qiyoslanadi.

$$\forall ua \in UATT.ua: USERS \rightarrow \begin{cases} Range\ (ua) \text{ if att Type } (ua) = atomic \\ 2^{Range\ (ua)} \text{if att Type } (ua) = set \end{cases}$$

$\forall ra \in RATT.ra: ROLES$

$$\rightarrow \begin{cases} Range\ (ra) \text{ if att Type } (ra) = atomic \\ 2^{Range(ra)} \text{if att Type } (ra) = set \end{cases}$$

$\forall oa \in OATT.oa: PERMS$

$$\rightarrow \begin{cases} Range\ (oa) \text{ if att Type } (oa) = atomic \\ 2^{Range\ (oa)} \text{if att Type } (oa) = set \end{cases}$$

- filter_r (r:*ROLES*)$\rightarrow 2^{POLICIES\_R}$, rollar va siyosatlar to'plamini akslantirish.
- Har bir $pr \in POLICIES\_R$.
- pr: $USERS \times ROLES \times 2^{UATT} \times 2^{RATT} \times 2^{ENV} \rightarrow \{T,F\}$.
- filter_p(p:*PERMS*)$\rightarrow 2^{POLICIES\_P}$, vakolatlar siyosati to'plamini akslantirish.
- Har bir pp∈POLICIES_P.
- $pp: USERS \times ROLES \times PERMS \times 2^{RATT} \times 2^{OATT} \times 2^{ENV} \rightarrow \{T,F\}$,
- bu yerda $RATT' = UATT \cup RATT$.

Ushbu yangi naborlar va funksiyalardan tashqari, monografiya ishida OATT atributining funksiyasi o'zgaradi, u endi ob'ektdan qiymatga akslanishi, balki vakolatni qiymatga akslanishi, chunki monografiya ishida ob'ekt vakolat atributi sifatida ko'riladi, shuning uchun ob'ekt atributi ham vakolat atributi hisoblanadi.

4.3-jadval

Taklif etilayotgan modeldagi qo'shimcha naborlar va funksiyalar

- CatCon: tarkibida atributli ob'ektlar bo'lgan kategoriyalar konteynerlari uchun ishlatiladi.
- GActS: tarkibida manfaatlar ixtilofi (COI) bo'lgan harakatlarning umumiy nabori uchun ishlatiladi.
- *ops* (g_act:*GActS*)$\rightarrow$*{ops⊆OPS}*, COIli harakatlar harakatlarning umumiy naboriga akslantirish. Shunday qilib, umumiy harakatlar bilan bog'langan COIli harakatlar, g_act ni o'rnatadi.
- *obj* (*cat_con:* *CatCon*)$\rightarrow$*{obj⊆OBJ}*, ob'ekt atributlarini kategoriyalarning konteynerlariga akslantirish. Shunday qilib, orttirilgan ob'ektlar kategoriyalangan konteyner *cat_con* bilan bog'langan.
- $PERMS \in 2^{(OPS \times OBS)} \cup 2^{(OPS \times CatCon)} \cup 2^{(GActS \times CatCon)} \cup 2^{(GActS \times OBS)}$, nizolashuvchi va nizolashmaydigan atributli vakolatlar nabori.
- $PASIGN \subseteq PERMS \times ROLES$ orttirilgan vakolatlarni, orttirilgan

rollarga akslantirish.

- *Permission_auto_assigned (r:ROLES)→2^{PERMS}*, atributlardan foydalanib, nizolashuvchi va nizolashmaydigan vakolatlar naboriga, atributli rol-*R* ni avtomatik akslantirish.
- *Permission_auto_assigned (r)={p∈PERMS\(p, r)∈PASIGN}*
- *UASIGN⊆USERS×ROLES* atributli foydalanuvchilarni atributli rolga tayinlash munosabati.
- *Users_auto_assigned:(r:ROLES)→2^{USERS}*, atributlar yordamida orttirilgan foydalanuvchilar naboriga, *r*-atributli rolni avtomatik qiyoslash.
- *Users_auto_assigned (r)={u∈USERS\(u, r)∈UASIGN}*
- Activate: foydalanuvchi vakolatlarni aktivlashtirish uchun, ma'lum bir vakolatli foydalanuvchiga foydalanish huquqini beruvchi funksiya.
- ¬Activate: ushbu funksiya foydalanuvchining ma'lum bir vakolatdan foydalanishini cheklash uchun ishlatiladi.
- Activated: bu ko'rsatkichni qaytarish uchun ishlatiladigan funksiya. Bundan tashqari, u foydalanuvchi qaytish qiymatidan ma'lum bir vakolatni aktivlashtirgani haqida ham xabar beradi.
- ¬Activated: ushbu funksiya foydalanuvchining muayyan vakolatni aktivlashtirmaganini ko'rsatish uchun ishlatiladi.
- ConfP: nizolashuvchi ikkita vakolatni tayinlovchi funksiya. Bundan tashqari, bir foydalanuvchi bu ikki vakolatni aktivlashtira olmaydi.
- ConfOP: ikki harakatni nizoli deb e'lon qiluvchi funksiya. Bu foydalanuvchi bir vaqtning o'zida COIIi, ikkita vakolatdan foydalanish huquqini olmasligi uchun bajarilgan.
- User_request_activate: ma'lum bir vakolatni ko'rsatilgan roldan aktivlashtirish uchun ishlatiladigan so'rov; ushbu so'rov foydalanuvchidan keladi.

∀ p8, p10, p18, p20 ∈PERMS, user6, user7 ∈USERS,
role3, role4 ∈ROLES, user6 ∈role3, role4, user7 ∈role3, role4,
p8, p10 ∈role3, p18, p20 ∈role4:mex (p8, p18), mex (p10, p20)∧
user6_request_activate (user6, role3, p8) ∧ user6_request_activate (user6, role3, p10)∧
user7_request_activate (user7, role4, p18) ∧ user7_request_activate (user7, role4, p20)∧
¬activated (user6, role4, p18)⇒activates (user6, role3, p8)∧

$\neg activated(user6, role4, p20) \Rightarrow activates(user6, role3, p10) \wedge$
$\neg activated(user7, role3, p8) \Rightarrow activates(user7, role4, p18) \wedge$
$\neg activated(user7, role3, p10) \Rightarrow activates(user7, role4, p20)$

Foydalanish boshqarish jarayoni quyidagi 4 qadamli ish jarayon bosqichlaridan iborat, ulardan 1-qadam va 2-qadam *Sessions_Step1*ga, 3-qadam va 4-qadamlar *Sessions_Step2*ga mos keladi. 2-qadam va 4-qadam ish jarayonidagi eng murakkab va eng muhim qadamlardir. Agar foydalanishni boshqarishning butun ish jarayoni qora quti sifatida ko'rilsa, foydalanuvchining kirish ma'lumotlari U, $U \in USERS$, va uning chiqish ma'lumotlari P', $R' \subseteq PERMS$. Kirishda 1-qadam U, va chiqishda 4-qadam P' bo'ladi. Quyida boshqarish jarayonining har bir qadami bayon etilgan:

1-qadam uchun kirish U, chiqish esa R, $R \subseteq ROLES$. Unda 1-qadam algoritmi sodda, *avail_session_role* funksiyasidan foydalanib Rni olish mumkin, ya'ni $R=avail\_session\_roles(u)$.

Ushbu qadamda bitta chiqish ma'lumotlari mavjud: rollar nabori *R*dan olingan rollarning qismto'plami *R'*. Funksiyalar siyosati algoritmda foydalanuvchi atributlari, rol atributlari va muhit qiymatlariga asoslangan [77, 78]. 1-algoritmning blok-sxemasi 4.1-rasmda tasvirlangan.

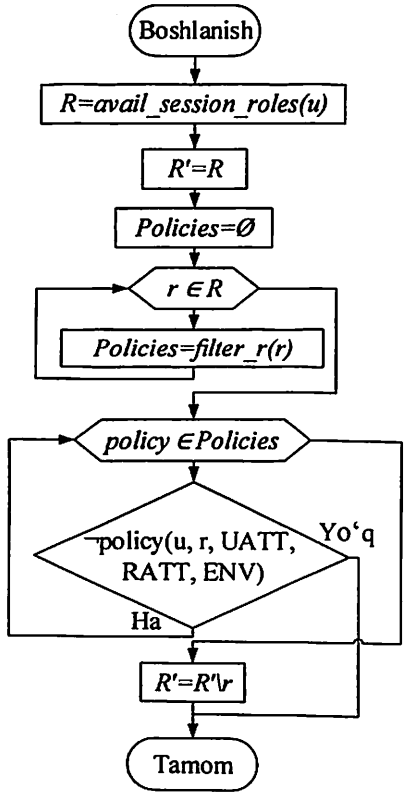
Funksiya mantiqiy amallar va relyatsion amallardan iborat ifoda sifatida mavhumlashtirilishi mumkin. Har bir tartiblangan foydalanuvchi va rol jufti siyosat naboriga mos keladi. Ushbu siyosatda, agar siyosat qiymati *F* bo'lsa, unda foydalanuvchi-rol munosabati aktiv emas. Ushbu jarayonning batafsil qadamma-qadam detalizatsiyasi quyida keltirilgan:

1-algoritm. Foydalanuvchi-rol qiyoslanishini dinamik pasayishi (2-qadam).

Talab qilinadi:
foydalanuvchi: U, $U \in USERS$; rollar to'plami: R, $R \subseteq ROLES$.
Ta'minlanadi:
rollarning yangi nabori: R', $R' \subseteq ROLES$.

```
1:    R'=R;
2:    Policies=Ø;
3:    for r ∈ R do
4:        Policies=filter_r(r);
5:        for policy ∈ Policies do
6:            if ¬policy(u, r, UATT, RATT, ENV) then
```

7: R′ = R′\r;
8: break;
9: **end if**
10: **end for**
11: **end for**



4.1-rasm. Foydalanuvchi-rol qiyoslanishining dinamik pasayishi algoritmining blok-sxemasi

Ushbu qadamda, *avail_session_perms* funksiyasini ishlatib R′ rollar to‘plamida har bir rolga mos vakolatlar belgilanadi [77, 78]. So‘ngra RP to‘plamiga rollar va vakolatlardan iborat mos juftlikni qo‘shib, kirish ma’lumotlari bo‘yicha 2-qadamdan chiqish-R′ ishlatiladi, natijada chiqish-RP. Bundan tashqari, ushbu qadam UATT va RATTni

birlashtirib, RATT' yangi atributlarini hosil qiladi, ya'ni *RATT'=UATTURATT*. Ushbu jarayonning batafsil qadamma-qadam detalizatsiyasi quyida keltirilgan va 2-algortimning blok-sxemasi 4.2-rasmda tasvirlangan.

2-algoritm-3-qadamning bajarilishi. Rol va vakolatlarning qiyoslanishi (3-qadam).

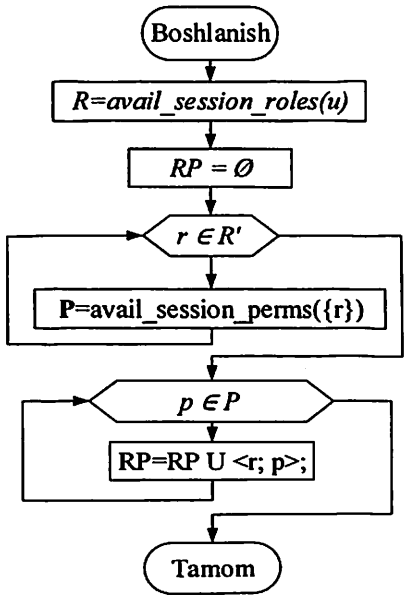
Talab qilinadi:

rollarning yangi to'plami: R'.

Ta'minlanadi:

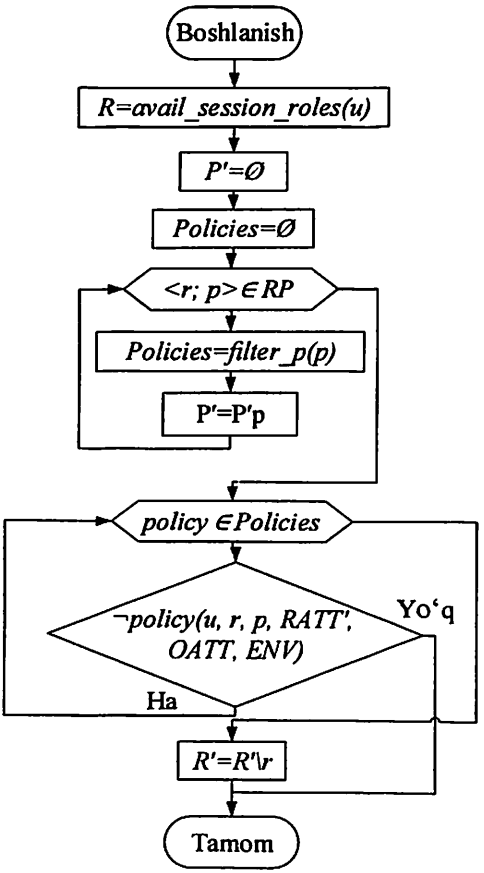
tartiblangan juftliklar nabori: RP, $RP \subseteq ROLES \times PERMS$.

1: **RP** = Ø;
2: **for** $r \in R'$ **do**
3: **P**=avail_session_perms({r});
4: **for** $p \in P$ **do**
5: **RP=RP** U <r; p>;
6: **end for**
7: **end for**



4.2-rasm. Rollar va vakolatlarning qiyoslanishi algoritmining blok-sxemasi

Ushbu qadamda foydalanuvchilar uchun foydalaniluvchi P′ vakolatning yakuniy natijasi chiqariladi. Algoritm asosini rolning yangi atributlari, ob'ekt atributlari va atrof-muhit qiymatlari tashkil etadi. Bu yerda rolning yangi atributlari foydalanuvchi atributlari va rol atributlarini o'z ichiga oladi. Foydalanuvchi atributlari qiymatlarini olish uchun foydalanuvchi nomini kirish parametri sifatida ishlatish, so'ngra foydalanuvchi atributlari qiymatlarini olish uchun, UATTdagi funksiyalardan foydalanish kerak. 3-algortimning blok-sxemasi 4.3-rasmda keltirilgan [77, 78].



4.3-rasm. Vakolatlar-rollar qiyoslanishini dinamik pasayishi algoritmining blok-sxemasi

Ushbu jarayonning batafsil qadamma-qadam detalizatsiyasi quyida keltirilgan.

3-algoritm-4-qadamning bajarilishi. Vakolat-rol qiyoslanishini dinamik pasayishi (4-qadam).

Talab qilinadi:

foydalanuvchi: U, $U \in USERS$; tartiblangan juftlik to'plami: ***RP***, $RP \subseteq ROLES \times PERMS$.

Ta'minlanadi:

vakolatlarning yangi to'plami: P′, $P' \subseteq PERMS$.

```
1:    P′=Ø;
2:    Policies=Ø;
3:    for<r; p> ∈ RP do
4:    Policies=filter_p(p);
5:      P′=P′p;
6:      for policy ∈ Policies do
7:      if¬policy(u, r, p, RATT′, OATT, ENV) then
8:              P′=P′\p;
9:              break;
10:     end if
11:    end for
12:             end for
```

Har safar, foydalanuvchi foydalanish huquqini olishga yoki nizolashuvchi vakolatlarni aktivlashtirishga uringanida, u ushbu muayyan nizolashuvchi vakolatning aktivlashtirishini so'raydi. Biroq, ushbu turdagi so'rovlar va tekshiruvlar nizolashmagan vakolatlar uchun talab qilinmaydi. Monografiyada vakolatlar, rollar va foydalanuvchi nomlari 3.8-rasmda ko'rsatilgan namunaga muvofiq ishlatilgan.

