

004  
К 15

М. М. КАДИРОВ

# ИНФОКОММУНИКАЦИОН ТИЗИМЛАРДА АХБОРОТДАН ФЙДАЛАНИШНИ БОШҚАРИШ УСУЛ ВА МОДЕЛЛАРИ



**ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА  
МАХСУС ТАЪЛИМ ВАЗИРЛИГИ**

**ИСЛОМ КАРИМОВ НОМИДАГИ  
ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ**

**М. М. КАДИРОВ**

**ИНФОКОММУНИКАЦИОН  
ТИЗИМЛАРДА АХБОРОТДАН  
Фойдаланишни бошқариш  
УСУЛИ ВА МОДЕЛЛАРИ**

Монография

**ТОШКЕНТ – 2022**

**УЎК: 004.056.5**  
**КВК 32.973.202-04**  
**К 15**

**К 15**

**М.М. Кадилов.** Инфокоммуникацион тизимларда ахборотдан фойдаланишни бошқариш усул ва моделлари. – Т.: “Fan va texnologiyalari nashriyot-matbaa uyi”, 2022. 128 б.

**ISBN 978–9943–7976–7–3**

Мазкур монографияда фойдаланишни бошқаришнинг дискрецион, мандатли ва ролларга асосланган хавфсизлик моделлари батафсил кўриб чиқилган. Инфокоммуникацион тизимларида маълумотлар махфийлиги ва яхлитлиги талаб қилинадиган иккита қийматли панжарани киритиш йўли билан мандатли хавфсизлик сиёсатини бирлаштириш усули баён этилган. Ролли ва мандатли хавфсизлик сиёсатини бирлаштириш усули келтирилган.

Ушбу китоб илмий-педагогик ходимлар, мутахассислар, бакалавр талабалари ва магистрантлар, ҳамда ахборот хавфсизлиги соҳасида изланишлар олиб бораётган илмий изланувчилар учун фойдали бўлади.

**УЎК: 004.056.5**  
**КВК 32.973.202-04**

***Тақризчилар:***

**Ж.У. Севянов** – техника фандари доктори, профессор;  
**А.Х. Нишонов** – техника фанлари доктори, профессор.

*Ислом Каримов номидаги Тошкент давлат техника университети Кенгашининг 2022 йил 11 февралдаги 6-сон қарорига асосан нашрга тавсия этилган.*

**ISBN 978–9943–7976–7–3**

© «Fan va texnologiyalar nashriyot-matbaa uyi», 2022.

## КИРИШ

Жаҳонда инфокоммуникацион тизимларда ахборотдан рухсатсиз фойдаланишни аниқлаш ва бартараф этиш, тизимларнинг ҳимояланганлигини баҳолаш ва рухсатсиз фойдаланишдан ҳимоялаш воситаларини яратиш ҳамда такомиллаштиришга алоҳида эътибор қаратилмоқда. Рақамли иқтисодиётда ахборот технологияларини қўллаш орқали барча соҳаларнинг самарадорлиги ошиб бормоқда. Бу эса ахборотнинг ҳимояланганлик масаласида муайян хавф-хатарларни келтириб чиқаради. 2021 йилнинг биринчи чорагида киберинцидентлар сони тез суръатлар билан ошиб борди ва бунинг натижасида ахборот тизимларга бўладиган хужумлар сони 2020 йилга нисбатан 22,5% га ошганини яққол кўриш мумкин. Шунингдек, жорий йилнинг ўзида мақсадли хужумлар сони 67% фоизни ташкил этди<sup>1</sup>.

Жаҳонда ахборотни қайта ишлаш ва сақлаш тизимлари бир нечта ихтисослашган ахборот хизматлари бирлашмасидан иборат. Ихтисослашган ахборот хизматлари учун алоҳида математик моделлар ишлаб чиқилган. Шу нуқтаи назардан бир нечта хавфсизлик моделларини бир тизимга бирлаштириш ҳозирги кунда муҳим вазифалардан бири саналади. Бироқ хавфсизлик моделларини ўзгартирмасдан бир нечта хизматларни бир тизимга бирлаштириш умумий тизимнинг ишлаш самарадорлигини пасайтиришга имкон яратади. Шу сабабли инфокоммуникацион тизимларда маълумотлар базасини бошқариш тизимлари махфийлигини ошириш ва роллар ёрдамида бошқаришни амалга оширишда такомиллаштирилган хавфсизлик моделларини ишлаб чиқиш долзарб масала ҳисобланади.

Республикамизда давлат ва хўжалик бошқарув органларида инфокоммуникацион тизимларини ривожлантириш ҳамда шу тизимларда маълумотларни сирқиб чиқишини ва ахборотдан

---

<sup>1</sup> <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/>

рухсатсиз фойдаланишни чеклаш усул ва воситаларини кенг татбиқ этишга алоҳида эътибор қаратилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан, «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилиқ кўрсатиш»<sup>2</sup> вазифалари белгиланган. Мазкур вазифаларни амалга ошириш, жумладан, инфокоммуникацион тизимларда ахборотдан рухсатсиз фойдаланишни чекловчи хавфсизлик моделларини замонавий талаблар асосида такомиллаштириш муҳим масалалардан бири ҳисобланади.

Жаҳон ва республикамиз миқёсида илмий - тадқиқотлар натижасида ахборотнинг ҳимояланганлигини оширишда ахборотдан фойдаланишни бошқаришнинг усул ва моделларини ривожлантиришга: D. Elliott Bell, Leonard J. LaPadula, R.S. Sandhu, D. Richard Kuhn, Zoran Stojanovich, Ajantha Dahana-yake, Karsten Sohr, Jürgen Schlegelmilch, Bernhard J. Berger, Han Jinguang, Ali Abdallah, Jason Crampton, Philippe Balbiani, Pierangela Samarati, S. De Capitani di Vimercati, В. Мухин, А.М. Волокита, А.Ю. Щеглов, К.А. Щеглов, Н.А.Гайдамакин, Д.П. Зегжда, А.Ю. Щербаков, В.А. Герасименко, С.В. Белим, Н.Ф. Богаченко, Ю.С. Ракицкий каби етакчи хорижий олимлар, ҳамда республикамиз олимлари С.К.Ганиев, М.М.Каримов, А.А.Ганиев, Д.Я. Иргашева, Ш.Р. Гуломов ва бошқалар ўзларининг муҳим ҳиссаларини кўшишган.

Хавфсизлик сиёсати математик, схемотехник, алгоритмик ва бошқа кўринишларда бўлиши мумкин. Хавфсизлик сиёсати хавфсиз ахборот тизимларни ишлаб чиқиш ва уларни тадқиқ қилишда муҳим роль ўйнайди. Фойдаланишни бошқаришнинг дискрецион, мандатли ва ролларга асосланган хавфсизлик моделлари тизим ҳимояланганлигини оширишда муҳим аҳамиятга эга.

Фойдаланишни бошқаришнинг дискрецион сиёсатининг асосий устунлиги фойдаланишни бошқаришни содда тизимини

---

<sup>2</sup> Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

яратиш имконини беради. Шунингдек, ушбу модел содда ва кўрғазмали бўлганлиги сабабли, мураккаб алгоритмларни талаб қилмайди. Фойдаланишни бошқаришнинг дискрецион моделида бошқарув самарадорлиги юқори ҳисобланиди, чунки бу модел фойдаланувчи бажарадиган амалларгача ҳуқуқларини аниқлик билан бошқариш имконини беради.

Фойдаланишни бошқаришнинг мандатли сиёсатининг асосий устунлиги ахборотни сирқиб чиқиб кетишини назорат қилиш орқали тизимнинг хавфсизлиги таъминланади. Фойдаланишни бошқаришнинг мандат модели фойдаланиш субъекти, субъектнинг махфийлик даражасидан кам бўлмаган махфийлик даражасига эга объектлардан фойдаланиш имконига эга бўлади ва субъект, унинг махфийлик даражасидан кам бўлган объектга маълумот ёзиш ҳуқуқига эга бўлмайди.

Ролларга асосланган фойдаланишни бошқариш модели тизимнинг ишлаш жараёнида эгилувчан, динамик ўзгарадиган фойдаланишни чеклаш қоидаларини амалга оширишга имкон беради. Ундан ташқари ягона тизим ёки илова доирасида фойдаланувчи ваколатларини бошқариш учун кенг қўлланилади ва ролларни шакллантиришда тизим фойдаланувчилари учун аниқ ва тушунарли фойдаланишни чеклаш қоидаларини белгилаш имконини яратади.

Ҳозирги кунда инфокоммуникацион тизимларнинг юқори хавфсизлигини таъминловчи модификацияланган ахборотнинг ҳимояланганлигини ошириш моделларини яратиш долзарб ҳисобланади. Инфокоммуникацион тизимларида маълумотлар махфийлиги ва яхлитлиги талаб қилинадиган иккита қийматли панжарани киритиш йўли билан мандатли хавфсизлик сиёсатини бирлаштириш усули ахборот хавфсизлигини оширишда катта аҳамиятга эга ҳисобланади.

Ахборот тизимидаги субъектлар фойдаланиш имкони бўлган маълумотларнинг яхлитлигини ҳимоя қилиш, ахборот тизимини формал мантиқий мандат ва ролли фойдаланишни бошқаришнинг хавфсизлик модели ва ахборот оқимларини ва яхлитлигини назорат қилиш орқали таъминланади.

Инфокоммуникацион тизимларда мандат ва ролли фойдаланишни бошқаришнинг ягона механизмини амалга ошириш бузгунчи субъектларга роллар параметрларидан фойдаланиб тақиқланган ахборотдан фойдаланиш имкониятини олди олилади. Операцион тизимларда маълумотлардан фойдаланишни бошқаришни амалга ошириш хусусиятлари ҳисобига фойдаланувчининг қайд маълумотларини ваколатли ролларини, субъект-сессиянинг жорий роли ва фойдаланиш ҳуқуқларининг вазибаларини белгилаш имконини берувчи фойдаланишни бошқаришнинг мандат ва ролли модели ахборот хавфсизлигини юқори кўрсаткичга олиб чиқиш имконини яратади.

# **I БОБ. ИНФОКОММУНИКАЦИОН ТИЗИМЛАРДА АХБОРОТНИНГ ҲИМОЯЛАНГАНЛИГИНИ ОШИРИШНИНГ УСУЛ ВА ВОСИТАЛАРИНИ ТАҲЛИЛИ**

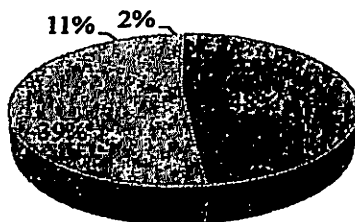
## **1.1. Инфокоммуникацион тизимларнинг ҳимояланганлиги муаммоларининг таҳлили**

ИКТ ахборотни қайта ишлаш соҳасининг ривожланиши билан бир қаторда, ахборот тизимларининг комплекс ҳимояси талаблари ва унинг асосида ахборот ресурсларни моделлаштириш зарурияти муҳим рол ўйнайди. Тизимнинг ушбу кўрсаткичи ахборотни қайта ишлаш жараёнининг барча босқичларида тадқиқ этилади ва яхши ўрганиб чиқилган муаммо сифатида ахборотнинг ҳимояланганлигини таъминлашни эътироф этиш мумкин.

«Positive technologies» компаниясининг маълумотларига кўра, 2021 йилнинг III – чорагида маълумотларни олишга йўналтирилган ҳужумларнинг улуши ўсишда давом этган [1]. Кибер ҳодисаларнинг 48%ида жиноятчилар мақсади ахборотни олишга йўналтирилган, 39%и эса – молиявий фойдага қаратилган. Ҳисоб маълумотлари сотилиши ва улардан фойда кўрилиши мумкин, шу сабабли, ҳужум орқасидан олинган маълумотдан сўнг, ахборот эгаларига ёки ходимларнинг компанияларига маълумотларни ошкор қилиш учун янги ҳужумлар уюштирилиши мумкин.

2021 йилнинг учта чорагида қандай маълумотлар жиноятчиларни энг кўп жалб қилганлиги кўриб чиқамиз. Ҳужум қилувчи ёвуз ниятли фойдаланувчиларнинг мақсадлари юридик шахсларга қилинган ҳужумларда шахсий маълумотларни (логин ва пароллар) олиш ташкил этган. Шахсий маълумотлардан турли хил сервис ва тизимларга кириш мақсадида фойдаланилган, жумладан, компания ходимларининг электрон почталари.





