**ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ**

**ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ**

**ИРГАШЕВА ДУРДОНА ЯКУБДЖАНОВНА**

# КОМПЬЮТЕР ТИЗИМЛАРИДА ФОЙДАЛАНИШНИ ЧЕКЛАШ ВОСИТАЛАРИ САМАРАДОРЛИГИНИ ОШИРИШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05-Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

**Тошкент – 2021**

**УДК 004.056.52**

**Докторлик (DSc) диссертацияси автореферати мундарижаси**

**Оглавление автореферата докторской (DSc) диссертации**

**Contents of the abstract of Doctoral (DSc) dissertation**

**Иргашева Дурдона Якубджановна**
Компьютер тизимларида фойдаланишни чеклаш воситалари самарадорлигини ошириш усуллари ва алгоритмлари.....3

**Иргашева Дурдона Якубджановна**
Методы и алгоритмы повышения эффективности средств разграничения доступа в компьютерных системах.....29

**Irgasheva Durdona Yakubdjanovna**
Methods and algorithms for increasing the efficiency of access control facilities in computer systems……..55

**Эълон килинган ишлар руйхати**
Список опубликованных работ
List of published works…….59

**ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ**

**ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ**

**ИРГАШЕВА ДУРДОНА ЯКУБДЖАНОВНА**

# КОМПЬЮТЕР ТИЗИМЛАРИДА ФОЙДАЛАНИШНИ ЧЕКЛАШ ВОСИТАЛАРИ САМАРАДОРЛИГИНИ ОШИРИШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05-Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

**Тошкент – 2021**

**Техника фанлари доктори (DSc) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2020.4.DSc/T109 рақам билан рўйхатга олинган.**

Диссертация Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.tuit.uz) ва "Ziyonet" ахборот-таълим порталида (www.ziyonet.uz) жойлаштирилган.

| | |
|---|---|
| **Илмий маслаҳатчи:** | **Ғаниев Салим Каримович**<br>техника фанлари доктори, профессор |
| **Расмий оппонентлар:** | **Рахматуллаев Марат Алимович**<br>техника фанлари доктори, профессор |
| | **Нигматов Ҳикматулла**<br>техника фанлари доктори, профессор |
| | **Керимов Комил Фикратович**<br>техника фанлари доктори, доцент |
| **Етакчи ташкилот:** | **Мирзо Улуғбек номидаги Ўзбекистон Миллий университети** |

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.01 рақамли Илмий кенгашнинг 2021 йил «03» июнь да соат 14:00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университетининг Ахборот-ресурс марказида танишиш мумкин (201 рақам билан рўйхатга олинган). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43).

Диссертация автореферати 2021 йил "21" май да тарқатилди.
(2021 йил «06» май даги 10 рақамли реестр баённомаси).

**Р.Ҳ.Ҳамдамов**
Илмий даражалар берувчи илмий кенгаш раиси, техника фанлари доктори, профессор

**Ф.М.Нуралиев**
Илмий даражалар берувчи илмий кенгаш илмий котиби, техника фанлари доктори, доцент

**Б.Ф.Абдурахимов**
Илмий даражалар берувчи илмий кенгаш ҳузуридаги илмий семинар раиси ўринбосари физика-математика фанлари доктори, профессор

## КИРИШ (докторлик диссертацияси автореферати (DSc))

**Диссертация мавзусининг долзарблиги ва зарурати.** Умумжаҳон ахборот глобаллашуви жараёни компьютер тизимларини (КТ) инсон фаолиятининг барча соҳаларига нафақат жорий этишни, балки ахборот тизими хавфсизлигини таъминлаш шароитларининг заруратини кўзда тутади. Компьютер тизимида кечаётган ахборот жараёнининг ўзига хос хусусияти ишланаётган ахборот хавфсизлигига юқори талабларнинг таъминланиши зарурати ҳисобланади. Бу, бир томондан КТда ишланаётган ахборотнинг қиймати орқали, иккинчи томондан эса компьютер тизимидаги ахборот хавфсизлигига таҳдидларнинг катта сонининг мавжудлиги орқали аниқланади. Шу билан бирга таъкидлаш лозимки, турли таҳдидларни сони вақт ўтиши билан доимо ортади. Ривожланган мамлакатларда, жумладан, АҚШ, Россия Федерацияси, Япония, Франция, Жанубий Корея ва бошқа давлатларда компьютер тизимларида ахборот яхлитлиги ва конфиденциаллигини таъминлаш имкониятини берувчи фойдаланишларни чеклаш ва назорат қилиш воситалар ишлаб чиқиш муҳим аҳамият касб этмоқда.

Жаҳонда рухсатсиз фойдаланишларни бартараф этишга ва улардан ҳимоялашга қаратилган модель, усул ва алгоритмларни ишлаб чиқишга, шунингдек мавжудларини такомиллаштиришга йўналтирилган илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, ҳозирги кунда компьютер тизимларида фойдаланишни чеклаш тизимини қуришда шаклланган ёндашиш, одатда статик характерга эга бўлиб, бундай ёндашиш ишланувчи ахборотнинг конфиденциаллигини кафолатли таъминлаш бўйича талабларнинг қондирилишига мўлжалланган усулларини ва алгоритмларни ишлаб чиқиш муҳим вазифалардан бири ҳисобланмоқда. Шу билан бирга фойдаланишни чеклаш тизимларида юритиладиган ахборот хавфсизлиги сиёсатини динамик ўзгариши ва вазифаларни тақсимлаш технологияси орқали фойдаланувчиларнинг ваколалатларини низолашиши жараёнларини бошқаришни усулларини такомиллаштиришни илмий асослаш зарур бўлмоқда.

Республикамизда давлат ва хўжалик бошқарув органларида миллий ахборот коммуникация технологиялари инфратузилмасини ривожлантириш ва уларда сақланадиган, ишлов бериладиган ва узатиладиган маълумотлар хавфсизлигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. «Киберхавфсизлик маркази» Давлат унитар корхонаси томонидан давлат ташкилотларининг ахборот тизимлари мониторинги бўйича тақдим этилган 2019 йил ҳисоботида келтирилган «… «Ахборот хавфсизлиги ҳодисаларини мониторинг қилиш» ахборот тизими томонидан давлат органларининг ахборот тизимларини кузатишда 17 620 025 та ҳодисалар аниқланган» ҳолати ахборот тизими нуфузининг йўқолишига олиб келиши мумкин[1]. Шуни таъкидлаш лозимки, 2017-2021 йилларда Ўзбекистон

[1] https://review.uz/post/kiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda

Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Мазкур вазифаларни бажаришда ахборотнинг криптографик ҳимоя воситалари, хусусан турли ҳодиса манбаларидан келаётган тасодифий қийматлар асосида самарали криптографик калитларни генерациялаш усуллари ва воситаларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасининг янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари ва 2018 йил 21 ноябрдаги ПҚ-4024-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга мазкур диссертация тадқиқоти маълум даражада хизмат қилади.

**Тадқиқотнинг Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги.** Мазкур тадқиқот республика фан ва технологиялари ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

**Диссертация мавзуси бўйича илмий-тадқиқотлар обзори.** Компьютер тизимларини самарали ҳимоя қилиш учун ролларга асосланган фойдаланишни чеклаш моделлари ва алгоритмларини ишлаб чиқишга қаратилган илмий тадқиқотлар дунёнинг етакчи илмий марказлари ва олий ўқув юртларида, шу жумладан Фрайбург университети (Германия), Люксембург технология ва алоқа университети (Люксембург), Тунисning олий бошқарув институти (Тунис), Ислом Азад университети (Эрон), Пекин технология институти, Компьютер фанлари ва технологиялари Хуачжун фан ва технология университети, Чангчун фан ва технология университети (Хитой), Омск давлат университети, Тюмен давлат университети, Олтой давлат университети (Россия Федерацияси), «Киберхавфсизлик маркази» ДУК (Ўзбекистон)да олиб борилмоқда.

Дунёда компьютер тизимларини ҳимоя қилишда фойдаланишни чеклаш моделлари ва усуллари бўйича олиб борилган изланишлар натижасида бир қатор илмий натижаларга эришилди, шу жумладан: ахборот тизимларидаги хавфсизлик таҳдидларининг таснифи (Higher Institute of Management Tunisia); Пекин технология институти олимлари томонидан ролларга асосланган динамик фойдаланишни чеклаш модели ишлаб чиқилди

[2] Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон “Ўзбекистон Республикасининг янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида”ги Фармони

(Key Laboratory of Intelligent Information Technology School of Computer Science and Technology, Beijing Institute of Technology, China); таҳлил асосида ахборот тизимларида фойдаланишни чеклашнинг типик моделлари ишлаб чиқилди (Тюмен давлат университети, Россия Федерацияси); таҳлиллар асосида эквивалент объектларга эга тизимларда фойдаланишни чеклаш моделлари ишлаб чиқилди (Олтой давлат университети, Россия Федерацияси); интеллектуал таҳлил асосида ролларга асосланган фойдаланишни чеклаш моделлари ишлаб чиқилди (School of Computer Science and Technology, Huazhong University of Science and Technology, China); ролига асосланган фойдаланишни чеклаш моделлари сиёсати учун кенг қамровли моделлаш муҳити ишлаб чиқилди (Faculty of Science, Technology and Communication, University of Luxembourg); Озод Ислом университети (Горган) олимлари фавқулодда вазиятга асосланган фойдаланишни чеклаш моделини ва Alloy тили моделининг хусусиятларини таҳлил қилдилар (Department of Computer Engineering, Islamic Azad University, Iran).

Дунёда ролга асосланган фойдаланишни чеклаш тизимларида ваколатларнинг сирқиб чиқиши хавфини баҳолашнинг иерархик усулларини ишлаб чиқишнинг устувор йўналишлари, шунингдек фойдаланишни ҳуқуқини чеклаш моделларида роллар иерархияси асосида ваколат моделларини ишлаб чиқиш ва атрибутларга асосланган фойдаланишни чеклаш усулларини такомиллаштириш бўйича тадқиқотлар олиб борилмоқда.

**Муаммонинг ўрганилганлик даражаси.** Ахборот хавфсизлигини таъминлаш муаммоларининг назарий ва амалий жиҳатларини таъминлашда турли ёндашишларга, ҳимояланган компьютер тизимларини қуриш усулларига Leonard J. La Padul, M. Harrison, W. Ruzzo, J. Uhlman, H. Pham, Sandhu ва Samarati, David Ferraiolo, Rick Kuhn ва А.В. Барабанов, Н.А. Гайдамакин, В.А. Галатенко, П.Н. Девянин, Д.П. Зегжда, Д.Ю. Гужва, С.С. Куликов, Р.М. Алгулиев, В.Ф. Шаньгин ва бошқа чет эл олимларининг кўп сонли илмий-тадқиқот ишлари бағишланган.

Ўзбекистон Республикасида ушбу муаммоларни, хусусан, ахборот хавфсизлиги бўйича қуйидаги олимлар бошчилигидаги илмий жамоаларнинг илмий изланишларида ўрганилган: Т.Ф. Бекмуратов, П.Ф. Хасанов, М.М. Арипов, С.К. Ганиев, М.М. Каримов.

Аммо, компьютер тизимларидан фойдаланишни чеклаш тизимини қуришда муайян формал моделларни танлаш ва қўллаш масалалари етарлича ўрганилмаган. Ундан ташқари, фойдаланишни бошқаришнинг мавжуд моделларининг бирортасида ҳам КТ фойдаланувчиларнинг ролли структураси, ўзаро таъсирдаги функционал модулларга мувофиқ, ҳисобга олинмайди.

**Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги.** Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг илмий-тадқиқот режасининг №Ф4-019 «Ахборот хавфсизлиги кўрсаткичлари ва мезонлари тизимини шакллантириш муаммоларининг тадқиқи» (2012-2016),

№Ф706-17 «Ахборот тизимларида биометрик-криптографик технологиялар қўлланилишининг тадқиқи» (2017-2018) мавзусидаги лойиҳалар доирасида бажарилган.

**Тадқиқотнинг мақсади** компьютер тизимларини самарали ҳимоялаш учун фойдаланишни чеклаш воситаларини қуриш, ваколатларни назоратлаш моделлари, усуллари ва алгортимларини ишлаб чиқиш ва такомиллаштириш.

**Тадқиқотнинг вазифалари:**

компьютер тизимларидаги инцидентларни таҳлиллаш асосида назоратлаш ва бошқариш воситаларига дахлдор таҳдидларни аниқлаш;

компьютер тизимларида фойдаланишни чеклаш тизимининг қуришда таҳдидларни аниқлаш моделини ишлаб чиқиш;

фойдаланишни чеклаш тизимининг концептуал моделини ишлаб чиқиш;

фойдаланишни чеклаш тизимини синтезлаш самарадорлигини баҳолаш кўрсаткичларини аниқлаш;

динамик бошқаришни таъминловчи фойдаланишни чеклаш моделини ишлаб чиқиш;

ваколатлар асосида вазифаларни тақсимлашни (SOD) қўллаш учун атрибутлар ёрдамида фойдаланишни ролли чеклашнинг комбинацияланган моделини ишлаб чиқиш;

фойдаланишни чеклашда низолашувчи ва низолашмаган ваколатларни аниқлашга имкон берувчи усул ва алгоритмларни ишлаб чиқиш.

**Тадқиқотнинг объекти** сифатида компьютер тизимларида фойдаланишни бошқариш ва назоратлаш жараёни олинган.

**Тадқиқотнинг предмети** сифатида хавфсизлик моделлари, усуллари, алгортимлари ва ахборотни ҳимоялашнинг дастурий воситалари олинган.

**Тадқиқотнинг усуллари.** Тадқиқот жараёнида эҳтимоллик назарияси, тўпламлар назарияси, графлар назарияси, ахборотни ҳимоялаш усуллари, Alloy моделлаш тизими, дастурлаш усулларидан фойдаланилган.

**Тадқиқотнинг илмий янгилиги** қуйидагилардан иборат:

ахборот хавфсизлиги стандартлари асосида компьютер тизимларида фойдаланишни назоратлаш ва бошқариш воситаларига дахлдор таҳдидлар рўйхати, ҳамда ахборотни ҳимоялаш тизими самарадорлигини баҳолаш кўрсаткичлари шакллантирилган;

фойдаланишни чеклаш тизимига таҳдидларнинг таъсир этиши эҳтимоллигини ҳисоблаш орқали таҳдидларни аниқлаш модели ишлаб чиқилган;

формал моделлар ва фойдаланишни чеклаш жараёнларида реконфигурацияга қарор қабул қилишни ҳисобга олган ҳолда концептуал модел ишлаб чиқилган;

фойдаланишни чеклаш схемаларини, улардаги элементларнинг ноаниқ характерга эга эканлигини ҳисобга олган ҳолда динамик бошқаришни таъминловчи фойдаланишни чеклаш модели ишлаб чиқилган;

ваколатлар асосида вазифаларни тақсимлашни (SOD) турли атрибутлар ёрдамида ролларга ваколатларни, ҳамда ролларга фойдаланувчиларни динамик тарзда тайинловчи комбинацияланган модел ишлаб чиқилган;

фойдаланишни ролли чеклаш моделида низолашувчи ва низолашмаган ваколатларни аниқлашнинг «кўпга-кўп», «кўпга-бир», «бирга-кўп», «бирга-бир» режим усуллари ва алгоритмлари ишлаб чиқилган.

**Тадқиқотнинг амалий натижалари** қуйидагилардан иборат:

ролларга низолашувчи ва низолашмаган ваколатларни динамик тарзда тайинлаш ҳисобига, вақтни тежашга ва маъмурга юкламани камайтиришга ҳамда фойдаланишни мослашувчан, динамик бошқаришга имкон берувчи модел ишлаб чиқилган;

маълумотлардан фойдаланишни назоратлашни деталлаштириш мақсадида, ролли базани фойдаланишни белгилар асосида назоратлаш билан бирлаштириш усули ишлаб чиқилган;

комбинацияланган модел асосида ишлаб чиқилган дастурий таъминотнинг фирибгарлик каналларини камайтиришга имкон бериши компьютер тизимларидан рухсатсиз фойдаланишдан ҳимояланишини оширишга ва маълумотлар базасининг ишончли ишлашини таъминлашга имкон беради.

**Тадқиқот натижаларининг ишончлилиги** масалалар қўйилишининг корректлиги, компьютер тизимларининг ахборот ихтилофи шароитида ахборотдан рухсатсиз фойдаланишнинг ахборот ҳимояланганлигига таъсир этувчи омиллар мажмуининг ва характерининг тўлиқ ҳисобга олиниши, масалаларини вақтнинг реал режимида самарали ечишга имкон берувчи тақдим этилган фойдаланишни чеклаш тизими моделини синтезлаш ва бошқаришнинг мукаммаллиги, тавсия этилган ечимларнинг бошқа усуллар асосида олинганлари билан зиддиятли эмаслиги билан изоҳланади.

**Тадқиқот натижаларининг илмий ва амалий аҳамияти.** Тадқиқот натижаларининг илмий аҳамияти компьютер тизимларининг ахборот ихтилофи шароитида ишлаши хусусиятларини ифодаловчи, формал моделларини ишлаб чиқишда зарурий илмий-методологик базани таъминловчи фойдаланишни чеклаш тизими модели ва синтезлаш самарадорлигини баҳолашдан иборат.

Тадқиқот натижаларининг амалий аҳамияти фойдаланишни чеклаш тизимини синтезлаш ва фойдаланишни ролли чеклашнинг комбинацияланган моделининг компьютер тизими маълумотлар базасининг рухсатсиз таъсирлардан ҳимояланганлигини ва ишончли ишлашини таъминлаш имкониятини беришидан иборат. Ундан ташқари, олинган натижалар дастурий амалга оширилиш даражасигача етказилган.

**Тадқиқот натижаларининг жорий қилиниши.** Компьютер тизимларида фойдаланишни чеклаш усуллари ва алгоритмларининг самарадорлигини оширишдан олинган илмий натижалар асосида компьютер тизимларини самарали ҳимоя қилишни таъминлаш, ролларга асосланган фойдаланишни чеклаш моделлари ва алгоритмлари ишлаб чиқилди:

ишлаб чиқилган ролларга асосланган фойдаланишни чеклаш моделининг низолашувчи ва низоланмаган ваколатларни аниқлаш усуллари ва алгоритмлари «Агробанк» ва «Қишлоқ қурилиш банк» банкларга татбиқ қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 03 февралдаги №33-8/821-сон маълумотномаси). Илмий тадқиқот натижаларидан фойдаланиш таҳдидларнинг мавжудлигига тезкор жавобни 37%га оширишга, шунингдек ваколатларни яратишга сарфланадиган вақт 24%га камайишга имкон берган;

ахборот тизимининг ҳимоялашда таҳдидларнинг таъсири эҳтимоллиги ва ахборот ҳимоя тизимининг фош этилиши эҳтимоллигини моделлаш, яъни таҳдидлар ҳолатининг хавфсизлик модели Ўзбекистон Республикасининг «Ўзархив» агентлигига татбиқ қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 03 февралдаги №33-8/821-сон маълумотномаси). Илмий тадқиқот натижасидан фойдаланиш таҳдидларни тезда аниқлаш ҳолатининг 1,5 баравар ошишига ва ишончлиликни таъминлашга имкон берган;

фойдаланишни чеклаш тизимига таҳдидларнинг таъсир этиши эҳтимоллигини ҳисоблаш орқали, таҳдидларни аниқлаш модели асосида ишлаб чиқилган дастурий таъминот «OFFICIAL DEALER TRADE» МЧЖга татбиқ қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 03 февралдаги №33-8/821-сон маълумотномаси). Илмий тадқиқот натижаси фойдаланишга таҳдидларни тезда аниқлаш ҳолатининг 2,5 баравар ошишига ва ишончлиликни таъминлашга имкон берган;

фойдаланишни ролли чеклашнинг комбинацияланган C-RBAC моделига асосланган дастурий таъминот Олий ва ўрта махсус таълим вазирлиги ҳузуридаги Олий таълим тизими педагог ва раҳбар кадрларини қайта тайёрлаш ва уларнинг малакасини оширишни ташкил этиш Бош илмий-методик маркази ахборот тизимига татбиқ қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 03 февралдаги №33-8/821-сон маълумотномаси). Натижада ваколатларни ролларга, ролларнинг фойдаланувчиларга тайинлаш автоматик тарзда амалга оширилиши эвазига 2 баробар вақт тежалиш имконини яратди;

фойдаланишни чеклаш тизимини синтезлаш усули Ички ишлар вазирлигининг Академиясига татбиқ этилди (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 03 февралдаги №33-8/821-сон маълумотномаси). Илмий натижаларни жорий этиш самарадорлиги ўқув материалларини ўзлаштириш даражасини ошиши билан изоҳланди ва натижа малакали мутахассисларни тайёрлашда амалий ёрдам бериши билан тасдиқланди.

**Тадқиқот натижаларининг апробацияси.** Мазкур тадқиқот натижалари 7 та халқаро ва 11 та Республика илмий-техник ва илмий-амалий анжуманларда муҳокамадан ўтган.