Foydalanuvchi nizolashuvchi vakolatlardan foydalanish huquqini olishi va ularni "Aktivlashtirish" funksiyasi yordamida aktivlashtirishi mumkin.

4.3. Vakolatlarni dinamik taqsimlovchi foydalanishni cheklash modelining algoritmi

Agar foydalanuvchi vakolat uchun avtorizatsiyadan o'tmagan bo'lsa yoki foydalanuvchi COIga ega bo'lgan ikkita nizolashuvchi vakolatni aktivlashtirishga urinsa, foydalanish taqiqlanadi va bu haqida foydalanuvchi xabar oladi. Shundan so'ng, birinchi bo'lib foydalanilgan

vakolatga foydalanish huquqi beriladi, ikkinchi vakolatga foydalanish taqiqlanadi. Shu bilan birga funksiyalar foydalanuvchi, ma'lum bir rol uchun avtorizatsiyalanganligini yoki avtorizatsiyalanmaganligini ham tekshiradi. Foydalanish huquqi tekshirilganidan so'ng, foydalanuvchining vakolatga, hamda COI bilan vakolatga avtorizatsiyasini tekshirishni amalga oshirish uchun, rol funksiyalari oldinga siljiydi. Taklif etilayotgan model algoritmi olti qadamda tavsiflangan [77, 78]:

1-qadam. RBACning bazaviy mohiyatini yaratish: atributli ob'ektlar, COIli ta'sirlar, atributli rollar va atributli foydalanuvchilar.

2-qadam. Kategoriya konteynerlarini yaratish va atributli ob'ektlarni belgilash. Umumiy ta'sirlar naborini yaratish va COI yordamida ta'sirlarni belgilash.

3-qadam. Nizolashuvchi va nizolashmagan atributli vakolatlar to'rtta usul bilan yaratilishi mumkin (4-algoritm):

- vakolatlarni birma-bir yaratish uchun ob'ektlarga ta'sirlarni qo'llash (an'anaviy RBAC);
- bir xil ta'sirli va turli ob'ektli bir necha vakolatlarni yaratish uchun kategoriyalar konteyneriga umumiy ta'sirlar naborini qo'llash (yangi funksiya);
- bir xil ob'ektli va turli ta'sirli bir necha vakolatlarni yaratish uchun ob'ektlarga umumiy ta'sirlar naborini qo'llash (yangi funksiya);
- turli ob'ektli va turli ta'sirli uchun bir necha vakolatlarni yaratish uchun kategoriyalar konteyneriga ta'sirlarning umumiy naborini qo'llash (yangi funksiya).

4-qadam. Nizolashuvchi va nizolashmagan vakolatlar atributlar yordamida atributli rollarga avtomatik ravishda tayinlanadi.

5-qadam. Atributli rollar atributli foydalanuvchilarga avtomatik ravishda tayinlanadi.

6-qadam. Foydalanuvchi tayinlangan rollar va vakolatlardan foydalanishga ruxsat olishi mumkin. Foydalanuvchi ikkita nizolashuvchi vakolatdan bir vaqtning o'zida foydalanishga ruxsat ola olmaydi va "Foydalanish taqiqlangan" xabarini qabul qiladi (5-algoritm).

Ushbu jarayonning batafsil qadamma-qadam detalizatsiyasi quyida keltirilgan.

4-algoritm. Vakolatlarni to'rt xil usullar bilan yaratish.

1: ***if*** foydalanuvchi "Ko'pga-ko'p" usulini tanlasa ***then***

2: Ma'lumotlar bazasidan barcha kategoriyali konteynerlarni olish

3: Ma'lumotlar bazasidan barcha umumiy ta'sirlar to'plamini olish
4: *sContainer*=Categorize Container tanlangan
5: *sSet*=Generic Action Set tanlangan
6: **for** *obj* ∈*sContainer* **do**
7: **for** *act*∈*sSet* **do**
8: T=**new** *Permission(obj, act)*
9: Ma'lumotlar bazasida yangi *T* vakolatni yangilash
10: **end for**
11: **end for**
12:**end if**
13:***if*** foydalanuvchi "Ko'pga-bir" usulini tanlasa ***then***
14:Ma'lumotlar bazasidan barcha kategoriyali konteynerlarni olish
15:Ma'lumotlar bazasidan barcha ta'sirlarni olish
16: *sContainer*=Categorize Container tanlangan
17: *sAction*=Action tanlangan
18: **for** *obj*∈*sContainer* **do**
19: *T*=**new** *Permission*(*obj, sAction*)
20: Ma'lumotlar bazasida yangi *T* vakolatni yangilash
21: **end for**
22:**end if**
23:***if*** foydalanuvchi "Birga-ko'p" usulini tanlasa ***then***
24: Ma'lumotlar bazasidan barcha ob'ektlarni olish
25:Ma'lumotlar bazasidan barcha umumiy ta'sirlar to'plamini olish
26: *sObject*=Object tanlangan
27: *sSet*= Generic Action Set tanlangan
28: **for** *act*∈*sSet* **do**
29: T=**new** *Permission* (*sObject, act*)
30: Ma'lumotlar bazasida yangi *T* vakolatni yangilash
31: **end for**
32:**end if**
33:***if*** foydalanuvchi "Birga-bir" usulini tanlasa ***then***
34: Ma'lumotlar bazasidan barcha ob'ektlarni olish
35: Ma'lumotlar bazasidan barcha ta'sirlarni olish
36: *sObject*=Object tanlangan
37: *sAction*=Action tanlangan
38: T=**new** *Permission* (*sObject, sAction*)

39: Ma'lumotlar bazasida yangi *T* vakolatni yangilash
40:**end if**

5-algoritm. Foydalanuvchining rollar va vakolatlardan foydalanish huquqini olishi

1: *Roles*=Ma'lumotlar bazasidagi barcha rollar ro'yxati
2: *Permissions*=Ma'lumotlar bazasidagi barcha vakolatlar ro'yxati
3: *privilegedRoles*=[]
4: *privilegedPermissions*=[]
5: **for** *permiss* ∈ *Permissions* **do**
6: **if** *is RightTime(permiss.Object.Time)*= =1 **then**
7: *privilegedPermissions*.**Append**(*permiss*)
8: **end if**
9: **end for**
10: **for** *role* ∈ *Roles* **do**
11: **if** *isRightTime(role.Time)*= =1 **then**
12: *privilegedRoles*.**Append**(*role*)
13: **end if**
14: **end for**
15: *historyPermissions*=[]
16: **if** *do Execute()*= =1 **then**
17: *sPermission*=Permission tanlangan
18: *sAction=sPermission.Action*
19: *sObject=sPermission.Object*
20: *isConflicted*=0
21: **for** *permission* ∈ *historyPermissions* **do**
22: **if** *sObject* = = *permission.Object* **and** *sAction* = = *permission.Action.ConflictedAction* **then**
23: *isConflicted*=1
24: **end if**
25: **end for**
26: **if** *isConflicted* = = 1 **then**
27: Foydalanuvchini "bir xil ob'ektga tegishli ta'sirlar to'g'risida" ogohlantirish
28: **else**
29: *historyPermissions*.**Append**(*sPermission*)
30: Vakolatdan muvaffaqiyatli foydalanishga ruxsat berildi

31: **end if**

Taklif etilayotgan modelda faoliyatning katta qismi atributlar asosida bo'lganligi sababli, ma'murga yuklama hajmi kamayadi. RBACning tipik standartida ma'mur rolga vakolatni va foydalanuvchiga rolni tayinlashni qo'lda amalga oshirar edi [77]. Vakolatlarni to'rt xil usullar bilan yaratish algoritmining blok-sxemasi 4.4-rasmda keltirilgan.

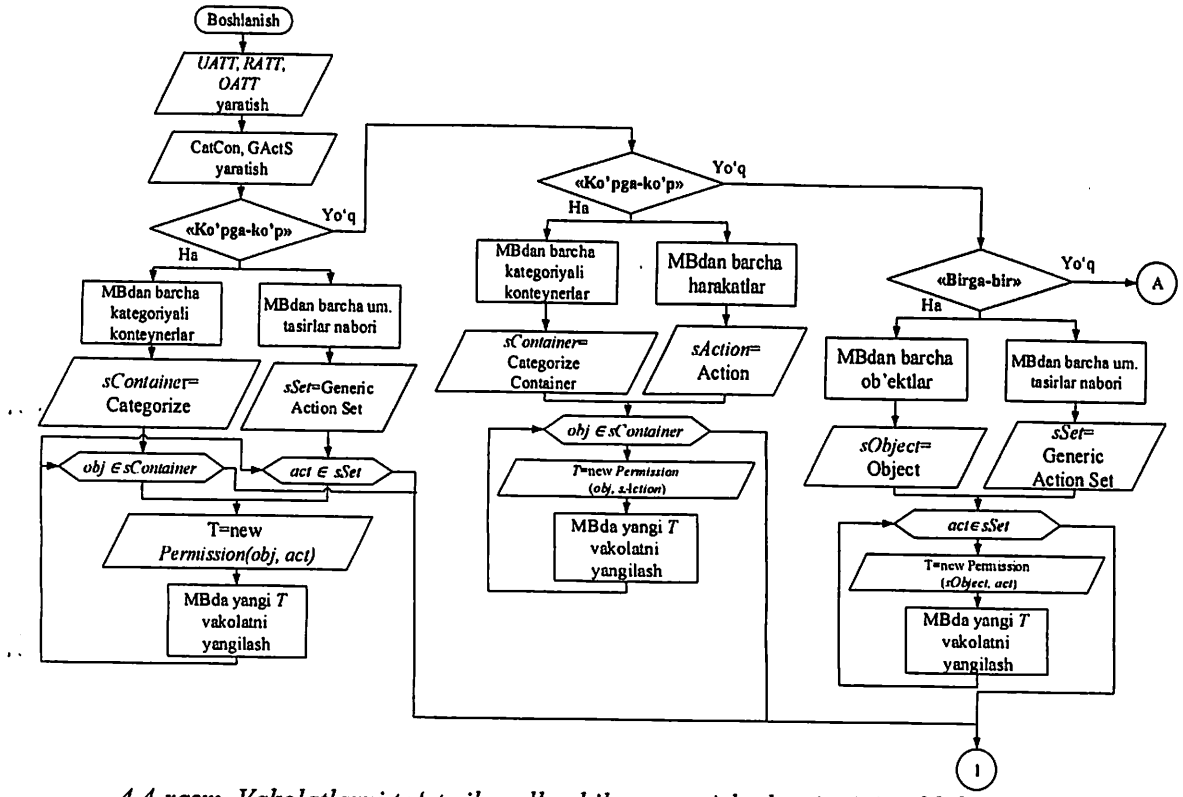
Tavsiya etilgan model foydalanuvchini nufuzi doirasini pasaytirmaydi, chunki u SODni rol sathida emas, balki vakolat sathida to'ldiradi.

Shunday qilib, foydalanuvchi tayinlangan rollarning nizolashmagan barcha vakolatlaridan, shuningdek, bir-biri bilan COIga ega, ikkita nizolashgan vakolatdan bittasidan foydalanish huquqini olishi mumkin. Avval RBAC standartida, agar foydalanuvchi nizolashuvchi vakolatga bitta roldan murojaat qilsa, u ikkinchi nizolashuvchi vakolatdan foydalanish huquqini ola olmas edi, shuningdek foydalanuvchining ushbu nizolashuvchi vakolatning barcha tayinlangan rollaridan ham, foydalana olmas edi. Shu tariqa, RBAC standarti foydalanuvchilarning nufuzini pasaytirar edi [77]. Yo'q

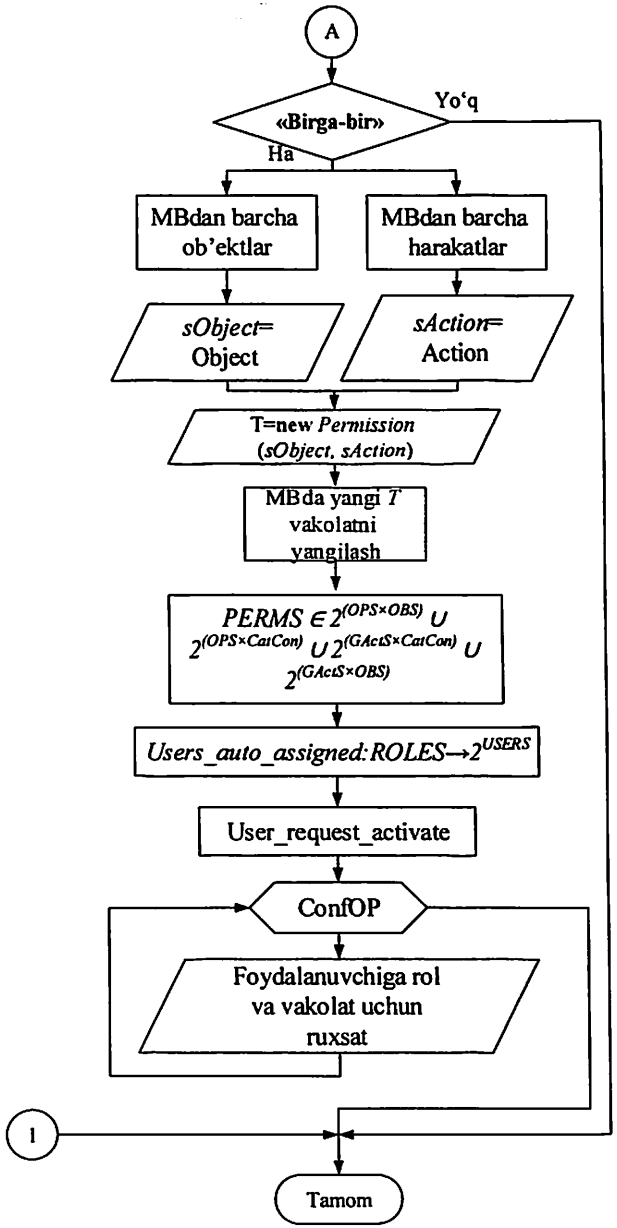
Monografiyada taklif etilgan modelda foydalanuvchilar barcha tayinlangan rollarning nizolashmagan vakolatlaridan foydalanishlari mumkin, chunki SOD rollar sathida emas, balki vakolatlar sathida amalga oshiriladi.

Boshqa tomondan, taklif qilingan modelda foydalanuvchilarga, bitta seansda yoki turli seanslarda foydalanish huquqlarini olishga urinishlaridan qat'iy nazar, COIga ega nizolashuvchi ikkita vakolatdan foydalanish huquqi berilmaydi.

Monografiyada taklif etilgan model kombinatsiyalangan model sifatida ishlaydi, vakolatlarni rollarga dinamik ravishda tayinlaydi, shuningdek turli atributlardan foydalanib foydalanuvchilarni rollarga tayinlaydi. Ushbu muayyan yondashuv faqat RBACning asosiy ob'ektlariga taalluqli. Bundan tashqari, taklif etilayotgan model SODni vakolat sathida amalga oshiradi. Taklif etilayotgan model faqat RBACning qismkategoriyalarini, ya'ni SODni qamrab oladi. Tavsiya etilayotgan modelda RBAC modeli bilan bog'liq, rollar iyerarxiyasi, salbiy avtorizatsiya va vorislik ko'rilmaydi.