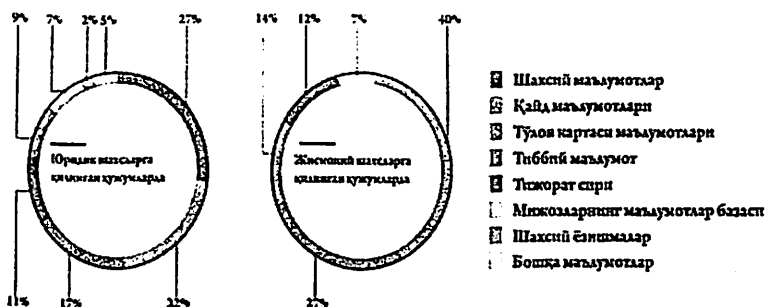
- Маълумотларни олиш
- Молиявий фойда
- Хактивизм
- Кибер уруш

**1.1-расм. Хужум қилувчи ёвуз ниятли фойдаланувчиларнинг мақсадлари**

Шуни таъкидлаш лозимки, хужум қилувчи ёвуз ният фойдаланувчилар қайд маълумотларини олишда махсус дастурий таъминот ёрдамисиз амалга оширилган. Бунга сабаб фойдаланувчилар қайд маълумотларига кириш учун паролли сифатида туғилган сана, телефон рақам, уй ҳайвонларини лақаблари ва шунга ўхшаш маълумотлардан фойдаланганлиги бўлган. Жисмоний шахсларга қилинган хужумларда асосий мақсад фойдаланувчиларнинг қайд маълумотлари бўлган.

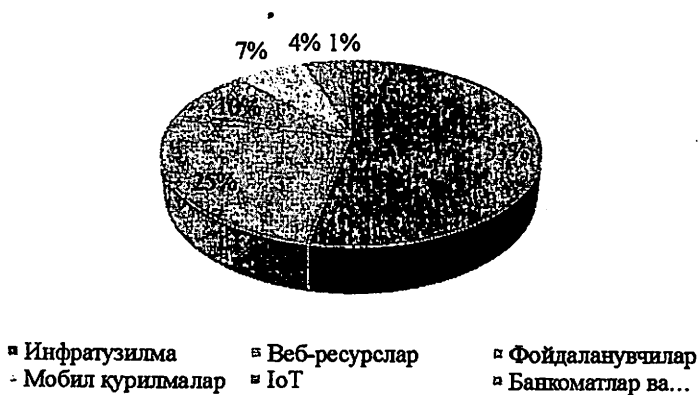
Кейинги ўринларда хужумлар тўлов карталарининг маълумотлари ўғирланган, уларни амалга оширган ёвуз ният фойдаланувчилар кўпинча бу маълумотларни жосус зарарқилганда дастурий воситалар ёки ошкор этилган сайтлар ёрдамида олишган.

Мақсадли хужумлар сонининг кўпи турли хил ташкилотларга уюштирилган, хусусан, мақсадли хужумларнинг улуш оммавий хужумларнинг улушидан ошиб кетган ва 60%ни ташкил этган. Хужумлардан кўриш мумкинки, ҳар бир хужум учун ёвуз ниятли фойдаланувчилар индивидуал ёндашу қўллашган. 2.2-расмда ўғрилган маълумотларнинг турлари кўрсатилган.

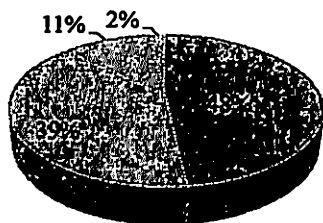


1.2-расм. Ўғрилган маълумотларнинг турлари

Кенг миқёсли кибер ҳужумлар, асосан зараркуанда эпидемиялар бўлиб, битта соҳага таъсир кўрсатиш билан чекланиб қолмайдилар. 2021 йилнинг III чорагида инфратузилмага қаратилган ҳужумларнинг улуши 53%ни ташкил этган, веб-ресурсларга бўлган ҳужумларнинг улуши ўтган йилнинг айнан шу вақтига нисбатан ошган ва 25%ни ташкил этган. Бундан ташқари, IoT-қурилмаларига ҳужумлар улуши III чоракка нисбатан ошган: бу асосан PyRoMineIoT, Muhstik, Wicked Mirai каби янги ботнетларнинг пайдо бўлиши билан боғлиқ.



1.3-расм. Ҳужум объектлари



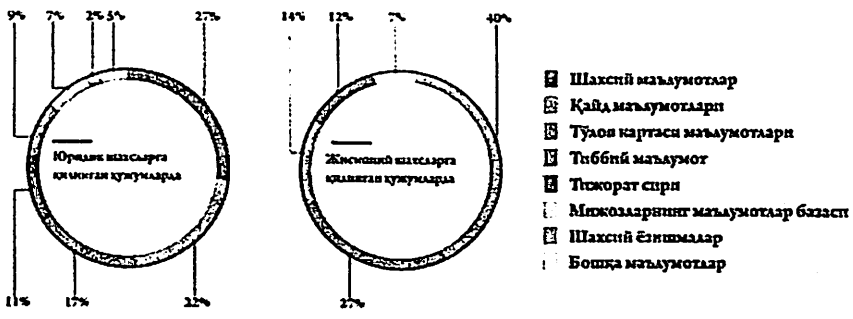
- Маълумотларни олиш
- Молиявий фойда
- Хактивизм
- Кибер уруш

**1.1-расм. Хужум қилувчи ёвуз ниятли фойдаланувчиларнинг мақсадлари**

Шуни таъкидлаш лозимки, хужум қилувчи ёвуз ниятли фойдаланувчилар қайд маълумотларини олишда махсус дастурий таъминот ёрдамисиз амалга оширилган. Бунга сабаб фойдаланувчилар қайд маълумотларига кириш учун пароллар сифатида туғилган сана, телефон рақам, уй ҳайвонларининг лақаблари ва шунга ўхшаш маълумотлардан фойдаланганлиги бўлган. Жисмоний шахсларга қилинган хужумларда асосий мақсад фойдаланувчиларнинг қайд маълумотлари бўлган.

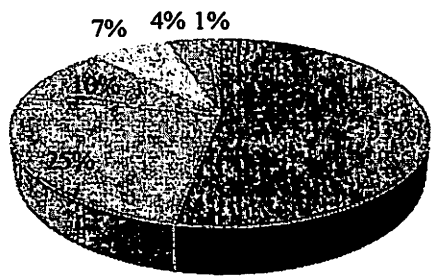
Кейинги ўринларда хужумлар тўлов карталарининг маълумотлари ўғирланган, уларни амалга оширган ёвуз ниятли фойдаланувчилар кўпинча бу маълумотларни жосус зараркуанда дастурий воситалар ёки ошкор этилган сайтлар ёрдамида олишган.

Мақсадли хужумлар сонининг кўпи турли хил ташкилотларга уюштирилган, хусусан, мақсадли хужумларнинг улуши оммавий хужумларнинг улушидан ошиб кетган ва 60%ни ташкил этган. Хужумлардан кўриш мумкинки, ҳар бир хужум учун ёвуз ниятли фойдаланувчилар индивидуал ёндашув қўллашган. 2.2-расмда ўғрилган маълумотларнинг турлари кўрсатилган.



1.2-расм. Ўғрилган маълумотларнинг турлари

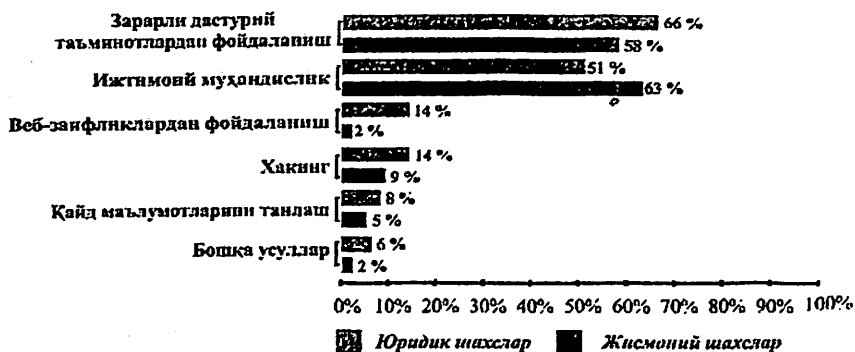
Кенг миқёсли кибер хужумлар, асосан зараркунанда эпидемиялар бўлиб, битта соҳага таъсир кўрсатиш билан чекланиб қолмайдилар. 2021 йилнинг III чорагида инфратузилмага қаратилган хужумларнинг улуши 53%ни ташкил этган, веб-ресурсларга бўлган хужумларнинг улуши ўтган йилнинг айнан шу вақтига нисбатан ошган ва 25%ни ташкил этган. Бундан ташқари, IoT-қурилмаларига хужумлар улуши III чоракка нисбатан ошган: бу асосан PyRoMineIoT, Muhstik, Wicked Mirai каби янги ботнетларнинг пайдо бўлиши билан боғлиқ.



- Инфратузилма
- Веб-ресурслар
- Фойдаланувчилар
- Мобил қурилмалар
- IoT
- Банкоматлар ва...

1.3-расм. Хужум объектлари

2021 йилнинг якунларига кўра ёвуз ниятли фойдаланувчилар томонидан амалга оширилган хужум усуллари қуйидагича тақсимланган (1.4-расм):



1.4-расм. Хужум турлари

Тадқиқотлар шуни кўрсатдики, асосий хужумлар фойдаланувчиларнинг шахсий маълумотларига нисбатан қаратилган. Шуларни инобатга олиб тизим хавфсизлигини ошириш воситаларига катта эътибор қаратиш лозим.

## 1.2. Инфокоммуникацион тизимларида ахборот ҳимояланганлигини ошириш усуллари таҳлили

Ахборотнинг ҳимояланганлигини ошириш усулларида иккитасининг хусусиятларини кўриб чиқамиз [2], улар орасида:

1. Хавфсизликни бошқаришнинг маъмурий-ташқилий усули.
2. Хавфсизликни бошқаришнинг адаптив усули.

1. ИКТ ахборот хавфсизлигини маъмурий бошқариш бу ресурсларни тақсимлаш, фойдаланувчилар орасидаги низоларни ҳал этиш, хавфсизликни таъминлаш мақсадида ИКТ ресурсларидан фойдаланишнинг оптимал режимини аниқлашни назарда тутади. Маъмурий бошқариш доирасида қуйидаги вазифалар ечилади [3, 4, 5, 6]:

– хавфсизликни бошқаришнинг дастурий ва техник воситаларини ўрнатиш, соzлаш, қўллаш ва такомиллаштириш;

– компьютер тизимлари ва тармоқлари ресурсларига фойдаланувчилар, вазифалар ва жараёнларнинг фойдаланишини чеклаш;

– хавфсизлик тизимининг ишлашини назорат қилиш;

– фавқулодда вазиятлар пайдо бўлганда ИКТ функцияларини қайта тиклаш.

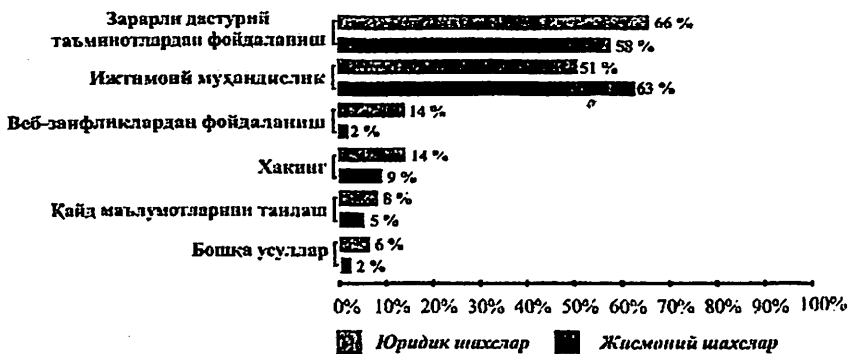
Хавфсизлик жараёнларини бошқаришга маъмурий-ташқилий ёндашув қўлланилганида дастлаб ахборотни ҳимоя қилиш воситаларини танлаш ва соzлаш вазифалари ҳал этилади. Оқибатда, маъмур тизим ишлашини баҳолаш ва тузилмасини ўзгартиришни, яъни ахборотни ҳимояланганлигини оширишнинг янги воситаларининг амалга оширишни, эски ва самарасизларини ўчиришни ҳамда умуман тизимнинг ишлаш самарадорлигини ошириш учун параметрларни қайта соzлашни бажаради.

ИКТдан фойдаланиш тажрибаси шуни кўрсатадики, маъмурий бошқаришни ташкиллаштириш машаққатли вазифадир. Бу маъмурий бошқарувнинг мустақил қуйи тизимини ИКТнинг таркибий қисми сифатида ажратишнинг мақсадга мувофиқлигини, тегишли меъёрий ҳужжатларни ишлаб чиқиш ва амалга оширишнинг долзарблигини, шунингдек, хавфсизликни бошқаришнинг автоматлаштирилган тизимини жорий этилиши мақсадга мувофиқлигини белгилайди.

Ҳозирги вақтда кўплаб ИКТларида хавфсизликни бошқариш учун айнан шу усул қўлланилади. Шундай қилиб, ушбу усулнинг асосий афзаллиги бу ИКТга жорий этиш соддалигидадир.

Шу билан бирга ушбу усулнинг асосий камчилиги ИКТ хавфсизлигини бошқариш самарадорлигига таъсир кўрсатувчи инсон омили ҳисобланади. Бошқарув тизимининг фавқулодда вазиятларга жавоб беришнинг тезлиги ниҳоятда паст. Шундай экан, фавқулодда вазиятларнинг пайдо бўлиш эҳтимолини камайтириш учун ахборотни ҳимоя қилиш воситаларидан фойдаланишга бўлган харажатлар салмоқли ортади.