**Тадқиқот натижаларининг эълон қилинганлиги.** Диссертациянинг мавзуси бўйича 30та илмий иш чоп этилган, жумладан, Ўзбекистон

Республикаси Олий аттестация комиссиясининг диссертациялар асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрлар рўйхатидан 13 та мақола, 8 таси хорижий ва 5 таси республика журналларида нашр этилган, ҳамда ЭҲМ учун яратилган дастурий воситаларни қайдлаш гувоҳномалари 2 та.

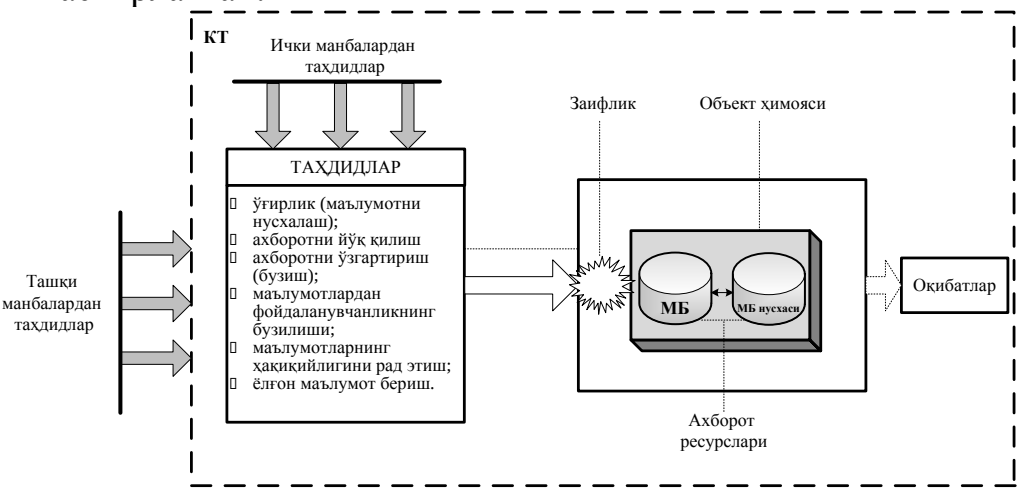
**Диссертациянинг тузилиши ва ҳажми.** Диссертация таркиби кириш, бешта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертациянинг ҳажми 180 бетни ташкил этади.

## ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

**Кириш қисмида** диссертация мавзусининг долзарблиги асосланган, Ўзбекистон Республикасида компьютер тизимлари ахборот хавфсизлиги муаммолари ҳолатининг қисқача таҳлили келтирилган, тадқиқот мақсади ва вазифалари аниқланган. Илмий янгилиги таърифланган ва иш натижаларининг амалий аҳамияти кўрсатилган, ҳимояга олиб чиқиладиган асосий илмий ҳолатлар келтирилган, тадқиқот натижаларини жорий этиш, натижаларнинг нашр этилиши ва диссертациянинг тузилиши тўғрисида маълумотлар берилган.

Диссертациянинг «**Компьютер тизимларида ахборот хавфсизлигининг замонавий ҳолати»** деб номаланувчи биринчи боби компьютер тизимларини ҳимоялаш муаммоларининг ҳамда фойдаланишни чеклаш моделларининг таҳлили асосида ҳимояланган компьютер тизимларини лойиҳалашга асосий талабларни шакллантириш ва таҳдидларининг таҳлиллаш масаласига бағишланган.

Ахборотни ҳимоялашни таъминлаш комплекс характерга эга бўлиши лозим. У хилма-хил салбий оқибатларни теран таҳлиллашга асосланиши лозим. Заифликларнинг пайдо бўлишига ва натижада ахборот хавфсизлигининг муҳим таҳдидларини аниқлашга имкон берувчи салбий оқибатларни таҳлиллаш таҳдидларнинг хилма-хил манбаларини сўзсиз идентификациясини кўзда тутади. 1-расмда таҳдидларни амалга оширилиш жараёни тасвирланган.




**1-расм. Таҳдидларнинг амалга оширилиши жараёнлари**

Таҳдид манбалари ахборот хавфсизлиги таҳдидларининг элтувчиси ҳисобланади. Шу билан бирга таҳдид манбалари компьютер тизимининг ичида (ички манбалар) ва ташқарисида (ташқи манбалар) бўлиши мумкин.

O'Z Dst ISO/IEC 27033-3:2016 миллий стандартда компьютер тизимлари билан боғлиқ назоратлаш ва бошқариш воситаларига дахлдор таҳдидлар баён этилган. Компьютер тизимларидаги назоратлаш ва бошқариш воситаларига дахлдор рухсатсиз фойдаланишдан ҳимояланганликка таъсир этиши мумкин бўлган соҳаларнинг таҳлили мос омилларни аниқлашга имкон берди (1-жадвал).

**1-жадвал**

**Компьютер тизимларида назоратлаш ва бошқариш воситалари таҳдидларининг турли хилларига мисоллар**

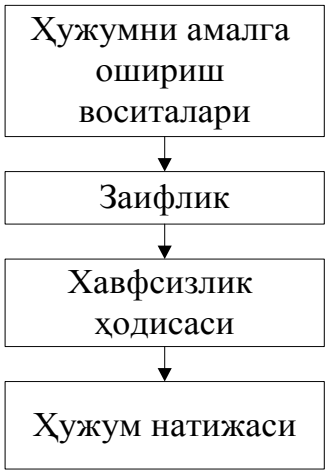
| **Барқарорликни бузиш омиллари** | **Маълумотларнинг ўғирланиши ва сохталаштирилиши** | **Конфиденциаллик-нинг бузилиши** | **Яхлитликнинг йўқотилиши** |
|---|---|---|---|
| Маълумотларнинг сервер базасидан фойдаланилганда веб иловалар учун рухсатнинг сони чекланган. | + | | |
| Фойдаланувчиларнинг рухсатсиз фойдаланишларини олдини олиш ёки бошқа шахснинг фойдаланиш ҳуқуқларини ишлатиш учун бошқариш рўйхатлари. | + | | + |
| Бажарилишига рухсат берилган фойдаланувчи функциясини чеклаш учун ролларга асосланган фойдаланишни бошқариш. | + | + | |
| Маълумотларнинг рухсатсиз ўзгартирилиши ёки нусхаланиши. | + | | + |
| Маълумотларнинг ўғирланиши. | + | + | |
| Фойдаланиш ваколати ҳақиқий фойдаланувчиларга берилганлигига ишончни таъминлаш учун фойдаланувчини хавфсиз рўйхатдан ўтказиш. | + | + | |
| Рақамли сертификатлардан, пароллардан, биометриядан ёки смарткарталардан фойдаланиб аутентификациялаш. | + | | + |
| Иловалардан ва бошқа тармоқ ресурсларидан фойдаланиш ҳуқуқларининг бузилиши каби хавфсизлик сиёсатининг бузилишини аниқлаш учун дастурий воситаларнинг мониторинги. | | | + |

Хавфсизлик таҳдидларининг асосий объектларидан бири компьютер тизимининг маълумотлар базасида сақланувчи оператив ахборот ҳисобланади. Аммо, қатор ҳолларда оператив ахборотга таҳдидларни амалга оширишда, ахборотдан фойдаланиш бўйича керакли ваколатларнинг мавжудлиги кўзда тутилади. Ушбу ваколатларни компьютер тизими маълумотлар базасининг технологик ахборотига, жумладан ҳимоя тизими ахборотига таъсир этиш йўли билан олиш мумкин.

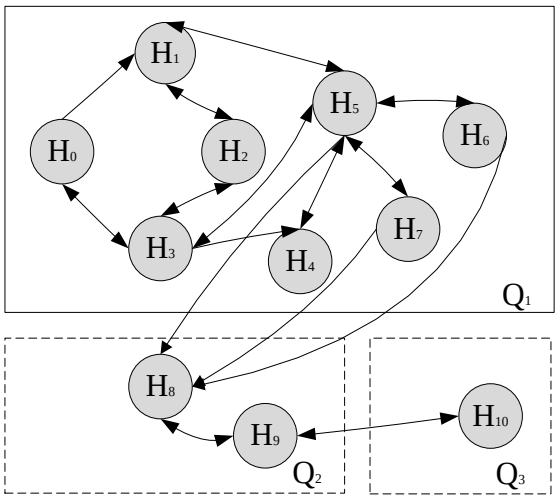
Диссертациянинг «**Компьютер тизимларида фойдаланишни чеклаш тизимини синтезлаш»** деб номаланувчи иккинчи боби фойдаланишни чеклаш тизимига таҳдидларнинг таъсири ва ушбу тизимнинг фош этилиши эҳтимолликларини ҳисоблашга имкон берувчи таҳдидлар моделининг тавсифи, фойдаланишни чеклаш тизими ва унинг концептуал модели, ҳамда фойдаланишни чеклаш тизимининг самарадорлиги кўрсаткичларининг баёнига бағишланган

Диссертациянинг биринчи бобида келтирилган, фойдаланишни чеклаш тизимига тааллуқли таҳдидлар хилига биноан, бузғунчи ҳаракати тавсифланувчи фойдаланишни чеклаш тизимига таҳдидлар моделини шакллантириш мумкин. Бузғунчи сифатида, ҳаракати компьютер тизимидаги ахборотдан рухсатсиз фойдаланишга йўналтирилган, ахборот тизимидан штатли воситалар орқали фойдаланувчи субъект кўрилиши лозим.

Таҳдидлар моделини қуриш ҳужумларнинг ноформал моделини шакллантиришдан бошланади (2-расм). Ҳужумни амалга оширишда нияти бузуқ, исталган натижага олиб келувчи қандайдир хавфсизлик ҳодисасини моделлайди. Ноформал моделдан таҳдидлар моделига ўтиш мумкин. Таҳдидлар ҳолатининг моделини, ҳар бири таҳдиднинг *i*-ҳолатига мос келувчи, блоклар мажмуи сифатида кўриш мақсадга мувофиқ ҳисобланади. Ушбу модел 3-расмда келтирилган.




**2-расм. Ҳужумнинг ноформал модели**




**3-расм. Таҳдидлар ҳолатининг модели**

Ушбу хавфсизлик таҳдидлари модели $H_i$ *(i=0…10)* таҳдид ҳолатлар сифатида ифодаланади, бунда $H_0$ – фойдаланишни чеклаш тизимининг

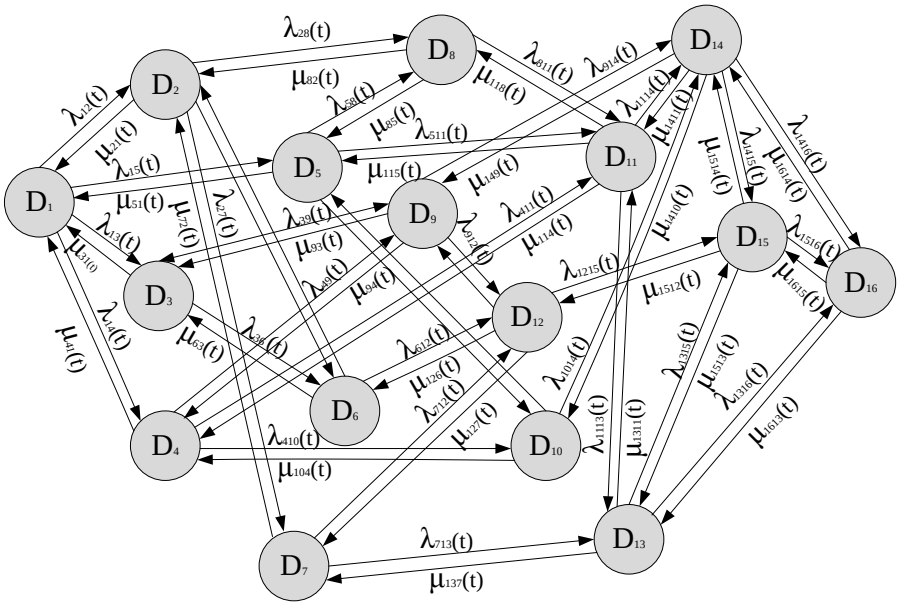
дастлабки ёки хавфсиз ҳолати, $H_1 - H_{10}$ турли таҳдидлар ҳолати. Шунингдек, $Q_1 - Q_3$ таҳдидларни тайёрлаш, амалга ошириш ва якунлаш қисмтизимлари.

Таҳдидлар тизими ҳолати $H(t)$ нинг вақт онидаги эҳтимоллиги, ушбу тизимнинг $H_t$ ҳолатида бўлишлигининг эҳтимолликлари мажмуи сифатида кўрилади ва қуйидагича ифодаланади: $e_i(t) = e(H(t) = h_i)$, бу ерда $H(t)$ вақт онидаги тизимнинг тасодифий ҳолати. Ўтиш эҳтимоллиги қуйидагича аниқланади: $e_{ij}(t) = e(Hk = H_j | H(k-1) = H_j$.

Таҳдидлар тизимининг $k$-нчи қадамда бўлиши эҳтимолликлари, тўлиқ эҳтимоликлар формуласини қўллаб ва $(k-1)$-нчи қадамдан $k$-нчи қадамга ўтиш орқали, аниқланади ва қуйидаги рекуррент кўринишда ифодаланади:

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

Таҳдидлар моделининг асосий параметрлари-компьютер тизими ахборотининг ҳимоя тизимига таҳдидлар тизимининг таъсири эҳтимоллиги ва ахборот ҳимоя тизимининг фош этилиши эҳтимоллиги. 3-расмда келтирилган моделдан белгиланган граф кўринишидаги моделга ўтилади (4-расм).




**4-расм. Ҳимоя тизими ҳолатининг белгиланган графи**

Бунинг учун қуйидаги белгилашлар қабул қилинади:

$\mu_i$ - ахборот ҳимояси тизимини тиклашга йўналтирилган интенсивлик;

$\gamma_i$ - ҳимоя тизимининг фош этилиши интенсивлиги;

$e_i$ - ҳодисаларнинг бошланиши ҳолати эҳтимоллиги ($e_1$ - ташқи ҳужум бўлмаганлиги эҳтимоллиги; $e_2$- ташқи ҳужум бўлганлиги эҳтимоллиги; $e_3$- ички хил (кўринишда) ҳужум бўлганлиги эҳтимоллиги; $e_4$- номаълум ҳужум бўлганлиги эҳтимоллиги; $e_5$ - бошқариш тизимига ҳужум бўлганлиги эҳтимоллиги).

$D_i$ – ҳимоя тизими ҳолати. Ҳимоя тизими ҳолатлари 4-расмда графда келтирилган 16та ҳолатни ўз ичига олади ва бунда таҳдид ҳолатлари ҳодисаларнинг бошланиши эҳтимоллиги ҳолатлари тизим учун бир вақтда таъсир ўтказишни кўзда тутади. Кўзга ташланувчанликни таъминлаш мақсадида ҳужумлар оқими $\lambda_i(t)$ ва ҳужумларга қарши таъсир қилувчи

оқимлар $\mu_i(t)$ стрелкалар "⇆" орқали белгиланган. Белгиланган графни ёки интенсивлик матрицасини билган ҳолда, мнемоник қоидадан фойдаланиб, ахборотни ҳимоялаш тизими ҳолати эҳтимоллиги учун дифференциал тенгламалар системасини ёзиш мумкин:

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

Унда ўзгармас коэффициентли бир жинсли дифференциал тенгламалар системаси ўрнига ўзгармас коэффициентли бир жинсли алгебраик тенгламалар системасини олиш мумкин. Бу алгебраик тенгламалар системасини, қуйидаги нормалланган шартни ҳисобга олган ҳолда, ечиш мумкин:$\sum_{i=1}^{16} e_i(t) = 1, (0 \le e_i(t) \le 1; t \ge 0)$. Дифференциал тенгламани ўзгармас коэффициентли бир жинсли алгебраик тенгламалар системасига ўзгартирилади: $e_i = \sum_{j=1}^{n}\lambda_{ij}e_j - e_i\sum_{j=1}^{n}\lambda_{ij}$. (1)

(1) ифодани қуйидаги кўринишига келтириш мумкин:

$e_i\sum_{j=1}^{n}\lambda_{ij} = \sum_{j=1}^{n}\lambda_{ij}\,e_j$, ёки янада содда кўриниши:

$e_i = \frac{\sum_{j=1}^{n}\lambda_{ij}e_j}{\lambda_i}$ $(i = 1,2,3,\dots,n)$, бу ерда $\lambda_i = \sum_{j=1}^{n}\lambda_{ij}$.

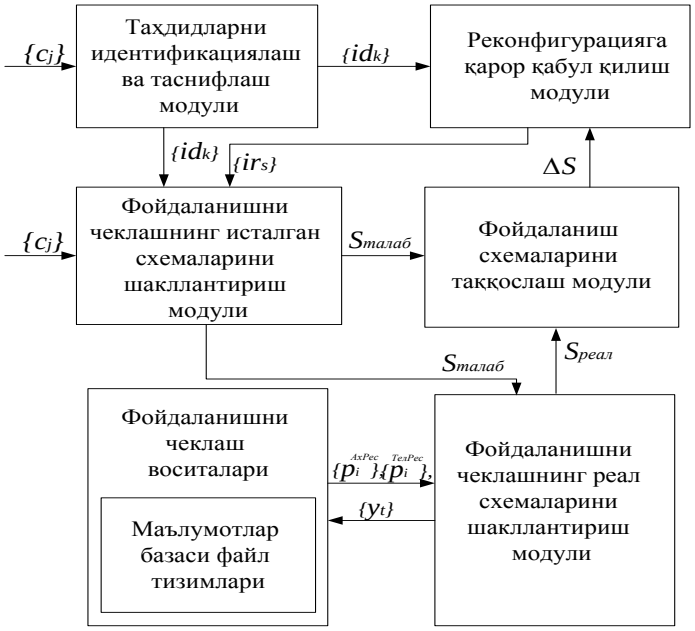
Алгебраик тенгламалар системасини ечиш учун ушбу тенгламалардан бирини нормаловчи шарт $\sum_{j=1}^{n} e_i = 1$ билан алмаштириш керак.

Қуйида ҳимоя тизимига ҳужумларнинг турли интенсивлигида ва ҳужумларга қайта таъсир қилишга йўналтирилган ҳимоя тизими интенсивлигида ҳимоя тизимининг ўтишлари эҳтимолликлари ҳисобланган.

Ҳужум оқимлари $\lambda$ ва ҳужумга қарши ҳимоя коэффициент $\mu$ ларнинг йиғиндиси 1 га тенг деб олинади. Бу ҳолда, $\lambda$ ва $\mu$ бир-бирига тескари мутаносиб. Ишлаб чиқилган модел асосида қуйидаги хулосаларга келиш мумкин: ҳимоя тизимига ҳужумларнинг максимал оқими таъсирида ва ушбу ҳужумларга ушбу тизим тарафидан ҳар қандай қарши таъсирнинг йўқлигида тизимнинг фош этилиши эҳтимоллиги 1га тенг; ҳужумларнинг ва ҳужумларга қарши таъсир оқимларининг тенглигида ҳимоя тизимининг тўлиқ фош этилиши эҳтимоллиги 0.0625 га тенг; $\lambda = 0.75$ ва $\mu = 0.25$ ҳолида ҳимоя тизимининг тўлиқ фош этилиши эҳтимоллиги 0.3 га тенг. Демак, ҳимоя тизимига таъсир этувчи ҳужумлар оқими $\lambda$га самарали қарши таъсир этиш учун $\mu = 0.3 - 0.5$ га тенг интенсивлик билан ишловчи қарши таъсир тизими зарур. Интенсивликнинг ошиши ҳимоя тизимининг қимматлашига олиб келади.

Фойдаланишни бошқариш тизимини амалга ошириш учун ахборот тизимининг модели яратилади. У ахборот тизимининг барча ҳолатларини, бир ҳолатдан бошқа ҳолатга ўтишларини моделлаши, ҳамда қайси ҳолатни хавфсиз деб ҳисоблашни кўрсатиши мумкин. Ахборот тизимини, танланган хавфсизлик сиёсатига асосан, ҳимоялаш тизимини синтезлаш масаласини формаллаштиришнинг турли ёндашувлари мавжуд. Ҳимоя усулларини ишлаб чиқишдаги ҳаражатларни, эксплуатациясини ва хавфсиз вақтни уларнинг асосий характеристикаларига оид деб ҳисоблаш мумкин. Яхлитликни назоратлаш воситалари ҳимоя воситаларининг ва ахборот ресурсларининг яхлитлигини тиклашни амалга оширади. Натижада,

фойдаланишни чеклаш тизимининг анъанавий функционал компонентларига, ахборотдан фойдаланишни ва таҳдидларни аниқлаш ва уларнинг пайдо бўлишини сезувчи ресурсларни оператив назоратлаш функцияларини амалга оширувчи қўшимча модуллар қўшилади. Фойдаланишни чеклаш тизими таркибига, юқорида келтирилган функцияларни амалга оширувчи, мос ҳолда лойиҳаланган ва бошқарувчи воситалар қўшилишининг шартлиги кўзда тутилади. Фойдаланишни чеклаш тизимининг концептуал модели 5-расмда келтирилган.