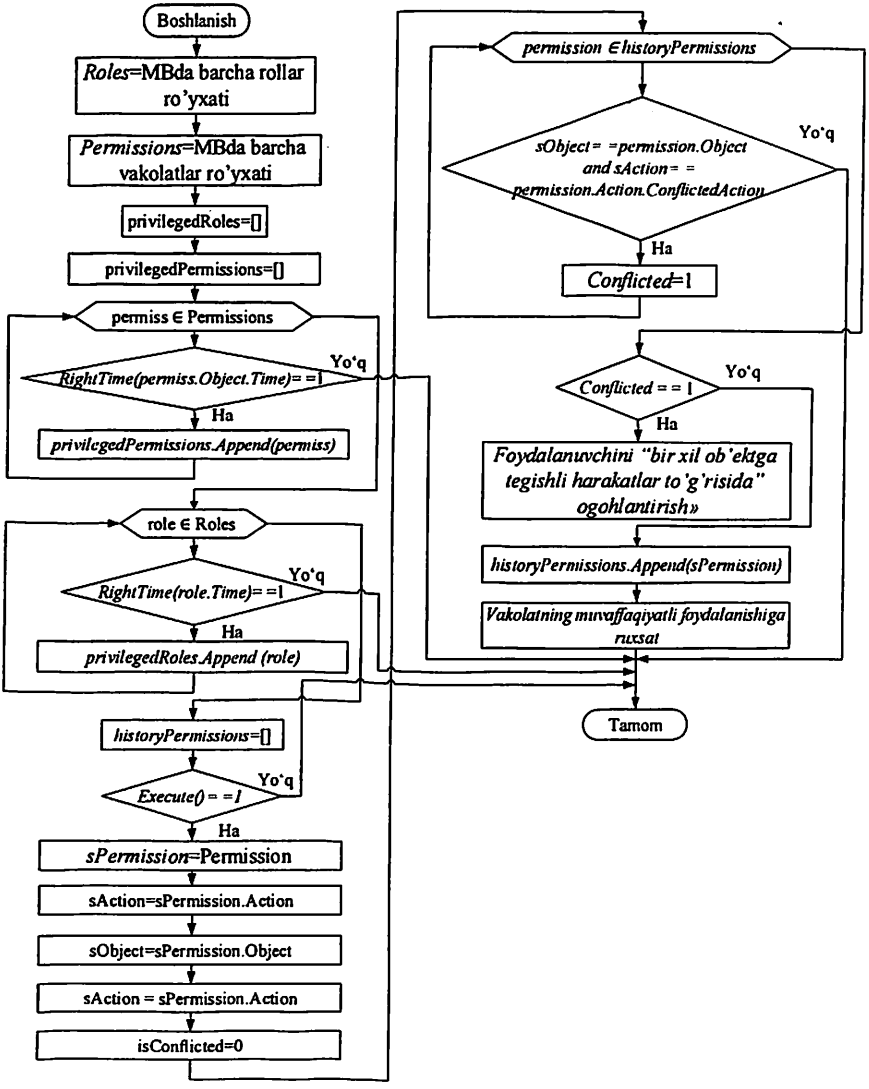


4.4-rasm. Vakolatlarni to'rt xil usullar bilan yaratish algoritmining blok-sxemasi



4.4-rasm. Vakolatlarni to'rt xil usullar bilan yaratish algoritmining blok-sxemasi (davomi)

Foydalanuvchining rollar va vakolatlardan foydalanish huquqini olishi algoritmining blok-xemasi 4.5-rasmda keltirilgan.



4.5-rasm. Foydalanuvchining rollar va vakolatlardan foydalanish huquqini olishi algoritmining blok-xemasi

Monografiyada taklif etilgan modelda, rol-vakolat munosabatlarini aniqlashda foydalanuvchi atributlarining foydalanuvchi bo'lishligi talabi ta'minlanadi. Chunki, rol-vakolat munosabatini aniqlashda ishlatilishi mumkin bo'lgan atributlar tarkibida foydalanuvchi atributlari, rol atributlari, muhit atributlari va ob'ekt atributlari (vakolat atributlari) mavjud. Taklif etilgan model, foydalanuvchi atributlari va vakolatlariga muvofiq, rollar-vakolatlar munosabatlarini yanada detallashtirilgan holda nazoratlash imkonini beradi.

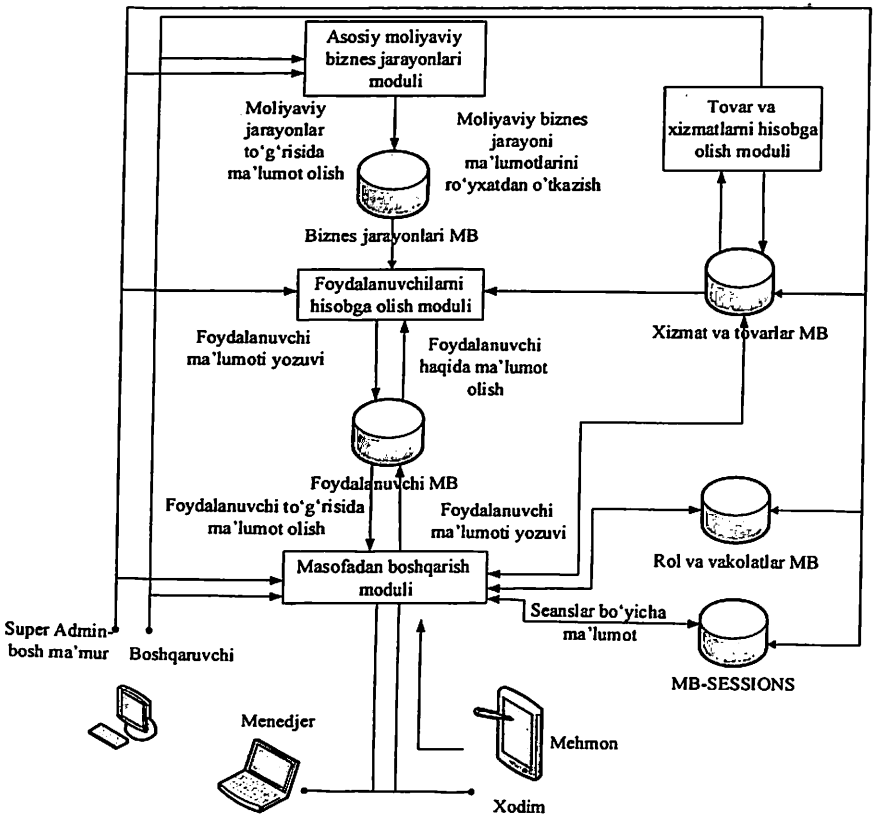
4.4. Ishlab chiqilgan foydalanishni cheklash tizimi modelining tatbiqi

Ushbu tadqiqot ishida marketing sohasida mijozlarga texnik va savdo-sotiq bo'yicha xizmat ko'rsatish xususida axborotni yig'ish, qaror qabul qilish orqali tovar aylanmasini, tovar aylanmasi logistikasini ta'minlovchi va mijoz kommunikatsiya tizimini tashkil etishga mo'ljallangan "Business Process" axborot tizimi uchun, rollar asosida foydalanishni cheklash tizimi ishlab chiqilgan. 4.6-rasmda "Business Process" axborot tizimi ishlashining tarkibiy ko'rinishi keltirilgan.

"Business Process" axborot tizimida foydalanishni cheklashni boshqarishning rolli modelidan foydalanishdan maqsad foydalanuvchilarga faqat rolni amalga oshirish uchun uchun zarur ob'ektlardan yoki jarayonlardan foydalanish, jumladan rolni amalga oshirish uchun faqat kerakli axborotni ishlash huquqini berish hisoblanadi. Ish jarayonini unumli amalga oshirish uchun, foydalanuvchilarga axborot doimo foydalanuvchan bo'lishi lozim. Har bir foydalanuvchiga rollarni qo'shish tizimda amalga oshiriluvchi rollarni aniqroq va yetarlicha moslashuvchan taqsimlashga imkon beradi.

C-RBAC modelining aksariyat veb-resurslarda ishlatilishi foydalanuvchining, berilgan rol asosida, ma'lumotlardan foydalanishlarini osongina aniqlashga imkon beradi. "Business Process" axborot tizimi uchun foydalanishni cheklash tizimida rol ma'mur yordamida hisobga olish yozuvi orqali identifikatsiyalanadi va foydalanuvchining muayyan rolda ishlashi uchun xususiy hisobga olish yozuvi yaratiladi. Bu holda, xodimning tizimga kirishi unga taqdim etilgan yagona hisobga olish yozuvi bo'yicha amalga oshiriladi. Ammo tizimga kirishda foydalanuvchini identifikatsiyalash va autentifikatsiyalash bilan birga, unga rolni tanlash taklif etiladi. Foydalanuvchi mos rolni (unga ruxsat etilgan rollar naboridan) tanlaganidan so'ng,

ushbu rolga tayinlangan ob'ektlardan foydalanishni cheklash huquqlari kuchga kiradi.



4.6-rasm. "Business Process" axborot tizimining tarkibiy ko'rinishi

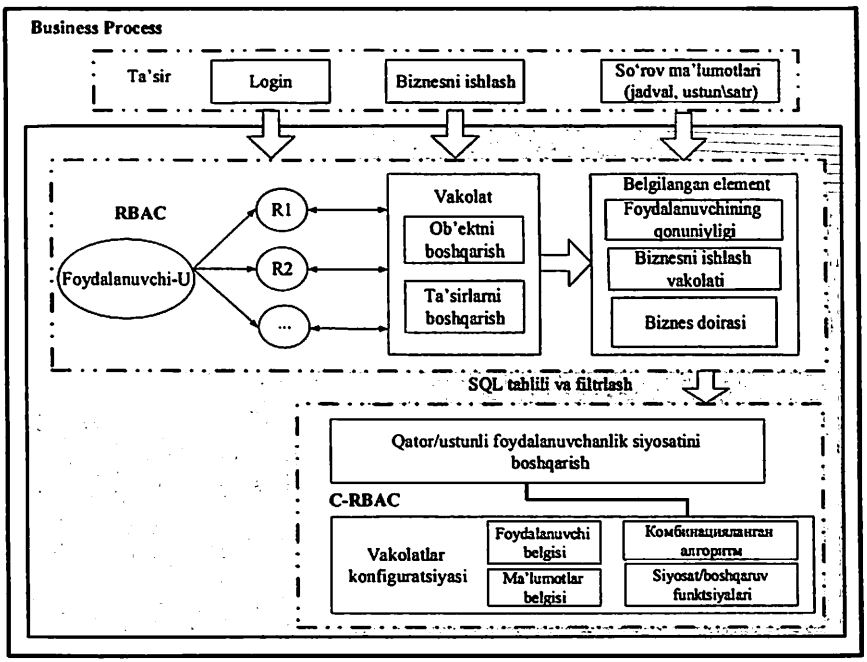
Rolni almashtirish uchun foydalanuvchini o'zgartirish zaruriyati yo'q, hisobga olish yozuvini almashtirmasdan yangi rolni tanlashga imkon beruvchi mos ilovani ishga tushirish kifoya. Foydalanishni cheklash tizimi modeli foydalanuvchi roli bo'yicha ma'lumotlardan foydalanish prinsipini amalga oshiradi va resurs ma'lumotlaridan foydalanish huquqini olish bosqichlaridan iborat bo'ladi [77, 97].

Birinchi bosqich-foydalanuvchiga atalgan rolni taqdim etish.

Ikkinchi bosqichda foydalanuvchi, unga taqdim etilgan rolga atalgan kerakli atributlarni oladi. Atributlar olinganidan so'ng, ularni ishlash jarayoni boshlanadi va foydalanuvchi, atributga bog'liq holda, atribut taqdim etgan mos ma'lumotlar belgisidan foydalanish huquqini oladi.

Uchinchi bosqich tipiklashtirilgan ma'lumotlarni olish bilan yakunlanadi.

4.7-rasmda taklif etilgan foydalanishni rolli cheklash tizimi modelining umumiy arxitekturasi keltirilgan. Tizim tarkibi quyidagicha: 1) ta'sir sathi, 2) RBAC sathi, 3) SQL tahlili va filtrlash va 4) C-RBAC sathi.



4.7-rasm. Taklif etilgan foydalanishni rolli cheklash tizimi modelining umumiy arxitekturasi

Monografiyada taklif etilgan model asosida foydalanishni boshqarish moduli, sozlanuvchi siyosatlardan foydalanib, detallashtirilgan ma'lumotlardan foydalanishni amalga oshirishi mumkin [77, 97].

Birinchi sath-ta'sirlar sathi. Uning tarkibiga tizimga kirish, biznes-ishlov, ma'lumotlar so'rovi va h. kabi tizim taqdim etuvchi amallar kiradi. So'rov ma'lumotlari shakli-jadval, satr va ustun.

Ikkinchi stah-RBAC bo'lib, u foydalanuvchilar vakolatlarini to'liq nazoratlashda ishlatiladi. Ob'ektlarni boshqarish va ta'sirlarning o'zaro ta'sirida tushunarli vakolatni olish mumkin. Aynan ushbu vakolatni tekshirishni RBAC amalga oshiradi [77, 97].

Uchinchi sath-SQL tahlili va filtrlash. Ushbu sathda taklif etilgan model yordamida ma'lumotlar bazasiga so'rovlar tilidan yoki so'rovlar sinflaridan so'rov tahlillanadi. Masalan, SQL "SELECT COUNT (col1) From tables WHERE col2=value AND col3 = value" so'rovi tahlili natijasi 5.1-jadvalida keltirilgan.

4.4-jadval

SQL tahlili va filtrlash natijalari

```
{
  SELECT_COLUMNS: [col1],
  WHERE_COLUMNS: [col2, col3]
  WHERE_CONDITION: "col2=value AND col3=value"
  WHERE_EXPRESSION: ["col2=value", "col3=value"]
}
```

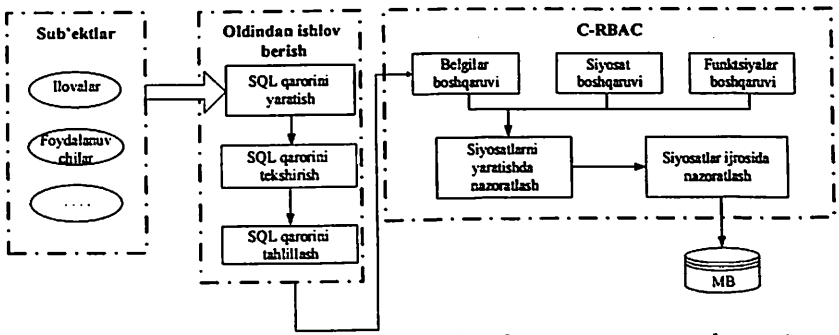
Agarda tahlil natijalari tarkibiy axborot bo'lsa, u o'zida quyidagilarni qamrab oladi:

1. SELECT_COLUMNS;
2. WHERE_COLUMNS;
3. WHERE_CONDITION;
4. WHERE_EXPRESSION.

To'rtinchi sath- C-RBAC. Uning tarkibida starlar/ustunlar bo'yicha vakolatlar siyosatining boshqaruvi va vakolatlarni sozlash mavjud. Vakolatlar siyosati atributlar orqali berilgan foydalanuvchi belgisi, ma'lumotlar belgisi, kombinator algoritmi, siyosatlar/funksiyalar boshqaruvi asosida belgilanadi. Ushbu sath C-RBACni va RBAC va SQL larning tahlillash va filtrlash tahlil natijalari bilan birlashtiradi. Shu tariqa vakolatlarni detallashtirilgan nazorati strukturasi 4.8-rasmda keltirilgan [77, 97].