2021 йилнинг якунларига кўра ёвуз ниятли фойдаланувчилар томонидан амалга оширилган ҳужум усуллари куйидагича тақсимланган (1.4-расм):



1.4-расм. Ҳужум турлари

Тадқиқотлар шуни кўрсатдики, асосий ҳужумлар фойдаланувчиларнинг шахсий маълумотларига нисбатан қаратилган. Шуларни инобатга олиб тизим хавфсизлигини ошириш воситаларига катта эътибор қаратиш лозим.

## 1.2. Инфокоммуникацион тизимларида ахборот ҳимояланганлигини ошириш усуллари таҳлили

Ахборотнинг ҳимояланганлигини ошириш усулларида иккитасининг хусусиятларини кўриб чиқамиз [2], улар орасида:

1. Хавфсизликни бошқаришнинг маъмурий-ташқилий усули.
2. Хавфсизликни бошқаришнинг адаптив усули.

1. ИКТ ахборот хавфсизлигини маъмурий бошқариш бу ресурсларни тақсимлаш, фойдаланувчилар орасидаги низоларни ҳал этиш, хавфсизликни таъминлаш мақсадида ИКТ ресурсларидан фойдаланишнинг оптимал режимини аниқлашни назарда тутди. Маъмурий бошқариш доирасида куйидаги вазифалар ечилади [3, 4, 5, 6]:

– хавфсизликни бошқаришнинг дастурий ва техник воситаларини ўрнатиш, соzлаш, қўллаш ва такомиллаштириш;

– компьютер тизимлари ва тармоқлари ресурсларига фойдаланувчилар, вазифалар ва жараёнларнинг фойдаланишини чеклаш;

– хавфсизлик тизимининг ишлашини назорат қилиш;

– фавқулодда вазиятлар пайдо бўлганда ИКТ функцияларини қайта тиклаш.

Хавфсизлик жараёнларини бошқаришга маъмурий-ташкилий ёндашув қўлланилганида дастлаб ахборотни ҳимоя қилиш воситаларини танлаш ва соzлаш вазифалари ҳал этилади. Оқибатда, маъмур тизим ишлашини баҳолаш ва тузилмасини ўзгартиришни, яъни ахборотни ҳимояланганлигини оширишнинг янги воситаларининг амалга оширишни, эски ва самарасизларини ўчиришни ҳамда умуман тизимнинг ишлаш самарадорлигини ошириш учун параметрларни қайта соzлашни бажаради.

ИКТдан фойдаланиш тажрибаси шуни кўрсатадики, маъмурий бошқаришни ташкиллаштириш машаққатли заифадир. Бу маъмурий бошқарувнинг мустақил куйи тизимини ИКТнинг таркибий қисми сифатида ажратишнинг мақсадга мувофиқлигини, тегишли меъёрий ҳужжатларни ишлаб чиқиш ва амалга оширишнинг долзарблигини, шунингдек, хавфсизликни бошқаришнинг автоматлаштирилган тизимини жорий этилиши мақсадга мувофиқлигини белгилайди.

Ҳозирги вақтда кўплаб ИКТларида хавфсизликни бошқариш учун айнан шу усул қўлланилади. Шундай қилиб, ушбу усулнинг асосий афзаллиги бу ИКТга жорий этиш соддалигидадир.

Шу билан бирга ушбу усулнинг асосий камчилиги ИКТ хавфсизлигини бошқариш самарадорлигига таъсир кўрсатувчи инсон омили ҳисобланади. Бошқарув тизимининг фавқулодда вазиятларга жавоб беришнинг тезлиги ниҳоятда паст. Шундай экан, фавқулодда вазиятларнинг пайдо бўлиш эҳтимолини камайтириш учун ахборотни ҳимоя қилиш воситаларидан фойдаланишга бўлган харажатлар салмоқли ортади.



2. Хавфсизликни бошқаришнинг маъмурий-ташкилий усулининг аниқланган камчиликларини инobatга олган ҳолда, фавқулодда вазиятларнинг олдини олиш учун ИКТ хавфсизлигини бошқариш ва ишлаш самарадорлигини ошириш учун бошқарув субъектларига автоматик таъсир ўтказиш воситалари қўлланилади.

Умумий ҳолатда ИКТ хавфсизлигини бошқаришнинг мослашувчан тамойилларини амалга ошириш, мустақил қийматга эга учта вазифани ҳал этиш зарурияти билан боғлиқ [4, 5, 7]:

– кўзда тутилмаган вазиятларни (бостириб киришларни) аниқлаш ва идентификация қилиш;

– бузғунчилар ва ҳужумларни (бостириб киришларни) блоклаш мақсадида ахборотни ҳимоя қилиш воситаларига бошқариш таъсирини шакллантиришга нисбатан қарорларни қабул қилиш;

– талаб этилаётган ҳимояланганлик даражасини таъминлаш учун ахборотни ҳимоя қилиш тизимини модификация қилиш.

Рухсатсиз фойдаланишларни аниқлаш ва идентификация қилиш вазифасини ҳал этиш, ИКТга бўлган ҳужумларни аниқлаш жараёнини формаллаштиришга, яъни назорат қилинадиган белгилар асосида тезкор вақт режимида ҳужумнинг таниқли турларини аниқлаш ва идентификация қилиш имконини берувчи таҳлилий моделни ишлаб чиқишга асосланган. Бунда модел, назорат қилинадиган белгилар тўплами кенгайтмаси ҳисобига ҳужумларнинг янги синфларини аниқлаш ва идентификация қилиш қобилиятига эга бўлиши лозим.

ИКТга бўлган ахборот таъсирини аниқлашда рухсатсиз хатти-ҳаракат уринишларни блокланадиган ҳолатга ўтказадиган оптимал ечимни топиш зарур [2, 4, 8, 9].

Хавфсизлик жараёнларини бошқариш усулининг афзаллиги, ҳужумларга чора кўришнинг тезкорлиги ҳисобланади. Шу билан бирга ҳужумларга қарши ҳаракатни амалга ошириш учун турли хил ҳимоя воситаларидан фойдаланишга кетган харажатлар, ахборотни ҳимоя қилиш тизимига тақдим этилган,

умуман чекланган ресурсларда тизимнинг юқори ҳимояланганлигини таъминлашга имкон берувчи актив, ахборот таъсирининг турларига қараб ўзгаради.

Камчиликлари мавжуд ИКТ бошқариш тизимларига ушбу усулни жорий этиш мураккаблигини кўрсатиш лозим, чунки мазкур усул ҳар бири алоҳида ИКТ учун соzлашни назарда тутади, бу эса ўз навбатида етарли даражада мураккаб жараён ҳисобланади. Ушбу вазифани, ахборот хавфсизлигини таъминлаш тизими самарадорлигини назорат қилиш ва ошириш бўйича тадбирларни шакллантириш ҳисобига ҳал этиш мумкин.

## II БОБ. ИНФОКОММУНИКАЦИОН ТИЗИМЛАРИДА ФЙДАЛАНИЛАДИГАН ХАВФСИЗЛИК МОДЕЛЛАРИНИНГ АСОСИЙ ТУШУНЧАЛАРИ

### 2.1. Ахборотдан фойдаланишни назоратлашда фойдаланиладиган асосий тушунчалар

Компьютер тизимининг (КТ) хавфсизлиги таъминоти сифатида куйидаги тушунчалардан фойдаланилади: “объект” (object), “субъект” (subject), “моҳият” (entity) ва “фойдаланиш” (access). Ички тузилманинг моҳияти кўрилатганда КТ хусусиятларини тавсифлашда “объект” тушунчасидан ташқари “контейнер” (container) тушунчаси ҳам кенг қўлланилади.

Объект ёки контейнер – субъектлар бажараётган операциялар ҳақида ахборот (маълумот) олувчи ёки ўз ичида мужассамлаштирган КТнинг ташкил этувчиси. Субъект КТ моҳиятини ташкил этувчилари устида операциялар бажарувчи. Таърифларга кўра куйидагилар тахмин қилинади [10, 11]:

- контейнерлар объектлардан ва бошқа контейнерлардан ташкил топган бўлиши мумкин;

- КТ субъектлари бутун объектдан фойдаланиш имкониятига эга бўладилар, лекин объектнинг қисмларидан фойдаланиш имкониятига эга бўлмайдилар.

- КТ субъектлари контейнер ва унинг ташкил этувчиларидан фойдаланиш имкониятига эга бўладилар.

ИКТ субъектлари объектлар устида операциялар бажаришлари учун объектлардан фойдаланиш ҳуқуқига эга бўлишлари керак бўлади. Фойдаланишни куйидаги турлари кенг амалиётда фойдаланилади:

*read* – ташкил этувчиларни ўқиш учун фойдаланиш;

*write* – ташкил этувчиларга ёзиш учун фойдаланиш;

*execute* – ташкил этувчи субъектни активизация қилиш.

Ҳозирги кунда компьютер хавфсизлигида хавфсизликни формал моделлаштиришда субъектлар ИКТ ташкил этувчила-

ридан фойдаланиш турларини бериш орқали амалга оширил-моқда, яъни ИКТда ахборот хавфсизлигининг барча масалалари субъектларнинг ташкил этувчилардан фойдаланишлари тавсиф асосида амалга оширилади [12].

*Ахборот хавфсизлигига бўладиган таҳдидларнинг тавсифи.*

*Ахборот хавфсизлигига ёки ИКТга таҳдид* – ахборотга ёки ИКТга потенциал таъсир кўрсатиш орқали ИКТ ёки фойдаланувчи ёки ахборот эгаларига тўғридан-тўғри ёки билвосита зарар келтириш [13].

*Ахборотнинг конфиденциаллиги* – ахборотдан фойдаланиш имкониятига эга бўлган субъектларга чекловлар ўрнатиш. Бунда ахборотдан фойдаланиш ҳуқуқига эга бўлмаган субъектларга ахборотни ўқиш, ёзиш ва устида амаллар бажаришни тақиқлаш.

*Ахборот яхлитлиги* – рўйхатга олинмаган фойдаланувчилар томонидан ресурслардан фойдаланишни ёки модификацияланишини ҳамда рўйхатга олинган фойдаланувчилар томонидан уларга тегишли бўлмаган ресурслардан фойдаланишни ёки модификацияланишини олдини олиш.

*Ахборотнинг фойдаланувчанлиги* – ИКТ (муҳит, воситалар ва қайта ишлаш технологияси) хусусияти бўлиб, субъектлар томонидан сўралган сўровларни (амалларни) ўз вақтида фойдаланишини таъминлаш.

*Ахборотнинг конфиденциаллиги бўладиган таҳдид* – ахборотдан фойдаланишга ўрнатилган чекловларни бузилишидир.

*Ахборот яхлитлигига бўладиган таҳдид* – атайин ёки тасодифан ахборотни рухсатсиз ўзгартириш.

*Ахборотнинг фойдаланувчанлигига бўладиган таҳдид* – ахборотдан фойдаланишга рухсатсиз блоклаш (блоклаш доимий ёки вақтинчалик бўлиши мумкин, бунда ахборот фойдасиз бўлиб қолгунга қадар кетган вақт етарли бўлади) амалга оширилган ҳолат.

*КТ параметрларини ошкор қилиш таҳдиди* – ИКТ ҳимоясини енгиш, тизим хавфсизлигини хусусиятларини, функцияларини ва параметрларни аниқлаш.

## **2.2. Фойдаланишни назоратлаш усулининг умумлаштирилган схемаси**

Фойдаланишни назоратлаш ҳимоялаш тизимининг марказий элементи фойдаланиш диспетчери орқали амалга оширилади. Фойдаланиш диспетчери субъектларнинг объектларга бўлган барча сўровларини назоратлаш ва таҳлил қилишни амалга оширади. Таҳлил натижасига кўра, дастлабки белгиланган (одатда тизим маъмури томонидан) фойдаланиш қоидаларига (фойдаланишни чегаралаш сиёсати асосида) мувофиқлигини таққослайди ва фойдаланиш диспетчери кўриб чиқилган фойдаланиш қоидалари асосида субъектга ўзи сўраган объектга фойдаланиш турига қараб (субъектга рухсат этилган фойдаланиш тури асосида) рухсат беради ёки унга фойдаланишни тақиқлайди.

Фойдаланиш диспетчери субъектларнинг объектларга юборётган барча сўровларини бошқариб бориши кераклиги сабабли, у одатда операцион тизим ядроси даражасида амалга оширилади [14].