**5-расм. Фойдаланишни чеклаш тизимининг концептуал модели**

Бу ҳолда, фойдаланишнинг чеклаш тизими ишлаши жараёнини қуйидаги ифода орқали тавсифлаш мумкин:

$y\,(t_2) = Y\left(S_{\text{талаб}}(t_1), \vec{V}^{\text{АхРес}}(t_1), \vec{V}^{\text{ТелРес}}(t_1)\right)$, бу ерда: $\text{S}_{\text{талаб}}(t_1)$ - $\text{t}_1$ вақт онида фойдаланишни чеклаш тизимининг исталган схемаси; $\vec{V}^{\text{АхРес}}(t_1) = \left\{v_i^{\text{АхРес}}\right\}$ - $\text{t}_1$ вақт онида компьютер тизимининг ахборот ресурсларидан (маълумотлар базасидан, файл тизимларидан) фойдаланишни чеклаш воситалари характеристикаларининг вектори; $\vec{V}^{\text{ТелРес}}(t_1) = \left\{v_i^{\text{ТелРес}}\right\}$ - $\text{t}_1$ вақт онида компьютер тизимининг телекоммуникация ресурсларидан (виртуал тармоқларидан) фойдаланишни чеклаш воситалари характеристикаларининг вектори; $y(t_2)$- $t_2$ вақт онида фойдаланишни чеклаш тизими томонидан шакллантирилган фойдаланишни чеклаш буйича ечим, $t_2 > t_1$. Фойдаланишни чеклашнинг исталган схемаси $t_2$ вақт онида фойдаланишни чеклашнинг исталган схемаларини шакллантириш модулида яратилади: $\text{S}_{\text{талаб}}(t_2) = F(\vec{C}(t_1), \overrightarrow{Id}(t_1), \overrightarrow{Ir}(t_1))$.

Бу ерда: $\vec{C}(t_1) = \{c_j\}$- $t_1$ вақт онида компьютер тизими ахборот ва телекоммуникация ресурсларининг ички параметрларининг вектори; $\overrightarrow{Id}(t_1) = \{id_k\}$- идентификациялаш ва таснифлаш модулида $\text{t}_1$ вақтида аниқланган таҳдидлар вектори; $\overrightarrow{Ir}(t_1) = \{ir_s\}$- реконфигурациялаш лозимлигини белгиловчи модулда $t_1$ вақт онида шакллантирилган ечимлар

вектори. Фойдаланишни чеклашнинг реал схемаси $t_2$ вақт онида фойдаланишни чеклашнинг реал схемаларини шаклантириш модулида яратилади:$\mathrm{S}_{\text{реал}}(t_2) = \Pi\left(\mathrm{S}_{\text{талаб}}(t_1), \vec{V}^{\text{АхРес}}(t_1), \vec{V}^{\text{ТелРес}}(t_1)\right)$.

Фойдаланишни чеклашнинг исталган ва реал схемаларини таққослаш баҳоси фойдаланиш схемаларини таққослаш модулида, қуйидаги ифодага биноан шакллантирилади: $\Delta S(t_2) = \Phi\ (\mathrm{S}_{\text{талаб}}(t_1), \mathrm{S}_{\text{реал}}\ (t_1))$.

Фойдаланишни чеклаш тизимини реконфигурациялаш зарурияти хусусидаги ечим реконфигурациялаш лозимлигини белгиловчи модулда $t_2$ вақт онида қуйидаги ифодага биноан шакллантирилади:

$Ir(t_2) = Ir(\overrightarrow{Ir}(t_1), \Delta S(t_1))$.

Идентификациялаш ва таснифлаш модулида таҳдидлар вектори $t_2$ вақт онида қуйидаги ифодага биноан аниқланади: $\overrightarrow{Id}(t_2) = Id\left(\vec{C}(t_1)\right)$.

Демак, фойдаланишни чеклаш тизими ишлаши жараёнини амалга ошириш учун унинг таркибига таҳдидларни идентификациялаш ва таснифлаш билан боғлиқ фойдаланишни чеклашни бошқариш функцияларини бажарувчи воситалар киритилиши лозим.

Мақсадга йўналтирилган жараёнлар самарадорлигини баҳолашнинг маълум методологияси, кўрсаткичлар тизимини шакллантиришда, унинг таркибига баҳоланувчи жараённи тавсифловчи натижалилик, ресурслар кўлами, оперативлик ва ишончлилик каби кўрсаткичларнинг сўзсиз киритилишини кўзда тутади. Ушбу кўрсаткичлар биргаликда кўп сатҳли тизимни ҳосил қилади.

Синтезлаш жараёнининг натижалилигини қуйидаги комплекс кўрсаткичлари орқали баҳолаш мумкин: $\text{Э}_{\text{РФСҲ}}$ - ахборотни рухсатсиз фойдаланишдан статик ҳимояланганлигини тавсифловчи ахборотдан рухсатсиз фойдаланиш эҳтимоллиги; $\text{Э}_{\text{РФДҲ}}$ - ахборотни рухсатсиз фойдаланишдан динамик ҳимояланганлигини тавсифловчи, берилган вақт мобайнида ахборотни рухсатсиз фойдаланишдан ҳимоялашни таъминлаш эҳтимоллиги. $\text{Э}_{\text{РФ}}$ қиймати фойдаланишни чеклаш тизимининг рухсатсиз фойдаланишга уринишларини бартараф этиш қобилиятини ифодалайди; $\text{Э}_{\text{РФҲ}}$ нинг эҳтимоллиги, рухсатсиз фойдаланишга уринишлар ва дастурий ҳужумлар мавжудлигида, фойдаланишни чеклаш тизимининг ахборотни рухсатсиз фойдаланишдан ҳимоялаш қобилиятини акс эттиради.

Юқорида келтирилган кўрсаткичлар комплекс сатҳининг самарадорлик кўрсаткичлари ҳисобланади. Улардан ташқари, ушбу сатҳга куйидагилар тегишли: $K_{\Phi}^{\text{ХР}}$- ҳисоблаш ресурсларининг ишлатилиш коэффициенти; $K_{\Phi}^{\text{ТР}}$- тармоқ ресурсларининг ишлатилиш коэффициенти; N - нархи.

Самарадорликнинг хусусий кўрсаткичлари сатҳига иккита кўрсаткич-оперативлик ва ишончлилик тегишли. Оперативлик кўрсаткичи қуйидагича: Э $(t_{\text{И}} <= T^{\text{ишонч}})$- хавфсизлик таҳдидларини ўз вақтида идентификациялаш ва таснифлаш эҳтимоллиги; Э $(t_{\text{Қ}} <= T^{\text{ишонч}})$- фойдаланишни чеклаш тизимини бошқариш вариантларини ўз вақтида қидириш эҳтимоллиги;

Э ($t_{Ш} <= T^{ишонч}$)- фойдаланишни чеклаш схемасини ўз вақтида шакллантириш эҳтимоллиги.

Ишончлилик кўрсаткичларига қуйидагилар тегишли: $Э_{ИХ}$ - таҳдидларни идентификациялаш хатоликлари эҳтимоллиги; $Э_{БХ}$ - бошқариш хатоликлари эҳтимоллиги; $Э_{ШХ}$ - фойдаланишни чеклаш схемаларини шакллантириш хатоликлари эҳтимоллиги.

Фойдаланишни чеклаш тизими элементлари кўрсаткичлари сатҳи, яъни компьютер тизимида ишлатилувчи фойдаланишнинг дискрецион, мандатли ва ролли усуллари схемаларида қуйидаги кўрсаткичлардан фойдаланилади: $K_{конф}$- конфиденциаллик бўйича талабларнинг амалга оширилишининг тўлиқлик коэффициенти; $K_{фойд}$- фойдаланувчанлик бўйича талабларнинг амалга оширилишининг тўлиқлик коэффициенти.

Юқорида келтирилган кўрсаткичларни фойдаланишни чеклашнинг мавжуд моделларига, таклиф этилган фойдаланишни чеклашнинг концептуал моделини ҳисобга олган ҳолда, қўллаш орқали фойдаланишни чеклаш тизимларининг қиёсий баҳосига эга бўлиш мумкин.

Фойдаланишни назоратлашнинг дискрецион (DAC) ва мандатли (MAC) моделларининг ролли моделдан (RBAC) битта муҳим фарқи мавжуд. Ушбу моделларда тизим хавфсизлик сиёсати олдиндан аниқланади ва уни ҳар бир муайян вазият учун созлаш имкони мавжуд. Ролли модел эса хавфсизлик сиёсатини асло олдиндан аниқламайди, балки уни ташкилотга зарур кўринишда созлашга имкон беради. 2 - жадвалда фойдаланишни чеклаш тизими элементлари даражалари кўрсаткичиларини таққослаш натижалари келтирилган.

**2 - жадвал**

**Фойдаланишни чеклаш тизими элементлари даражалари кўрсаткичларини таққослаш**

| **ФЧТ элементлари даражалари** / **Фойдаланишни чеклаш тизимлари** | **Амалга оширилиш-нинг соддалиги** | **Маъмур-лашнинг соддалиги** | $K_{конф}$ | $K_{фойд}$ | **Реконфи гурация га қарор қабул қилиш** |
|---|---|---|---|---|---|
| DAC | + | - | - | - | - |
| MAC | - | - | + | - | - |
| RBAC | - | + | + | + | + |

Ролли сиёсатнинг ўзига хос хусусиятлари фойдаланувчилар ва объектлар сони кўп, мураккаб тизимларда яхшигина бошқарувчанликка эга фойдаланишни чеклаш тизимини қуришга имкон беради ва шунинг учун, амалий тизимларда кенг қўлланилади.

Диссертациянинг «**Фойдаланишни ролли чеклаш тизими моделининг самарадорлигини ошириш»** деб номаланувчи учинчи боб мосланувчанликни, маъмурга юкламанинг пасайишини таъминлаш ва динамик фаолият муаммосини ҳал этишга имкон берувчи фойдаланишни ролли чеклаш тизими динамик моделининг тавсифига бағишланган.

RBAC модели фойдаланувчиларни битта каталогда бошқариш ёки бир хил ҳуқуқларга эга фойдаланувчиларнинг катта гуруҳларини бошқариш каби муаммолар учун фойдали ечим ҳисоблансада, турли фойдаланувчиларнинг ҳуқуқларини бошқариш ва фойдаланувчиларнинг динамик фойдаланиш учун етарли натижа бермайди. Ушбу муаммоларни ҳал қилиш учун субъектлар ва объектларни атрибутлар тўплами билан белгилашга имкон берувчи атрибутли фойдаланишни чеклаш (Attribute Based Access Control - ABAC) усулидан фойдаланилади. RBAC ва ABACлар ўзларининг афзалликларига ва камчиликларига эга ва уларнинг афзалликлари бир-бирини тўлдиради. Шу сабабли, ABAC мослашувчанлигини сақлаш мақсадида RBAC\ABAC гибрид ёндашуви (RABAC модели) тақдим этилган. RBAC билан ABACнинг қўшилиши, яъни комбинацияланган фойдаланишни бошқаришда маъмурлашни соддалаштириш ва RBACдаги муаммоларни бартараф этиш имкониятларини беради. Иккала моделнинг қўшилиши ички хавфсизлик таҳдидларидан ҳимояламайди. Мазкур ишда, ички таҳдидлардан хавфсиз схемани яратиш учун ваколатлар сатҳида (роллар сатҳида эмас) вазифаларни тақсимлаш-SODни амалга ошириш таклиф этилади. Шундай қилиб, фойдаланувчиларнинг ваколатлари илгаридек қолади ва тизим таклиф этилаётган моделдаги SODни бузмайди. SOD, битта одам назоратидан қутилиш ва фирибгарликларнинг ўсиши йўлларини камайтириш учун, амалга оширилади.

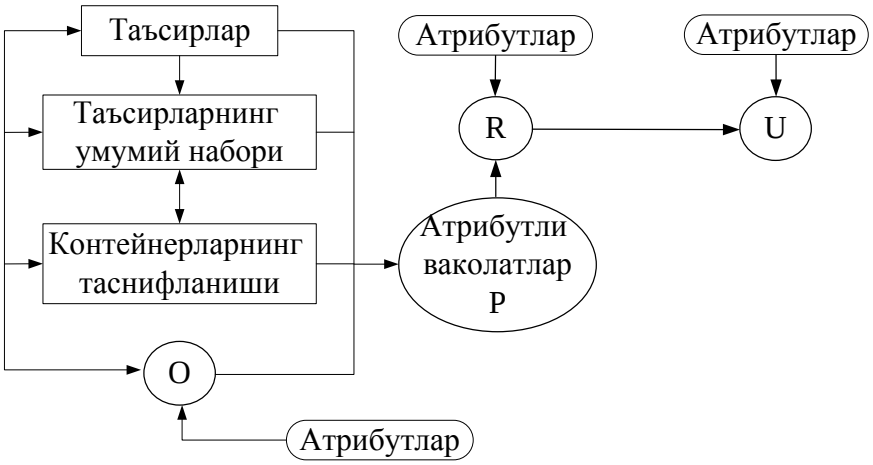
RBAC стандартида SOD низолашувчи роллар сонига боғлиқ. Бунда, таркибида битта ёки бир неча низолашувчи ваколатлар бўлган рол низолашувчи рол деб аталади. Фойдаланишни бошқаришга аталган ваколатлар ва роллар ўз ичида манфаатлар ихтилофини (Conflict Of Interest-COI) бошлаб бермайди, аммо ваколатлар ва роллар орасида COIнинг мавжудлиги жоиз ҳисобланади. Маъмур ваколатларни, вазиятга боғлиқ ҳолда, турлича яратиши мумкин. Агар объектлар сони биттадан кўп бўлса ва маъмур барча объектларга бир хил таъсирни қўллашни истаса, маъмур умумий таъсирли бир неча ваколатларни яратиш учун категориялаш контейнерларига таъсирни қўллаши мумкин. Шу тариқа маъмур турли ваколатларни, типик RBAC моделига, нисбатан кам вақт сарфи эвазига, яратиши мумкин. RBACнинг динамик модели 6- расмда келтирилган.

Ваколат атрибутлари объект атрибутлари каби, чунки ваколат-объект ва таъсир комбинацияси. Шундай қилиб, орттирилган объектлар орттирилган ваколатларни яратади. Орттирилган ваколатлар орттирилган ролларга автоматик тарзда тайинланади.

Маъмур ваколатларни тўртта усул асосида яратиши мумкин.

*1-усул.* Маъмур ваколатларни яратиш учун орттирилган объектларга таъсирни COI билан бирга ёки усиз бевосита қўллаши мумкин. Ушбу усул типик RBAC моделидаги ваколатлар яратиш усулига ўхшаш, яъни маъмур бир мартада битта ваколатни яратиши мумкин.

*2-усул*. Маъмур бир хил номли таъсирли биттадан кўп ваколатни яратиш учун контейнерларни категориялашда таъсирни COI билан ёки усиз қўллаши мумкин. Ушбу усул олдин таклиф этилган усуллардан фарқланади.

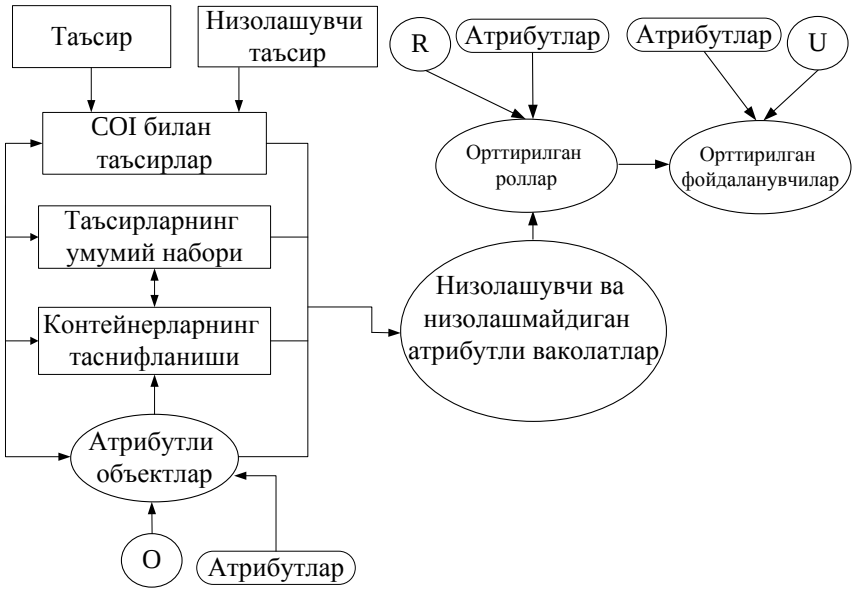



**6-расм. Атрибутлар қўшилган роллар орасидаги фойдаланишни динамик назоратлаш модели**

*3-усул.* Маъмур битта объект ва турли таъсирлар учун бир неча ваколатларни яратишда орттирилган объектларга таъсирларнинг умумий наборини қўллаши мумкин. Ушбу усулни аввал таклиф этилган моделларда амалга ошириб бўлмайди.

*4-усул.* Маъмур бир неча ваколатларни яратиш учун категориялаш контейнерларига таъсирларнинг умумий наборини қўллаши мумкин.

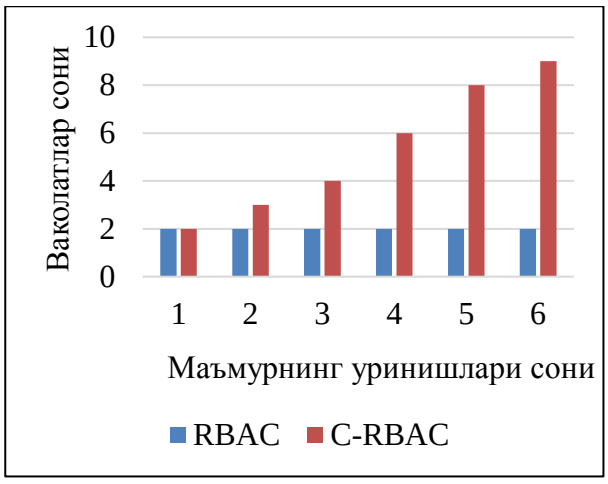
Юқорида келтирилган усуллар асосида яратилган ваколатлар, низоли – атрибутли ваколатлар ва низосиз-атрибутли ваколатлар ҳисобланади (7-расм).



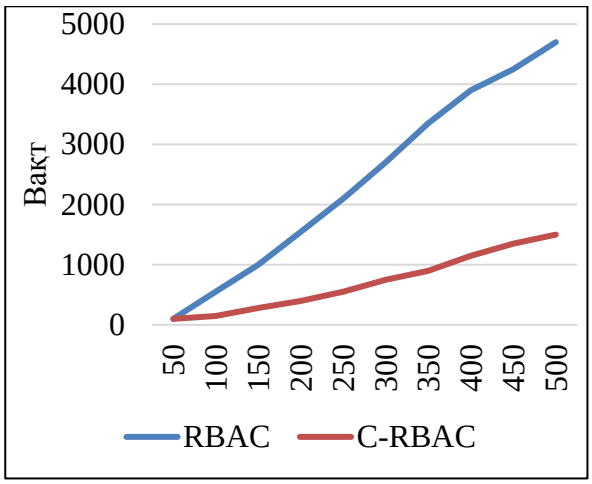

**7-расм. Динамик моделида ваколатлар асосидаги SODнинг амалга оширилиши**

Ушбу созланувчи ваколатлар илгари амалга киритилмаган эди. Маъмур ролларни ва фойдаланувчиларни турли атрибутлар билан яратади. Сўнгра атрибутланган низоли ва низосиз ваколатлар автоматик тарзда атрибутланган ролларга (орттирилган ролларга) тайинланади.

Таклиф этилаётган, ваколатлар асосидаги, динамик RBAC модели C-RBACнинг фойдаланишни бошқаришнинг турли моделлари билан таққослаш 8 (1,2)-расмда график кўринишда келтирилган.




1) Бир мартада яратилувчи ваколатлар сонини қиёслаш




2) Вақт бўйича унумдорликни қиёслаш

**8-расм. RBAC ва C-RBAC моделларининг қиёслаш графиклари**

Таклиф этилаётган модел C-RBAC бир вақтнинг ўзида бир неча ваколатларни яратади, бу унинг, фақат битта ваколат яратувчи RBAC моделидан афзаллигини кўрсатади (8 (1)-расм). 8 (2)-расмда C-RBAC моделининг типик RBAC моделига нисбатан вақт бўйича самарадорлиги график кўринишда акс эттирилган. Кўк чизиқ типик модел RBAC унумдорлигини кўрсатаса, қизил чизиқ C-RBAC модели унумдорлигини кўрсатади.