Foydalanish so'rovi ilova, foydalanuvchi va h. kabi sub'ektlar tomonidan boshlanadi, va oldindan ishlov berishda so'rov uchun SQL

qarori yaratiladi. Shu bilan birga, SQL qarori dastlabki natijani olish uchun, tekshiriladi va tahlillanadi. Dastlabki natija tarkibida amallar, ob'ektlar jadvali ustuni, ob'ektlar jadvali satri, foydalanuvchi va h. xususida axborot bo'ladi.



4.8-rasm. Foydalanishni detallashtirilgan nazorati strukturasi

So'ngra, dastlabki natija C-RBACdagi belgilarni, siyosatlarni va funksiyalarni boshqarish orqali tekshiriladi. Foydalanuvchi belgisi bilan siyosatlarni ishlab chiqarish bo'limidagi ma'lumotlar belgisini taqqoslab, yakuniy natija generatsiyalanadi. Generatsiyalash siyosatlarni bajarish bo'limida amalga oshirilishi mumkin.

Monografiyada taklif etilgan modelda foydalanuvchining foydalanish huquqi ta'sir qiymatiga binoan belgilanadi. Ob'ekt ham, ta'sir doirasi ham, foydalanishning qandaydir detallangan vakolatining mos huquqi kabi belgilanadi. Bundan tashqari C-RBAC modeli tarkibida yuridik shaxsning qandaydir boshqa detallashtirilgan huquqlari mavjud bo'lib, ular quyidagicha ta'riflanadi.

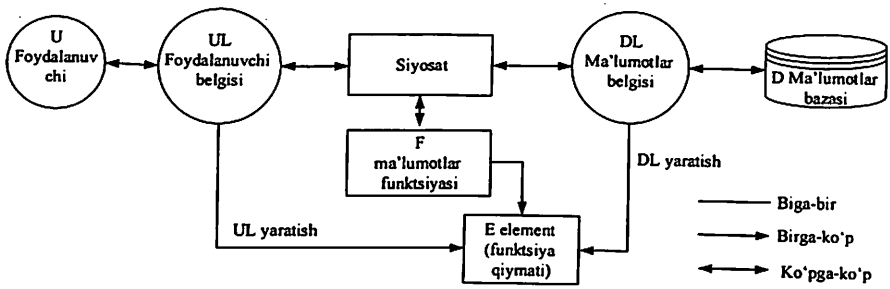
Xavfsizlik funksiyasi- ma'lumotlar atributining identifikatori. Identifikator uchun, haqiqiy ssenariy nuqtai nazaridan ma'lumotlarni tahlillash yo'li bilan, vakolatlarning muayyan diapazoni belgilanishi mumkin.

Xavfsizlik funksiyasi elementi-himoyalash funksiyasining o'ziga xos elementi. Element himoya vositasining muayyan variantini belgilaydi.

Himoya belgisi-tarkibida himoya funksiyalari elementlarining muayyan qiymatlari bo'lgan ob'ekt sifatida belgilanadi. Himoya belgisi berilgan vakolatga muayyan huquqni belgilashda ishlatiladi.

Xavfsizlik siyosati-bir yoki bir necha xavfsizlik siyosatini o'z ichiga oladi va ma'lum funksiyali foydalanishga vakolatlar ko'lamini tayinlaydi [77].

Yuqorida keltirilgan ta'riflardan tashqari 4.9-rasmda taklif etilgan modelning komponentlari ko'rsatilgan.



4.9-rasm. Foydalanishni kombinatsiyalangan rolli cheklash modelining komponentlari

Ushbu komponentlar orasida rol huquqi *foydalanuvchi belgisi*, ma'lumotlar belgisi esa *ma'lumotlar belgisi* sifatida belgilanishi mumkin. Ularning munosabatlari-ko'pga-ko'p. Foydalanuvchilar belgisi (createUL) va ma'lumotlar belgisi (createDL) bitta siyosat asosida boshqariladi. Undan tashqari, UL/DL siyosat orasidagi munosabatlari "Ko'pga-ko'p" munosabatlar.

Ma'lumotlar funksiyasi bir necha siyosatlarda bo'lishi mumkinligi sababli, siyosat bir necha funksiyalarda tavsiflanishi mumkin. Shunday qilib, siyosat va ma'lumotlar funksiyasi orasida "Ko'pga-ko'p" munosabatlar mavjud. Belgi qiymati bitta ma'lumotlar ob'ektidan olinadi, ma'lumotlar elementi esa faqat bitta bo'lishi mumkin. Shunday qilib, DL va xarakterli element qiymati (Ye) orasidagi munosabatlar o'zaro bir ma'noli. Foydalanish diapazonini ifodalovchi rol belgisi UL uchun, bir xil ma'lumotlar funksiyasiga ega, bir necha qiymatlarni sanab chiqish mumkin. Shunday qilib, UL i E orasidagi munosabatlar "Birga-ko'p".

Ustunlar sathidagi xavfsizlik funksiyasining o'zaro bog'liqligi.

Monografiyada taklif etilayotgan modelda ustunlar sathida xavfsizlik funksiyasining uchta turi: ARRAY, SET va TREE mavjud.

Ularning o'zaro munosabatlarini ko'rsatish uchun ular elementlarini mos ma'lumotlar strukturasida akslantirish mumkin.

1. Xavfsizlik funksiyasi ARRAY elementlari odatiy holda ustuvorliklarning chiziqli munosabatiga ega. Masalan, ma'lumotlar maydonlari orasida aniqlik bo'yicha bog'liqlik bo'lishi mumkin. Axborotning ustuvorligi qanchalik aniq bo'lsa, foydalanish huquqini talab qilish shunchalik yuqori bo'ladi.

2. Xavfsizlik funksiyasi SET elementlari foydalanuvchi vakolatlar diapazonini aniqlashda ishlatilishi mumkin. Agar element belgilangan naborga tegishli bo'lsa, unga belgilangan diapazonda vakolat berilishi mumkin. Masalan, bitta element ("username"-"foydalanuvchi nomi", "usersex"-"foydalanuvchi jinsi", "userage"-"foydalanuvchi vazni") tarkibida vakolatlarning sakkizta mos elementlari bo'lishi mumkin. Huquqlarni o'rnatish misoli 4.5-jadvalda keltirilgan.

4.5-jadval

Huquqlarni o'rnatish

Vakolatlar qismto'plami	**Kommentariyalar**
{}	xavfsizlik funksiyasi orqali belgilangan barcha elementlar foydalanuvchan emas
{"username"}	"username" foydalanish mumkin
{"usersex"}	"usersex" foydalanish mumkin
{"username", "usersex"}	"username" va "usersex" foydalanish mumkin
{"username", "userage"}	"username" va "userage" foydalanish mumkin
{"usersex", "userage"}	"usersex" va "userage" foydalanish mumkin
{"username", "usersex", "userage"}	xavfsizlik funksiyasi orqali o'rnatilgan barcha elementlarga mos ma'lumotlardan foydalanish mumkin

3. Xavfsizlik funksiyasi TREE elementlari orasida "ota-o'g'il" yoki "aka-uka" munosabatlari mavjud. Tipik misol sifatida geografik o'rinni ("shahar", "viloyat", "tuman") keltirish mumkin. Shaharlar orasidagi munosabatlar aka-uka munosabatlaridir. Bir shahardagi rayonlar orasidagi munosabatlar ham aka-uka munosabatlari hisoblanadi, shahar bilan tuman orasidagi munosabatlar esa ota-o'g'il munosabatlari

hisoblanadi. Vakolatlar naborini daraxtdagi uzel sifatida tasavvur etish mumkin. Agar uzel bargsiz bo'lsa, u mavjud munosabatlarga muvofiq sho''ba uzeldan foydalanish huquqiga ega bo'ladi.

Satrlar sathidagi xavfsizlik funksiyasi qoidasi.

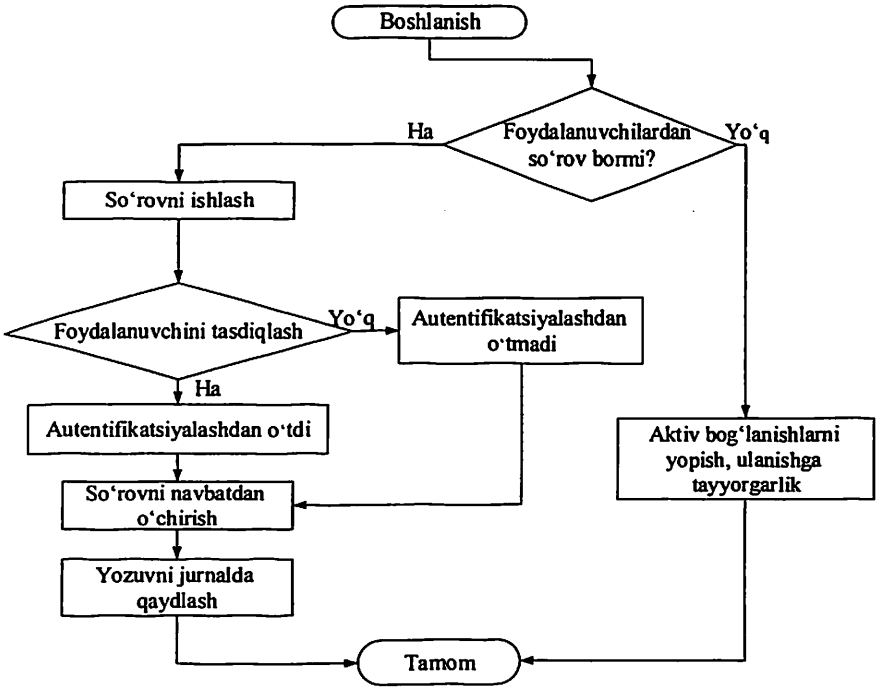
Monografiyada taklif etilgan modelda satrlar sathidagi xavfsizlik funksiyalari qoidalari oldindan belgilangan. Xususan, satrlar sathidagi himoya funksiyasining elementi SET strukturasi kabi o'rnatiladi va ma'lum qoidaga tayinlanadi. Har bir qoida uchlikdan iborat: {FIED: maydon nomi, operator: operator, qiymat: ma'lumotlar qiymati}. Maydon nomi ko'rsatilgan joy, jadval satri nomi bo'lib, mos operatorlar tarkibida "=", ">", "<"lar va h. mavjud. Ma'lumotlar qiymatlari [value1, value2] ro'yxatlarda saqlanadi.

Siyosatdagi xavfsizlik funksiyalari orasidagi munosabatlar.

Xavfsizlik siyosati tarkibida bir necha xavfsizlik funksiyalarining mavjudligi sababli, siyosatni ishlab chiqish tartibi, taklif etilayotgan modelning muhim muammosi hisoblanadi. Vakolatlar natijasi himoya elementlarining paydo bo'lishi ketma-ketligiga muvofiq shakllantiriladi. Foydalanish vakolatini tekshirish uchun siyosatdagi xavfsizlikning turli xil funksiyalarining ba'zi xavfsizlik elementlari ishlatilganida, vakolatlar xususidagi har bir yechim xavfsizlikning turli funksiyalariga muvofiq generatsiyalanadi va vakolatlar natijasi barcha yechimlarni birlashtirish yo'li bilan generatsiyalanadi. Taklif etilayotgan modelda yechimlar bog'liqligi prinsipiga qa'tiy rioya qilinadi, ya'ni bitta yechim qabul qilinmasa, foydalanish taqiqlanadi.

4.5. Foydalanishni rolli cheklash tizimida autentifikatsiya va avtorizatsiya mexanizmlari

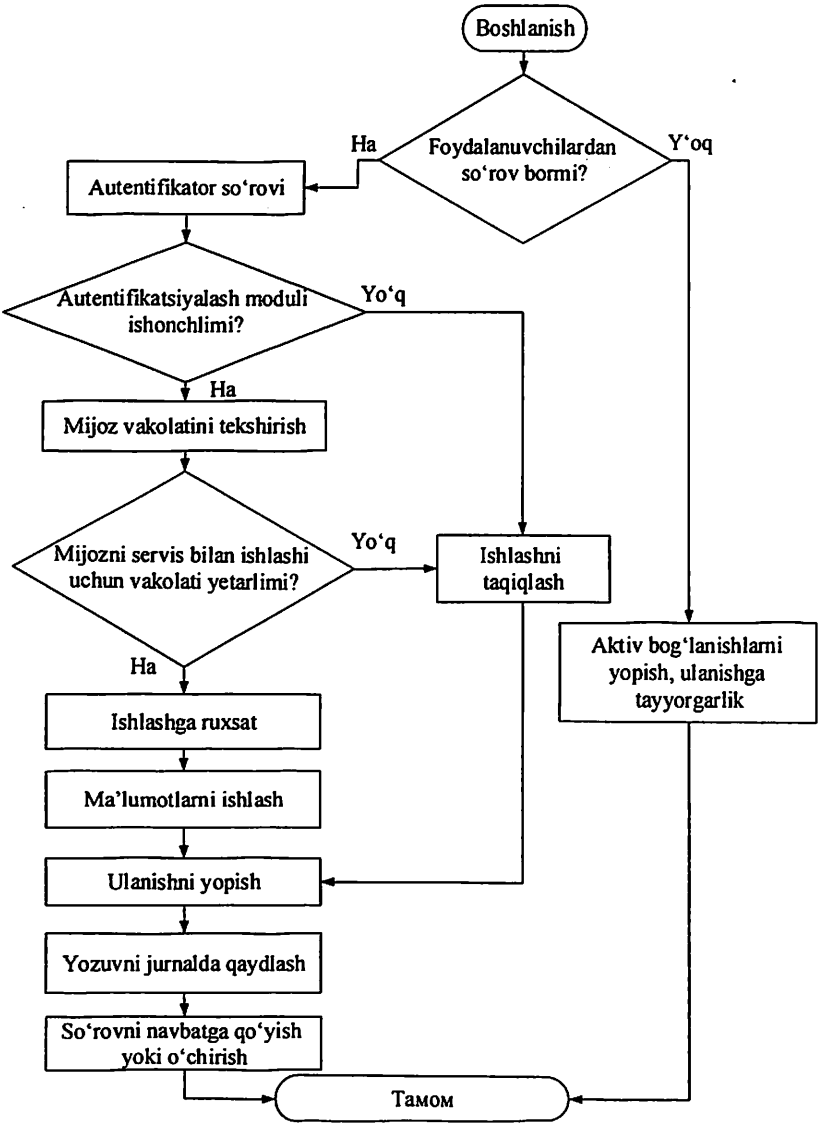
Autentifikatsiyani amalga oshirish. Tizimga kirishda foydalanuvchi tizimda ro'yxatdan o'tishi lozim, ushbu bosqichni muvaffaqiyatli o'tkazgan foydalanuvchi autentifikatorga ega bo'ladi. Autentifikator, foydalanuvchi so'rovi bo'yicha servislarni taqdim etishga xizmat qiluvchi, axborot moduliga taqdim etiladi. Modulning ijobiy javob holida (foydalanuvchi tanilgan va foydalanishning yetarli huquqlariga ega) aloqaning xavfsiz kanalini muvofiqlashtirish boshlanadi. 4.10-rasmda autentifikatsiya moduli ishlashi algoritmining blok-sxemasi keltirilgan.



4.10-rasm. Autentifikatsiya moduli ishlashi algoritmining blok-sxemasi

Axborot serveri foydalanuvchi so'rovlariga xizmat ko'rsatish uchun servislarni taqdim etadi. Amalga oshiriluvchi xavfsizlik siyosatiga bog'liq holda, resurslardan foydalanish ruxsati barcha foydalanuvchilarga (jumladan autentifikatsiyadan o'tmaganlarga) yoki oldindan ma'lum vakolatlarga ega foydalanuvchilar guruhiga berilishi mumkin. Axborot tizimi serveri ishlashi algoritmining blok-sxemasi 4.11-rasmda keltirilgan.