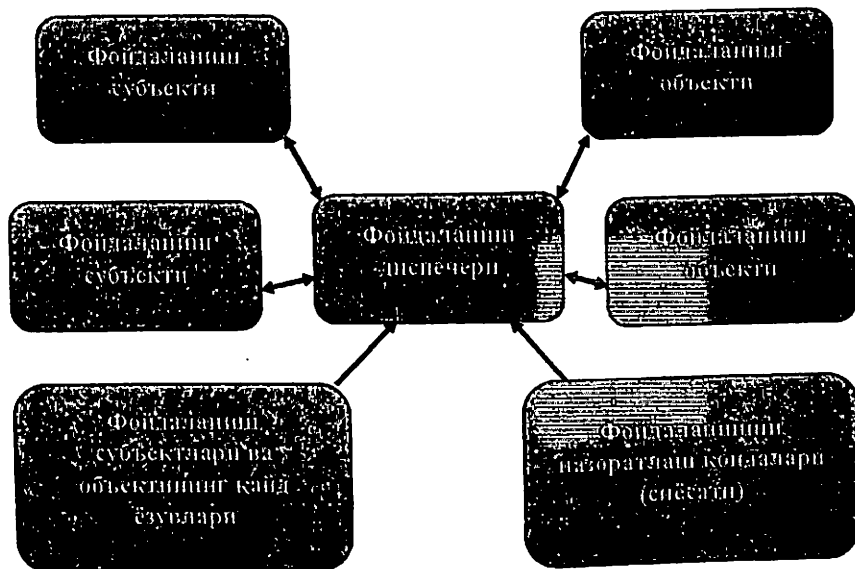
Фойдаланишни назоратлаш субъектлар ва объектлар орасидаги жараёнларни идентификациялаш маълумотларини қайд ёзуви деб белгилайди. Фойдаланиш диспетчери субъектга объектдан фойдаланишига рухсат бериш (ёки рад этиш) тўғрисидаги қарор қабул қилиш қоидалари фойдаланишни назоратлаш қоидалари (ёки сиёсати) баъзи ҳолларда фойдаланишни назоратлаш сиёсати деб аталади.

Фойдаланишни назоратлаш усулининг умумлашган схемаси 2.1-расмда келтирилган.

Фойдаланишни назоратлаш усуллари субъект ва объектларни идентификациялаш усуллари, фойдаланишни назоратлаш қоидаларини (сиёсати) ўрнатиш ва уларни сақлаш усулларида фарқланади.

Фойдаланишни назоратлаш усулларида куйидагилари мавжуд:

- фойдаланиш матричасига асосланган фойдаланишни назоратлаш усули;
- хавфсизли белгиларига асосланган фойдаланишни назоратлаш усули.

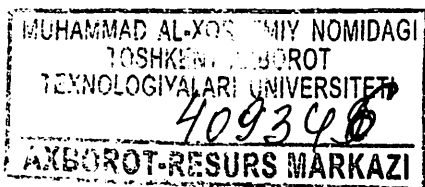


2.1-расм. Фойдаланишни назоратлаш усулининг умумлашган схемаси

### 2.3. Ахборотдан фойдаланишни назоратлашда сиёсат турлари

ИКТнинг хавфсизлик сиёсати – ИКТ доирасида ресурсларни бошқариш, уларни ҳимоя қилиш ва тақсимлашни тартибга солувчи қондалар тўплами [13, 15, 16, 17].

Хавфсизлик сиёсати математик, схемотехник, алгоритмик ва бошқа кўринишларда бўлиши мумкин. Хавфсизлик сиёсати хавфсиз ИКТ ишлаб чиқиш ва уларни тадқиқ қилишда муҳим роль ўйнайди, чунки улар қуйидаги муҳим вазифаларни ҳал қилишни таъминлайди:



- ахборотни ҳимоя қилиш воситалари ва усулларини амалга ошириш механизмларини белгиловчи хавфсиз ИКТ архитектурасининг асосий тамойилларини танлаш ва асослаш;

- ишлаб чиқилган тизимларнинг хусусиятларини (хавфсизлигини) хавфсизлик сиёсатига (талаблар, шартлар, мезонлар) мувофиқлигини формал исботлаш орқали тасдиқлаш;

- ишлаб чиқиляётган ҳимояланган ИКТ маъмурий-ташқилий ва ҳужжатли таъминлашнинг муҳим қисми сифатида хавфсизлик сиёсатининг расмий спецификациясини ишлаб чиқиш.

Ҳозирги кунда ахборотдан фойдаланишни бошқариш сиёсатларидан куйдагиларни санаб ўтиш мумкин:

- фойдаланишни бошқаришнинг дискрецион сиёсати (*Discretionary Access Control*);

- фойдаланишни бошқаришнинг мандатли сиёсати (*Mandatory Access Control*);

- фойдаланишни бошқаришнинг ролларга асосланган сиёсати (*Role – based Access Control*);

Фойдаланишни бошқаришнинг дискрецион сиёсати куйидаги талабларга жавоб беради:

- барча объектлар ва субъектлар идентификация қилинган бўлиши керак, яъни ҳар бир ташкил этувчига уникал идентификатор рақами ўзлаштирилади;

- фойдаланишлар матрицаси берилади, унда сатрларда ИКТ субъектлари, қаторларда ИКТ объектлари берилади. Ячейкалар ўз ичида субъектларнинг объектлардан фойдаланиш ҳуқуқлари билан тўлдирилади ва улар тўпламларни ташкил этади;

- субъект ИКТнинг объектдан фойдаланиш ҳуқуқи фақат фойдаланишлар матрицасидаги ячейкада субъектнинг объектдан фойдаланиш ҳуқуқи берилган бўлса фойдаланишни амалга ошириш имконияти пайдо бўлади.

Фойдаланишни бошқаришнинг дискрецион сиёсатининг асосий устунлиги фойдаланишни бошқаришни содда тизимини яратиш имконини беради. Бу сиёсатнинг асосий камчилиги сифатида унинг фойдаланиши бошқариш учун ўрнатилган қоидаларнинг

ўзгармаслигидир (статик). Бу сиёсат ИКТ ҳолатини динамик ўзгариб боришини назарда тутмаган. Бундан ташқари, фойдаланишни бошқаришнинг дискрецион сиёсатини қўллаш фойдаланишни бошқариш қоидаларини белгилаш ва ИКТ хавфсизлигига таъсирини таҳлил қилишда баъзи бир қийинчиликлар пайдо бўлади.

Фойдаланишни бошқаришнинг маънавий сиёсати қуйидаги талабларга жавоб беради:

- ИКТнинг барча элементлари идентификация қилинган бўлиши керак;

- ахборотнинг конфиденциаллик даражасининг панжараси берилади;

- ИКТнинг ҳар бир объектига конфиденциаллик даражаси ўзлаштирилади ва ҳар бир объектдан фойдаланишни чеклаш қоидалари ўрнатилади;

- ИКТда ҳар бир субъектга ваколат даражасини берувчи субъектга фойдаланишлик даражаси ўзлаштирилади;

- субъект ИКТ объектдан фойдаланиш учун субъектнинг фойдаланишлик ва конфиденциаллик даражаси бунга мос келиши керак.

Фойдаланишни бошқаришнинг маънавий сиёсатининг асосий устунлиги ахборотни сирқиб чиқиб кетишини назорат қилиш орқали тизимнинг хавфсизлиги таъминланади.

Фойдаланишни бошқаришнинг ролларга асосланган сиёсати қуйидаги талабларга жавоб беради:

- ИКТнинг барча элементлари идентификация қилинган бўлиши керак;

- кўплаб роллар берилади, бунда берилган ролларга тизим элементларидан фойдаланиш ҳуқуқлари белгиланади;

- ҳар бир субъект руҳсат (авторизациялашган) этилган ролларга эга бўлади;

- субъект ИКТ объектдан фойдаланиш учун фойдаланишлик ҳуқуқига эга бўлган ролга эга бўлиши керак.

Ролларга асосланган фойдаланишни бошқариш тизимнинг ишлаш жараёнида эгилувчан, динамик ўзгарадиган фойдаланишни чеклаш қоидаларини амалга оширишга имкон беради.



Ўтказилган қиёсий таҳлил асосида ахборотдан фойдаланишни бошқариш сиёсатининг умумий камчиликлари ва афзалликлари ажратиб олинди [18]. Фойдаланишни бошқариш сиёсатларининг таққослаш натижалари 2.1-жадвалда келтирилган.

2.1-жадвал

**Фойдаланишни бошқариш сиёсатларининг камчиликлари ва афзалликлари**

Фойдаланишни бошқариш сиёсати	Афзалликлар	Камчиликлар
Мандатли	<ul style="list-style-type: none"> <li>- фойдаланиш субъекти, субъектнинг махфийлик даражасидан кам бўлмаган махфийлик даражасига эга объектлардан фойдаланиш имконига эга бўлади;</li> <li>- субъект, унинг махфийлик даражасидан кам бўлган объектга маълумот ёзиш ҳуқуқига эга эмас;</li> <li>- ахборотни сирқиб чиқиб кетишни назорат қилиш.</li> </ul>	<ul style="list-style-type: none"> <li>- масофадан ўқиш тақсимланган тизимлардаги муаммо ҳисобланади;</li> <li>- ишончли субъектларнинг муаммоси;</li> <li>- объектни қайта таснифлаш;</li> <li>- хавфсизлик даражаларини таснифлашнинг қатъий тизимлари.</li> </ul>
Дискрецион	<ul style="list-style-type: none"> <li>- ушбу модел содда ва кўргазмали бўлганлиги сабабли, мураккаб алгоритмларни талаб қилмайди;</li> <li>- бошқарув самардорлиги, чунки бу модел фойдаланувчи бажарадиган амалларгача ҳуқуқларини аниқлик билан бошқариш мумкин;</li> <li>- хавфсизликнинг кучли мезони.</li> </ul>	<ul style="list-style-type: none"> <li>- исгалган тизим учун хавфсизликни текшириш алгоритми мавжуд эмас;</li> <li>- троян оти ёрдамида амалга оширилган ҳужумга заифлиги, чунки мазкур моделда субъектлар орасидаги ахборот оқими назорати мавжуд эмас;</li> <li>- субъектнинг фойдаланиш ҳуқуқи мажмуи статикдир. Субъектнинг тизимда қандай вазифа бажаришидан қатъи назар, ундан фойдаланиш ҳуқуқлари мажмуи донмий бўлиб қолади.</li> </ul>

## 2.1-жадвалнинг давоми

Ролларга асосланган	<ul style="list-style-type: none"> <li>- ягона тизим ёки илова доирасида фойдаланувчи ваколатларини бошқариш учун кенг қўлланилади;</li> <li>- ролларни шакллантириш тизим фойдаланувчилари учун аниқ ва тушунарли фойдаланишни чеклаш қоидаларини белгилашга чақирилган;</li> <li>- тизимнинг ишлаш жараёнида эгилувчан, динамик ўзгарадиган фойдаланишни чеклаш қоидаларини амалга оширишга имкон беради.</li> </ul>	<ul style="list-style-type: none"> <li>- фойдаланувчи, қайси мавжуд фойдаланувчи ролларига авторизациялаш қарорини ўзи қабул қилади;</li> <li>- тизимда фойдаланувчининг ҳақиқий функционал мажбуриятлари сонига нисбатан белгиланаётган ролларнинг сони салмоқли ортади;</li> <li>- унинг ҳам шакллантириш, ҳам ўзгартиришлар киритиш босқичларида хавфсизлик тизимини бошқариш тартиб-таомиллари мураккаблашади.</li> </ul>
---------------------	--	---

Юқорида кўриб чиқилган фойдаланишни бошқариш сиёсатларининг афзаллик ва камчиликларини ҳисобга олиб, 2.2-жадвалда ИКТ ресурсларидан бошқариш сиёсатларининг асосий характеристикаларини таққослаш амалга оширилган.

## 2.2-жадвал

### Фойдаланишни чеклаш моделларининг характеристикаларини таққослаш

	Дискрецион	Мандат	Ролларга асосланган
Амалга оширишнинг мураккаблиги	Ўрта	Юқори	Юқори
Ҳимояланганлиги	Ўрта	Юқори	Юқори
Фойдаланишни мураккаблиги	Ўрта	Юқори	Ўрта
Унумдорлик	Кам ресурслардан фойдаланади	Кам ресурслардан фойдаланади	Кўп ресурслардан фойдаланади

## 2.2-жадвалнинг давоми

Тизим хавфсизлигининг формал исботи	Тўлиқ эмас	Тўлиқ	Тўлиқ эмас
Тармоқда хавфсизликни таъминлаш	Таъминламайди	Таъминламайди	Таъминлайди
Ахборотни сирқиб чиқиб кетишини назорат қилиш	Тўлиқ эмас	Тўлиқ	Тўлиқ эмас

Шундай қилиб, янги усулларни ҳамда тизимнинг юқори хавфсизлигини таъминловчи модификацияланган ахборотнинг ҳимояланганлигини ошириш моделларини яратиш долзарб ҳисобланади.

## III БОБ. ФОЙДАЛАНИШНИ БОШҚАРИШНИНГ ДИСКРЕЦИОН МОДЕЛИ

### 3.1. Харрисон-Руззо-Ульман фойдаланиш матрицаси модели

Харрисон-Руззо-Ульман модели (ХРУ) [13, 19, 20, 21] фойдаланишни бошқаришнинг дискрецион сиёсатини амалга оширадиган ҳимоя тизимини таҳлил қилиш учун қўлланилади.

ХРУ моделида қуйидаги таърифлар қўлланилади:

$O$  — тизим объектларининг мажмуи;

$S$  — ( $S \subseteq O$ ) тизим субъектларининг мажмуи;

$R$  — субъектларнинг объектларга фойдаланиш ҳуқуқи мажмуининг турлари, масалан, ўқиш учун ҳуқуқ (*read*), ёзиш учун (*write*), эгалик қилиш учун (*own*).

$M$  — фойдаланишлар матрицаси, бу ерда сатрлар субъектларга мос келади, устунлар объектларга мос келади.  $M[s, o] \subseteq R - s$  субъектнинг  $o$  объектга бўлган фойдаланиш ҳуқуқлари.