Таклиф этилаётган моделда ваколатларни ролларга, ролларнинг фойдаланувчиларга тайинлаш автоматик тарзда амалга оширилади. 3-жадвалда фойдаланишни назоратлаш моделлари характеристикаларининг таҳлили келтирилган.

**3-жадвал**

**Фойдаланишни назоратлаш моделлари характеристикаларининг таҳлили**

| Моделлар / Харак-теристикалари | RBAC | ABAC | RABAC | Таклиф этилаётган C-RBAC |
|---|---|---|---|---|
| Динамиклиги | - | + | + | + |
| Энг кам ваколатлар | + | - | + | + |
| Оддийлик | + | - | + | + |
| Мослашувчанлик | - | + | - | + |
| SODнинг самарали амалга оширилиши | - | - | - | + |
| Сиёсатни аниқлаш ва техник хизмат кўрсатиш | + | - | + | + |
| Маъмурга иш жараёнининг енгиллиги | - | + | + | + |

C-RBAC моделининг базавий структураси RBAC моделига асосланганлиги сабабли, C-RBAC модели оддийликни, энг кам имтиёзликни

ва хизмат кўрсатишда енгилликни таъминлайди. Таклиф этилаётган модел маъмурлашнинг оддийлигини, фаолиятнинг динамиклигини, қатъий хавфсизликни ва SODнинг самарали амалга оширилишини таъминлайди.

Диссертациянинг **«Фойдаланишни ролли чеклаш тизимини қуриш усуллари ва алгоритмлари»** деб номланган тўртинчи боби роллар асосида фойдаланишни бошқаришнинг динамик моделининг таҳлилига, динамик моделдаги расмий спецификация ва алгоритмлари ҳамда ишлаб чиқилган фойдаланишни ролли чеклаш тизими модели алгоритмининг тавсифига бағишланган.

Таклиф этилаётган модел алгоритми олти қадамда тавсифланган:

1-қадам. RBACнинг базавий моҳиятини яратиш: атрибутли объектлар, COIли таъсирлар, атрибутли роллар ва атрибутли фойдаланувчилар.

2-қадам. Категория контейнерларини яратиш ва атрибутли объектларни белгилаш. Умумий таъсирлар наборини яратиш ва COI ёрдамида таъсирларни белгилаш.

3-қадам. Низолашувчи ва низолашмаган атрибутли ваколатлар тўртта усул билан яратилиши мумкин (1-алгоритм, 9-расм):

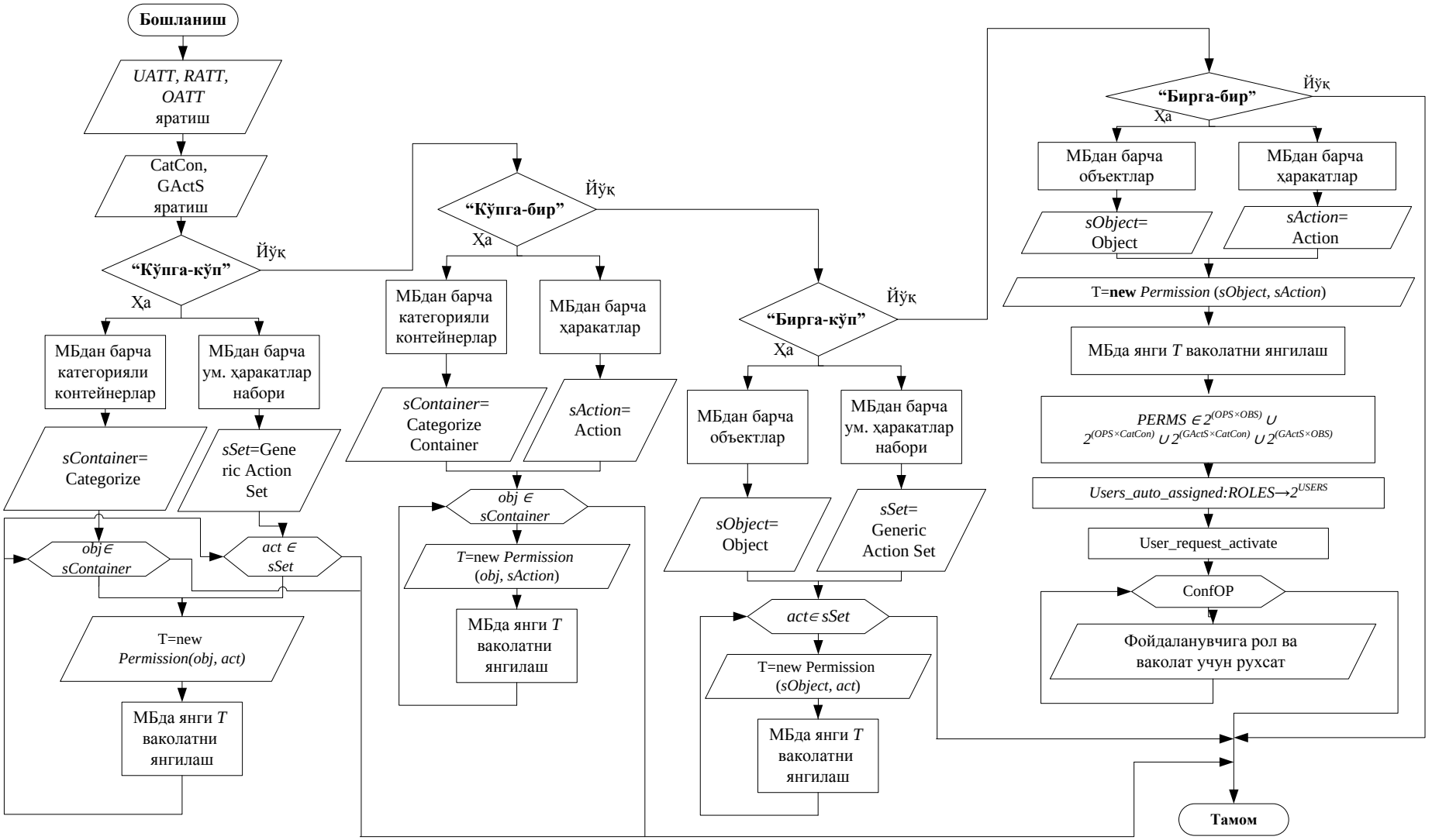
- ваколатларни бирма-бир яратиш учун объектларга таъсирларни қўллаш (анъанавий RBAC);
- бир хил таъсирли ва турли объектли бир неча ваколатларни яратиш учун категориялар контейнерига умумий таъсирлар наборини қўллаш (янги функция);
- бир хил объектли ва турли таъсирли бир неча ваколатларни яратиш учун объектларга умумий таъсирлар наборини қўллаш (янги функция);
- турли объектли ва турли таъсирли учун бир неча ваколатларни яратиш учун категориялар контейнерига таъсирларнинг умумий наборини қўллаш (янги функция).

4-қадам. Низолашувчи ва низолашмаган ваколатлар атрибутлар ёрдамида атрибутли ролларга автоматик равишда тайинланади.

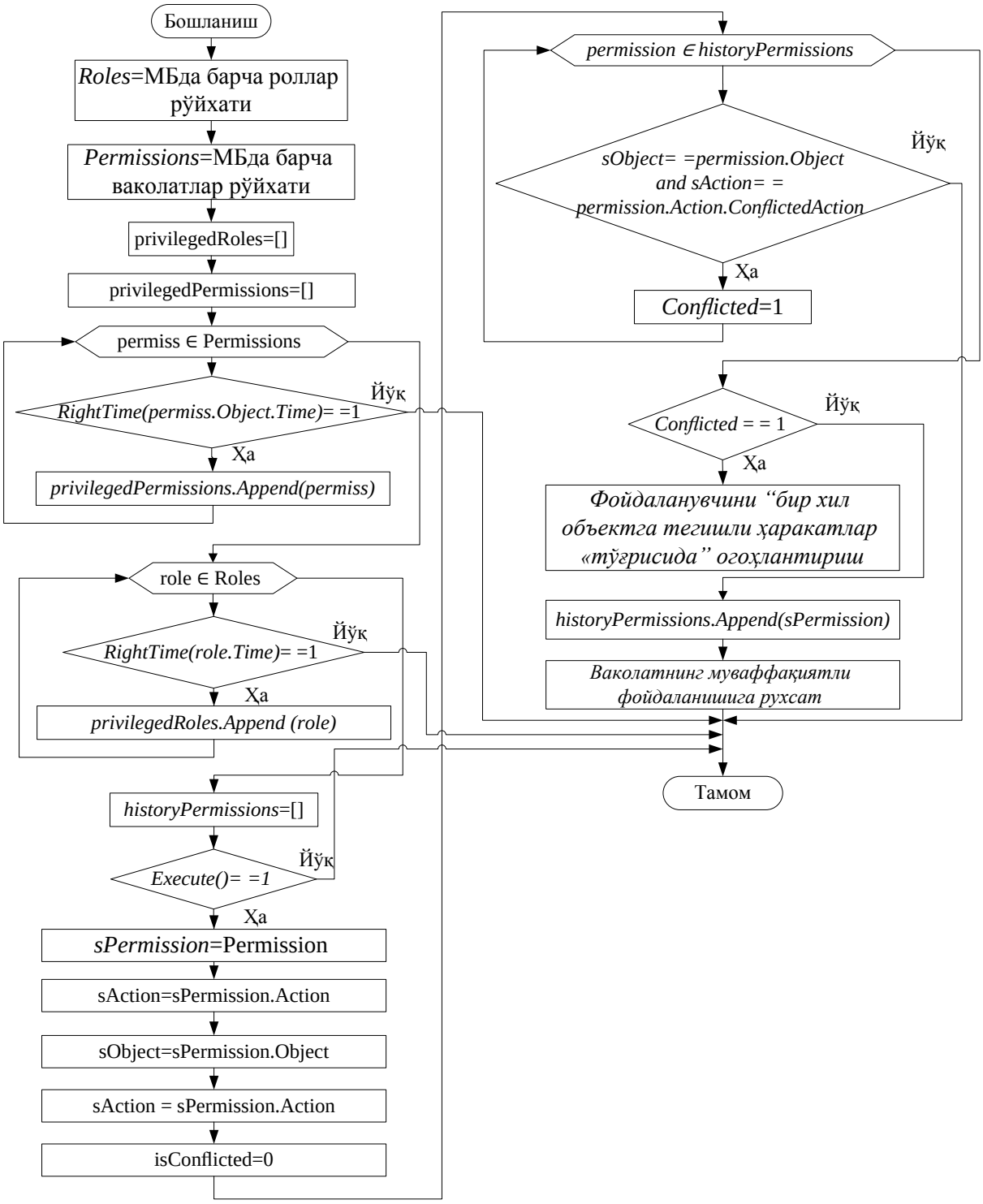
5-қадам. Атрибутли роллар атрибутли фойдаланувчиларга автоматик равишда тайинланади.

6-қадам. Фойдаланувчи тайинланган роллар ва ваколатлардан фойдаланишга рухсат олиши мумкин. Фойдаланувчи иккита низолашувчи ваколатдан бир вақтнинг ўзида фойдаланишга рухсат ола олмайди ва “Фойдаланиш тақиқланган” хабарини қабул қилади (2-алгоритм, 10-расм).

Таклиф этилаётган моделда фаолиятнинг катта қисми атрибутлар асосида бўлганлиги сабабли, маъмурга юклама ҳажми камаяди. RBACнинг типик стандартида маъмур ролга ваколатни ва фойдаланувчига ролни тайинлашни қўлда амалга оширар эди. Таклиф этилаётган моделда ваколат ва ролларни тайинланлаш автоматик тарзда амалга оширилади. Шундай қилиб, маъмурга юклама ҳажми RBACнинг типик стандартига нисбатан камаяди.




**9-расм. Ваколатларни тўрт хил усуллар билан яратиш алгоритмининг блок-схемаси**



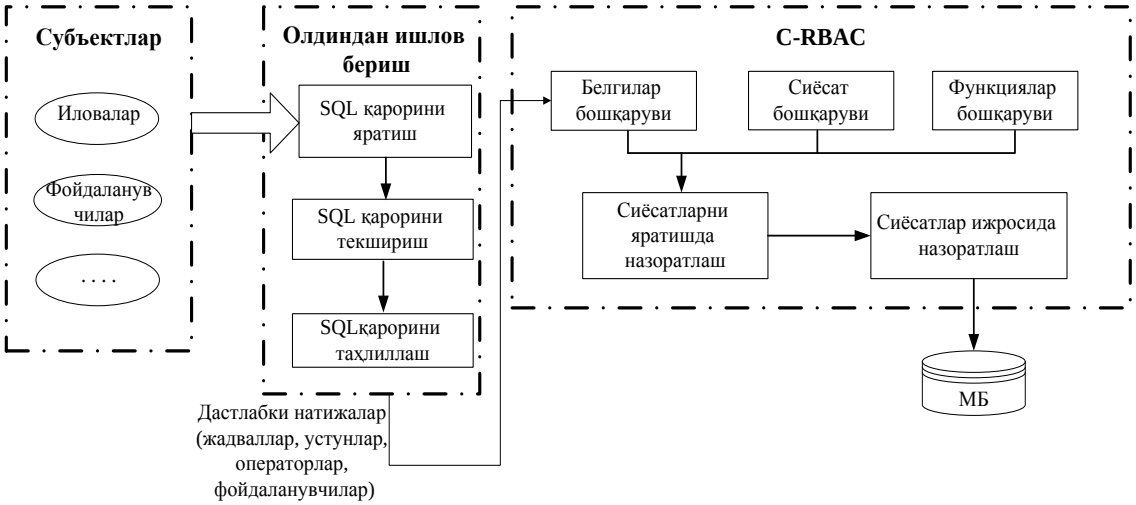

**10-расм. Фойдаланувчининг роллар ва ваколатлардан фойдаланиш ҳуқуқини олиши алгоритмининг блок-хемаси**

Диссертациянинг «**Ишлаб чиқилган усул ва алгоритмларнинг амалий татбиқи»** деб номаланувчи бешинчи бобда маълумотлардан фойдаланишни бошқаришни деталлаштиришни амалга ошириш учун, атрибутлар асосида ролли базани фойдаланишни бошқариш билан

бирлаштирувчи фойдаланишни чеклаш тизимини ишлаб чиқишга бағишланган.

Ушбу тадқиқот ишида маркетинг соҳасида мижозларга техник ва савдо-сотиқ бўйича хизмат кўрсатиш хусусида ахборотни йиғиш, қарор қабул қилиш орқали товар айланмасини ва унинг логистикасини таъминловчи ва мижоз коммуникация тизимини ташкил этишга мўлжалланган «Business Process» ахборот тизими учун, роллар асосида фойдаланишни чеклаш модели татбиқ этилган.

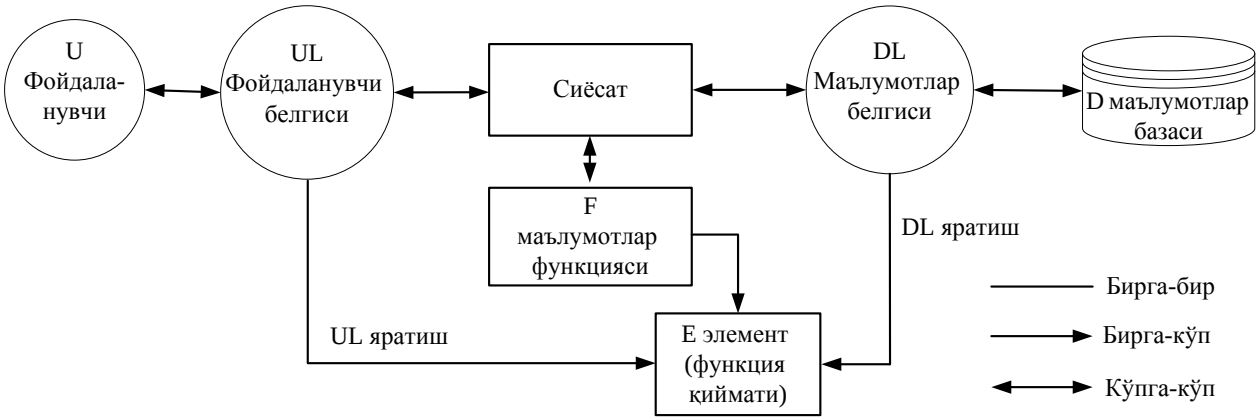
Фойдаланиш сўрови илова, фойдаланувчи ва ҳ. каби субъектлар томонидан бошланади, ва олдиндан ишлов беришда сўров учун SQL қарори яратилади. Шу билан бирга, SQL қарори дастлабки натижани олиш учун, текширилади ва таҳлилланади. Дастлабки натижа таркибида амаллар, объектлар жадвали устуни, объектлар жадвали сатри, фойдаланувчи ва ҳ. хусусида ахборот бўлади.




**11-расм. Фойдаланишни деталлаштирилган назорати структураси**

Сўнгра, дастлабки натижа C-RBACдаги белгиларни, сиёсатларни ва функцияларни бошқариш орқали текширилади. Фойдаланувчи белгиси билан сиёсатларни ишлаб чиқариш бўлимидаги маълумотлар белгисини таққослаб, якуний натижа генерацияланади. Генерациялаш сиёсатларни бажариш бўлимида амалга оширилиши мумкин.

Таклиф этилган модел асосида фойдаланишни бошқариш модули, созланувчи сиёсатлардан фойдаланиб, деталлаштирилган маълумотлардан фойдаланишни амалга ошириши мумкин. Таклиф этилган моделда фойдаланувчининг фойдаланиш ҳуқуқи таъсир қийматига биноан белгиланади. Объект ҳам, таъсир доираси ҳам, фойдаланишнинг қандайдир деталланган ваколатининг мос ҳуқуқи каби белгиланади. 12-расмда таклиф этилган моделнинг компонентлари кўрсатилган.




**12-расм. Фойдаланишни комбинацияланган ролли чеклаш моделининг компонентлари**

Ушбу компонентлар орасида рол ҳуқуқи *фойдаланувчи белгиси,* маълумотлар белгиси эса *маълумотлар белгиси* сифатида белгиланиши мумкин. Уларнинг муносабатлари-кўпга-кўп. Фойдаланувчилар белгиси (createUL) ва маълумотлар белгиси (createDL) битта сиёсат асосида бошқарилади. Ундан ташқари, UL/DL сиёсат орасидаги муносабатлари «Кўпга-кўп» муносабатлар ҳисобланади.

Маълумотлар функцияси бир неча сиёсатларда бўлиши мумкинлиги сабабли, сиёсат бир неча функцияларда тавсифланиши мумкин. Шундай қилиб, сиёсат ва маълумотлар функцияси орасида «Кўпга-кўп» муносабатлар мавжуд. Белги қиймати битта маълумотлар объектидан олинади, маълумотлар элементи эса фақат битта бўлиши мумкин. Шундай қилиб, DL ва характерли элемент қиймати (E) орасидаги муносабатлар ўзаро бир маъноли. Фойдаланиш диапазонини ифодаловчи рол белгиси UL учун, бир хил маълумотлар функциясига эга, бир неча қийматларни санаб чиқиш мумкин. Шундай қилиб, UL и E орасидаги муносабатлар «Бирга-кўп».

Фойдаланишни чеклашнинг комбинацияланган модели турли объект маълумотларини бир-бири билан боғлашни якунлашда ишлатилади. Бу маълумотларни текшириш натижаларини таъминлаб, ўрнатилувчи технологияларни яратиш характеристикаларига мос келади ва фойдаланиш чеклаш моделига маълумотларни текшириш жараёнини янада аниқроқ белгилаш имконини беради.

## ХУЛОСА

«Компьютер тизимларида фойдаланишни чеклаш воситалари самарадорлигини ошириш усуллари ва алгоритмлари» мавзуси бўйича олиб борилган тадқиқот натижалари асосида қўйидаги асосий хулосалар тақдим этилди:

1. Фойдаланишни бошқариш қисмтизимларига қўйиладиган талаблар, ахборотни рухсатсиз фойдаланишдан ҳимоялашга қаратилган тизимни қуришда, асосий механизмлар сифатида ажралиб туриши ва тизим ишончлилигини ошириши кўрсатиб берилди.

2. Мавжуд хавфсизлик моделларининг таҳлили, махфийликни муҳофаза қилиш нуқтаи назаридан, махсус мақсадли ахборот тизимини ишлаб чиқишда конфиденциаллик, яхлитлик ва фойдаланувчанлик критерийлари бўйича қўйилган талабларга жавоб бера оладиган фойдаланишни чеклаш тизимини қуришда RBAC моделини қўллаш самарали аҳамиятга эга эканлигини асослаб берилди.

3. Ахборот тизимини ишлаб чиқиш босқичида ҳужумлар оқимининг ва қарши таъсир чоралари интенсивликларини ҳисоблаш асосида ҳимояланганлигини инобатга олишда қўлланилувчи ахборот таҳдидлари ҳолатини аниқлаш модели таклиф этилган. Ушбу моделнинг ҳимояланган ахборот тизимларини ишлаб чиқишда қўлланилиши натижасида ҳимоя тизимига таъсир этувчи ҳужумлар оқими $\lambda$ га самарали қарши таъсир этиш учун $\mu$ = 0.3 - 0.5 га тенг интенсивликга эга қарши таъсир воситасини қўлланилиши зарурлиги кўрсатиб берилди.