Umuman holda, axborot tizimi serveri vazifasiga, autentifikatsiyadan o'tgan foydalanuvchilarning o'zlarining serverlardan foydalanish so'rovlariga xizmat ko'rsatish kiradi. Buning uchun axborot serveri foydalanuvchilar taqdim etgan, unga ma'lum autentifikatsiya serverlaridan olinishi lozim bo'lgan, identifikatorni tekshiradi.



4.11-rasm. Axborot tizimi serveri ishlashi algoritmining blok - sxemasi

Autentifikatsiya siyosatining maqsadi-foydalanuvchi belgilarini, ma'lumotlar belgilarini va SQL so'rovlarini tekshirish va avtorizatsiya qoidalariga muvofiq yakuniy natijani generatsiyalash.

Avtorizatsiya qoidalari tavsifi quyida keltirilgan:

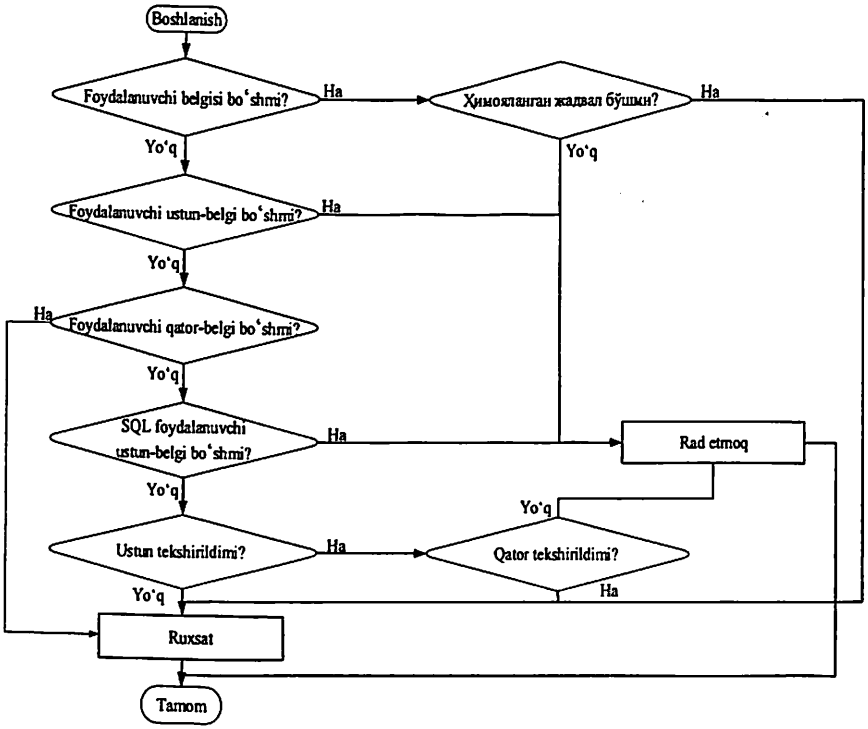
Agar tahlillangan foydalanuvchi belgisi bo'sh va barcha ma'lumotlar jadvallari xavfsizlik siyosati bilan himoyalanmagan bo'lsa, foydalanuvchiga tizimga kirish huquqi beriladi.

2. Faraz qilaylik, tahlillangan foydalanuvchi belgisi bo'sh emas, va ma'lumotlar jadvali xavfsizlik siyosati bilan himoyalangan. Foydalanuvchi belgisining barcha ustunlar uchun mos xavfsizlik funksiyalari mavjud emas. Bu ma'lumotlar jadvalining foydalanish cheklashlariga ega ekanligini, ammo foydalanuvchining mos foydalanish huquqiga ega emasligini anglatadi. Shunday qilib foydalanuvchiga tizimga kirish huquqi berilmaydi.

3. Faraz qilaylik, tahlillangan foydalanuvchi belgisi bo'sh emas, ma'lumotlar jadvali esa xavfsizlik siyosati bilan himoyalangan. Foydalanuvchi belgisining barcha satrlari uchun uchun mos xavfsizlik funksiyalari mavjud emas. Bu foydalanuvchi belgisining mos satridan foydalanish vakolati odatiy holda ruxsat etilganligini bildiradi. Ya'ni vakolatlar diapazoni-ma'lumot jadvalining barcha satrlari va, demak, foydalanuvchiga tizim kirish huquqi beriladi.

4. Faraz qilaylik, tahlillangan foydalanuvchi belgisi bo'sh emas, ma'lumotlar jadvali esa xavfsizlik siyosati bilan himoyalangan. Tahlillangan SQL-so'rovi natijasidagi taklifda ma'lumotlar jadvalining ustunlari mavjud emas, bu SQL taklifning noto'g'ri ekanligini ko'rsatadi. Shunday qilib, foydalanuvchiga tizimga kirish huquqi berilmaydi.

4.12-rasmda yuqorida tavsiflangan qoidalar asosida vakolatlarni tekshirish algoritmining blok-sxemasi keltirilgan. Birinchidan, agar foydalanuvchi belgisi bo'sh bo'lsa va so'rovlar jadvali himoya siyosatiga ega bo'lmasa, 1-qoida bo'yicha foydalanuvchiga tizimga kirish huquqi beriladi. Ikkinchidan, agar foydalanuvchi belgisi bo'sh va so'rovlar jadvali himoya siyosatiga ega bo'lsa 2-qoida bo'yicha foydalanuvchiga tizimga kirish huquqi berilmaydi. So'ngra so'rov va foydalanuvchi ma'lumotlari tekshiriladi.



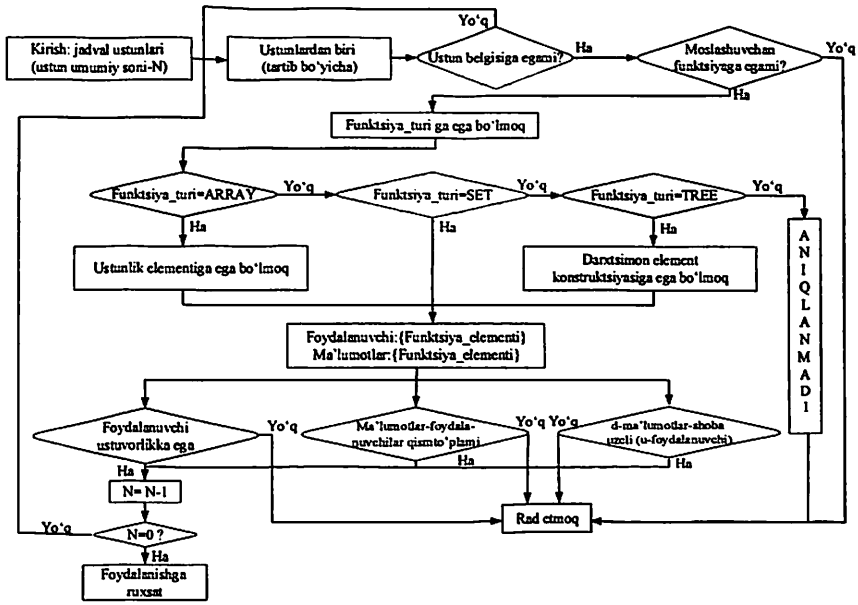
4.12-rasm. Vakolatlarni tekshirish algoritminingblok-sxemasi

So'rov ma'lumotlari himoyalangan va foydalanuvchi ushbu ma'lumotlardan foydalanish huquqiga ega. Foydalanuvchi belgisiga kiritilgan ustun belgisining bo'shligi, foydalanuvchining himoyalangan ma'lumotlardan foydalanish huquqiga ega emasligini anglatadi. Aksincha, foydalanuvchi belgisiga kiritilgan satr belgisining bo'shligi barcha satrlardan foydalanish mumkinligini va 3-qoida bo'yicha foydalanuvchiga tizimga kirish huquqiga egaligini anglatadi. SQLning tahlil natijasi ustunlarining bo'shligi SQLning sintaktik tahlil natijasining noto'g'riligini va 4-qoida bo'yicha foydalanuvchiga tizimga kirish huquqi berilmasligini anglatadi. Va nihoyat, agar barcha kerakli axborot bo'sh bo'lmasa, ustun va satr belgilari tekshiruvdan o'tgan bo'lsa, foydalanuvchiga tizimga kirish huquqi beriladi.

Kombinatsiyalangan modelda vakolatlarni tekshirish ikki qismga- ustunlar sathida vakolatlarni tekshirish va satrlar sathida vakolatlarni

tekshirishga ajratiladi. Ustunlar sathida vakolatlarni tekshirish ham xavfsizlik funksiyalari elementlarini tekshirish qoidalariga bog'liq.

Ustunlar sathida vakolatlarni tekshirish parametrlari-ustun vakolatlari xususidagi axborot, foydalanuvchi belgisi va so'rov axborotidagi ustunlar. Bir himoya belgisiga ega ustunlar uchun axborotini taqqoslash, himoya belgilari elementlari orasida tekshiruv qoidalariga muvofiq amalga oshiriladi. Tekshiruv qoidalari tafsiloti 4.13-rasmda keltirilgan.



4.13-rasm. Ustunlar sathida vakolatlarni tekshirish qoidalari

Agar funksiya turi ARRAY bo'lsa, barcha shartli elementlarning chiziqli ustuvorligi kombinatsiyalangan modelning oldindan belgilangan tartibiga muvofiq olinadi. Foydalanuvchi belgisining shartli elementlari va ustun sathidagi funksiyalar orasidagi ustuvorlikni taqqoslash natijalari foydalanuvchi belgisi ustuvorligining yuqoriligini ko'rsatsa, foydalanuvchiga foydalanishga ruxsat beriladi. Aks holda, foydalanishga ruxsat berilmaydi.

Agar xavfsizlik funksiya SET bo'lsa, foydalanuvchi belgisining elementlari mos xavfsizlik funksiyasi belgisi bilan ustun sathida taqqoslanadi. Agar foydalanuvchi belgisi elementlari tarkibida ustun sathi funksiyasi bo'lsa, foydalanuvchiga foydalanishga ruxsat beriladi. Aks holda, foydalanishga ruxsat berilmaydi.

Agar funksiya turi TREE bo'lsa, barcha shart elementlarining iyerarxik strukturasi xavfsizlik siyosati bilan olinishi lozim. Agar shart elementi, ma'lumotlar funksiyasi yoki ma'lumotlarning ota-ona uzeli tomonidan tahlillangan shart elementiga teng bo'lsa, foydalanuvchiga foydalanishga ruxsat beriladi. Aks holda, foydalanishga ruxsat berilmaydi.

Satr sathidagi vakolatlarni tekshirish taqqoslashni talab etadi va ikkita ob'ektni o'z ichiga oladi: foydalanuvchi belgisi bo'yicha tahlillanuvchi satr qoidalari konfiguratsiyasi va so'rov operatoridagi "WHERE" ifodasi. Ikkala ob'ekt, mos holda ma'lumotlar doirasini ifodalaydi. Uchlik shakldagi qoidani: {fayl: maydon nomi, operator: operator, qiymat: ma'lumotlar qiymati} olish uchun, foydalanuvchi belgisidagi har bir satr belgisi tahlillanishi lozim.

Ma'lumotlar doirasi "WHERE" ifodasidan olinganligiga ishonch hosil qilinsa, har bir satr qoidalari konfiguratsiyasi orasidagi "OR" munosabatiga moslashishi lozim. Bu muayyan ifoda SQL "WHERE" ni identifikatsiyalashdagi muammolarni oldini olishga imkon beradi. Masalan, "WHERE" ifodasi "WHERE (col1=1 OR col1=2) AND col2=3" satr qoidalari konfiguratsiyasi bilan taqqoslanadi va ma'lumotlar doirasi "col1" ning ifodalanganligiga ishonch hosil qilinmaydi.

Yuqoridagi muammolarni hal qilish uchun, satr sathidagi vakolatlarni tekshirish tavsiya etilgan modelning ishlashi bosqichlarida amalga oshiriladi. Birinchidan, "WHERE" ifodasi dekonstruksiya paradigmasiga aylanadi va ular qismlari orasidagi munosabat esa-"OR". Masalan, "WHERE (col1=1 OR col1=2) AND col2=3" ifodasi-"(col1=1 AND col2=3) OR (col1=2 AND col2=3)" ga aylanadi. Shundan so'ng, satr qoidalari konfiguratsiyasini "OR" orqali yuboriladigan"WHERE" ifodasining har bir qismi bilan taqqoslash mumkin. Ma'lum foydalanuvchi belgisi bilan satrlar qoidalari orqali tahlillangan ustunlar tarkibida SQL ifodasida tahlillangan ustunlarning bo'lishi, "WHERE" ifodasining har bir qismida tahlillangan ustunlar naborining satrlar qoidalari bilan tahlillangan ustunlar qismtizimi hisoblanishi, SQL so'rov ma'lumotlari hajmining foydalanuvchi vakolatidagi so'rov ma'lumotlari

hajmidan kattaligini anglatadi. Shunday qilib, foydalanuvchiga foydalanish huquqi berilmaydi. Foydalanuvchi tomonidan taqdim etilgan diapazon, so'rov ifodasi diapazonidan kichik bo'lsa ham foydalanuvchiga foydalanish huquqi berilmaydi. Foydalanish huquqini olishga tekshirishda barcha taqqoslashning amalga oshirilishi shart.

Avtorizatsiyani amalga oshirish. Kombinatsiyalangan modelda avtorizatsiya ma'lumotlar avtorizatsiyasini va foydalanuvchi avtorizatsiyasini o'z ichiga oladi. Avtorizatsiyani ishlashda ma'lumotlarga va foydalanuvchiga mos holda, himoya funksiyalari belgilari beriladi. Himoya belgilari jadvaldagi satr va, ustun ma'lumotlaridan ajratib olinadi va ajratib olingan belgilarning turli xil himoya elementlariga muvofiq, mos himoya belgilari tayinlanadi.

Ma'lumotlar xavfsizligi funksiyasini tahlillab, funksiya elementi mos satr/ustun bilan bog'lanadi va element qiymati satr/ustunga element belgisi sifatida beriladi.

Foydalanuvchi belgisini yaratish uchun, barcha ma'lumotlar xavfsizligi funksiyalari tahlillanadi va ma'lumotlarga mos xavfsizlikning noyob elementlari tanlab olinadi. Foydalanuvchi ushbu elementlardan har bir funksiyada foydalana olishi mumkin. Xavfsizlik elementlari barcha xavfsizlik funksiyalaridan, foydalanuvchini foydalanish huquqini identifikatsiyalashda foydalanish belgisi ko'rinishida, aniqlanadi.

Avtorizatsiyani ishlashda, foydalanuvchi belgisi orqali aniqlangan foydalaniluvchi diapazon so'rovning haqiqiy diapazoni bilan taqqoslanadi. Xususan, foydalanish belgisi xavfsizligi elementini taqqoslash lozim.

Xavfsizlikning xuddi shu elementlaridagi bir-biriga bog'liqlik va va element amallari ta'riflariga muvofiq, foydalanish belgisi ko'rsatilgan xavfsizlik elementi qiymati ustuvorligi ma'lumotlar xavfsizligi elementi qiymatiga teng yoki undan katta bo'lsa, foydalanuvchi ma'lumotlar belgisi diapazonidan foydalanishi mumkin. Avtorizatsiya qoidalari 4.6-jadvalda ko'rsatilganidek tavsiflash mumkin.