Тизимнинг ишлаши фақатгина матрицада киришнинг ўзгариши нуқтаи назаридан кўриб чиқилади. Эҳтимолий ўзгаришлар 3.1-жадвалда келтирилган содда операторларнинг олтига тури билан аниқланади.

$\alpha$  содда операторини бажариш натижасида  $q = (S, O, M)$  ҳолатидан  $q' = (S', O', M')$  натижавий ҳолатга ўтиш амалга оширилади. Мазкур ўтишни  $q \mapsto \alpha q'$  орқали белгилаш мумкин.

Содда операторлардан ХРУ тизими командаларининг якуний рақами тузилади. Ҳар бир команда иккита қисми ўз ичига олади:

1) Команда бажариладиган шартлар.

2) Содда операторларнинг кетма-кетлиги.

## ХРУ моделининг содда операторлари.

Содда операторлар	Бошланғич ҳолат $q = (S, O, M)$	Натижавий ҳолат $q' = (S', O', M')$
$r$ ҳуқуқини $M[s, o]$ га “киритиш”	$s \in S,$ $o \in O,$ $r \in R$	$S' = S, O' = O, M'[s, o] = M[s, o] \cup \{r\}, (s', o') \neq (s, o)$ учун $M'[s', o'] = M[s', o']$ тенглик бажарилади
$r$ дан $M[s, o]$ ҳуқуқини “ўчириш”	$s \in S,$ $o \in O,$ $r \in R$	$S' = S, O' = O, M'[s, o] = M[s, o] \setminus \{r\}, (s', o') \neq (s, o)$ учун $M'[s', o'] = M[s', o']$ тенглик бажарилади
$s'$ субъектини “яратиш”	$s' \in O$	$S' = S \cup \{s'\}, O' = O \cup \{s'\},$ $(s, o) \in S \times O$ учун $M'[s, o] = M[s, o]$ тенглик бажарилади, $o \in O'$ учун $M'[s', o] = \emptyset$ тенглик бажарилади, $s \in S'$ учун $M'[s', s'] = \emptyset$ тенглик бажарилади
$o'$ объектини “яратиш”	$o' \notin O$	$S' = S, O' = O \cup \{o'\}, (s, o) \in S \times O$ учун $M'[s, o] = M[s, o]$ тенглик бажарилади, $s \notin S'$ учун $M'[s, o'] = \emptyset$ тенглик бажарилади
$s'$ субъектини “ўчириш”	$s' \notin S$	$S' = S \setminus \{s'\}, O' = O \setminus \{s'\}, (s, o) \in S' \times O'$ учун $M'[s, o] = M[s, o]$ тенглик бажарилади
$o'$ объектини “ўчириш”	$o' \notin O,$ $o' \notin S$	$S' = S, O' = O \setminus \{o'\}, (s, o) \in S' \times O'$ учун $M'[s, o] = M[s, o]$ тенглик бажарилади

Шу тарзда, командаларнинг ёзуви қуйидаги кўринишга эга:  
*command*  $c(x_1, \dots, x_k)$

*if*  $(r_1 \in M[x_{s1}, x_{o1}])$  and ... and  $(r_m \in M[x_{sm}, x_{om}])$  then  
 $\alpha_1;$

```

...
 $\alpha_n$ ;
endif;
end,

```

бу ерда  $r_1, \dots, r_m \in R$  — фойдаланиш ҳукуки;  $\alpha_1, \dots, \alpha_n$  — параметрлари ҳамда шартларининг параметрлари бўлиб  $x_1, \dots, x_k$  командаларининг параметрлари ҳисобланувчи содда операторлар кетма-кетлиги. Таъкидлаш жоизки, команда танасида шартнинг мавжудлиги мажбурий ҳисобланмайди.

$c(x_1, \dots, x_k)$  буйруқнинг бажарилиши тизимнинг  $q$  ҳолатдан  $q'$  ҳолатга ўтади. Бу ўтишни қуйидагича белгилаймиз:

$$q \mapsto c(x_1, \dots, x_k) q'$$

бунда  $q' = q$ ,  $c(x_1, \dots, x_k)$  буйруқнинг шартлари бажарилмаса,  $q' = q_n$ ,  $c(x_1, \dots, x_k)$  шартлар бажарилган ва  $q_1, \dots, q_k$  ҳолат мавжуд бўлганда  $q = q_0 \mapsto \alpha_1 q_1 \mapsto \alpha_2 \dots \mapsto \alpha_n q_n$ .

### 3.2. Типик фойдаланиш матрицаси модели

Фойдаланишни бошқаришнинг дискрецион моделининг яна бири типик фойдаланиш матрицаси модели деб аталади. Бу модел ХРУ моделининг ривожлантирилган варианты ҳисобланади [22, 23, 24].

Типик фойдаланиш матрицаси модели (ТФМ) қуйидаги элементларни ўз ичига олади:

$O(o_1, o_2, \dots, o_m)$  — тизим объектларининг мажмуи;

$S(s_1, s_2, \dots, s_n)$  — тизим субъектларининг мажмуи, бу ерда ( $S \subseteq O$ );

$A$  — фойдаланиш матрицаси, ҳар бир ячейка объектлардан фойдаланиш ҳуқуқларини  $R(r_1, r_2, \dots, r_k)$  чекланган тўпладан фойдаланган ҳолда белгилайди. Бу ерда  $A[s, o] \subseteq R$ .

$T(t_1, t_2, \dots, t_l)$  — барча объектлар яратиладиган хавфсизлик турлари мажмуи. Объектнинг тури кейинчалик ўзгармайди. Объектга мос келувчи маълум бир турни ўрнатувчи  $f_t: O \rightarrow T$  функция берилган.

Фойдаланиш матрицаси ҳолатини ўзгартириш учун объектларнинг типик хусусиятларини ҳисобга олган ҳолда қуйидаги оддий операторлар киритилади:

- *Enter r into A[s, o]* –  $A[s, o]$  ячейкага  $r$  ҳуқуқини киритиш;
- *Delete r from A[s, o]* –  $A[s, o]$  ячейкадан  $r$  ҳуқуқини ўчириш;
- *Create subject s of type t* –  $t$  туридаги  $s$  субъектни яратиш;
- *Create subject o of type t* –  $t$  туридаги  $o$  объектни яратиш;
- *Destroy subject s* –  $s$  субъектни йўқ қилиш;
- *Destroy subject o* –  $o$  объектни йўқ қилиш.

Оддий операторларнинг бажарилиши натижасида  $q = (S, O, A)$  ҳолатидан янги  $q' = (S', O', A')$  ҳолатга ўтиш амалга оширилади.

Объектларнинг типик хусусиятларини ҳисобга олган ҳолда оддий операторларнинг таъсири остида тизим ҳолатини ўзгаришининг ўзига хос хусусияти ва шартлари 3.2-жадвалда келтирилган.

3.2-жадвал

**Объектларнинг типик хусусиятларини ҳисобга олган ҳолда оддий операторларнинг таъсири остида тизим ҳолатини ўзгаришининг ўзига хос хусусияти ва шартлари**

ТФМ моделнинг оддий оператори	Бажарилиш шарти	Тизимнинг янги ҳолати
<i>Enter r into A[s, o]</i>	$s \in S,$ $o \in O$	$S' = S, O' = O, \forall o \in O$ $f'_t(o) = f_t(o),$ $A'[s, o] = A[s, o] \setminus \{r\},$ агар $(s', o') \neq (s, o)$ $\Rightarrow A'[s', o']$ $= A[s, o]$

3.2-жадвалнинг давоми

<i>Delete r from A[s, o]</i>	$s \in S,$ $o \in O$	$S' = S, O' = O, \forall o \in O$ $f'_t(o) = f_t(o),$ $A'[s, o] = A[s, o] \setminus \{r\},$ агар $(s', o') \neq (s, o)$ $\Rightarrow A'[s', o']$ $= A[s, o]$
<i>Create subject s' of type t_s</i>	$s' \notin S$	$S' = S \cup \{s'\}, O'$ $= O \cup \{s'\},$ $\forall o \in O f'_t(o) =$ $f_t(o),$ агар $(s, o) \in S \times$ $O \Rightarrow A'[s, o] = A[s, o],$ агар $o \in O' \Rightarrow A'[s', o] =$ $\emptyset,$ агар $s \in S' \Rightarrow A'[s, s'] = \emptyset$
<i>Create subject o' of type t_o</i>	$o' \notin O$	$S' = S, O' = O \cup \{o'\},$ $f'_t(o') = t_o, \forall o \in O$ $f'_t(o) = f_t(o),$ агар $(s, o) \in S \times O \Rightarrow$ $A'[s, o] = A[s, o],$ агар $s \in S' \Rightarrow A'[s, o] = \emptyset$
<i>Destroy subject s'</i>	$s' \in S$	$S' = S \setminus \{s'\}, O' = O \setminus \{s'\},$ $\forall o \in O f'_t(o) =$ $f_t(o),$ агар $(s, o) \in S' \times O' \Rightarrow$ $A'[s, o] = A[s, o]$ бўлса $f'_t(s') =$ аниқланмаган
<i>Destroy subject o'</i>	$o' \in O \setminus S$	$S' = S, O' = O \setminus \{o'\},$ $\forall o \in O f'_t(o) =$ $f_t(o),$ агар $(s, o) \in S' \times O' \Rightarrow$ $A'[s, o] = A[s, o]$ бўлса $f'_t(o') =$ аниқланмаган



Тизимнинг ҳолати ХРУ моделида бўлгани каби фойдаланиш матричасини ўзгартириш бўйича сўровлар таъсири остида буйруқлар кўринишида амалга ошириш мумкин бўлади. Бунда тизим объектларининг типиклаштирилган хусусиятини ҳисобга олган ҳолда қуйидаги шаклга эга бўлади:

*command*  $\alpha(x_1: t_1, x_2: t_2 \dots, x_k: t_k)$   
*if*  $(r_1 \text{ in } A[x_{s1}, x_{o1}])$  *and* (буйруқни бажарилиш шarti)  
 $(r_2 \text{ in } A[x_{s2}, x_{o2}])$  *and*  
 $\vdots$   
 $\vdots$   
 $\vdots$   
 $(r_m \text{ in } A[x_{sm}, x_{om}])$   
*then*  
 $op_1, op_2, \dots, op_n$  (буйруқни ташкил этувчи операторлар)

Шундай қилиб, фойдаланиш матричасини ўзгартириш бўйича буйруқлар бажарилганда, буйруқнинг ҳақиқий параметрлари турларини назорат қилиш амалга оширилади. Бунда буйруқни бажариш шартларига жалб қилинган объектлар ва субъектлар турларини назорат қилиш жорий этилади. Шу асосда, тизимнинг хавфсизлик шартларини юмшатиш мумкин бўлган буйруқларга қўйилган чекловларни шакллантириш мумкин.

### 3.3. Take-Grant фойдаланишни тарқатиш модели

Take-Grant классик модели дискрецион фойдаланишни бошқариш тизимларида фойдаланиш ҳуқуқларини тарқатишни таҳлил қилишга йўналтирилган [25, 26, 27].

Take-Grant моделининг асосини қуйидаги элементлар ташкил этади:

- $O$  – объектлар мажмуи;
- $(S \subseteq O)$  – субъектлар мажмуи;

$R = \{r_1, r_2, \dots, r_m\} \cup \{t, g\}$  – фойдаланиш ҳукуқи турларининг мажмуи, бу ерда  $t(take)$  – фойдаланишни ҳуқуқини олиш,  $g(grant)$  – фойдаланиш ҳуқуқини бериш.

$G = (S, O, E)$  – тизим ҳолатини тавсифловчи белгиланган фойдаланишлар графи.  $S$  ва  $O$  элементлари графинининг чўққилари ҳисобланади ва уларни қуйидагича белгилаймиз:  $\otimes$  – объектлар (мажмуа элементлари  $O \setminus S$ ) ва  $\circ$  – субъектлар (мажмуа элементлари  $S$ ). Мажмуа элементлари  $E \subseteq O \times O \times R$  графнинг қирралари ҳисобланади. Ҳар бир қирра  $R$  фойдаланиш ҳуқуқлари турлари билан белгиланган.

Тизимнинг ҳолати мувофиқ келувчи фойдаланиш графлари орқали тавсифланади. ХРУ моделидан фарқли равишда Take-Grant моделида субъектларнинг объектлардан фойдаланиш ҳуқуқидан ташқари объектлардан объектлар фойдаланиш ҳуқуқи мавжуд бўлади.

Take-Grant моделининг асосий мақсади тизимнинг маълум бир ҳолатига мос келувчи бошланғич фойдаланиш графининг фойдаланиш ҳуқуқларини сирқиб чиқиб кетиши эҳтимолини текшириш учун алгоритмик шартларни аниқлаш ва асослашдир.