4. Фойдаланишни чеклаш тизимининг анъанавий “пассив” компоненталари билан бир қаторда “актив” компоненталарини ўз ичига олувчи концептуал модел ишлаб чиқилган ва ушбу модел асосида қуриладиган фойдаланишни чеклаш тизимини синтезлашда “Маъмурлашнинг соддалилиги” ва “Реконфигурацияга қарор қабул қилиш” критерийлари бўйича RBAC модели самарадорлик кўрсаткичлари юқори эканлиги асослаб берилди.

5. RBAC билан ABAC моделларининг комбинациялашуви асосида фойдаланишни бошқаришда маъмурлашни соддалаштириш ва улардаги муаммоларни бартараф этиш имкониятларини берувчи динамик ролларга, атрибутларга ва ролларга асосланган моделнинг комбинациялари таклиф этилди. Бунда ушбу модел комбинациялар мавжуд моделлардан фарқли ўлароқ ваколатларни аниқ созланиши ва маъмурлашда мослашувчанлик имкониятлари билан тўлдирилди.

6. Ахборот тизимларида мавжуд бўладиган низолашадиган ва низолашмайдиган ролларни тартибга солишга имкон берувчи вазифаларни тақсимлаш (SOD)ни ваколатлар сатҳида амалга оширадиган динамик RBAC модели ишлаб чиқилган. Ушбу моделда атрибутлар қўшилиши мослашувчанликни таъминлашга, маъмур юкламаси ҳажмини камайтиришга ва маъмур томонидан бузилишлар содир этилмаслигига имкон берди.

7. Ахборот тизимларини маъмурлашда оддийлиги, динамиклиги, қатъий хавфсизликни ва SODнинг самарали амалга оширилиши орқали тизимдан фойдаланувчи ички ходимлар ва ташқи мижозлар учун ваколатлар яратилишида SODни ваколатлар сатҳида фойдаланишни бошқаришнинг комбинацияланган C-RBAC модели таклиф этилди.

Ушбу SODни ваколатлар сатҳида фойдаланишни бошқаришнинг комбинацияланган C-RBAC моделининг татбиқ этилиши тизимдан фойдаланувчи ички ходимлар ва ташқи мижозлар учун ваколатлар яратилишига сарфланадиган вақт 3 баробарга камайишига, бир хил

уринишлар сонида (N=6) ваколатларни яратиш тезлиги 2.7 мартага ошишига ахборот тизимини ҳимояланганлик даражаси эса 37%га ошишига олиб келди.

8. Ваколатларни бирма-бир яратиш учун объектларга таъсирларни қўллаш, бир хил таъсирли ва турли объектли бир неча ваколатларни яратиш учун категориялар контейнерига умумий таъсирлар наборини қўллаш, бир хил объектли ва турли таъсирли бир неча ваколатларни яратиш учун объектларга умумий таъсирлар наборини қўллаш ва турли объектли ва турли таъсирли учун бир неча ваколатларни яратиш учун категориялар контейнерига таъсирларнинг умумий наборини қўллаш орқали низолашувчи ва низолашмаган атрибутли ваколатлар яратишнинг 4 та усули алгоритмлари ишлаб чиқилган. Таклиф этилаётган усулларнинг алгоритми татбиқ этилиши натижасида ахборот тизими маъмури фаолиятининг юклама ҳажми 24%га камайди.

9. Таклиф этилган C-RBAC модели фойдаланишни назоратлашнинг деталлаштирилиши ва мослашувчанлиги нуқтаи назаридан, анъанавий RBAC моделига нисбатан қарор қабул қилиш самарадорлигига эга.

10. Фойдаланишни бошқаришнинг комбинацияланган модели асосида ишлаб чиқилган дастурий таъминот амалий ҳолатда қўлланилганда ахборот тизими хизматлардан фойдаланилишида хавфсизлик даражаси ортганини ва фойдаланувичларга яратилаётган алоҳида ваколатлар уларнинг хавфсизлигини таъминлаганини кўрсатди. Хусусан, ахборот тизимининг ҳужумлар оқимига тегишлича интенсивлик билан қарши туриш учун, нафақат ҳужум ўтказиш босқичида, балки разведка босқичида ишловчи ҳимоя элементларини самарали бошқаруви амалга оширилди. Ушбу дастурий таъминотни қўлланилиши натижасида таҳдидларга қарши тезкор жавобини 2,5 мартага оширишга шунингдек ишончлиликни кўтарилиши олиб келди.

11. Таклиф этилган моделда, рол-ваколат муносабатларини аниқлашда фойдаланувчи атрибутларининг фойдаланилувчи бўлишлиги талаби таъминланади. Таклиф этилган модел, фойдаланувчи атрибутлари ва ваколатларига мувофиқ, роллар-ваколатлар муносабатларини янада деталлаштирилган ҳолда назоратлаш имконини беради.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.01 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ИРГАШЕВА ДУРДОНА ЯКУБДЖАНОВНА**

# МЕТОДЫ И АЛГОРИТМЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СРЕДСТВ РАЗГРАНИЧЕНИЯ ДОСТУПА В КОМПЬЮТЕРНЫХ СИСТЕМАХ

05.01.05 - Методы и системы защиты информации. Информационная безопасность

**АВТОРЕФЕРАТ ДОКТОРСКОЙ (DSc)**
**ДИССЕРТАЦИИ ПО ТЕХНИЧЕСКИМ НАУКАМ**

**Ташкент – 2021**

**Тема докторской диссертации по техническим наукам (DSc) зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2020.4.DSc/T109.**

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб странице (www.tuit.uz) и на Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

| | |
|---|---|
| **Научный консультант:** | **Ганиев Салим Каримович**<br>доктор технических наук, профессор |
| **Официальные оппоненты:** | **Рахматуллаев Марат Алимович**<br>доктор технических наук, профессор |
| | **Нигматов Хикматулла**<br>доктор технических наук, профессор |
| | **Керимов Комил Фикратович**<br>доктор технических наук, доцент |
| **Ведущая организация:** | **Национальный университет Узбекистана имени Мирзо Улугбека** |

Защита диссертации состоится «03» июня 2021 года в 14:00 часов на заседании научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz.

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер № 201). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «21» мая 2021 года.
(протокол рассылки №10 от «06» мая 2021 года).

**Р.Х.Хамдамов**
Председатель научного совета
по присуждению учёных степеней
доктор технических наук, профессор

**Ф.М.Нуралиев**
Ученый секретарь научного совета
по присуждению учёных степеней
доктор технических наук, доцент

**Б.Ф.Абдурахимов**
Зам. председатель научного
семинара при научном совете
по присуждению учёных степеней
доктор физико-математических наук, профессор

## ВВЕДЕНИЕ (аннотация диссертации доктора наук (DSc))

**Актуальность и востребованность темы диссертации.** Общемировые процессы информационной глобализации подразумевают не только внедрение компьютерных систем (КС) во все сферы деятельности человека, но и необходимость обеспечения безопасности информационных систем. Отличительной особенностью информационного процесса в компьютерной системе является необходимость обеспечения высоких требований к безопасности обрабатываемой информации. Это определяется, с одной стороны, ценностью информации, обрабатываемой в КС, а с другой - наличием большого количества угроз информационной безопасности в компьютерной системе. По данному направлению в развитых странах, таких как США, Российская Федерация, Япония, Франция, Южная Корея и др. имеет важность разработки средств ограничения и мониторинга, которые предоставляют возможность обеспечения целостности и конфиденциальности информации в компьютерных системах.

Во всем мире проводятся исследования по разработке моделей, методов и алгоритмов направленные на предотвращение и защиту от несанкционированного использования, а также улучшения существующих. В этой сфере текущий подход к построению системы ограничения использования в компьютерных системах обычно статичен, и при таком подходе одной из важных задач является разработка методов и алгоритмов для удовлетворения требований по обеспечению конфиденциальности и целостности обрабатываемой информации. В то же время существует необходимость научного обоснования динамического изменения политики информационной безопасности в системах разграничения доступа и совершенствования методов управления процессом конфликта полномочий пользователей посредством технологии распределения задач.

В нашей республике государственные и хозяйственные органы принимают комплексные меры по развитию инфраструктуры национальной информационно-коммуникационной технологии и обеспечению безопасности данных, хранящихся, обрабатываемых и передаваемых в них. Согласно отчету, государственного унитарного предприятия «Центр кибербезопасности» за 2019 год «… при мониторинге информационных систем государственных органов «Информационной системой мониторинга событий информационной безопасности», выявлено 17 620 025 событий» [1]. Необходимо отметить, что в Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг. отмечены задачи, в том числе «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[2]. Одной из важных задач при выполнении исследовательских работ является разработка эффективных,

[1] https://review.uz/post/kiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda

[2] Указ Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

безопасных и основанных на паролях методов и инструментов для проверки подлинности пользователей.

Данное диссертационное исследование в определенной степени вносит вклад в выполнении задач предусмотренных Указами Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», Постановлением №ПП-4024 от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» и другх нормативно-правовых документов, принятых в данной сфере.

**Соответствие исследования приоритетным направлениям развития науки и технологий республики.** Данное исследование выполнено в соответствии с приоритетными направлениями развития науки и технологий республики IV. «Развитие информатизации и информационно-коммуникационных технологий».

**Обзор научных исследований по теме диссертации.** Научные исследования, направленные на разработку моделей и алгоритмов ролевого разграничения доступа для эффективной защиты компьютерных систем осуществляются в ведущих научных центрах и высших образовательных учреждениях мира, таких как Фрайбургский университет (Германия), Люксембургский университет технологии и коммуникации (Люксембург), Высший институт менеджмента Туниса (Тунис), Исламский университет Азад (Иран), Пекинский технологический институт, Хуачжунского университета науки и технологий, Чанчуньский университет науки и технологий (Китай), Омский Государственный университет, Тюменский государственный университет, Алтайский государственный университет (Российская Федерация), «Центр кибербезопасности» государственное унитарное предприятие (Узбекистан).

В результате исследований, проведенных в мире по моделям и методам разграничения доступа для защиты компьютерных систем получены ряд научных результатов, в том числе: описана классификация угроз безопасности в информационных системах (Higher Institute of Management Tunisia); учеными Пекинского технологического института разработана модель динамического контроля доступа на основе ролей (Key Laboratory of Intelligent Information Technology School of Computer Science and Technology, Beijing Institute of Technology, China); на основе анализа разработаны нетиповые модели разграничения доступа в информационных системах (Тюменский государственный университет, Российская Федерация); на основе анализа разработаны модели разграничения доступа в системах, обладающих равнозначными объектами (Алтайский государственный университет, Российская Федерация); на основе интеллектуального анализа разработаны модели разграничения доступа на

основе ролей (School of Computer Science and Technology, Huazhong University of Science and Technology, China); разработана комплексная среда моделирования для политик управления доступом на основе ролей (Faculty of Science, Technology and Communication, University of Luxembourg); учеными Исламского университета Азад разработаны модель аварийного ролевого контроля доступа и анализ характеристик модели со сплавом (Department of Computer Engineering, Islamic Azad University, Iran).

В мире проводятся исследования приоритетных направлений по развитию методов иерархий для оценки рисков утечки полномочий в компьютерных системах с ролевым разграничением доступа, также по разработке моделей полномочий иерархии ролей в моделях разграничения доступа, совершенствуются методы атрибутного разграничения доступа.

**Степень изученности проблемы.** Исследованию теоретических и практических аспектов проблем обеспечения информационной безопасности, различным подходам к их решению, методам построения защищенных компьютерных сетей и систем посвящены многочисленные работы таких зарубежных ученых как: Leonard J. La Padul, M. Harrison, W. Ruzzo, J. Uhlman, H. Pham, Sandhu и Samarati, David Ferraiolo, Rick Kuhn и А.В. Барабанов, Н.А. Гайдамакин, В.А. Галатенко, П.Н. Девянин, Д.П. Зегжда, Д.Ю. Гужва, С.С. Куликов, Р.М. Алгулиев, В.Ф. Шаньгин и других.

В Республике Узбекистан проблемы защиты информации, в частности информационной безопасности, изучены в исследованиях таких ученых, как Т.Ф. Бекмуратов, П.Ф. Хасанов, М.М. Арипов, С.К. Ганиев, М.М. Каримов и других. Однако к настоящему времени вопросы выбора и применения конкретных формальных моделей для построения систем разграничения доступа к компьютерным сетям недостаточно проработаны. Кроме того, ни одна из существующих моделей управления доступом не учитывает особенности ролевой структуры пользователей КС применительно к взаимодействующим функциональным модулям.

**Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация.** Диссертационная работа выполнялась в рамках фундаментальной научно-исследовательской работы №Ф4-019 «Исследование проблем формирования системы показателей и критериев информационной безопасности» (2012-2016), №Ф706-17 «Исследование применения биометрико-криптографических технологий в информационных системах» (Ахборот тизимларида биометрик-криптографик технологиялар қўлланилишининг тадқиқи) (2017-2018) выполненных в Ташкентском университете информационных технологий.

**Целью исследования** является разработка и усовершенствование модели, методов и алгоритмов построения средств разграничения доступа и контроля полномочий для эффективной защиты компьютерных систем.

**Задачи исследования:**

выделение угроз на основе анализа инцидентов в компьютерных системах, касающихся средств контроля и управления;

разработка модели выявления угроз при построении системы разграничения доступа в компьютерных системах;

разработка концептуальной модели функционирования системы разграничения доступа;

формирование показателей оценки эффективности для систем разграничения доступа;

разработка динамической модели разграничения доступа;

разработка комбинированной модели ролевого разграничения доступа для применения разделения обязанностей (SOD) на основе атрибутов;

разработка методов и алгоритмов разграничения доступа для определения конфликтующих и неконфликтных полномочий.

**Объектом исследования** является процесс контроля и управления доступом в компьютерных системах.

**Предметом исследования** являются методы, модель безопасности, алгоритмы и программные средства защиты информации.

**Методы исследования.** Основными методами исследований являются: теория вероятностей, теория множеств, теория графов, методы защиты информации, система моделирования Alloy, методы программирования.

**Научная новизна исследования** заключается в следующем:

сформирован список угроз, относящихся к средствам контроля и управления доступом в компьютерных системах, на основе стандартов информационной безопасности и показатели определяющие оценку эффективности систем защиты информации;

разработана модель выявления угроз в системах управления доступом, позволяющая рассчитывать вероятность воздействия угроз на систему разграничения доступа;

разработана концептуальная модель системы разграничения доступа, отражающая решения на реконфигурацию процессов формальных моделей и методов разграничения доступа;

разработаны аналитические выражения и методика функционирования систем разграничения доступа, обеспечивающих динамическое управление схемами разграничения с учетом нечеткого характера содержащихся в них элементов;

разработана комбинированная модель с применением разделения обязанностей (SOD), которая динамически назначает полномочия ролям, а также назначает пользователей ролям с помощью различных атрибутов;

разработаны алгоритмы в режиме «многие ко многим», «многие ко одному», «один ко многим», «один ко одному» в модели ролевого разграничения доступа для определения конфликтующих и неконфликтных полномочий.

**Практические результаты исследования** заключаются в следующем:

разработана модель, которая экономит время и снижает нагрузку на администратора за счет динамического назначения конфликтующих и неконфликтных полномочий ролям, обеспечивая гибкую, динамическую и безопасную модель управления доступом;

предложен метод доступа к данным, объединяющий ролевую базу и контроль доступа на основе меток, для выполнения детального контроля доступа к данным;

разработано программное обеспечение на основе комбинированной модели, которое позволяет уменьшить каналы увеличения мошенничества и обеспечивает надёжное функционирование базы данных компьютерных систем.

**Достоверность результатов исследования** подтверждается корректностью постановок задач, полнотой учета совокупности и характера факторов, влияющих на защищенность информации от НСД в КС при их функционировании в условиях информационного конфликта, полнотой представленных моделей синтеза и управления несанкционированного доступа, непротиворечивостью предлагаемых решений известным результатам, полученным другими способами.

**Научная и практическая значимость результатов исследования.** Научная значимость результатов диссертационной работы заключается в разработке модели и метода синтеза системы разграничения доступа, обеспечивающих необходимый научно-методологический базис для дальнейшей разработки формальных моделей и методов построения и функционирования данных систем, отражающих особенности функционирования КС в условиях информационного конфликта и оценки на их основе эффективности синтеза данных систем.

Практическая значимость результатов исследования диссертационной работы заключается в том, что синтез системы разграничения доступа и комбинированная модель ролевого разграничения доступа позволяют повысить защищенность от несанкционированных воздействий и надёжное функционирование базы данных компьютерных систем. Кроме того, полученные результаты доведены до уровня программной реализации.

**Внедрение результатов исследования.** На основе полученных научных результатов по повышениию эффективности методов и алгоритмов разграничения доступа в компьютерных системах разработаны модели и алгоритмы ролевого разграничения доступа, обеспечивающие эффективную защиту компьютерных систем:

разработанные методы и алгоритмы определения конфликтующих и неконфликтующих полномочий модели разграничения доступа на основе ролей внедрены в информационных системах банка «Agrobank» и «Qishloq Qurilish Bank». (справка Министерства по развитию информационных технологий и коммуникаций от 03 февраля 2021 года №33-8/821). Использование результатов научных исследований позволило увеличить

скорость быстрого реагирования на угрозы на 37%, а также сократить время, затрачиваемое на создание полномочий на 24%;

модель состояния угроз безопасности, являющаяся моделированием вероятности воздействия угроз на систему безопасности информационной системы и вероятности раскрытия системы защиты информации, внедрена в Агенство «O'zarxiv» Республики Узбекистан (справка Министерства по развитию информационных технологий и коммуникаций от 03 февраля 2021 года №33-8/821). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие угроз в 1,5 раза и повысить надежность.

программное средство, разработанное на основе модели определения угроз, позволяющее вычислить вероятность влияния угроз на систему разграничения доступа внедрено в ООО «OFFICIAL DEALER TRADE» (справка Министерства по развитию информационных технологий и коммуникаций от 03 февраля 2021 года №33-8/821). Использование результатов научного исследования позволило увеличить оперативное реагирование на наличие угроз в 2,5 раза и повысить надежность;

программное средство, основанное на комбинированной модели C-RBAC разграничения доступа на основе ролей внедрено в информационную систему Головного научно-методического центра при Министерстве высшего и среднего специального образования Республики Узбекистан (справка Министерства по развитию информационных технологий и коммуникаций от 03 февраля 2021 года №33-8/821). В результате получена экономия времени в 2 раза за счет того, что назначение полномочий ролям, назначение ролей пользователям происходит автоматически;

метод синтеза систем разграничения доступа внедрен в Академии Министерства внутренных дел (справка Министерства по развитию информационных технологий и коммуникаций от 03 февраля 2021 года №33-8/821). Эффективность внедрения научных результатов показана повышением уровня усвоения учебных материалов, в результате подтверждена практическая помощь в подготовке квалифицированных специалистов.

**Апробация результатов исследования.** Результаты данного исследования обсуждались на 7 международных и 11 республиканских научно-технических и научно-практических конференциях.

**Опубликованность результатов исследования.** Основные результаты исследования опубликованы в 30 научных работах, из которых 13 опубликованы в журналах, перечня научных изданий рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, в том числе 8 в зарубежных и 5 в республиканских журналах, а также получены 2 свидетельства об официальной регистрации программы для ЭВМ.

**Структура и объём диссертации.** Диссертационная работа содержит 180 страниц и состоит из введения, пяти глав, заключения, списка использованной литературы и приложений.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

**Во введении** обоснована актуальность темы диссертации, приведен краткий анализ состояния проблемы информационной безопасности в компьютерных системах Республики Узбекистан, определены цель и задачи исследования. Охарактеризована научная новизна и показана практическая значимость результатов работы, сформулированы основные научные положения, выносимые на защиту, приведены результаты внедрения исследований, сведения об опубликованности результатов и структуре диссертации.

Первая глава диссертации «**Современное состояние информационной безопасности компьютерных систем**» посвящена анализу проблем защиты и формированию основных требований и угроз к проектированию защищенных компьютерных систем на основе анализа моделей разграничения доступа.

Организация обеспечения информационной безопасности должна носить комплексный характер. Она должна основываться на глубоком анализе всевозможных негативных последствий. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих возникновению уязвимостей и как следствие, определение актуальных угроз информационной безопасности. Процесс реализации угроз представлен на рисунке 1.