Foydalanuvchi belgisi UL va ma'lumotlar belgisi DL autentifikatsiya funksiyasining kirish parametrlari hisoblanadi. Faraz qilaylik, DL da *El* va UL da esa mos holda *Ye2* mavjud. Agar *El E2* ga ekvivalent bo'lsa (yoki *Ye2* ustuvorligi yuqori bo'lsa), *Yel* ga foydalanish ruxsati beriladi.

Ma'lumotlar funksiyasi ham vakolatlar siyosatida muhim rol o'ynaydi [77]. Tavsiya etilgan modelda ma'lumotlar jadvali ma'muri himoya belgilarini tayinlash uchun vakil sifatida tanlangan.

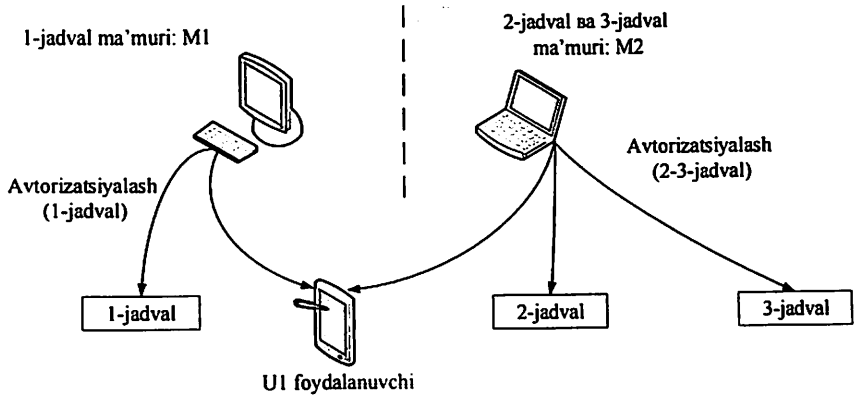
4.6-jadval

Avtorizatsiya qoidalarining tavsifi

I.Asosiy elementlar
U-foydalanuvchi: foydalanishni boshqarish sub'ekti, bu bir xil funksiyaga ega bitta foydalanuvchi yoki foydalanuvchilar guruhi. D-ma'lumotlar: foydalanishni boshqarish ob'ekti, bu vakolatga aniqliklik kiritishi talablariga mos, ma'lumotlar bazasi jadvalining satr va ustuni. UL-foydalanuvchi belgisi: foydalanuvchilar foydalanishi mumkin bo'lgan ma'lumotlar diapazonini belgilaydi. DL-ma'lumotlar belgisi: foydalanish belgisi egasi, foydalanishi mumkin bo'lgan ma'lumotlar funksiyasini belgilaydi. F-ma'lumotlar funksiyasi: ma'lumotlar funksiyasini va funksiya qiymatlari o'rtasidagi munosabatni, jumladan meros va farqlash qoidalarini belgilaydi. E-vaziyat elementi: ma'lumotlar belgisi qiymati, ma'lumotlar belgisini muayyan taqsimlanishini belgilaydi.
II.Joylashuv strategiyasi
$createDL: \{createDL(e,n) \mid e \in E, E \in f\ (f \in F), n = 1\}$ $createUL: \{createUL(e,n) \mid e \in E, E \in f\ (f \in F), n = [1, count\ (F)], \forall e1 \in f1, e2 \in f2, e1 \neq e2, f1 \neq f2\}$ $POLICY: \{UL \times DL \mid \forall UL = createUL\ (e1,n), DL = createDL\ (e2,n), e1 \in f1, e2 \in f2, f1 = f2\}$ $policy(d): \{policy(d) \in POLICY, d \in DATA \rightarrow hasf \in F\}$
III.Avtorizatsiya qoidasi
$is\_authorizaed\ (ul, dl) = \forall e1 \in dl, exists\ e2 \in ul, e1 = e2\ or\ priority\ (e2) \gg priority\ (e1)$

Buning sababi, jadval ma'muri, xavfsizlik belgilarini markazlashgan tarzda taqsimlash yuzaga keltiruvchi, juda katta ish yuklamasini kamaytirishi, hamda foydalanuvchilarga va ma'lumotlarga foydalanishning identifikatsiya huquqlarini aniq tayinlashi mumkin [77].

4.14-rasmda ma'murlar tomonidan jadvalni avtorizatsiyalash misoli keltirilgan.



4.14-rasm. Ma'murlar tomonidan jadvalni avtorizatsiyalash

Ikkita jadval ma'murlari mavjud: M1 (1-jadval ma'muri) va M2 (2 va 3-jadval ma'muri). M1 ma'mur U1 -foydalanuvchiga 1-jadvaldan foydalanish vakolatini tayinlash huquqga ega, M2 ma'mur esa U2-foydalanuvchiga 2 va 3-jadvallarning foydalanish vakolatini tayinlash huquqiga ega.

Foydalanuvchi nizolashuvchi vakolatni aktvlashtirganda, u ushbu vakolat bilan COIga ega ikkinchi nizolashuvchi vakolatdan foydalanish huquqini ola olmaydi, ya'ni foydalanuvchiga "Foydalanish taqiqlangan" xabari keladi. Foydalanuvchi birinchi action='approve' (ma'qullash) va object ='objl' vakolatini aktivlashtirib bo'ldi. Endi foydalanuvchi action='submit2' (bo'ysunish) va object='objl' vakolatini olishga urinadi. Bu ikkala vakolatlar "ma'qullash" va "bo'ysunish" ta'sirlarning nizolashuvi tufayli, nizolashadi. Foydalanuvchi 1-vakolatni aktivlashtirib bo'ldi, 2-vakolatdan foydalanish uchun esa avtorizatsiyalanmadi. Foydalanuvchining "Foydalanish taqiqlangan" xabari olishning sababi shunda.

Monografiyada taklif etilgan modelning ishonchliligi uchun foydalanuvchi belgisi va SQL so'rovi yordamida, misol tariqasida, kombinatsiyalangan model asosida foydalanish huquqini tekshirish natijalari generatsiyalanadi. Faraz qilaylik, foydalanuvchida barcha jadvallar uchun foydalanish huquqi belgisi mavjud. Xavfsizlik funksiyalari shakli va xavfsizlik elementlari, xavfsizlik siyosati tomonidan 4.7-jadvalda ko'rsatilganidek, tahlillanadi.

4.7-jadvalda tahlil natijalari tarkibida to'rtta maydon mavjud: xavfsizlik funksiyasi, xavfsizlik funksiyasining turi, himoya funksiyasining tasnifi va element.

4.7-jadval

Foydalanuvchi belgisi axboroti

Tahlillanuvchi foydalanuvchi belgisi axboroti	**Sharhlar**

[
{
xavfsizlik funksiyasi:FEATURE1,
xavfsizlik funksiyasining turi: SET,
himoya funksiyasining tasnifi: ROW,
element:ELEMENT1
},
{
xavfsizlik funksiyasi:FEATURE2,
xavfsizlik funksiyasining turi: SET,
himoya funksiyasining tasnifi: ROW,
element:ELEMENT2
},
{
xavfsizlik funksiyasi: FEATURE3,
xavfsizlik funksiyasining turi: ARRAY,
himoya funksiyasining tasnifi: COLUMN
element:ELEMENT3
}
]
	ELEMENT1 rolining konfiguratsiyasi:
	{
	field:"col1",
	operator :"=",
	value : ["val1","val2"]
	}
	
	ELEMENT2 rolining konfiguratsiyasi:
	{
	
	field:"col5",
	operator :"=",
	value:["val5"]
	}
	ELEMENT3 tahlili va chiziqli ustuvorlik munosabati:
	ELEMENT3=E2
	Qisman tartib munosabati:
	E1>E2>E3

Dastlab, jadvalning har bir ustuniga ma'lumotlar belgisi beriladi. Faraz qilaylik, ma'lumotlar jadvali tarkibida beshta maydon [col1, col2, col3, col4, col5] mavjud. Vakolatlar siyosatiga muvofiq olingan foydalanish natijalari foydalanishni detallashtirilgan nazoratini amalga oshiradi (4.8-jadval).

4.8-jadval

Foydalanilanuvchi vakolatlar

SQL so'rovi	Foydalanish natijasi
SELECT col1 FROM table WHERE (col1=val1 OR col1=val2) AND col5=val5	TRUE
SELECT COUNT (col1) FROM table WHERE (col1=val1 OR col1=val2) AND col5=val5	TRUE
SELECT*FROM table WHERE (col1=val1 OR col1=val2) AND col5=val5	FALSE
SELECT col1 FROM table WHERE col1=val1 OR (col1=val2 AND col4=val4)	FALSE

Monografiyada Taklif etilgan modelni tahlillashda uning uning texnik iqtisodiy asoslanganligiga va boshqarishning murakkabligiga e'tibor berish lozim.

1. Imkoniyati. Taklif etilgan model talabning amaliy rejasiga asoslangan va undan ishlayotgan tizim platformasiga aralashuvisiz ulanishda foydalanish mumkin.

2. Boshqarishning murakkabligi. Belgilarni yaratish amali va avtorizatsiyalash jadval ma'muri tomonidan bajariladi. U vakolat ma'murining vakolatlarini taqsimlaydi. Taklif etilayotgan model avtorizatsiyani qa'tiyroq qilishi va, markazlashtirilgan avtorizatsiya yuzaga keltiruvchi, ish yuklamasini kamaytirishi mumkin.

Xavfsizlik siyosati bir nechta xavfsizlik funksiyalarini o'z ichiga olishi mumkinligi sababli, siyosatni ishlab chiqish tartibi taklif etilayotgan modelning muhim muammosi hisoblanadi. Vakolatlar himoya elementlarining paydo bo'lish ketma-ketligiga muvofiq shakllantiriladi.

Kombinatsiyalangan modelda vakolatni tekshirish, asosan, ikkita modulda-ustun sathidagi tekshirish modullarida amalga oshiriladi.

Foydalanishni cheklashning kombinatsiyalangan modeli turli ob'ekt ma'lumotlarini bir-biri bilan bog'lashni yakunlashda ishlatiladi. Bu foydalanish cheklash modeliga nafaqat ma'lumotlarni tekshirish jarayonini yanada aniqroq belgilash imkonini beradi, balki ma'lumotlarni tekshirish natijalarini ta'minlab, o'rnatiluvchi texnologiyalarni yaratish xarakteristikalariga mos keladi.

XULOSA

Foydalanishni cheklash usullarining samaradorligini oshirish bo'yicha olib borilgan tadqiqot natijalari asosida foydalanishni boshqarish qismtizimlariga qo'yiladigan talablar, axborotni ruxsatsiz foydalanishdan himoyalashga qaratilgan tizimni qurishda, asosiy mexanizmlar sifatida ajralib turishi va tizim ishonchliligini oshirishi ko'rsatib berildi.

Axborot tizimini ishlab chiqish bosqichida hujumlar oqimining va qarshi ta'sir choralari intensivliklarini hisoblash asosida himoyalanganligini inobatga olishda qo'llaniluvchi axborot tahdidlari holatini aniqlash modeli taklif etilgan. Ushbu modelning himoyalangan axborot tizimlarini ishlab chiqishda qo'llanilishi natijasida himoya tizimiga ta'sir etuvchi hujumlar oqimi λ ga samarali qarshi ta'sir etish uchun $\mu = 0.3 - 0.5$ ga teng intensivlikga ega qarshi ta'sir vositasini qo'llanilishi zarurligiga aniqlik kiritildi.

Mavjud xavfsizlik modellarining tahlili, maxfiylikni muhofaza qilish nuqtai nazaridan, maxsus maqsadli axborot tizimini ishlab chiqishda konfidentsiallik, yaxlitlik va foydalanuvchanlik kriteriylari bo'yicha qo'yilgan talablarga javob bera oladigan foydalanishni cheklash tizimini qurishda RBAC modelini qo'llash samarali ahamiyatga ega ekanligini asoslab berildi. Foydalanishni cheklash tizimining an'anaviy "passiv" komponentalari bilan bir qatorda "aktiv" komponentalarini o'z ichiga oluvchi konseptual model ishlab chiqilgan va ushbu model asosida quriladigan foydalanishni cheklash tizimini sintezlashda "Ma'murlashning soddaliligi" va "Rekonfiguratsiyaga qaror qabul qilish" kriteriylari bo'yicha RBAC modeli samaradorlik ko'rsatkichlari yuqori ekanligi asoslab berildi.

RBAC bilan ABAC modellarining kombinatsiyalashuvi asosida foydalanishni boshqarishda ma'murlashni soddalashtirish va ulardagi muammolarni bartaraf etish imkoniyatlarini beruvchi dinamik rollarga, atributlarga va rollarga asoslangan modelning kombinatsiyalari taklif etildi. Bunda ushbu model kombinatsiyalar mavjud modellardan farqli o'laroq vakolatlarni aniq sozlanishi va ma'murlashda moslashuvchanlik imkoniyatlari bilan to'ldirildi.

Axborot tizimlarida mavjud bo'ladigan nizolashadigan va nizolashmaydigan rollarni tartibga solishga imkon beruvchi vazifalarni taqsimlash (SOD)ni vakolatlar sathida amalga oshiradigan dinamik RBAC modeli ishlab chiqilgan. Ushbu modelda atributlar qo'shilishi moslashuvchanlikni ta'minlashga, ma'mur yuklamasi hajmini kamay-

tirishga va ma'mur tomonidan buzilishlar sodir etilmasligiga imkon berdi.

Monografiyada axborot tizimlarini ma'murlashda oddiyligi, dinamikligi, qat'iy xavfsizlikni va SODning samarali amalga oshirilishi orqali tizimdan foydalanuvchi ichki xodimlar va tashqi mijozlar uchun vakolatlar yaratilishida SODni vakolatlar sathida foydalanishni boshqarishning kombinatsiyalangan C-RBAC modeli taklif etildi. Ushbu SODni vakolatlar sathida foydalanishni boshqarishning kombinatsiyalangan C-RBAC modelining tatbiq etilishi tizimdan foydalanuvchi ichki xodimlar va tashqi mijozlar uchun vakolatlar yaratilishiga sarflanadigan vaqt 3 barobarga kamayishiga, bir xil urinishlar sonida (N=6) vakolatlarni yaratish tezligi 2.7 martaga oshishiga axborot tizimini himoyalanganlik darajasi esa 37%ga oshishiga olib keldi.

Vakolatlarni birma-bir yaratish uchun ob'ektlarga ta'sirlarni qo'llash, bir xil ta'sirli va turli ob'ektli bir necha vakolatlarni yaratish uchun kategoriyalar konteyneriga umumiy ta'sirlar naborini qo'llash, bir xil ob'ektli va turli ta'sirli bir necha vakolatlarni yaratish uchun ob'ektlarga umumiy ta'sirlar naborini qo'llash va turli ob'ektli va turli ta'sirli uchun bir necha vakolatlarni yaratish uchun kategoriyalar konteyneriga ta'sirlarning umumiy naborini qo'llash orqali nizolashuvchi va nizolashmagan atributli vakolatlar yaratishning 4 ta usuli algoritmlari ishlab chiqilgan. Taklif etilayotgan usullarning algoritmi tatbiq etilishi natijasida axborot tizimi ma'muri faoliyatining yuklama hajmi 24%ga kamaydi.