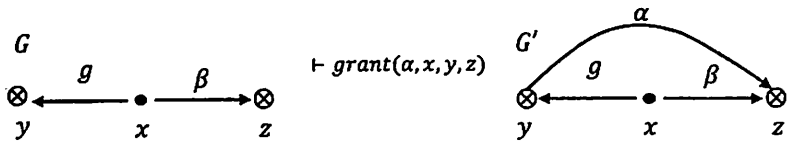
Take-Grant модели тизимнинг бир ҳолатдан бошқа ҳолатга ўтиш тартиби классик моделда де-юре деб аталадиган фойдаланиш графини ўзгартириш қоидалари билан белгиланади. *op* қоидасини бажарилиши натижасида  $G$  графини  $G'$  графига ўзгартиришни қуйидагича белгиланади.

$$G \vdash_{op} G'.$$

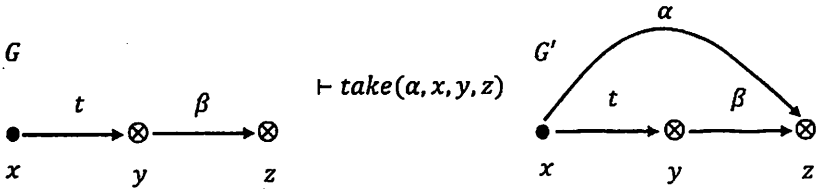
Take-Grant классик моделида графни ўзгартиришнинг 4 та де-юре қоидаси кўриб чиқилади. Ҳар бир қоиданинг бажарилиши тизимнинг актив компонентаси бўлган субъект томонидан амалга оширилади:

*take* – фойдаланишни ҳуқуқини олиш;

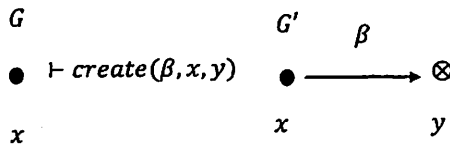
*grant* – фойдаланиш ҳуқуқини бериш.



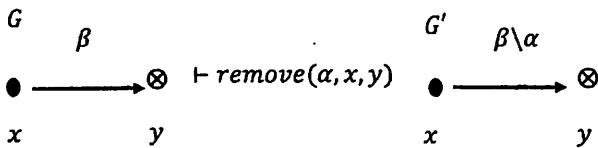
3.1-расм.  $\text{take}(\alpha, x, y, z)$  қойдани қўллаш



3.2-расм.  $\text{grant}(\alpha, x, y, z)$  қойдани қўллаш



3.3-расм.  $\text{create}(\beta, x, y)$  қойдани қўллаш



3.4-расм.  $\text{remove}(\alpha, x, y)$  қойдани қўллаш

$G = (S, O, E)$ нинг дастлабки ҳолати ва  $G' = (S', O', E')$  нинг натижавий ҳолати учун Де-юре қойдаларини қўллаш шартлари 3.3-жадвалда келтирилган.

*create* – янги объект ёки субъектни яратиш, бунда субъект яратувчи яратилган субъект учун ихтиёрий фойдаланиш ҳуқуқини олиши мумкин;

*remove* – фойдаланиш ҳуқуқини ўчиради.

### 3.3-жадвал

#### Take-Grant классик моделида Де-юре қондалари

Қоида	Дастлабки ҳолат $G = (S, O, E)$	Натижавий ҳолат $G' = (S', O', E')$
<i>take</i> ( $\alpha, x, y, z$ )	$x \in S, y, z \in O, (x, y, \{t\}) \subset E,$ $(y, z, \beta) \subset E, x \neq z, \alpha \subseteq \beta$	$S' = S, O' = O,$ $E' = E \cup \{(x, z, \alpha)\}$
<i>grant</i> ( $\alpha, x, y, z$ )	$x \in S, y, z \in O, (x, y, \{g\}) \subset E,$ $(y, z, \beta) \subset E, y \neq z, \alpha \subseteq \beta$	$S' = S, O' = O,$ $E' = E \cup \{(y, z, \alpha)\}$
<i>create</i> ( $\beta, x, y$ )	$x \in S, y \notin O, \beta \neq \emptyset$	$O' = O \cup \{y\}$ , агар $y$ субъект, унда $S' = S \cup \{y\}$ акс ҳолда $S' = S,$ $E' = E \cup \{(x, y, \beta)\}$
<i>remove</i> ( $\alpha, x, y$ )	$x \in S, y \in O,$ $(x, y, \beta) \subset E, \alpha \subseteq \beta$	$S' = S, O' = O,$ $E' = E \setminus \{(x, y, \alpha)\}$

$G_0 = (S_0, O_0, E_0)$  ихтиёрий фойдаланишлар графи,  $x, y \in O_0, x \neq y$ . *can\_share*( $\alpha, x, y, G_0$ ) ҳолати рост бўлади, агар  $(x, y, \alpha) \subset E_0$  ёки қуйидаги 1-3 шарт бажарилса:

1-шарт.  $s_1, \dots, s_m \in O_0$  объектлари мавжуд:

$(s_i, y, \gamma_i) \subset E_0$  учун  $i = 1, \dots, m$  ва  $\alpha = \gamma_1 \cup \dots \cup \gamma_m$ .

2-шарт.  $x'_1, \dots, x'_m, s'_1, \dots, s'_m \in S_0$  объектлари мавжуд:

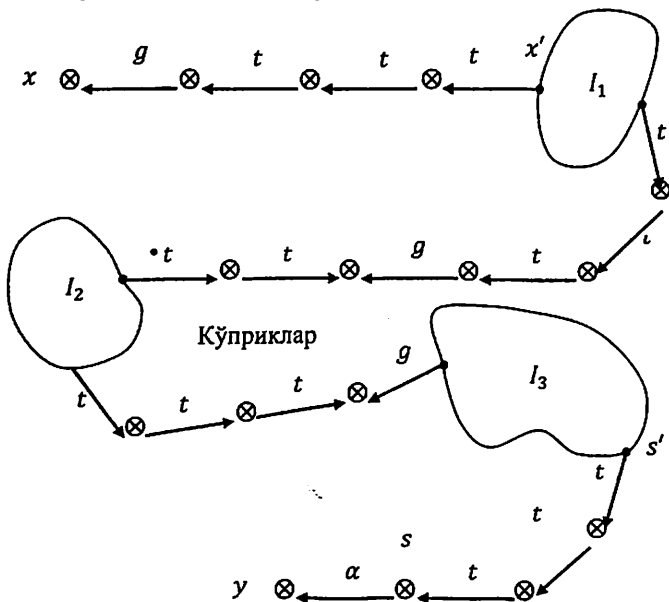
а)  $x = x'_i$  ёки  $x'_i \in G_0$  графнинг  $x$  кўприкнинг бошланғич оралиғига уланади, бу ерда  $i = 1, \dots, m$ ;

б)  $s_i = s'_i$  ёки  $s'_i \in G_0$  графнинг  $s_i$  кўприкнинг сўнги оралиғига уланади, бу ерда  $i = 1, \dots, m$ .

3-шарт.  $G_0$  графнинг  $(x'_i, s'_i), i = 1, \dots, m$ , жуфтликлар учун оралиқларда  $I_{i,1}, \dots, I_{i,u_i}$  бўш жойлар мавжуд бўлади, бу ерда  $u_i \geq 1$ .  $x'_i \in I_{i,1}, s'_i \in I_{i,u_i}$  учун  $I_{i,j}$  ва  $I_{i,j+1}, j = 1, \dots, u_i - 1$ , бўш жойлар орасида кўприклар мавжуд бўлади.

Барча шартларнинг бажарилиши 3.5-расм кўринишида ифода қилинади. Субъектлар ўртасида фойдаланиш ҳуқуқларини кўприклар орқали жўнатиш мумкин бўлади.

Кўприкнинг бошланғич оралиғи



Кўприкнинг сўнги оралиғи

3.5-расм. у объект устидан  $\alpha$  фойдаланишлар ҳуқуқини  $x$  объектга ўтказиш йўлига мисол

## IV БОБ. Фойдаланишни мандатли бошқариш модели

### 4.1. Фойдаланишни мандатли бошқаришга асосланган Белл-ЛаПадула модели

Белл-ЛаПадуланинг классик моделида [20, 28, 29, 30] ИКТдаги юқори даражадаги конфиденциалликка эга бўлган объектлардан конфиденциаллик даражаси пастроқ бўлган объектларга маълумот узатилиши мумкин бўлмаган шартлар кўриб чиқилади. Классик Белл-ЛаПадула моделининг асосий элементлари қуйидагилар ҳисобланади:

$S$  – субъектлар мажмуи;

$O$  – объектлар мажмуи;

$R$  – фойдаланиш турлари ва фойдаланиш ҳуқуқи турлари мажмуи (*read, write, append*);

$B = \{b \subseteq S \times O \times R\}$  – тизимда эҳтимолий кўплаб жорий фойдаланишлар мажмуи.

$(L, \leq)$  – конфиденциаллик даражалари панжараси, масалан,  $L = \{U(\text{unclassified}), C(\text{confidential}), S(\text{secret}), TS(\text{top secret})\}$ , бу ерда  $U < C < S < TS$ ;

$M = \{m_{|S| \times |O|}\}$  – эҳтимолий фойдаланиш матрицаларининг мажмуи, бу ерда  $m_{|S| \times |O|}$  – фойдаланишлар матрицаси,  $m[S, O] \subseteq R - S$  субъектининг  $O$  объектдан фойдаланиш ҳуқуқи.

$(f_s, f_o, f_c) \in F = L^S \times L^O \times L^S$  – функциялар учлиги  $(f_s, f_o, f_c)$ , қуйидагиларга мос равишда киритувчи:  $f_s: S \rightarrow L$  – субъектларнинг фойдаланиш даражаси;  $f_o: O \rightarrow L$  – объектларнинг конфиденциаллик даражаси;  $f_c: S \rightarrow L$  – субъектларнинг жорий фойдаланиш даражаси, бунда ҳар қандай  $s \in S$  учун  $f_c(s) \leq f_s(s)$  тенгсизлиги бажарилади;

$V = B \times M \times F$  – тизим ҳолатларининг мажмуи;

$Q$  – тизимга бўлган сўровлар мажмуи;

$D$  – сўровларга бўлган жавоблар мажмуи, масалан  $D = \{\text{yes, no, error}\}$ ;

$W \subseteq Q \times D \times V \times V$  — тизимдаги хатти-ҳаракатлар мажмуи, бу ерда тўртлик  $(q, d, v^*, v) \in W$ ,  $q$  сўров бўйича тизимнинг  $d$  жавоб билан бирга  $v$  ҳолатидан  $v^*$  ҳолатига ўтганлигини англатади;

$N_0 = \{0, 1, 2, \dots\}$  — вақт қийматларининг мажмуи;

$X$  — тизимга барча эҳтимолий сўровлар кетма-кетлигини киритувчи  $x: N_0 \rightarrow Q$  функцияларнинг мажмуи;

$Y$  — сўровлар бўйича тизимга барча эҳтимолий сўровлар кетма-кетлигини киритувчи  $y: N_0 \rightarrow D$  функцияларнинг мажмуи;

$Z$  — тизим ҳолатларининг барча мавжуд кетма-кетликларини киритувчи  $z: N_0 \rightarrow V$  функциялар мажмуи;

Изоҳ 1.:  $\Sigma(Q, D, W, z_0) \subseteq X \times Y \times Z$ , ҳар бир  $(x, y, z) \in \Sigma(Q, D, W, z_0)$  учун куйидаги шарт бажарилган тақдирда тизим деб аталади:  $t \in N_0, (x_t, y_t, z_{t+1}, z_t) \in W$  учун, бу ерда  $z_0$  — тизимнинг бошланғич ҳолати. Бунда ҳар бир тўпلام  $(x, y, z) \in \Sigma(Q, D, W, z_0)$  тизимни амалга ошириш,  $(x_t, y_t, z_{t+1}, z_t) \in W$  эса,  $t \in N_0$  вақт momentiда тизимнинг хатти-ҳаракати деб аталади.

Белл-ЛаПадуланинг классик моделида  $Q$  тўпلامга кирувчи сўровлар кўриб чиқилади:

-  $b$  — мавжуд фойдаланишлар тўпламига ўзгартириш киритиш учун сўровлар;

-  $f$  — функцияни ўзгартириш сўровлари;

-  $m$  — матрицада фойдаланиш ҳуқуқларини ўзгартириш сўровлари;

Куйида тизим ҳолатини ҳар бир элементи бўйича ўзгартириш имконини берувчи жараёни кўриб чиқамиз.

1. Мавжуд фойдаланишларни ўзгартириш:

- фойдаланиш ҳуқуқига эга бўлиш ( $b$  мавжуд фойдаланишлар тўпламига субъект, объект ва фойдаланиш турини киритиш);

- фойдаланиш ҳуқуқини бекор қилиш ( $b$  мавжуд фойдаланишлар тўпلامидан субъект, объект ва фойдаланиш турини ўчириб ташлаш);

2. Конфиденциаллик ва фойдаланиш даражалари функцияси қийматларини ўзгартириш:

- объектнинг конфиденциаллик даражасини ўзгартириш;
- субъектнинг фойдаланишлик даражасини ўзгартириш;

3. Фойдаланиш ҳуқуқларини ўзгартириш:

- фойдаланиш ҳуқуқини бериш ( $m$  фойдаланишлар матрицасининг талаб этилган элементига фойдаланиш ҳуқуқини қўшиб қўйиш);

- фойдаланиш ҳуқуқини бекор қилиш ( $m$  фойдаланишлар матрицасининг талаб этилган элементидан фойдаланиш ҳуқуқини ўчириш).