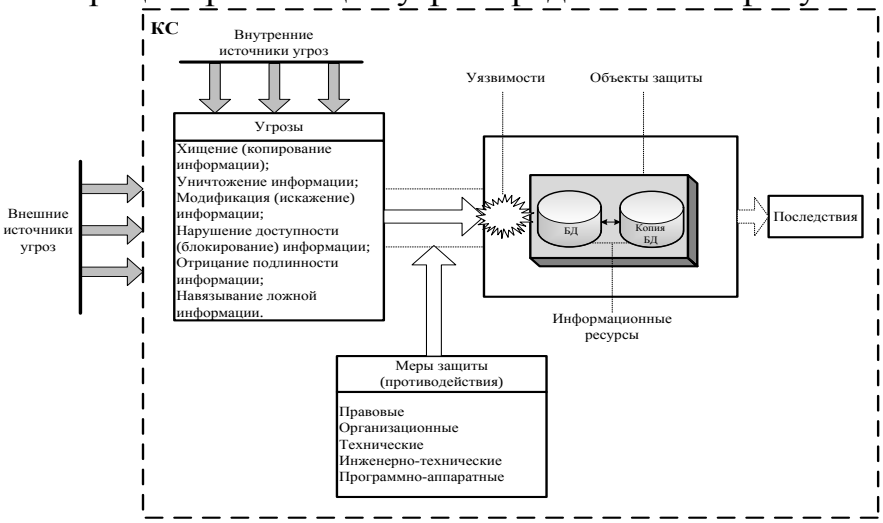



**Рис.1. Процесс реализации угроз**

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем источники угроз могут находиться как внутри КС - внутренние источники, так и вне нее - внешние источники.

В национальном стандарте O'Z Dst ISO/IEC 27033-3:2016 описываются угрозы к средствам контроля и управления, связанных с компьютерными

системами. Анализ областей, которые могут повлиять на защиту от несанкционированного использования средств контроля и управления в компьютерных системах, позволил выявить соответствующие факторы (таблица 1).

**Таблица 1.**

**Примеры различных типов угроз средств контроля и управления в компьютерных системах**

| **Дестабилизирующие факторы** | **Похищение и фальсификация данных в управлении доступом** | **Нарушение конфиденциальности** | **Утрата целостности** |
|---|---|---|---|
| Несанкционированное получение средств проведения аутентификации личности или программного обеспечения. | + | | |
| Взлом пароля или других видов средств удостоверения подлинности. | + | | + |
| Управление доступом, без разрешения администратора контроля доступа. | + | + | |
| Несанкционированное изменение или копирование данных. | + | | + |
| Похищение данных. | + | + | |
| Несанкционированное создание нового нелегального пользователя. | + | + | |
| Несанкционированное введение вредоносных программ и кодов. | + | | + |
| Несанкционированное прекращение работы компьютерной сети. | | | + |

Одним из основных объектов угроз безопасности является оперативная информация, хранящаяся в базе данных компьютерной системы. Однако в ряде случаев реализация угроз оперативной информации предполагает наличие необходимых полномочий для использования информации. Эти полномочия могут быть получены путем воздействия на технологическую информацию базы данных компьютерной системы, включая информацию системы защиты.

Во второй главе диссертации **«Синтез систем разграничения доступа в компьютерных системах»** приведено описание модели угроз, позволяющее вычислить влияние угроз на системы разграничения доступа и вероятности компрометации данной системы, системы разграничения

доступа и ее концептуальной модели, а также показателей эффективности системы разграничения доступа.

По типу угроз, относящихся к системе ограничения использования, представленных в первой главе диссертации, можно сформировать модель угроз системы разграничения доступа, которая характеризуется деструктивным поведением. В качестве злоумышленника должен рассматриваться субъект, действия которого направлены на несанкционированное использование информации в компьютерной системе с помощью штатных средств информационной системы.

Построение модели угроз начинается с формирования неформальной модели атак (рисунок 2). При проведении атаки намерение искажается, моделируя любое событие безопасности, которое приводит к желаемому результату. Можно перейти от неформальной модели к модели угроз. Модель статуса угрозы целесообразно рассматривать как набор блоков, каждый из которых соответствует *i*-му состоянию угрозы. Эта модель представлена на рисунке 3.


**Рис. 2. Неформальная модель атаки**

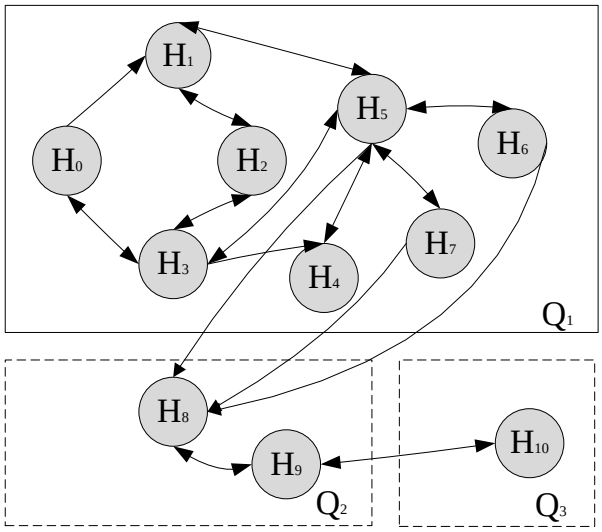



**Рис. 3. Модель состояние угроз безопасности**

Данная модель угрозы безопасности представлена как ситуация угрозы $H_i$ *(i=0…10)*, где $H_0 -$ начальное или безопасное состояние системы ограничений, $H_1 - H_{10}$ состояние различных угроз. Также $Q_1 - Q_3$ подсистемы подготовки, реализации и завершения угроз.

Вероятность на момент времени *H(t)* состояния системы угроз рассматривается в качестве комплекса вероятности $H_t$ состояния данной системы и выражается следующим образом: $e_i(t) = e(H(t) = h_i)$, здесь $H(t)$ случайное состояние системы в момент времени. Вероятность перехода определяется следующим образом: $e_{ij}(t) = e(Hk = H_j | H(k-1) = H_j)$.

Вероятности того, что система угроз будет на шаге $k$, определяется с помощью формулы полных вероятностей и перехода от шага *(k-1)* к шагу $k$ и выражается в следующей рекуррентной форме: $e_j(k) = \sum_{i=1}^{n} e_i(k-1)e_{ij}$.

Основными параметрами модели угроз являются вероятность воздействия системы угроз на систему защиты информации компьютерной системы и вероятность раскрытия системы защиты информации. При этом преобразование осуществляется с модели, приведенной на рисунке 3, это модель в виде определенного графа (рисунок 4).

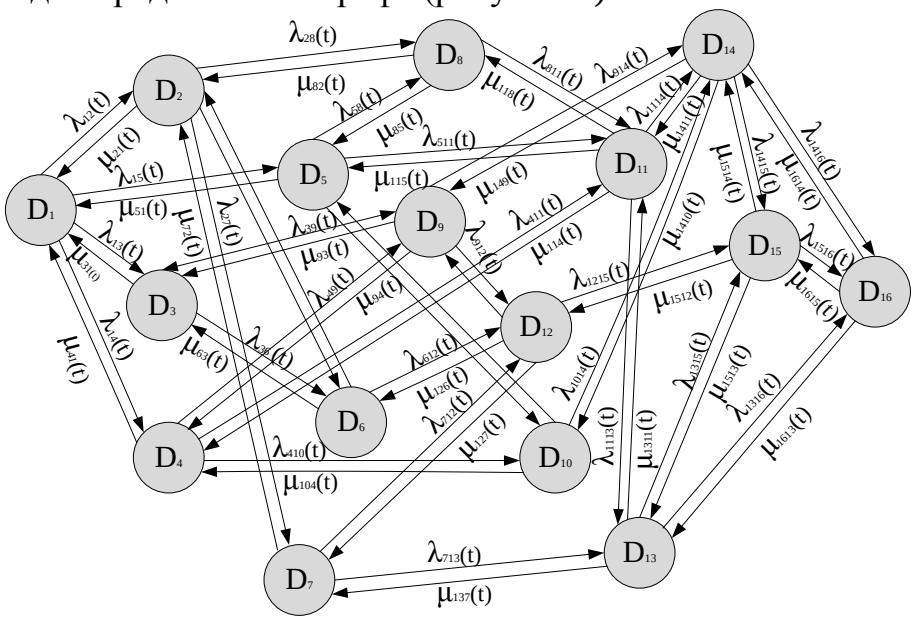



**Рис.4. Граф состояния системы защиты**

Для этого приняты следующие определения:

$\mu_i$ – интенсивность направленная на восстановления системы защиты информации;

$\gamma_i$ – интенсивность компрометации системы защиты;

$e_i$ – вероятность состояния начала событий ($e_1$ – вероятность неосуществления внешней атаки; $e_2$- вероятность осуществления внешней атаки; $e_3$- вероятность осуществления внутренних различных атак; $e_4$- вероятность осуществления неизвестной атаки; $e_5$ – вероятность осуществления атаки на систему управления).

$D_i$ – состояние системы защиты. Состояния системы защиты включает в себя 16 состояний, которые приведены на рисунке 4 и при этом подразумевает одновременное воздействие на систему событий, которые могут произойти. Для удобства понимания поток атак $\lambda_i(t)$ и поток влияния против атак $\mu_i(t)$ обозначены "⇆" стрелками.

Зная заданный граф или матрицу интенсивности, можно выражать систему дифференциальных уравнений для вероятности состояния системы защиты информации, используя мнемоническое правило:

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

Тогда вместо системы однородных дифференциальных уравнений с постоянными коэффициентами можно получить систему однородных алгебраических уравнений с постоянными коэффициентами. Эта система алгебраических уравнений может быть решена с учетом следующего нормированного условия: $\sum_{i=1}^{16} e_i(t) = 1, (0 \le e_i(t) \le 1; t \ge 0)$.

Дифференциальное уравнение преобразуется в систему однородных алгебраических уравнений с постоянными коэффициентами:

$$e_i = \sum_{j=1}^{n} \lambda_{ij} e_j - e_i \sum_{j=1}^{n} \lambda_{ij}. \quad (1)$$

выражение (1) можно преобразовать на следующий вид:

$e_i \sum_{j=1}^{n} \lambda_{ij} = \sum_{j=1}^{n} \lambda_{ij}\, e_j$, или более простой вид:

$e_i = \frac{\sum_{j=1}^{n} \lambda_{ij} e_j}{\lambda_i}$ $(i = 1,2,3, \dots, n)$, здесь $\lambda_i = \sum_{j=1}^{n} \lambda_{ij}$.

Чтобы решить систему алгебраических уравнений, одно из этих уравнений необходимо заменить нормирующим условием $\sum_{j=1}^{n} e_i = 1$.

Ниже приведены вероятности перехода системы защиты в систему защиты при разной интенсивности атак и интенсивности системы защиты, направленной на реагирование атаки.

Сумма потоков атаки $\lambda$ и коэффициентов защиты против атаки $\mu$ принимается равной 1. В этом случае $\lambda$ и $\mu$ обратно пропорциональны друг другу. На основании разработанной модели можно сделать следующие выводы: при воздействии максимального потока атак на систему защиты и при отсутствии каких-либо негативных воздействий на эти атаки со стороны этой системы вероятность раскрытия системы составляет 1; вероятность полного раскрытия системы защиты при равенстве токов атаки и контратаки 0,0625; в случае $\lambda = 0.75$ и $\mu = 0.25$ вероятность полного раскрытия системы защиты составляет 0,3. Следовательно, для эффективного противодействия потоку атак $\lambda$, влияющих на систему защиты, требуется система противодействия с интенсивностью $\mu = 0.3 - 0.5$. При этом необходимо учитывать, что увеличение интенсивности приводит к удорожанию системы защиты.

Для реализации системы управления доступом создается математическая модель информационной системы. Она может моделировать все ее состояния, переходы из одного состояния в другое, а также показывать, какие состояния можно считать безопасными. Существуют различные подходы к формализации задачи синтеза системы защиты информационной системы на основании выбранной политики безопасности. Рассмотрим один из наиболее эффективных, рассчитанный на современные программные технологии реализаций.

Все обращения к информационным ресурсам осуществляются под контролем средств управления доступом, обеспечивающих выполнение правил политик безопасности при доступе к тем информационным ресурсам, которые являются объектами. Средства контроля целостности обеспечивают целостность средств защиты и восстановление целостности информационных ресурсов. В результате дополнительно к традиционным функциональным компонентам системы разграничения доступа добавляются модули, реализующие функции оперативного контроля доступа к информациям и ресурсам обнаружения угроз и реагирования на их появление. При использовании подхода к моделированию сложных динамических систем

функционирование систем разграничения доступа может быть описано концептуальной моделью, представленной на рисунке 5.

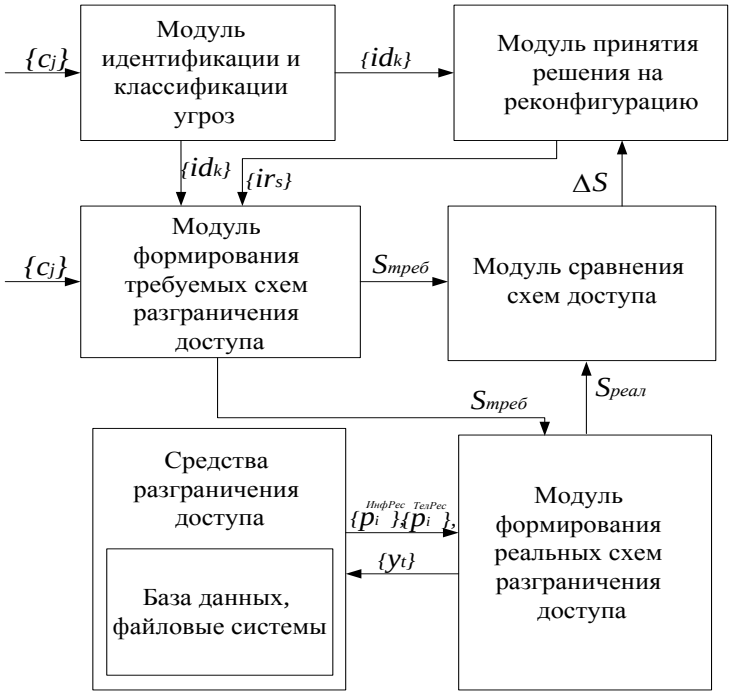



**Рис. 5. Концептуальная модель системы разграничения доступа**

В этом случае процесс функционирования системы разграничения доступа может быть описан выражением:

$y\,(t_2) = Y\left(S_{\text{треб}}(t_1), \vec{V}^{\text{ИнфРес}}(t_1), \vec{V}^{\text{ТелРес}}(t_1)\right)$, где $S^{\text{треб}}(t_1)$ – требуемая схема разграничения доступа в момент времени $t_1$; $\vec{V}^{\text{ИнфРес}}(t_1) = \left\{v_i^{\text{ИнфРес}}\right\}$ - вектор характеристик средств разграничения доступа к информационным ресурсам КС (базам данных, файловым системам) в момент времени $\mathrm{t}_1$; $\vec{V}^{\text{ТелРес}}(t_1) = \left\{v_i^{\text{ТелРес}}\right\}$ - вектор характеристик средств разграничения доступа к телекоммуникационным ресурсам КС (виртуальным сетям) в момент времени $\mathrm{t}_1$; $y(t_2)$- решение по разграничению доступа, которое вырабатывается системой разграничения доступа в момент времени $t_2$, $t_2 > t_1$. Требуемая схема разграничения доступа в момент времени $t_2$ образуется в модуле формирования требуемых схем разграничения доступа: $\mathrm{S}_{\text{треб}}(t_2) = F(\vec{C}(t_1), \overrightarrow{Id}(t_1), \overrightarrow{Ir}(t_1))$, где $\vec{C}(t_1) = \{c_j\}$ - вектор внутренних параметров информационных и телекоммуникационных ресурсов КС в момент времени $t_1$; $\overrightarrow{Id}(t_1) = \{id_k\}$ - вектор угроз, выявленных в момент времени, $\mathrm{t}_1$ в модуле идентификации; $\overrightarrow{Ir}(t_1) = \{ir_s\}$ - вектор решений, выработанных в момент времени $t_1$ в модуле принятия решений на реконфигурацию системы разграничения доступа. Реальная схема разграничения доступа в момент времени $\mathrm{t}_2$ образуется в модуле формирования реальных схем разграничения доступа:

$$\mathrm{S}_{\text{реал}}(t_2) = \Pi\left(\mathrm{S}_{\text{треб}}(t_1), \vec{V}^{\text{ИнфРес}}(t_1), \vec{V}^{\text{ТелРес}}(t_1)\right).$$

Оценка сравнения требуемой и реальной схем разграничения доступа $\Delta S$ в момент времени $t_2$ формируется в модуле сравнения схем доступа согласно выражению: $\Delta S(t_2) = \Phi\left(\mathrm{S}_{\text{треб}}(t_1), \mathrm{S}_{\text{реал}}(t_1)\right)$.

Решение о необходимости осуществления реконфигурации системы разграничения доступа в момент времени $t_2$ вырабатывается в модуле принятия решений в соответствии с выражением: $Ir(t_2) = Ir(\overrightarrow{Ir}(t_1), \Delta S(t_1))$.

Вектор угроз, обнаруженных модулем идентификации и классификации в момент времени $\mathrm{t}_2$, определяется на основании выражения: $\overrightarrow{Id}(t_2) = Id(\vec{C}(t_1))$.

Следовательно, для реализации процесса функционирования систем разграничения доступа в ее состав должны быть введены средства, реализующие функции саморегулируемого управления разграничением доступа, связанного с идентификацией и классификацией угроз.

Известная методология оценки эффективности целенаправленных процессов при формировании системы показателей требует, чтобы в ее состав были в обязательном порядке включены те показатели, которые характеризуют результативность (назначение), оперативность и ресурсоемкость оцениваемого процесса. Вместе показатели эффективности синтеза систем разграничения доступа образуют многоуровневую систему.

Результативность процесса синтеза систем разграничения доступа может оцениваться следующими комплексными показателями: $Э_{нсд}$ - вероятностью НСД к информации, которая характеризует статическую защищенность информации от НСД; $Э_{об.НСД}$ - вероятностью обеспечения защиты от НСД в течение заданного времени, которая раскрывает динамическую защищенность информации от НСД. Значение $Э_{нсд}$ выражает способность СРД к предотвращению попыток НСД, что соответствует традиционному подходу к оценке эффективности защиты информации от НСД. Вероятность $Э_{об.НСД}$, отражает способность СРД обеспечивать защищенность информации от НСД в условиях наличия попыток НСД и программных атак.

Указанные выше показатели являются показателями эффективности комплексного уровня. Кроме них, к данному уровню системы показателей эффективности следует отнести: $K_{\text{и}}^{\text{вр}}$ - коэффициент использования вычислительных ресурсов; $K_{\text{и}}^{\text{тр}}$ - коэффициент использования сетевых ресурсов; $N$ - стоимость.

Эти показатели определяют насколько загружаются, соответственно, вычислительные и сетевые мощности системы защиты информации в интересах разграничения доступа. Данные показатели являются безразмерными.

На уровне частных показателей эффективности следует выделить показатели двух свойств синтеза: оперативности и достоверности. Показателями оперативности являются: $Э\ (t_{\text{и}} <= T^{\text{дос}})$- вероятность своевременной идентификации и классификации угроз безопасности;

Э ($t_{\text{п}} <= T^{\text{дос}}$)- вероятность своевременного поиска вариантов управления СРД; Э ($t_{\text{ф}} <= T^{\text{дос}}$)- вероятность своевременного формирования схемы разграничения доступа.

Показателями достоверности являются: $Э_{ои}$ - вероятность ошибки идентификации угроз; $Э_{оу}$ - вероятность ошибки управления СРД; $Э_{оф}$ - вероятность ошибки формирования схем разграничения доступа.

Показателями уровня элементов систем разграничения доступа, а именно схем разграничения доступа, для каждого из используемых в КС способов доступа - дискреционного, мандатного или ролевого - выступают показатели: $K_{конф}$ - коэффициент полноты реализации требований по конфиденциальности; $K_{дост}$- коэффициент полноты реализации требований по доступности.

Если применять вышеприведенные показатели на существующие модели разграничения доступа с учетом предлагаемой модели системы формирования разграничения доступа, то можно получить сравнительную оценку систем разграничения доступа, которые базированы на конкретном одном из моделей.

Модели дискреционного (DAC) и мандатного (MAC) контроля доступом имеют одно фундаментальное отличие от ролевой модели (RBAC). В этих моделях заранее определяют политику безопасности системы и позволяют ее настраивать для каждой конкретной ситуации. В тоже время ролевая модель ни в коей мере не предопределяет политику безопасности, а позволяет ее настроить в том виде, в каком это требуется для организации, т.е. ролевое разграничение доступа предоставляет возможность повышения уровней надежности с перестраиваемой структурой для модели функционирования систем разграничения доступа. В таблице 2 приведены сравнения показателей уровня элементов в системах разграничения доступа.