Monografiyada taklif etilgan C-RBAC modeli foydalanishni nazoratlashning detallashtirilishi va moslashuvchanligi nuqtai nazaridan, an'anaviy RBAC modeliga nisbatan qaror qabul qilish samaradorligiga ega. Foydalanishni boshqarishning kombinatsiyalangan modeli asosida ishlab chiqilgan dasturiy ta'minot amaliy holatda qo'llanilganda axborot tizimi xizmatlardan foydalanilishida xavfsizlik darajasi ortganini va foydalanuvichlarga yaratilayotgan alohida vakolatlar ularning xavfsizligini ta'minlaganini ko'rsatdi. Xususan, axborot tizimining hujumlar oqimiga tegishlicha intensivlik bilan qarshi turish uchun, nafaqat hujum o'tkazish bosqichida, balki razvedka bosqichida ishlovchi himoya elementlarini samarali boshqaruvi amalga oshirildi. Ushbu dasturiy ta'minotni qo'llanilishi natijasida tahdidlarga qarshi tezkor javobini 2,5 martaga oshirishga shuningdek ishonchlilikni ko'tarilishi olib keldi. Shunugdek, taklif etilgan modelda, rol-vakolat munosabatlarini aniq-

lashda foydalanuvchi atributlarining foydalaniluvchi bo'lishligi talabi ta'minlanadi. Taklif etilgan model, foydalanuvchi atributlari va vakolatlariga muvofiq, rollar-vakolatlar munosabatlarini yanada detallashtirilgan holda nazoratlash imkonini beradi. Foydalanishni nazoratlash siyosatini amalga oshirishda dastlab siyosatga ega bo'lish, so'ngra uni tahlillash lozim. Siyosatni amalga oshirish samaradorligi, asosan, siyosatni aniqlash usuliga va tahlillashda ishlatiluvchi algortimga bog'liq. Siyosatni qidirish samaradorligini oshirish uchun siyosatni rollarga va vakolatlarga bog'lash mumkin, chunki foydalanishni boshqarish tizimlarida rollar va vakolatlar barqarorroq va, odatda, foydalanuvchilarga nisbatan, soni bo'yicha kam.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'z DSt ISO/IEC 27033-3:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 3-qism. Etalon tarmoq ssenariylari. Tahdidlar, loyihalashtirish usullari va boshqaruv masalalari".

2. O'z DSt ISO/IEC 27031:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot texnologiyalari va kommunikatsiyalarini biznesga joriy qilishga tayyorligi bo'yicha boshqaruvchilik ko'rsatmalari".

3. O'z DSt ISO/IEC 27033-1:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 1-qism. Sharh va konsepsiyalari".

4. O'z DSt ISO/IEC 27033-2:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 2-qism. Tarmoq xavfsizligini loyihalashtirish va joriy etish bo'yicha rahbariy ko'rsatmalar".

5. O'z DSt ISO/IEC 27033-3:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 3-qism. Etalon tarmoq ssenariylari. Tahdidlar, loyihalashtirish usullari va boshqaruv masalalari".

6. O'z DSt ISO/IEC 27033-4:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 4-qism. Xavfsizlik shlyuzlarini qo'llagan holda tarmoqlararo xavfsizlikni ta'minlash uchun kommunikatsiyalar".

7. O'z DSt ISO/IEC 27033-5:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 5-qism. Virtual hususiy tarmoqlarni qo'llagan holda tarmoqlararo xavfsizlikni ta'minlash uchun kommunikatsiyalar".

8. Getting Past The Cyberspace Hype. Adaptive Security. A Model Solution-A Solution Model. 15 June 1997. Internet Security Systems, Inc.

9. INCITS 359-2004 Information Technology - Role Based Access Control. STANDARD by InterNational Committee for Information Technology Standards (formerly NCITS), 02/03/2004,-P.2-10.

10. INCITS 359-2012 Role Based Access Control. STANDARD by InterNational Committee for Information Technology Standards (formerly NCITS), 05/29/2012.

11. NIST Special Publication. Guide to Attribute Based Access

Control (ABAC) Definition and Considerations/ Natl. Inst. Stand. Technol. Spec. Publ. January 2014. 800-162, 47 pages. URL: https://doi.org/10.6028/NIST.SP.-P.800-162.

12.Гужва Д.Ю. Теория и практика нейросетевого управления защитой информации в инфотелекоммуникационных системах. Монография-М: Издательство ВА РВСН им. Петра Великого, 2008.- С. 239.

13.Alam M., Emmanuel N., Khan T., Xiang Y., Hassan H. Garbled role-based access control in the cloud. J. Ambient Intell. Humaniz. Comput. 2018, 9, -P.1153-1166.

14. Sandhu R., Bhamidipati V., Munawer Q. The ARBAC97 model for role-based ad-ministration of roles//ACM Trans Inf Syst Secur Feb. 1999; 2(1):105-35.

15. Sandhu R., Munawer Q. The ARBAC99 model for administration of roles//In:Computer security applications conference, 1999. (ACSAC'99) proceedings. 15th annual; 1999. -P. 229-38.

16. Oh S., Sandhu R., Zhang X. An effective role administration model using organi-zation structure // ACM Trans Inf Syst Secur 2006; 9(2):113-37 May.

17.Ninglekhu J., Krishnan R. Attribute based administration of role based access control: a detail description // CoRR 2017. Vol. abs/1706.03171.

18.Barkley J. Comparing simple role based access control models and access control lists // In Proceedings of the second ACM workshop on Role-Based Access Control, Fairfax, VA, USA, 6-7 November 1997. -P. 127-132.

19.Chen B., Yang C., Yeh H., Lin C. Mutual Authentication Protocol for Role-Based Access Control Using Mobile RFID//Appl. Sci. 2016, 6. -P.215.

20.Crampton J., Morisset C. Monotonicity and completeness in attribute-based access control. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol. 8743; 2014. -P. 33-48.

21.Habib M.A., Mahmood N., Shahid M., Aftab M.U., Ahmad U. Faisal C.M.N. Permission Based Implementation of Dynamic Separation of Duty (DSD) in Role Based Access Control (RBAC)//In Proceedings of the 8th International Conference on Signal Processing and Communication Systems, Gold Coast, Australia, 15-17 December 2014.

-P.1-10.

22. Longhua Zhang, Gail-Joon, Ahn, Bei-Tseng Chu. A rule-based framework for role-based delegation and revocation//ACM Transactions on Information and System Security. 6 (3), 404-441. doi:10.1145/937527.937530.

23. Jackson D. Depandable Software by Design // 7 Scientific American, 2006; vol. 294, N 6. -P. 69-75.

24. Jin X. Sandhu R. Krishnan R. RABAC: role-centric attribute-based access control/In: Kotenko I., Skormin V., editors//Computer network security, 7531. Springer Berlin Heidelberg; 2012. -P. 84-96.

25. Jueneman R.R. Integrity controls for military and commercial applications//In Proceedings of the Fourth Aerospace Computer Security Applications, Orlando, FL, USA, 12-16 September 1988. -P. 298-322.

26. Kuhn D. R., Coyne E. J., Weil T.R. Adding attributes to role-based access control//Computer 2010, 43. P.79-81.

27. Kumar C. A. Mouliswaran S.C., Li J., Chandrasekar C. Role based access control design using triadic concept analysis//J Central South Univ 2016; 23(12):3183-91.

28. Kumar C. A. Designing role-based access control using formal concept analysis // Secur Commun Netw 2013; vol. 6 (3):373-83.

29. Li N. Discretionary access control. In Encyclopedia of Cryptography and Security // Springer: Berlin, Germany, 2011. -P. 353-356.

30. Rajpoot Q., Jensen C., Krishnan R. Attributes enhanced role-based access control model / In: Fischer-Hübner S, Lambrinoudakis C, López J, editors // Trust, privacy and security in digital business, vol. 9264. Springer International Publishing. 2015. -P. 3-17.

31. Samarati P., Vimercati S.C. Access control: Policies, models, and mechanisms//In Proceedings of the International School on Foundations of Security Analysis and Design, Bertinoro, Italy, 18-30 September 2000. -P.137-196.

32. Sandhu R., Munawer Q. How to do discretionary access control using roles//In Proceedings of the Third ACM Workshop on Role-Based Access Control, Fairfax, VA, USA, 22-23 October 1998. -P. 47-54.

33. Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E. Role-based access control models//Computer 1996, 29. -P.38-47.

34. Verma D.C. Simplifying network administration using policy-based management//IEEE Netw. 2002, 16. -P.20-26.

35. Wang X., Wang L., Li Y., Gai K. Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing//IEEE Access 2018, 6.-P. 47657-47665.

36. Yin H., Xiong Y., Zhang J., Ou L., Liao S., Qin Z. A Key-Policy Searchable Attribute-Based Encryption Scheme for Efficient Keyword Search and Fine-Grained Access Control over Encrypted Data // Electronics 2019, 8, 265.

37. Zheng R., Jiang J., Hao X., Ren W., Xiong F., Zhu T. CaACBIM: A Context-aware Access Control Model for BIM // Information 2019, 10, 47.

38. Zhou L., Su C., Li Z., Liu Z., Hancke G.P. Automatic fine-grained access control in SCADA by machine learning//Future Gener. Comput. Syst. 2019, 93, 548-559.

39. Zhu, Y., Huang, D., Hu C.-J., Wang X. From RBAC to ABAC: Constructing flexible data access control for cloud storage services // IEEE Trans. Serv. Comput. 2015, 8, 601-616.

40. Ghosh S., Karar V. Blowfish Hybridized Weighted Attribute-Based Encryption for Secure and Efficient Data Collaboration in Cloud Computing// Appl. Sci. 2018, 8, 1119.

41. Muhammad Umar Aftab, Zhiguang Qin, Negalign Wake Hundera, Oluwasanmi Ariyo, Zakria, Ngo Tung Son, Tran Van Dinh. Permission-Based Separation of Duty in Dynamic Role-Based Access Control Model // Symmetry. Published: 15 May 2019, 11, 669; doi:10.3390/sym11050669.

42. Ramadan Abdunabi, Indrakshi Ray, Robert France. Specification and analysis of access control policies for mobile applications // In: Proceedings of the 18th ACM Symposium on Access Control Models and Technologies (SACMAT 2013). ACM, pp. 173-184. doi:10.1145/2462410.2463206.

43. Gail-Joon Ahn. Specification and cassification of role-based authorization policies // In: Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2003). IEEE, pp. 202-207. doi:10.1109/ENABL.2003.1231408.

44. Al-Kahtani M.A., Sandhu R. A model for attribute-based user-role assignment // In Proceedings of the 18 th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 9-13 December 2002; pp. 1-10.

45. Алгулиев Р.М., Рагимов Э.Р. Об одном методе оценки информационной безопасности корпоративных сетей в стадии их проектирования// Информационные технологии. 2005 - №7.

46. Афонин С.А. Система логического разграничения доступа для облачных информационных систем//Научный сервис в сети Интернет: труды XVIII Всероссийской научной конференции. М.: ИПМ им.М.В. Келдыша, 2016. -С. 51-57. URL: http://keldysh.ru/abrau/2016/17.pdf.

47. Белим С.В., Богаченко Н.Ф. Использование решётки формальных понятий для построения ролевой политики разграничения доступа// Информатика и системы управления. 2018. № 1(55). -С. 16-28.

48. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Совмещение политик безопасности, основанное на алгоритмах поддержки принятия решений // Информационно управляющие системы. 2016. № 5. -С. 66-72.

49. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Теоретико-графовый подход к проблеме совмещения ролевой и мандатной политик
безопасности // Проблемы информационной безопасности. Компьютерные системы. 2010. №2. -С. 9-17.

50. Богаченко Н.Ф. Локальная оптимизация политики ролевого разграничения доступа (Local Optimization of the Role-Based Access Control Policy)//CEUR Workshop Proceedings. 2017. V. 1965. URL: http://ceur-ws.org/Vol-1965/paper14.pdf

51. Васенин В.А., Иткес А.А., Шапченко К.А., Бухонов В.Ю. Реляционная модель логического разграничения доступа на основе цепочек отношений // Программная инженерия. 2015. № 9. -С. 11-19.

52. Володина А.А., Лёвкин И.М. Адаптивный подход к защите информации в больших информационных системах//Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур : Межвузовский сборник трудов VI Всероссийской научно-технической конференции КОНФИБ'15. СПб. : Университет ИТМО, 2016. -С. 65-73.

53. Баландин А.В., Ващенко А.П., Войнов Ю.В., Мукминов В.А. Об архитектуре средств тестирования автоматизированных

систем в условиях моделирования информационных воздействий//Известия Института инженерной физики. 2011. № 1 (19). -С. 36-39.

54. Барабанов А.В., Гришин М.И., Марков А.С. Формальный базис и метабазис оценки соответствия средств защиты информации объектов информатизации//Известия института инженерной физики. 2011. № 3. -С. 82-88.

55. Барабанов А.В., Марков А.С., Цирлов В.Л. Разработка методики испытаний межсетевых экранов по требованиям безопасности информации // Вопросы защиты информации. 2011. № 3. -С.19-24.

56. Бойченко И.А., Сарайкин В.Г. Интегрированная модель политик безопасности в СУБД//Известия высших учебных заведений. Лесной журнал. 2005. № 5. -С. 132-138.

57. Девянин П.Н. О проблеме представления формальной модели политики безопасности операционных систем//Труды Института системного программирования РАН. 2017. Т. 29. № 3. - С. 7-16.

58. Ефанов Д.В., Рощин П.Г. Метод взаимодействия графических приложений с сессионными службами D-Bus в операционной системе с многоуровневым управлением доступом//Проблемы информационной безопасности. Компьютерные системы. 2015. № 1. -С. 34-45.

59. Зегжда Д.П. Общая схема мандатных моделей безопасности и её применение для доказательства безопасности систем обработки информации // Проблемы информационной безопасности. Компьютерные системы. 2000. № 2. -С. 28-32.

60. Иткес А.А. Объединение моделей логического разграничения доступа для сложно-организованных распределённых информационных систем // Проблемы информатики. 2010. № 1, -С. 85-94.

61. Качаева Г.И., Попов А.Д., Рогозин Е.А. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах//Вестник Дагестанского государственного технического университета. Технические науки. 2018.45(1):147-159.

62. Лапин С.А. Модель разграничения доступа для систем,

содержащих равнозначные объекты//Безопасность информационных технологий. 2016. № 2. -С. 49-54.

63. Попов В. ОС И СУБД: Мандатное разграничение доступа//Открытые системы. СУБД. 2017. №1. -С. 19-21.

64. Сердюк Виктор. Комплексный подход к защите компании от вредоносного кода//Журнал "Документальная электросвязь", №19, 2008. URL: https://www.dialognauka.ru/press-center/article/7516/.

65. Харечкин П. В. Методология построения функционально-ролевой модели управления доступом на основе среды радикалов//Молодой ученый.-2009.-№ 12 (12).-С. 22-27.-URL: https://moluch.ru/archive/12/1001/.

66. Шумилин А.В. Основные элементы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в СУБД PostgreSQL ОС специального назначения Astra Linux Special Edition// Прикладная дискретная математика. 2013. № 3(21). -С. 52-67.

67. Irgasheva D.Y., Abdurakhmanov A.A. Synthesis the structural protected computer network // "TATU xabarlari". -Toshkent, 2013. -№3. -B.13-18.

68. Ташев К.А., Иргашева Д.Я., Бекмирзаев О.Н. К вопросу анализа проблем информационной безопасности//«Вестник ТУИТ» -Ташкент, 2014. - №1(29). - С.49-54.

69. Irgasheva D.Y. Role model with zone differentiation of access// IJRET: International Journal of Research in Engineering and Technology. http://ijret.esatjournals.org. Volume:5. Issue:5, May 2016. -P.176-181

70. Иргашева Д.Я., Усманов А.К. Разработка ролевой модели с зональным разграничением доступа//Science and World, International scientific journal, 2016, № 6 (34), 2016, Vol. I, p.35-40.