□

#### 4.2. Ахборот ҳимояланганлик даражасини оширишда мандатли фойдаланишни чеклаш усули

Мандатли фойдаланишни чеклаш усули махфийлик даражаси юқори бўлган ахборотни қайта ишлаш жараёнида кенг амалиётда қўлланилади. Махфийлик даражаси бўйича ахборот конфиденциаллигини таснифлашда маълумотларни қайта ишлашни моделларидан бири ҳисобланади.

Объектнинг хавфсизлик белгилари ахборотнинг конфиденциаллик тоифасини акс эттиради ва унинг тегишли объектларда сақланишини таъминлайди.

Субъектнинг хавфсизлик белгилари субъектнинг турли хил махфийлик даражасидаги маълумотларга кириш ва фойдаланиш ваколатларини акс эттиради [32].

Субъектнинг ваколат даражаси ва объектнинг махфийлик даражаси юқори бўлса, субъектлар  $C = \{C_1, \dots, C_l\}$  ва  $O = \{O_1, \dots, O_l\}$  объектларнинг чизиқли ваколатлар тўпламларида уларнинг тартиб рақамлари паст бўлади. Шунингдек, уларга  $M_i, i = 1, \dots, k$  хавфсизлик белгиларининг қиймати шунча паст ўзлаштирилади, яъни  $M_1 < M_2 < M_3 < \dots < M_l$ .

Шундай қилиб, субъектнинг қайд маълумотлари ва фойдаланиш объектлари сифатида фойдаланиш диспетчериди ҳар



бир субъект ва объект учун  $M$  тўпладан хавфсизлик белгилари бериледи, идентификаторлар (исмлар) бундан мустасно.

Умумий ҳолатда хавфсизлик белгиси тенг ваколатли субъектлар гуруҳига ва бир хил махфийлик даражасидаги объектлар гуруҳига бериледи [5].

Қуйидаги белгилардан фойдаланамиз:

$M_c$  — фойдаланиш субъектининг хавфсизлик белгиси (субъектлар гуруҳи);

$M_o$  — фойдаланиш объектнинг хавфсизлик белгиси (объектлар гуруҳи).

Белла-ЛаПадула модели маълумотларнинг махфийлигини бузилишидан ҳимоя қилиш учун ишлатилади. Тизимда ахборотга ишлов бериш пайтида унинг конфиденциаллик даражасини пасайтиришни ва махфийлик даражасини бузилишини олдини олиш орқали амалга оширилади ва бу жараёни ишлаб туриши учун қуйидаги қоидалар амалга оширилиши керак:

1. Агар  $M_c \leq M_o$  шарт бажарилса, у ҳолда  $C$  субъект “Ўқиш” режимида  $O$  объектдан фойдаланиш ҳуқуқига эга бўлади.

2. Агар  $M_c = M_o$  шарт бажарилса, у ҳолда  $C$  субъект “Ёзиш” режимида  $O$  объектдан фойдаланиш ҳуқуқига эга бўлади.

Ҳозирги кунда замонавий дастурларнинг аксариятида камдан-кам ҳолларда фақат ёзиш учун очиладиган файлдан фойдаланилади. Аксарият-ҳолларда ёзиш учун очилган объект бир вақтнинг ўзида ёзиш ва ўқиш учун очилади. Натижада,  $M_c > M_o$  шартга асосан ёзиб олиш имкониятини назарий имконият сифатида кўриб чиқиш мумкин, чунки бундай имкониятни хавфсизлик тизимларига жорий қилиш кўпгина иловаларни нотўғри ишлашига олиб келади.

Шундай қилиб, субъектнинг объектдан фойдаланиш сўровини кириш диспетчери субъект объектга сўровни жўнатиш вақтида ушлаб олади ва субъектнинг хавфсизлик белгисини аниқлайди. Бунда ( $M_c$ ) фойдаланишга сўров жўнатган субъектнинг хавфсизлик белгиси ва ( $M_o$ ) сўралган объектнинг хавфсизлик белгиси, сўров тури ёзиш ва ўқиш. Шу билан бирга

фойдаланиш диспетчери  $M_c$  ва  $M_o$  хавфсизлик белгиларини бири-бири билан таққослайди ва кўриб чиқилган фойдаланиш қоидалари асосида субъектга ўзи сўраган объектга фойдаланиш турига қараб рухсат беради ёки унга фойдаланишни тақиқлайди.

$M_m$  фойдаланиш матрицасидан фойдаланиш қоидаларини тасвирлаш учун фойдаланиш мумкин (кенгайтирилган қоидалар асосида фойдаланиш матрицаси  $M_m(p)$ ):

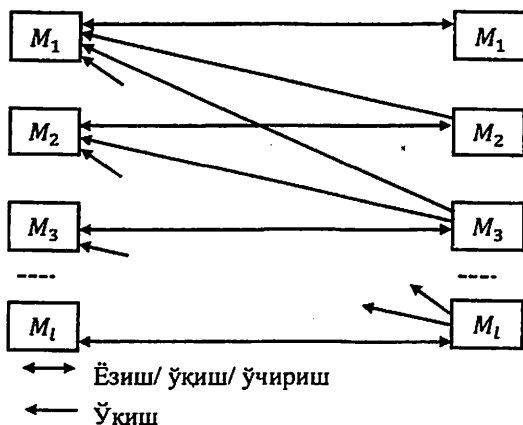
$$\begin{aligned}
 M_m &= \begin{matrix} C_1(M_1) \\ C_2(M_2) \\ \dots \\ C_{l-1}(M_{l-1}) \\ C_l(M_l) \end{matrix} \begin{bmatrix} O_1(M_1) & O_2(M_2) & \dots & O_l(M_l) \\ r, w, d & r & & r \\ 0 & r, w, d & & r \\ \dots & \dots & \dots & \dots \\ 0 & 0 & & r \\ 0 & 0 & & r, w, d \end{bmatrix} \\
 M_m(p) &= \begin{matrix} C_1(M_1) \\ C_2(M_2) \\ \dots \\ C_{l-1}(M_{l-1}) \\ C_l(M_l) \end{matrix} \begin{bmatrix} O_1(M_1) & O_2(M_2) & \dots & O_l(M_l) \\ r, w, d & r & & r \\ w & r, w, d & & r \\ \dots & \dots & \dots & \dots \\ w & w & & r \\ w & w & & r, w, d \end{bmatrix} \quad (4.1)
 \end{aligned}$$

Шундай қилиб, мандатли фойдаланишни чеклаш усули қайта ишлаш режимини ўзгартириш мақсадида амалга оширилаётган ишлов бериладиган маълумотларнинг хавфсизлик даражасини рухсатсиз пасайтиришдан ҳимоя қилиш орқали ахборотни конфиденциаллик бузилишидан ҳимоя қилишга имкон беради.

4.1-расмда маълумотларнинг хавфсизлик даражасини рухсатсиз пасайтиришдан ҳимоялаш схемаси келтирилган.

$M_c$  фойдаланиш субъекти-  
нинг хавфсизлик белгиси

$M_o$  фойдаланиш объекти-  
нинг хавфсизлик белгиси



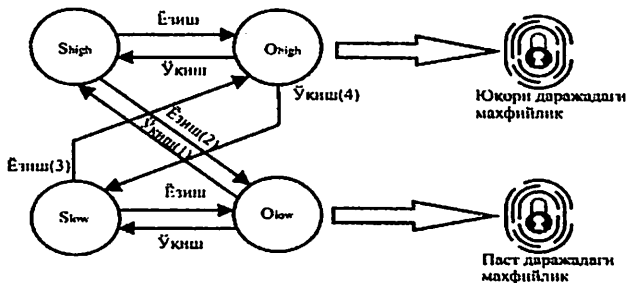
**4.1-расм.** Маълумотларнинг хавфсизлик даражасини рухсатсиз пасайтиришдан ҳимоялаш схемаси

Турли хил махфийлик даражасига эга маълумотлар турли қурилмалар ва объектлардан фойдаланган ҳолда ҳар хил режимларда қайта ишланади.

#### **4.3. ИКТда фойдаланишни бошқаришнинг математик моделини ишлаб чиқиш**

ИКТда ахборот ҳимояланганлигини оширишда яратилаётган файлларга мурожаат этишни бошқариш катта аҳамиятга эга. 4.2-расмда ахборотга чекловсиз мурожаат қилишда фойдаланишни бошқариш модели таклиф қилинган [34, 35]. Таклиф этилаётган модел махфийлик даражаси юқори ва махфийлик даражаси паст бўлган маълумотлар ўртасидаги маълумот алмашинуви жараёни орқали ахборот оқимини кўриш имконини беради.

Моделнинг доимий ишлаши, унинг ишончлилиги юқори бўлиши ва тизим ичида барқарор ишлаши учун бир қанча омиллар мажмуи таъсир қилади.



4.2-расм. Ахборотга чекловсиз мурожаат қилишда фойдаланишни бошқариш модели

Ахборотлаштириш объектига таъсир кўрсатадиган барча омилларнинг хилма-хилиги уларни икки тоифага бирлаштиради: ички ва ташқи омиллар [22].

$$F = \overline{F}_{\text{ички}} \cap \overline{F}_{\text{ташқи}} \quad (4.2)$$

бу ерда  $F_{\text{ички}}$  – ички омиллар тўплами ва  $F_{\text{ташқи}}$  – ташқи омиллар тўплами.

Тизимга таъсир этувчи омилларнинг мослашувчанлиги ва омиллар рўйхатини кенгайтириш имкониятини 4.1-жадвалда кўриб чиқамиз.

4.1-жадвал

Ахборот оқимининг рақамига қараб моделга таъсир этувчи омиллар мажмуи

Умумий омиллар		$F_{\text{№1}}$	$F_{\text{№2}}$	$F_{\text{№3}}$	$F_{\text{№4}}$
$F_{\text{ички}}$	$F_{\text{ташқи}}$	$F_{1,1}$	$F_{2,1}$	$F_{3,1}$	$F_{4,1}$
$F_1$	$F_2$	$F_{1,2}$	$F_{2,2}$	$F_{3,2}$	$F_{4,2}$
$F_3$	$F_4$	$F_{1,3}$	$F_{2,3}$	$F_{3,3}$	$F_{4,3}$
$F_5$	$F_6$	$F_{1,4}$	$F_{2,4}$	$F_{3,4}$	$F_{4,4}$
$F_7$	$F_8$	$F_{1,5}$	$F_{2,5}$	$F_{3,5}$	$F_{4,5}$
...	...	...	...	...	...
$F_K$	$F_G$	$F_{1,N}$	$F_{2,M}$	$F_{3,L}$	$F_{4,Q}$

4.1-жадвалда омиллар тоифалари 4.2-расмда тартиб рақам бўйича берилган ахборот оқимларига ажратилган. Агар  $S$  субъекти  $O$  объектини ўқиш (*read*) ҳуқуқи амалга оширилса, унда ахборот оқими  $O$  дан  $S$  ўтади ва ахборот оқимининг тартиб рақами №1 бўлади. Агар  $S$  субъекти  $O$  объектига ёзиш (*write*) ҳуқуқи амалга оширилса, унда ахборот оқими  $O$  дан  $S$  ўтади ва ахборот оқимининг тартиб рақами №2 бўлади. Худди шу тарзда №3 ва №4 рақамли ахборот оқимларида амалга оширилади. Фойдаланиш даврини яқунланиши бу ўзидан мураккаб ахборот оқимини ташкил этади.

Ахборот оқимига боғлиқ ҳолда умумий маънода кўплаб омилларни қуйидаги 4.3 ифода билан кўрсатиш мумкин:

$$F = \overline{F_{\text{ички}}} \cap \overline{F_{\text{ташқи}}} \cap \overline{F_{\text{№1}}} \cap \overline{F_{\text{№2}}} \cap \overline{F_{\text{№3}}} \cap \overline{F_{\text{№4}}} \cap \dots, \quad (4.3)$$

Бу ерда,

$$F_{\text{ички}} = \left\{ \frac{F_1 + F_K}{2} K \right\} \quad (4.4)$$

$$F_{\text{ташқи}} = \left\{ \frac{F_2 + F_G}{2} G \right\} \quad (4.5)$$

$$F_{\text{№1}} = \left\{ \frac{F_{1.1} + F_{1.N}}{2} N \right\} \quad (4.6)$$

$$F_{\text{№2}} = \left\{ \frac{F_{2.1} + F_{2.M}}{2} M \right\} \quad (4.7)$$

$$F_{\text{№3}} = \left\{ \frac{F_{3.1} + F_{3.L}}{2} L \right\} \quad (4.8)$$

$$F_{\text{№4}} = \left\{ \frac{F_{4.1} + F_{4.Q}}{2} Q \right\} \quad (4.9)$$

Агар керак бўлса, омиллар гуруҳлари мажмуи тўлдирилиши мумкин ва бу моделнинг асосий ғоясига таъсир қилмайди. Бунинг натижасида моделни такомиллаштириш ва ривожлантириш имконияти пайдо бўлади. Тадқиқот предметини яхшироқ тушуниш учун омилларнинг таъсирини юқорида кўрилган

4.4-4.9 гача бўлган олтита ифода орқали бир нечта омилларнинг гуруҳидан келиб чиққан ҳолда аниқ мисолда кўриб чиқамиз.