**Таблица 2.**

**Сравнения показателей уровня элементов в системах разграничения доступа**

| **Уровни элементов СРД** / **Системы разграничения доступа** | **Простота реализации** | **Простота администрирования** | **$K_{конф}$** | **$K_{дост}$** | **Принятия решения на реконфигурацию** |
|---|---|---|---|---|---|
| **DAC** | + | - | - | - | - |
| **MAC** | - | - | + | - | - |
| **RBAC** | - | + | + | + | + |

Данные особенности ролевой политики позволяют строить системы разграничения доступа с хорошей управляемостью в сложных системах с

большим количеством пользователей и объектов, и поэтому находят широкое применение в практических системах.

В третьей главе диссертации **«Повышение эффективности модели ролевого разграничения доступа»** дается динамическая модель ролевого разграничения доступа, реализованная для обеспечения гибкости, снижения нагрузки и решения проблемы динамического поведения.

RBAC является полезным решением для некоторых конкретных проблем: управление пользователями в одном каталоге или управление большими группами пользователей с одинаковыми правами. Но RBAC, как единственная модель предоставления доступа, не подходит для более общей проблемы управления правами большого количества разнообразных пользователей и динамического доступа пользователей во многих системах. Ввиду того, что ресурсы и пользователи зачастую располагаются в разных доменах, связи между субъектами и объектами в таких системах становятся более сложными и динамичными. Для решения этих проблем был предложен атрибутный метод разграничения доступа (Attribute Based Access Control - ABAC). Его цель заключается в обозначении субъектов и объектов совокупностями атрибутов и позволяет принимать решение по управлению доступом без предварительного знания субъектов или их отношения к поставщику услуг.

RBAC и ABAC имеют свои особые преимущества, а недостатки, и их преимущества дополняют друг друга. Поэтому предложен гибридный подход RBAC/ABAC (а именно модель RABAC), чтобы сохранить простоту и безопасность на основе ролей, а также гибкость ABAC. Слияние RBAC и ABAC даёт возможности простоты администрирования в управлении доступом и устранения проблем в RBAC. Объединение обеих этих моделей не защищает от угроз внутренней безопасности. Для создания безопасной схемы от внутренних угроз в работе предлагается реализация разделения обязанностей-SOD на уровне полномочий, а не на уровне ролей. Таким образом, уровень полномочий конечных пользователей останется прежним, и система не будет нарушать SOD в предлагаемой модели. SOD реализовывается для того, чтобы избежать контроля со стороны одного человека и уменьшить каналы увеличения мошенничества.

SOD в стандарте RBAC зависит от количества конфликтующих ролей, при этом роль, которая содержит одно или несколько конфликтующих полномочий, называется конфликтующей ролью. Полномочия и роли предназначенные для управления доступом, не инициируют конфликт интересов внутри себя, а разрешения заставляют роли находиться COI (Conflict Of Interest-COI) между ними. Администратор может создавать полномочия по-разному в зависимости от ситуации. Если существует только один объект, а для создания полномочий требуется несколько действий, администратор может применить к объектам общий набор действий. С другой стороны, если существует более одного объекта, а администратор хочет применить одно и то же действие ко всем объектам, то он может

применить действие к контейнерам категоризации для создания нескольких полномочий с общим действием. Таким образом, администратор может создавать различные полномочия за меньшее время по сравнению с традиционной моделью RBAC. Динамическая модель RBAC представлена ниже на рисунке 6.

Атрибуты полномочий будут такими же, как атрибуты объекта, поскольку полномочия - это комбинация объекта и действия. Таким образом, приписанные объекты будут создавать приписанные полномочия. Приписанные полномочия автоматически назначаются приписанным ролям.

Администратор может создавать полномочия четырьмя способами:

*во-первых*, администратор может применять действия с COI и без него непосредственно к атрибутированным объектам для создания полномочий. Этот процесс создания полномочий аналогичен типичной модели RBAC, то есть администратор может создавать одно полномочие за раз;

*во-вторых,* администратор может применять действия с COI и без него для категоризации контейнеров для создания более одного полномочия с одним и тем же именем действия. Этот тип создания отличается от ранее предложенных моделей;

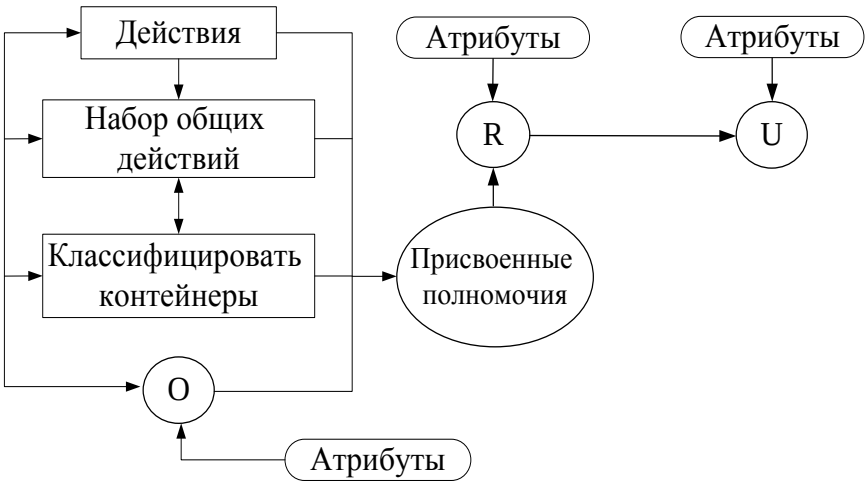



**Рис. 6. Модель динамического контроля доступа на основе ролей с добавлением атрибутов**

*в-третьих,* администратор может применить общий набор действий к атрибутированным объектам, чтобы создать несколько полномочий для одного и того же объекта и разных действий. Этот тип создания полномочий также недоступен в ранее предложенных моделях;

*в-четвертых,* администратор может применить общий набор действий к контейнерам категоризации для создания нескольких полномочий за раз.

Полномочия, созданные всеми способами, являются полномочиями с атрибутами-конфликтами и полномочиями с атрибутами-неконфликтными, как показано на рисунке 7.

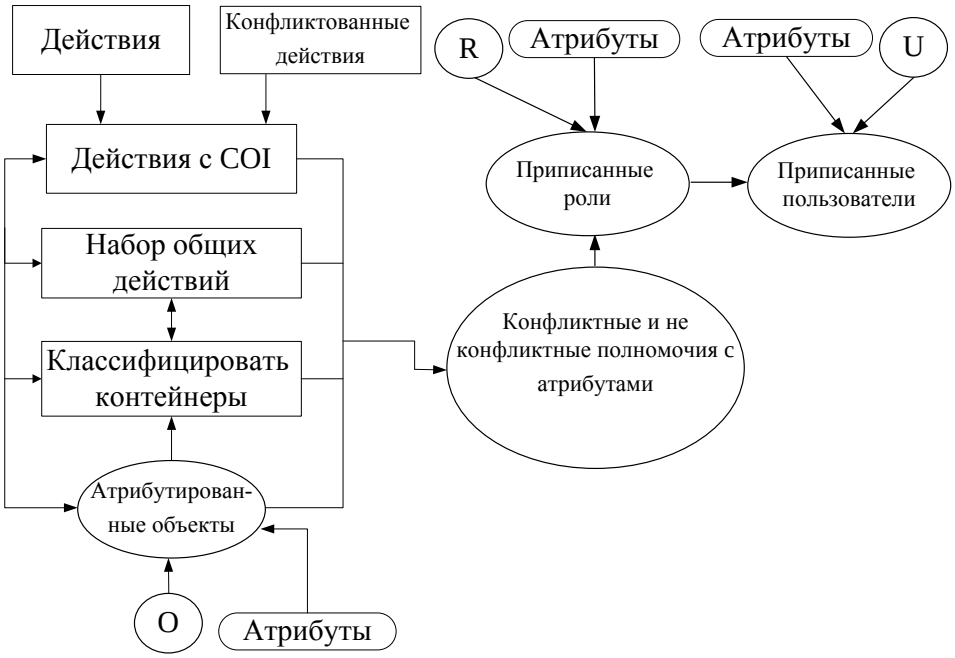
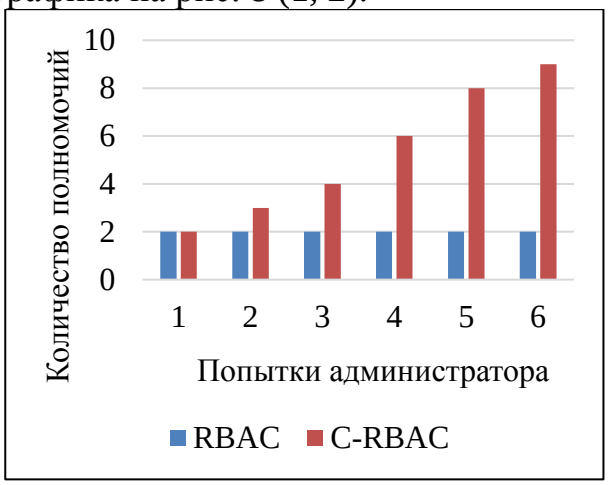


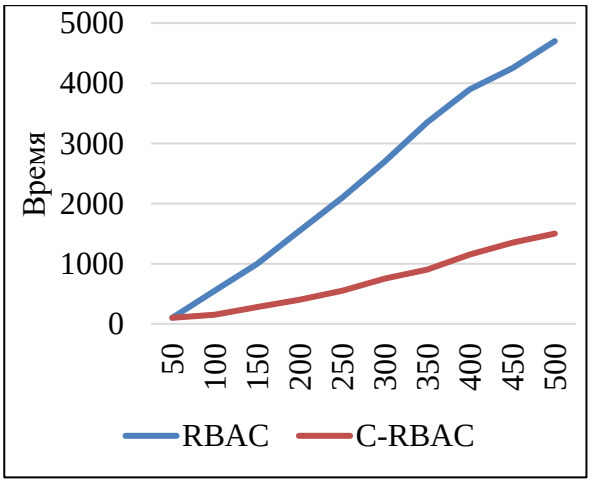

**Рис.7. Реализация SOD на основе полномочий в динамической модели RBAC**

Этот тип настраиваемых полномочий ранее не вводился. Администратор создает роли и пользователей с разными атрибутами. На следующем этапе атрибутированные конфликтующие и неконфликтные полномочия автоматически назначаются атрибутированным ролям из-за критериев атрибутов между ролями и полномочиями.

Сравнение предлагаемого динамического RBAC на основе полномочий C-RBAC с различными моделями управления доступом приведено в виде графика на рис. 8 (1, 2).




1) Сравнение количества полномочий, создаваемых за раз




2) Сравнение производительности по времени

**Рис. 8. Сравнение RBAC и C-RBAC моделей контроля доступа**

Предлагаемая модель C-RBAC превосходит модель RBAC, создавая одновременно несколько полномочий (рис. 8 (1)). На рисунке 8 (2) показано эффективность производительности на время предлагаемой модели C-RBAC в виде графика. Синяя линия показывает производительность типичной

модели RBAC, а красная линия показывает производительность предложенной модели.

В предлагаемой модели назначение полномочий на роли и ролей пользователям выполняется автоматически. Анализ особенностей моделей контроля доступа приведено в таблице 3.

**Таблица 3.**

**Анализ особенностей моделей контроля доступа с предложенной моделью**

| **Модели** / **Харак-теристики** | **RBAC** | **ABAC** | **RABAC** | **Предлагаемая модель C-RBAC** |
|---|---|---|---|---|
| Динамичность | - | + | + | + |
| Наименьшие привилегии | + | - | + | + |
| Простота | + | - | + | + |
| Гибкость | - | + | - | + |
| Эффективная реализация SOD | - | - | - | + |
| Спецификация и обслуживание политик | + | - | + | + |
| Меньше нагрузки на администратора | - | + | + | + |

Поскольку базовая структура предлагаемой модели C-RBAC основана на модели RBAC, это модель обеспечивает простоту, наименьшие привилегии и легкость обслуживания. Предлагаемая модель обеспечивает простоту администрирования, динамическое поведение, строгую безопасность и эффективную реализацию SOD.

Четвёртая глава диссертации «**Построение методов и алгоритмов систем с ролевым разграничением доступа**» посвящается детализации контроля доступа, гибкости и эффективности принятия решений модели ролевого разграничения доступа, предлагается метод анализа этих трёх характеристик. Представляется формальное описание и алгоритм предложенной модели.

Алгоритм предлагаемой модели описывается в шесть шагов.

Шаг 1. Создать базовые сущности RBAC: объекты с атрибутами, действия с COI, роли с атрибутами и пользователи с атрибутами.

Шаг 2: Создать контейнеры категорий и назначить объекты с атрибутами. Создать набор общих действий и назначить действия с помощью COI.

Шаг 3: Конфликтующие и неконфликтные полномочия с атрибутами могут быть созданы четырьмя различными способами (алгоритм 1, рисунок 9):

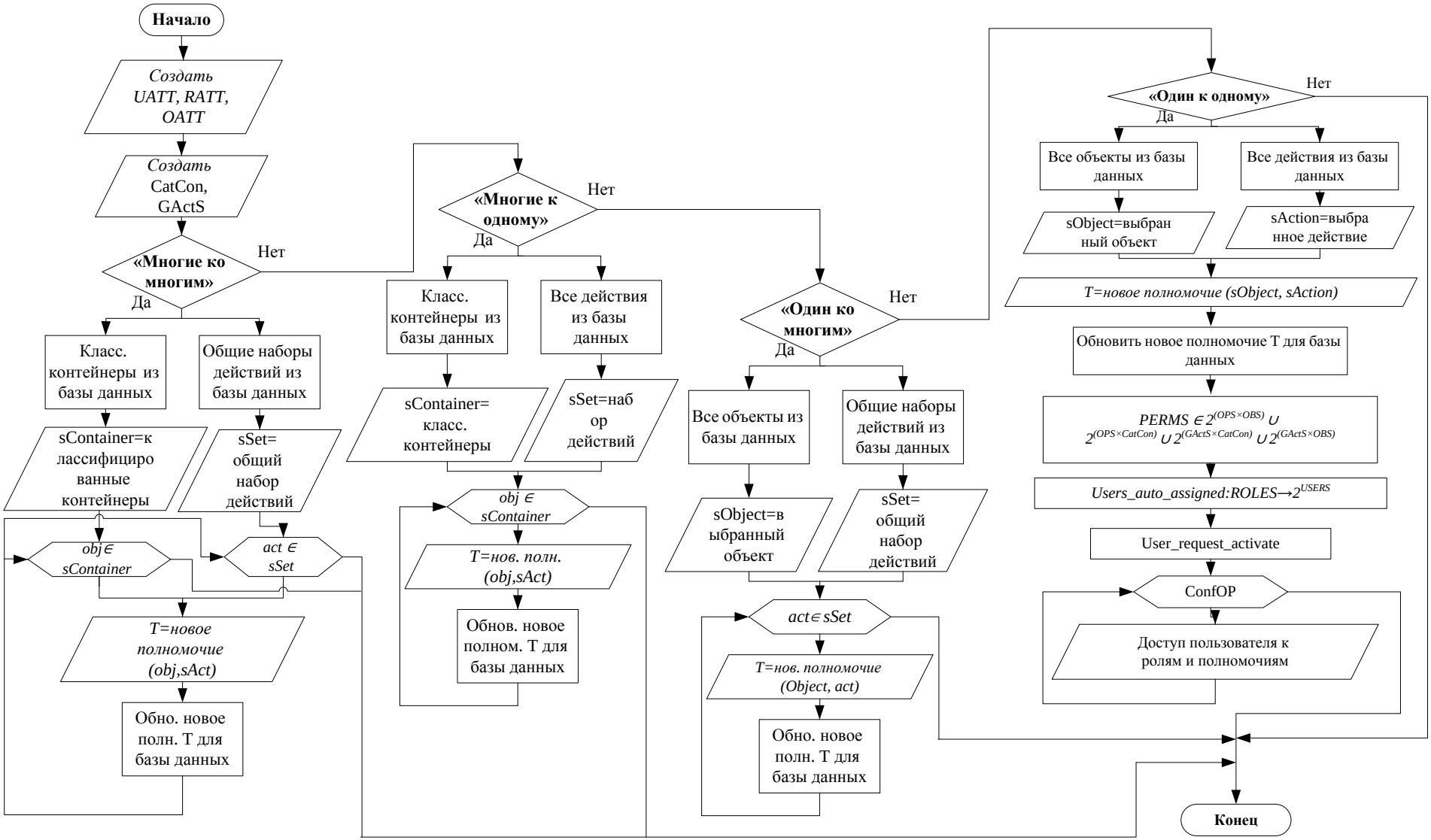



**Рис. 9. Блок - схема алгоритма создания полномочий четырьмя способами**

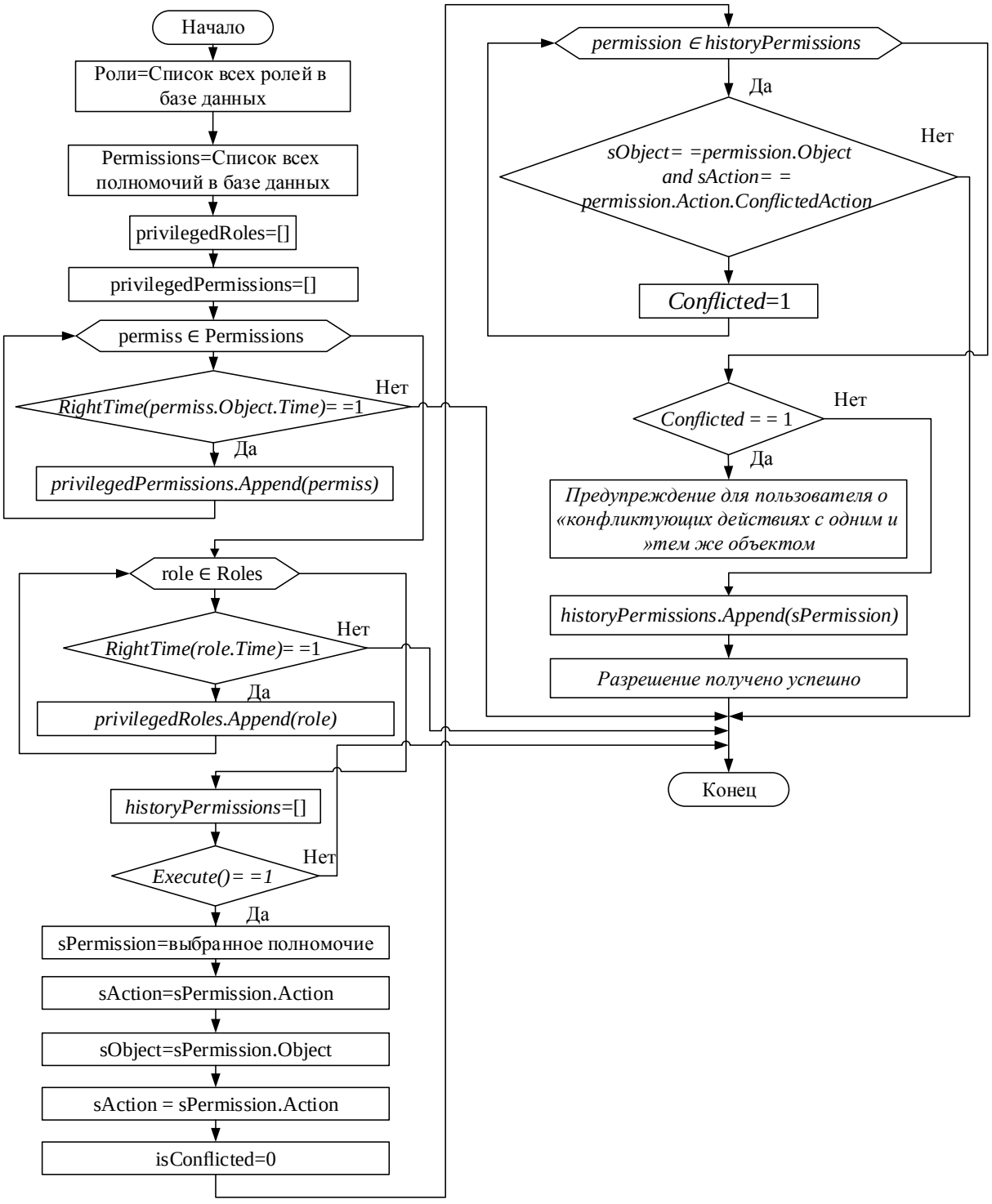



**Рис. 10. Блок схема алгоритма доступа пользователя к ролям и полномочиям**

- применить действия к объектам для создания полномочий одно за другим (традиционный RBAC);

- применение действий к контейнерам категорий для создания нескольких полномочий с одинаковыми действиями и разными объектами (новая функция);

- применение набора общих действий к объектам для создания нескольких полномочий с одинаковыми объектами и разными действиями (новая функция);

- применение набора общих действий к контейнерам категоризации для создания нескольких полномочий с разными объектами и различными действиями (новая функция).

Шаг 4: Конфликтующие и неконфликтные полномочия автоматически назначаются атрибутированным ролям с помощью атрибутов.

Шаг 5: Роли с атрибутами автоматически назначаются пользователям с атрибутами.