71. Ganiev S.K., Irgasheva D.Y. Model of the state of threats to the Access Control System // Bulletin of TUIT: Management and Communication Technologies. https://uzjournals.edu.uz/tuitmct/vol2/iss2/2/. 2019 2 (45). -P. 30-37.

72. Irgasheva D.Y., Rustamova, S.R. Development of Role Model for Computer System Security // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities. DOI:10.1109/ICISCT47635.2019.9012058.

ICISCT 2019.

73. Ganiev S.K., Irgasheva D.Y. About of One Methods Synthesis the Structural Protected Computer Network // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities. DOI: 10.1109/ICISCT47635.2019.9011891. ICISCT 2019.

74. Yakubgjanovna I.D., Ubaydullayevna X. Study the methods of internal audit of information security in organizations // International Journal of Emerging Trends in Engineering Research. DOI: 10.30534/ijeter/2020/163872020. 2020, 8(7). -P. 3935-3941.

75. Ganiyev S.K., Irgasheva D.Ya., Rustamova S.R. Foydalanishni cheklash tizimining konseptual modeli//Ilmiy-texnik jurnal "Axborotkommunikatsiyalar: Tarmoqlar, Texnologiyalar, Yechimlar".-Toshkent, 2020. -№4. (56). -B. 58-63.

76. Ganiyev S.K., Irgasheva D.Ya., Rustamova S.R. Foydalanishni cheklash tizimining rol va atribut asosida boshqarish modeli// "Muxammad al-Xorazmiy avlodlari" jurnali. -Toshkent, 2020. -№4 (14). -B.45-54.

77. Иргашева Д.Я. Повышение эффективности методов разграничения доступа на основе ролей // Журнал «Мухаммад ал-Хоразмий авлодлари». -Ташкент, 2020. -№4 (14) - С.144-149.

78. Durdona Yakubdjanovna Irgasheva / On the Basic Method for Solving the Problem of Synthesizing Access Control Systems // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities. DOI: 10.1109/ICISCT50599.2020.9351444. ICISCT 2020.

79. Иргашева Д. Концепция информационной безопасности в распределенных системах базы данных "Проблемы информационной безопасности и кибербезопасности в сфере информационно-коммуникационной технологии" сборник Республиканской научно-технической конференции. Ташкент - 2018. -С.39- 46.

80. Irgasheva D.Y., Abramov A.S. Access control policy subjects to objects in distributed Information and Communication systems//2013 International Conference in Central Asia on Internet (ICI 2013, 8th-10th of October).

81. Иргашева Д.Я. Модель администрирования прав доступа ролей // Сборник тезисов и докладов Республиканского семинара

"Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения"- Ташкент, 2013. -С. 14-16.

82. Иргашева Д.Я. Функционально - ролевая модель разграничения доступа с зональной политикой//Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Подготовлены по результатам международной молодежной научно-практической конференции СКФ МТУСИ. ИНФОКОМ-2015, часть I.- Ростов-на-Дону.: ПЦ. Университет. СКФ МТУСИ, 2015, (ISSN 2221-7975). -С.462-465.

83. Irgasheva D.Ya., Hamidov Sh.J. Tarmoq hujumlarini aniqlash usullarining tadbiqi // Iqtisodiyotning real tarmoqlarini innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining o'rni. Respublika ilmiy-texnik anjumanining Ma'ruzalar to'plami. 3-qism. Toshkent-2017. -B.150-152.

84.Иргашева Д.Я., Азимова У.А., Гаипназаров Р.Т. К вопросу обеспечения целостности структуры базы данных//Сборник тезисов и докладов Республиканского семинара "Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения". -Ташкент, 2013. -С. 35-37.

85.Ганиев С.К., Иргашева Д.Я. К вопросу обеспечения надежности системы защиты информации // Сборник докладов Республиканской научно - технической конференции "Информационные технологии и проблемы телекоммуникаций". - Ташкент, 2013. -С. 201-201.

86.Иргашева Д.Я., Гаипназаров Р.Т. К вопросу обеспечения информационной безопасности с помощью аутентификации на основе одноразового пароля//Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Международная молодёжная научно-практическая конференция СКФ, МТУСИ "ИНФОКОМ-2014". Ростов-на-Дону- 2014. -С.472-474.

87.Иргашева Д., Рустамова С. К вопросу формализации политики безопасности предприятия//Сборник тезисов и докладов Республиканского семинара "Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения". - Ташкент, 2020. -С. 43-47.

88.Иргашева Д., Ташев К., Рустамова С. Анализ моделей разграничения доступа в информационных системах//Сборник

тезисов и докладов Республиканского семинара “Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения”. -Ташкент, 2020. -С.20-27.

89.Иргашева Д.Я., Гаипназаров Р.Т., Отахонов А.У. Методы оценивания угроз информационной безопасности//Сборник тезисов и докладов Республиканского семинара “Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения”. -Ташкент, 2013. -С. 98-99.

90.Иргашева Д.Я., Гаипназаров Р.Т., Шомахамедов Ж.Ф. Повышения надежности системы защиты информации от несанкционированного доступа // Труды международной научно-практической конференции “ИНФОКОМ-2015”. - Ростов-на-Дону, 2015. -С.459-462.

91.Иргашева Д.Я., Гуломов Ш.Р.К вопросу обеспечения надежности компьютерных сетей // Международная научно – практическая конференция “INNOVATION – 2012”, Ташкент, Сборник научных статей. -С. 267-268.

92.Иргашева Д.Я., Усманов А.К. Анализ формальных моделей безопасности//“O‘zbekiston Respublikasi huquqni muhofaza qilish tizimlarida lokal kompyuter tarmoqlarini amalda joriy etish yo‘llari va ularning xavfsizligini ta’minlash” respublika ilmiy-amaliy seminari materiallari to‘plami. -Toshkent, 2016. -B.67-71.

93.Irgasheva D.Ya., Xolimtayeva I.U. Xurujlardan himoyalangan kompyuter tarmog‘ining strukturasini tashkillashtirish//Axborot va telekommunikatsiya texnologiyalari muammolari. Ilmiy-texnik konferensiyasining ma’ruzalar to‘plamiToshkent-2015. -B.466-468.

94.Иргашева Д.Я., Холмуратов О.Н. К вопросу анализа скрытых каналов утечки информации//Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Международная молодёжная научно-практическая конференция СКФ, МТУСИ “ИНФОКОМ-2013”, Россия, Ростов-на-Дону-2013. -С. 308-310.

95.Irgasheva D.Y., Islomov Sh.Z. Construction hardware protection info-communication systems from network attacks // Transactions of the International Scientific Conference “Perspectives for the Development of Information Technologies ITPA-2015”. Tashkent-2015. -P. 89-93.

96.Irgasheva D.Y., Nabiev I.M. Kompyuter tizimlarinini

himoyalashda ikki omilli autentifikatsiyalash usulining o'rni // Iqtisodiyotning real tarmoqlarini innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining o'rni. Respublika ilmiy-texnik anjumanining Ma'ruzalar to'plami. 3-qism. Toshkent-2017.-B. 85-87.

97. Irgasheva D., Sodikova D. Z. Analyzing security parameters of database management systems // Molodoy uchyonыy. Mejdunarodnыy nauchnыy jurnal. № 15 (305)/Aprel, 2020 g.-R.84-86.

98. Verlan Anatoliy Fedorovich, Ganiev Salim Karimovich, Irgasheva Durdona Yakudjanovna, Imamaliev Aybek Turapbayevich / Methods of Formation of a Security Policy in Access Differentiation Processes // 4Th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE - 2014). University of National and World Economy Sofia, Bulgaria. -P.204-211.

99. Иргашева Д.Я., Шомахамедов Ж.Ф. Требование к системе защиты информации при формировании политики безопасности инфокоммуникационных систем // Проблемы информационных и телекоммуникационных технологий. Сборник докладов Республиканской научно – технической конференции. Часть 1. Ташкент- 2015. -С. 455-457.

100. Иргашева Д.Я. Классификация и свойство компьютерных вирусов// «O'zbekiston Respublikasi huquqni muhofaza qilish tizimlarida lokal kompyuter tarmoqlarini amalda joriy etish yo'llari va ularning xavfsizligini ta'minlash» respublika ilmiy-amaliy seminari materiallari to'plami. -Toshkent-2016. -B.61-64.

101. Ташев К.А., Иргашева Д.Я., Абдурахманов А.А., Имамалиев А.Т. Модель системы мониторинга безопасности в инфокоммуникационных системах // Республиканский семинар-Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения. Сборник тезисов и докладов. Ташкент- 2013. -С. 25-27.

102. Batra G., Atluri V., Vaidya J., Sural S. Enabling the Deployment of ABAC Policies in RBAC Systems. In Proceedings of the 32nd IFIP Annual Conference on Data and Applications Security and Privacy, Bergamo, Italy, 16-18 July 2018. -P. 51-68.

103. Ganiyev S.K., Tashev K.A., Irgasheva D.Ya., Xudoykulov Z.T., Gaipnazarov R.T., Rustamova S.R. "SAS-foydalanishni cheklash tizimi dasturi"//O'ZBEKISTON RESPUBLIKASI ADLIYA

VAZIRLIGI HUZURIDAGI INTELLEKTUAL MULK AGENTLIGI. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro'yxatdan o'tkazilganligi to'g'risidagi guvohnoma. № DGU 09478. Toshkent, 25.11.2020.

104.Ganiyev S.K., Tashev K.A., Irgasheva D.Ya., Xudoykulov Z.T., Islomov Sh.Z., Rustamova S.R. "RBAS-foydalanishni cheklash tizimi dasturi"//O'ZBEKISTON RESPUBLIKASI ADLIYA VAZIRLIGI HUZURIDAGI INTELLEKTUAL MULK AGENTLIGI. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro'yxatdan o'tkazilganligi to'g'risidagi guvohnoma. № DGU 09608. Toshkent, 07.12.2020.

105.Huang J., Nicol D.M., Bobba R., Huh J.H. A framework integrating attribute-based policies into role-based access control. In: Proceedings of the 17th ACM symposium on access control models and technologies; 2012. -P.187-96.

106.Kolegov D.N., Tkachenko N.O., Chernov D.V. Razrabotka i realizatsiya mandatnыx mexanizmov upravleniya dostupom v SUBD MySQL//Prikladnaya diskretnaya matematika. Prilojeniye. 2013. № 6. - S. 62-67.

107.Ganiev S.K., Irgasheva D.Y., Ganiev A.A. Ma'lumotlar bazasi xavfsizligi:OTM uchun darslik.-T: "Fan va texnologiya" nashriyoti, Toshkent-2016. -B.225.

108.Аграновский А.В., Мамай В.И., Назаров И.Г., Язов Ю.К. Основы технологии проектирования систем защиты информации в информационно-телекоммуникационных системах. Изд-во СКНЦ ВШ, 2006. - С. 258.

109.Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий.М.:ДМК Пресс, 2017.- С.224.

110.Гайдамакин Н.А. Теоретические основы компьютерной безопасности:учеб. пособие. Екатеринбург: изд-во Уральского университета, 2008. - С. 212.

111.Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: изд-во Уральского университета, 2003.-С.328.

112.Галатенко В. А. Основы информационной безопасности. Учеб. пособие:под ред. В. Б. Бетелина.-4-е изд. М.:Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория

знаний, 2008. -С. 205.

113.Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. Учеб. пособие для вузов. - М.: Радио и связь, 2006. -С. 176.

114.Девянин П. Н. Модели безопасности компьютерных систем. Учеб. пособие для студ. высш. учеб. заведений:М.: Издательский центр "Академия", 2005.-С. 144.

115.Девянин П. Н., Михальский О. О., Правиков Д. И., Щербаков А. Ю. Теоретические основы компьютерной безопасности. Учеб. пособие для вузов-М.: Радио и связь, 2000. -С.192.

116.Зегжда Д. П. Основы безопасности информационных систем. Горячая линия Телеком, 2000. -С. 452.

117.Корт С. С. Теоретические основы защиты информации. Учеб. пособие-М.: Гелиос АРВ, 2004. -С. 240.

118.Куликов С.С. Модели безопасности компьютерных систем. Учеб. пособие[Электронный ресурс]. Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015, -С. 178.

119.Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. Под ред. А.С.Маркова. - М.: Радио и связь, 2012. -С.192.

120.Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей- М.: Академия, 2006.-С. 240.

121.Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учеб. пособие-М.: ИД "ФОРУМ": Инфра-М, 2017. -С. 416.

122. URL: http://www.rv-lab.ru/it/is_2008/part3.htm-Амелин Р.В. Информационная безопасность. Электронный учебник.

123. URL:https://studme.org/180195/informatika/modeli_metody_rolevogo_sessionnogo_kontrolya_dostupa_voprosy_identifikatsii_roley_sessiy-Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий.

124. URL:https://club.cnews.ru/blogs/entry/rolevaya_model_i_metod_kontrolya_dostupa- Ролевая модель и метод контроля доступа.

125. URL:https://kzref.org/-kurs-lekcij-problemi-bezopasnosti-v-informacionnih-tehnologiya.html-Курс лекций "Проблемы

безопасности в информационных технологиях".

126. URL:https://www.securitylab.ru/blog/company/solarsecurity/349044.php-Построение ролевую модель управления доступом. Часть первая.

127. URL: http://avtor.ua/resheniya/sistemy-upravleniya-dostupom.html-Системы управления доступом к информационным ресурсам.

QISQARTMA SO'ZLAR RO'YXATI

ABAC (Attribute Based Access Control) - foydalanishni atributli cheklash

AHT-axborotni himoyalash tizimi.

COI (Conflict Of Interest)-manfaatlar ixtilofi.

DAC (Discretionary Access Control)-xavfsizlikning diskretsion nazorati.

DoS - Denial of Service.

FChT - foydalanishni cheklash tizimi.

IP – Internet protocol.

KT-kompyuter tizimi.

MAC (Mandatory Access Control)-xavfsizlikning mandatli nazorati.

ME (Mutually Exclusive)-bir-birini inkor qilish.

MEP (Mutually Exclusive Permissions)-bir-birini inkor etuvchi vakolatlar.

MER (Mutually Exclusive Roles)-bir-birini inkor qiluvchi rollar.

NIST - National Institute of Standards and Technology.

OpenCV - Open Source Computer Vision Library.

PIN - Personal Identification Number.

RBAC (Role-Based Access Control)- xavfsizlikning rolli nazorati.

SOD (Segregation Of Duties)- vazifalarni taqsimlash.

SQL (Structured Query Language)- tili ma'lumotlarni qayta ishlash tili.

MUNDARIJA

Irgasheva Durdona Yakubdjanovna

FOYDALANISHNI CHEKLASH USULLARINING SAMARADORLIGINI OSHIRISH

(MONOGRAFIYA)

Toshkent – «ZEBO PRINT» – 2022

Muharrir: X. Tahirov
Texnik muharrir: S. Meliquziyeva
Musahhih: M. Yunusova
Sahifalovchi: A. Muhammad

Nashr. lits № 2244. 25.08.2020.
Bosishga ruxsat etildi 05.10.2022.
Bichimi 60x84 1/16. Ofset qog'ozi. ''Times New Roman'' garniturasi. Hisob-nashr tabog'i. 9,5.
Adadi 100 dona. Buyurtma № 115.

«ZEBO PRINT» MCHJ bosmaxonasida chop etildi.
Manzil: Toshkent sh., Yashnobod tumani, 22-harbiy shaharcha.