Шаг 6: Пользователь может получить доступ к назначенным ролям и полномочиям. Пользователь не может получить доступ к двум конфликтующим полномочиям одновременно и получает сообщение «Доступ запрещен» (алгоритм 2, рисунок 10).

Предлагаемая модель снижает нагрузку на администратора, поскольку в этой модели большая часть работы основана на атрибутах. В типичном стандарте RBAC администратор назначал полномочия на роли и роли пользователям вручную. В предлагаемой модели назначение полномочий и ролей происходит автоматически. Таким образом, нагрузка администратора в конечном итоге снижается по сравнению с типичным стандартом RBAC.

Пятая глава диссертации «**Практическое применение разработанных методов и алгоритмов**» посвящается разработке системы разграничения доступа, объединяющей ролевую базу и контроль доступа на основе атрибутов, для выполнения детального контроля доступа к данным.

В данной исследовательской работе внедрена модель разграничения доступа на основе ролей, в информационную систему «Business Process», предназначенную для сбора информации о техническом и торговом обслуживании клиентов в маркетинговой сфере, организации товародвижения посредством принятия решений, логистики товародвижения, систем коммуникаций с поставщиками и клиентами. Запрос доступа инициируется такими субъектами, как приложение, пользователь и т. д (рис.11).

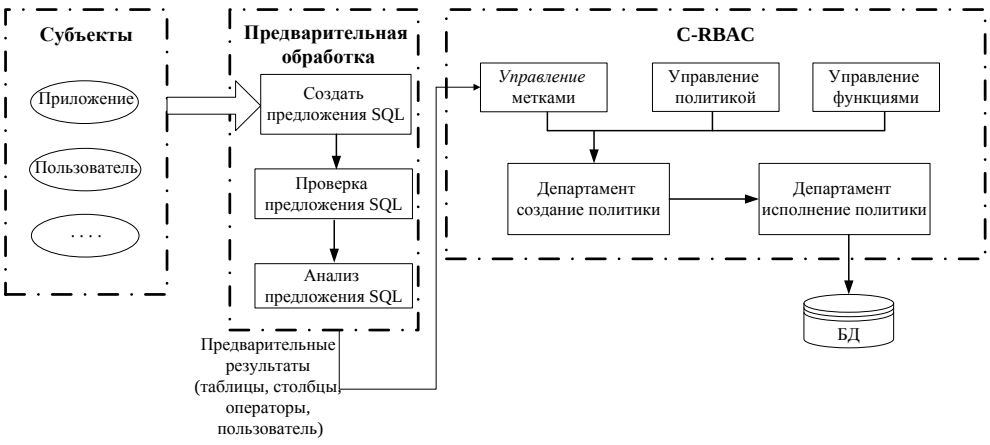



**Рис. 11. Структура детального контроля доступа**

И предложение SQL создается для запроса в предварительной обработке. Между тем, предложение SQL проверяется и анализируется для получения предварительного результата, который включает информацию об операции, таблице объектов, столбце объекта, строке объекта, пользователе и т. д. Затем предварительный результат проверяется с помощью управления метками, политиками и функциями в C-RBAC.

В предложенной модели право доступа пользователя назначается согласно значению действия. И объект, и область действия обозначаются как соответствующее право некоторого детального полномочия доступа. Компоненты предложенной модели показаны на рисунке 12.

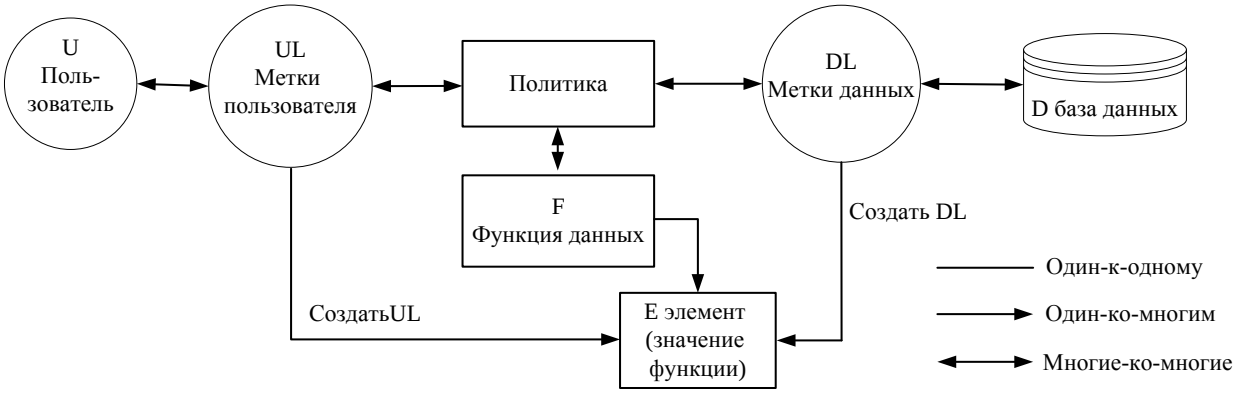



**Рис.12. Компоненты комбинированного ролевого разграничения доступа**

Среди этих компонентов право роли может быть обозначено как *метка пользователя*, а метка данных может быть обозначена как *метка данных*. Их отношения - многие ко многим. Метки пользователя и данных управляются одной и той же политикой, которые обозначаются как createUL и createDL соответственно. Кроме того, отношения между UL/DL и политикой являются отношениями «многие ко многим».

Поскольку функция данных может содержаться в нескольких политиках, а политика может быть описана в нескольких функциях. Таким образом, между политикой и функцией данных существует связь «многие ко многим». Значение признака извлекается из одного и того же объекта данных, а элемент данных может иметь только один. Таким образом, отношения между DL и элементом значения характеристики (E) взаимно однозначны. Для метки роли UL, представляющей доступный диапазон, может быть перечислено несколько значений с одной и той же функцией данных. Таким образом, отношения между UL и E - один ко многим.

Комбинированная модель разграничения доступом используются для завершения привязки данных различных объектов. Это не только позволяет более детально разграничивать процесс проверки данных модели управления доступом, но также отвечает характеристикам разработки встроенных технологий, обеспечивая при этом результаты проверки данных.

# ЗАКЛЮЧЕНИЕ

На основе результатов проведенного исследования на тему «Методы и алгоритмы повышения эффективности средств разграничения доступа в компьютерных системах» представлены следующие основные выводы:

1. Обосновано, что требования к подсистемам разграничения доступа являются ключевыми механизмами при построении системы, предназначенной для защиты информации от несанкционированного доступа и повышения надежности системы.

2. На основе анализа существующих моделей безопасности обоснованна важность использования модели RBAC при построении системы ограничения использования, которая удовлетворяет требованиям конфиденциальности, целостности и критерию удобства использования при разработке информационной системы специального назначения.

3. Предложена модель определения состояний информационных угроз учитывающая защищенность на основе вычисления интенсивностей потока атак и контрмер на этапе разработки информационной системы. В результате применения данной модели при разработке защищенных информационных систем было показано, что для эффективного противодействия потоку атак $\lambda$, влияющих на систему защиты, необходимо использовать меры противодействия с интенсивностью $\mu$ = 0,3 - 0,5.

4. Разработана концептуальная модель, которая включает «активные» компоненты в дополнение к традиционным «пассивным» компонентам системы разграничения доступа, а модель RBAC имеет высокую эффективность при синтезе системы разграничения доступа на основе этой модели в соответствии с критериями «Простота администрации» и «Принятие решения для реконфигурации».

5. Предложены комбинации модели на основе динамических ролей, атрибутов и ролей, которые позволяют упростить администрирование и устранение неполадок в управлении использованием на основе комбинации моделей RBAC и ABAC. В то же время эти комбинации моделей были дополнены возможностью точной настройки полномочий и гибкости в администрировании, в отличие от существующих моделей.

6. Разработана динамическая модель RBAC, которая реализует распределение задач (SOD) на уровне полномочий, позволяя регулировать конфликтующие и неконфликтующие роли, существующие в информационных системах. Добавление атрибутов в эту модель позволило добиться гибкости, уменьшить объем административной нагрузки и отсутствие администраторских нарушений.

7. Предложена комбинированная модель C-RBAC в управлении доступом для реализации SOD на уровне компетентности в создании полномочий для внутреннего персонала и внешних клиентов, использующих систему, за счет простоты, динамичности, строгой безопасности и эффективного внедрения SOD в администрирование информационных систем.

Внедрение в комбинированную модели C-RBAC управления доступом данной SOD на уровне полномочий привело к сокращению времени, затрачиваемого на создание полномочий для внутреннего персонала и внешних заказчиков, использующих систему, в 3 раза, увеличению скорости создания полномочий в 2,7 раза при одинаковом количестве попыток (N = 6), а защищенность информационной системы увеличилась на 37%.

8. Разработаны четыре алгоритма методов создания полномочий с конфликтующими и неконфликтующими атрибутами на основе применения общего набора влияний на контейнер категорий для создания нескольких полномочий к разным объектам и влияниям, таких как применение действий к объектам для создания полномочий одно за другим, применение функции действий к контейнерам категорий для создания нескольких полномочий с одинаковыми действиями и разными объектами, применение функции набора общих действий к объектам для создания нескольких полномочий с одинаковыми объектами и разными действиями, применение функции набора общих действий к контейнерам категоризации для создания нескольких полномочий с разными объектами и различными действиями. Конфликтующие и неконфликтные полномочия автоматически назначаются атрибутированным ролям с помощью атрибутов. В результате реализации алгоритма предложенных методов нагрузка администратора информационной системы снизилась на 24%.

9. Показано, что предложенная модель C-RBAC имеет эффективность принятия решений по сравнению с традиционной моделью RBAC с точки зрения детализации и гибкости управления доступом.

10. Разработанное программное обеспечение на основе комбинированной модели управления доступом, показало, что в практическом применении в информационной системе повышается уровень безопасности при использовании услуг, а специальные полномочия, созданные для пользователей, обеспечивают их безопасность. В частности, для противодействия потоку атак информационной системы с соответствующей интенсивностью осуществлялся эффективный контроль защитных элементов, действующих не только на этапе атаки, но и на этапе разведки. В результате, использование данного программного обеспечения позволило увеличить оперативное реагирование на наличие угроз в 2,5 раза и повышение надежности.

11. В предлагаемой модели выполняется требование, чтобы атрибуты пользователя использовались при определении отношений полномочий и ролей. Предлагаемая модель позволяет более детально контролировать отношения роль-полномочие в соответствии с атрибутами и полномочиями пользователя.

**SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.01 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES**

---

**TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES**

**IRGASHEVA DURDONA YAKUBDJHANOVNA**

# METHODS AND ALGORITHMS FOR INCREASING THE EFFICIENCY OF ACCESS CONTROL FACILITIES IN COMPUTER SYSTEMS

05.01.05 -Methods and systems of information protection. Information security

**ABSTRACT OF THE DOCTORAL (DSc) DISSERTATION OF TECHNICAL SCIENCES**

**Tashkent -2021**

**The theme of doctoral (DSc) dissertation of technical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2020.4.DSc/T109.**

The dissertation has been prepared at Tashkent University of Information Technologies.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website (www.tuit.uz) and on the website of «Ziyonet» Information and educational portal (www.ziyonet.uz.)

| | |
|---|---|
| **Scientific adviser:** | **Ganiev Salim Karimovich**<br>Doctor of Technical Sciences, Professor |
| **Official opponents:** | **Rakhmatullaev Marat Alimovich**<br>Doctor of Technical Sciences, Professor |
| | **Nigmatov Hikmatulla**<br>Doctor of Technical Sciences, Professor |
| | **Kerimov Komil Fikratovich**<br>Doctor of Technical Sciences, Docent |
| **Leading organization:** | **National University of Uzbekistan named after Mirzo Ulugbek** |

The defense will take place «03» june 2021 at 14:00 at the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of Tashkent University of Information Technologies (is registered under № 201). (Address: 100202, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on « 21 » may 2020 y.
(Dispatching protocol № 10 on « 06 » may 2021 y).

**R. Kh.Khamdamov**
Chairman of the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

**F.M. Nuraliev**
Scientific secretary of scientific council awarding scientific degrees, Doctor of Technical Sciences, Docent

**B.F.Abdurakhimov**
Deputy Chairman of the scientific seminar at the scientific council for the awarding of academic Degrees, Doctor of physics and mathematics, Professor

## INTRODUCTION (abstract of doctoral dissertation (DSc))

**The aim of the research work** is to develop and improve the model, methods and algorithms for constructing means of access control and authority control for effective protection of computer systems.

**The object of the research work** is the process of control and management of access in computer systems.

**The scientific novelty of the research work** is as follows:

a list of threats related to means of control and management of access in computer systems was formed, based on information security standards and indicators that determine the assessment of the effectiveness of information protection systems;

a model for identifying threats in access control systems has been developed, which makes it possible to calculate the probability of the impact of threats on the access control system;

a conceptual model of the access control system has been developed, reflecting decisions on the reconfiguration of the processes of formal models and methods of access control;

analytical expressions and a methodology for the functioning of access control systems have been developed, providing dynamic control of delimitation schemes, taking into account the fuzzy nature of the elements they contain;

developed a combined model using separation of duties (SOD), which dynamically assigns permissions to roles, and also assigns users to roles using various attributes;

algorithms have been developed in the «many-to-many», «many-to-one», «one-to-many», «one-to-one» modes in the role-based access control model to determine conflicting and non-conflicting powers.

**Implementation of research results.** On the basis of the obtained scientific results on increasing the efficiency of methods and algorithms for differentiating access in computer systems, models and algorithms for role-based access control have been developed, which ensure effective protection of computer systems:

developed methods and algorithms for determining conflicting and non-conflicting powers of the role-based access control model has been implemented in the information systems of the Agrobank and Qishloq Qurilish Bank. (Certificate of the Ministry for the Development of Information Technologies and Communications dated February 03, 2021 No. 33-8 / 821). Using the results of scientific research has increased the speed of rapid response to threats by 37%, as well as reduced the time spent on creating powers by 24%;

the model of the state of security threats, which is a simulation of the likelihood of the impact of threats on the security system of the information system and the likelihood of disclosing the information protection system, has been introduced into the Agency «O'zarxiv» of the Republic of Uzbekistan (reference of the Ministry for the Development of Information Technologies and Communications dated February 03, 2021 No. 33-8 / 821). The use of the results

of scientific research made it possible to increase the prompt response to the presence of threats by 1.5 times and increase reliability.

a software tool developed on the basis of a threat identification model that allows calculating the likelihood of the impact of threats on the access control system has been implemented in OFFICIAL DEALER TRADE LLC (reference of the Ministry for the Development of Information Technologies and Communications dated February 03, 2021 No. 33-8 / 821). The use of the results of scientific research has made it possible to increase the prompt response to the presence of threats by 2.5 times and increase the reliability;

a software tool based on the combined C-RBAC model of differentiation of access based on roles has been introduced into the information system of the Head Scientific and Methodological Center under the Ministry of Higher and Secondary Specialized Education of the Republic of Uzbekistan (reference of the Ministry for the Development of Information Technologies and Communications dated February 03, 2021 No. 33- 8/821). As a result, a 2-fold time saving was obtained due to the fact that the assignment of powers to roles, the assignment of roles to users occurs automatically;

the method of synthesis of access control systems has been introduced at the Academy of the Ministry of Internal Affairs (reference from the Ministry for the Development of Information Technologies and Communications dated February 03, 2021, No. 33-8 / 821). The effectiveness of the implementation of scientific results was shown by an increase in the level of mastering of educational materials, as a result, practical assistance in the training of qualified specialists was confirmed.

**Structure and volume of the dissertation.** The structure of the dissertation Consists of an introduction, five chapters, a conclusion, list of used literature, annexes. The volume of the dissertation is 180 pages.

**ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ**
**СПИСОК ОПУБЛИКОВАННЫХ РАБОТ**
**LIST OF PUBLISHED WORKS**

**I бўлим (I часть; part I)**

1. 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 (№35; CrossRef; IF=5.29).
2. 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 (№5; Global Impact; IF=0.325).
3. 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 (№3; Scopus; ОАК Раёсатининг қарори (30.09.2019 й. №269/8)).
4. 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 (№3; Scopus; ОАК Раёсатининг қарори (30.09.2019 й. №269/8)).
5. 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), стр. 3935-3941 (№3; Scopus; IF=0.350).
6. 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 (№3; Scopus; ОАК Раёсатининг қарори (30.10.2020 й. №287/9)).
7. 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), pp. 30-37 (ОАК Раёсатининг қарори (30.07.2020 й. №283/7.1)).
8. Irgasheva D., Sodikova D. Z. Analyzing security parameters of database management systems // Молодой учёный. Международный научный журнал. № 15 (305).2020г. Апрель.-С.84-86(№18; Ulrich's Periodicals Directory; РИНЦ).
9. Ганиев С.К., Иргашева Д.Я., Рустамова С.Р. Фойдаланишни чеклаш тизимининг концептуал модели // Илмий-техник журнал «Ахборотком-муникациялар: Тармоқлар, Технологиялар, Ечимлар». -Тошкент, 2020. -№4 (56). -Б. 58-63. (05.00.00; №2).
10. Ганиев С.К., Иргашева Д.Я., Рустамова С.Р. Фойдаланишни чеклаш

тизимининг рол ва атрибут асосида бошқариш модели // «Мухаммад ал-Хоразмий авлодлари» журнали. -Тошкент, 2020. -№4 (14). -С.45-54. (05.00.00; №10).

11. Иргашева Д.Я. Повышение эффективности методов разграничения доступа на основе ролей // Журнал «Мухаммад ал-Хоразмий авлодлари». -Ташкент, 2020. -№4 (14) - С.144-149. (05.00.00; №10).

12. Irgasheva D.Y., Abdurakhmanov A.A. Synthesis the structural protected computer network // «TATU xabarlari». -Тошкент, 2013. -№3. -Б.13-18. (05.00.00; №31).

13. Ташев К.А., Иргашева Д.Я., Бекмирзаев О.Н. К вопросу анализа проблем информационной безопасности // «Вестник ТУИТ». -Ташкент, 2014. - №1(29). - С.49-54. (05.00.00; №31).

**II бўлим (I часть; part I)**

14. 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.

15. 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.

16. 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.

17. 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.

18. Иргашева Д.Я., Гуломов Ш.Р. К вопросу обеспечения надежности компьютерных сетей // Сборник научных статей Международной научно-практической конференции «Innovation-2012». -Ташкент, 2012. -С.267-268.

19. 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.

20. 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.

21. Иргашева Д.Я. Классификация и свойство компьютерных вирусов// «Ўзбекистон Республикаси ҳуқуқни муҳофаза қилиш тизимларида локал компьютер тармоқларини амалда жорий этиш йўллари ва уларнинг хавфсизлигини таъминлаш» республика илмий-амалий семинари материаллари тўплами. -Тошкент, 2016. -Б.61-64.

22. Иргашева Д.Я., Усманов А.К. Анализ формальных моделей безопасности // «Ўзбекистон Республикаси ҳуқуқни муҳофаза қилиш тизимларида локал компьютер тармоқларини амалда жорий этиш йўллари ва уларнинг хавфсизлигини таъминлаш» республика илмий-амалий семинари материаллари тўплами. -Тошкент, 2016. -Б.67-71.

23. 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. -Sofia, Bulgaria, 2014. P.204-211.

24. Ташев К.А., Иргашева Д.Я., Абдурахманов А.А., Имамалиев А.Т. Модель системы мониторинга безопасности в инфокоммуникационных системах // Сборник тезисов и докладов Республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». -Ташкент, 2013. -С. 25-27.

25. 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.

26. 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). -Tashkent, 2013.

27. Иргашева Д.Я., Ҳамидов Ш.Ж. Тармоқ ҳужумларини аниқлаш усулларининг тадбиқи // «Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг ўрни» республика илмий-техник анжуманининг маърузалар тўплами. - Тошкент, 2017. -Б.150-152.

28. Иргашева Д.Я., Холимтаева И.У. Хуружлардан ҳимояланган компьютер тармоғининг структурасини ташкиллаштириш // «Ахборот ва телекоммуникация технологиялари муаммолари» Республика илмий-техник конференциясининг маърузалар тўплами. -Тошкент,2015. -Б.466-468.

29. Ганиев С.К., Ташев К.А., Иргашева Д.Я., Худойкулов З.Т., Гаипназаров Р.Т., Рустамова С.Р. «САС-фойдаланишни чеклаш тизими дастури» // 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.

30.Ганиев С.К., Ташев К.А., Иргашева Д.Я., Худойкулов З.Т., Исломов Ш.З., Рустамова С.Р. «RBAC-фойдаланишни чеклаш тизими дастури» // 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.

Автореферат «Муҳаммад ал-Хоразмий авлодлари» Илмий-амалий ва ахборот таҳлилий журнали таҳририятида таҳрирдан ўтказилди ҳамда ўзбек, рус ва инглиз тилларидаги матнлар ўзаро мувофиқлаштирилди.