1. Юқори ваколат даражасига эга субъект  $S_{high}$  махфийлик даражаси паст  $O_{low}$  объектни ўқиш.

Ушбу гуруҳ омиллари мутлақо ўзига хос хусусиятга эга, чунки таклиф қилинаётган моделнинг хавфсизлик тизими, агар улар 4.1-жадвал асосида 1 чи тартиб рақамли маълумотлар оқимида субъект ва объект ўзаро таъсирлашганда юзага келса, уларга таъсир қилади. Шу асосида кўргазмали бўлиши учун бир нечта омилларни кўриб чиқамиз:

$F_{1.1}$  — файлни юқори махфийлик даражасидан паст махфийлик даражасига нусхалаш;

$F_{1.2}$  — вирусларни аниқлаш;

2. Юқори ваколат даражасига эга субъект  $S_{high}$  махфийлик даражаси паст  $O_{low}$  объектга ёзиш.

$F_{2.1}$  — ахборотни рухсатсиз ўзгартириш;

$F_{2.2}$  — вирусларни аниқлаш, антивирус дастурларини ўчиб қолиши/ ишдан чиқиши;

3. Паст ваколат даражасига эга субъект  $S_{high}$  махфийлик даражаси юқори  $O_{low}$  объектга ёзиш.

$F_{3.1}$  — ахборотни рухсатсиз ўзгартириш;

$F_{3.2}$  — вирусларни аниқлаш, антивирус дастурларини ўчиб қолиши/ ишдан чиқиши;

4. Паст ваколат даражасига эга субъект  $S_{high}$  махфийлик даражаси юқори  $O_{low}$  объектни ўқиш.

$F_{4.1}$  — вирусларни аниқлаш;

$F_{4.2}$  — химояланаётган ахборотдан рухсатсиз фойдаланиш (ахборотдан рухсатсиз фойдаланишга уриниш), бунда фойдаланиш ҳуқуқига эга бўлмаган фойдаланувчи;

$F_{4.3}$  — файлни пастки даражадан юқори даражага нусхалаш;

Умумий гуруҳ омилларида барча ахборот оқимларининг ўзаро таъсири ҳисобга олинади:

$F_1$  — компьютер техникасининг нотўғри ишлаши;

$F_2$  — компьютерда ахборот хавфсизлиги сиёсатига мос келмайдиган тақиқланган дастурлардан фойдаланиш;

$F_3$  — электр таъминотидаги носозликлар, узилишлар ва авариялар;

$F_4$  — ахборотни рухсатсиз нусхалаш;

$F_5$  — рўйхатдан ўтмаган ахборот элитувчига маълумотни нусхалаш;

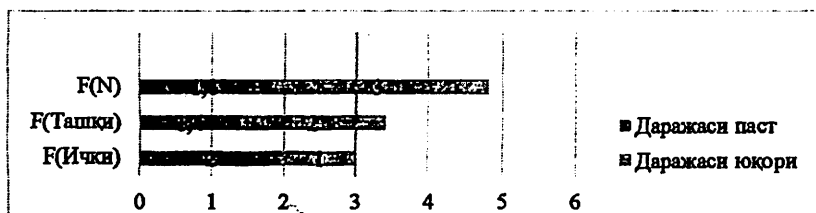
$F_6$  — техник тизимдан фойдаланишда хатоликлар, дастурий воситалар ва ахборот хавфсизлиги воситалари ва тизимларида носозликлар;

$F_7$  — дастурнинг ишлашига ўзгартиришлар киритиш;

$F_8$  — ахборотни ҳимоя қилиш талабларига риоя қилмаслик;

$F_9$  — ҳимояланган ахборотдан фойдаланиш ҳуқуқига эга бўлмаган шахсларга маълумотни ошкор қилиш.

4.3-расмда юқоридаги омиллар асосида ахборот даражаларини аниқлашнинг диаграммаси келтирилган.



4.3-расм. Ахборот даражаларини аниқлашнинг диаграммаси

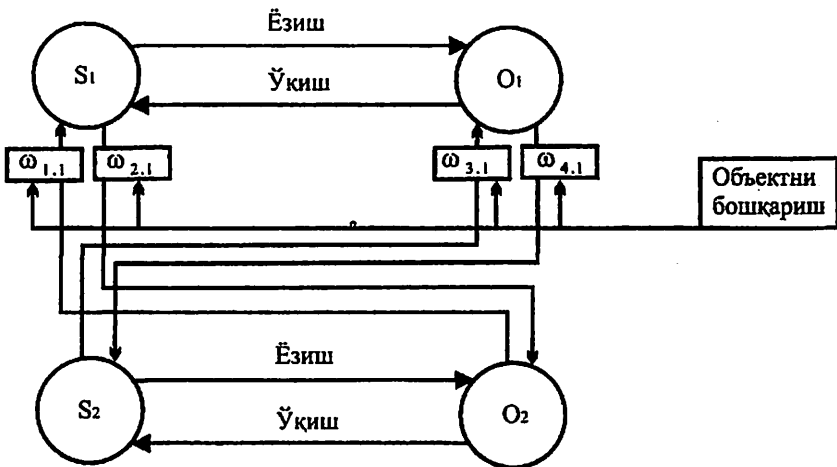
Юқорида келтирилган омилларнинг таклиф этилаётган хавфсизлик моделининг ишлаш сиёсатига таъсиридан келиб чиқиб, ахборот оқимининг тартиб рақамига асосланган ҳолда,  $S$  субъектларнинг  $O$  объектлар билан ўзаро муносабатини куйидаги ифода орқали тасвирлашимиз мумкин. Шундай қилиб, биринчи оқим субъектлари ва объектларининг ўзаро таъсири бинар функция орқали аниқланади, бунда натижа сифатида ноль ёки бир қиймат қабул қилади:

$$\omega_{1.1}(F) = \overline{F_1 \parallel F_2 \parallel F_3 \parallel F_4 \parallel F_5 \parallel F_6 \parallel F_7 \parallel F_8 \parallel F_9 \parallel F_{1.1} \parallel F_{1.2}} \quad (4.10)$$

4.10 бинар функциясининг мантикий кўпайтмаси, биринчи ахборот оқимининг қийматини кўрсатиб берилади, натижада иккита мумкин бўлган қийматлардан биттаси берилади:

- Агар тизимнинг ишлаши вақтида ҳеч бўлмаганда битта омил мавжуд бўлса, функциянинг умумий қиймати бирга тенг бўлади. Бу эса бошқарув объектига 1чи тартиб рақамли ахборот оқимини блокировка қилиш учун буйруқ беради (4.4-расм).

- Агар тизимнинг ишлаши вақтида бинар функциянинг қиймати нолга тенг бўлса, у ҳолда тизимнинг хавфсизлик сиёсатига таъсир этадиган омилларнинг йўқлигини ва ушбу ахборот оқимида ахборот алмашинуви очиқ ва нормал режимда ишлаётлигини билдиради.



4.4-расм. Бошқариш объекти ва бинар функцияларга асосланган фойдаланишни бошқариш модели

Иккинчи ахборот оқими субъектлари ва объектларининг ўзаро таъсирини қуйидагича ифодалаймиз:



$$\omega_{2,1}(F) = \overline{F_1 \parallel F_2 \parallel F_3 \parallel F_4 \parallel F_5 \parallel F_6 \parallel F_7 \parallel F_8 \parallel F_9 \parallel F_{2,1} \parallel F_{2,2}} \quad (4.11)$$

Ушбу ифодада тизимга таъсир кўрсатадиган умумий омиллардан ташқари, иккинчи ахборот оқимига хос бўлган омиллар мавжуд бўлиб, уларнинг мавжудлиги иккинчи ахборот оқимида ахборот алмашинувини блокировка қилади [36].

Учинчи ахборот оқими субъектлари ва объектларининг ўзаро таъсирининг бинар функция қуйидагича ифодалаймиз:

$$\omega_{3,1}(F) = \overline{F_1 \parallel F_2 \parallel F_3 \parallel F_4 \parallel F_5 \parallel F_6 \parallel F_7 \parallel F_8 \parallel F_9 \parallel F_{3,1} \parallel F_{3,2}} \quad (4.12)$$

Сўнги тўртинчи ахборот оқими субъектлари ва объектларининг ўзаро таъсирини қуйидагича ифодалаймиз:

$$\omega_{4,1}(F) = \overline{F_1 \parallel F_2 \parallel F_3 \parallel F_4 \parallel F_5 \parallel F_6 \parallel F_7 \parallel F_8 \parallel F_9 \parallel F_{4,1} \parallel F_{4,2}} \quad (4.13)$$

Ушбу 4.10-4.13 ифодалар биринчи ва иккинчи даражадаги субъектлар ва объектлар ўртасидаги муносабатни акс эттиради, моделга нисбатан буни 4.4-расмда кўришимиз мумкин. Бундай даражаларнинг сони чексиз бўлиши мумкин. Масалан, уларнинг сони  $i$  — та бўлсин. Унда юқоридаги субъектлар ва объектларнинг ўзаро таъсирини ифодаловчи функциялар бирдан то тўртгача бўлган ахборот оқимларининг кўриниши қуйидагича шаклланади:

$$\omega_{1,i-1}(F) = \overline{(F_1 \parallel F_2 \parallel F_3 \parallel \dots \parallel F_K \parallel F_G)} \& \overline{(F_{1,1} \parallel F_{1,2} \parallel \dots \parallel F_{1,N})}; \quad (4.14)$$

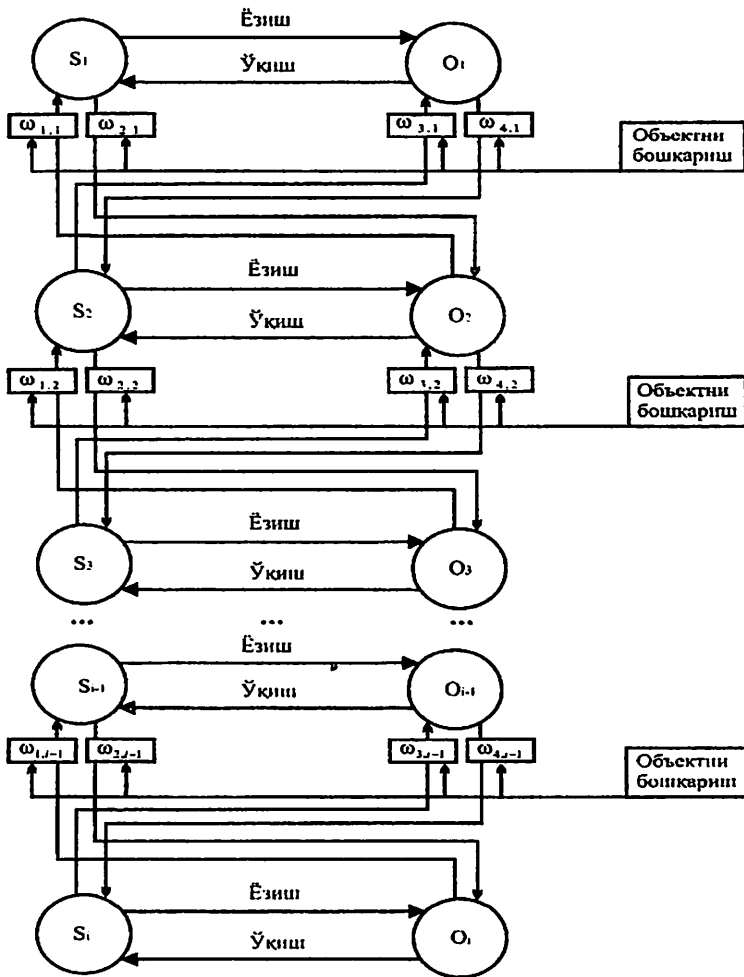
$$\omega_{2,i-1}(F) = \overline{(F_1 \parallel F_2 \parallel F_3 \parallel \dots \parallel F_K \parallel F_G)} \& \overline{(F_{1,1} \parallel F_{1,2} \parallel \dots \parallel F_{1,N})}; \quad (4.15)$$

$$\omega_{3,i-1}(F) = \overline{(F_1 \parallel F_2 \parallel F_3 \parallel \dots \parallel F_K \parallel F_G)} \& \overline{(F_{1,1} \parallel F_{1,2} \parallel \dots \parallel F_{1,N})}; \quad (4.16)$$

$$\omega_{4,i-1}(F) = \overline{(F_1 \parallel F_2 \parallel F_3 \parallel \dots \parallel F_K \parallel F_G)} \& \overline{(F_{1,1} \parallel F_{1,2} \parallel \dots \parallel F_{1,N})}; \quad (4.17)$$

4.14-4.17 ифодаларга асосланиб, омиллар чексиз тўпламга эга бўлиши мумкин деган хулосага келишимиз мумкин.

Биринчи навбатда, омилларни тавсифлашга ва комплекс тизим хавфсизлигига таъсир этувчи омилларни аниқлашга маълум бир вақт кетади.

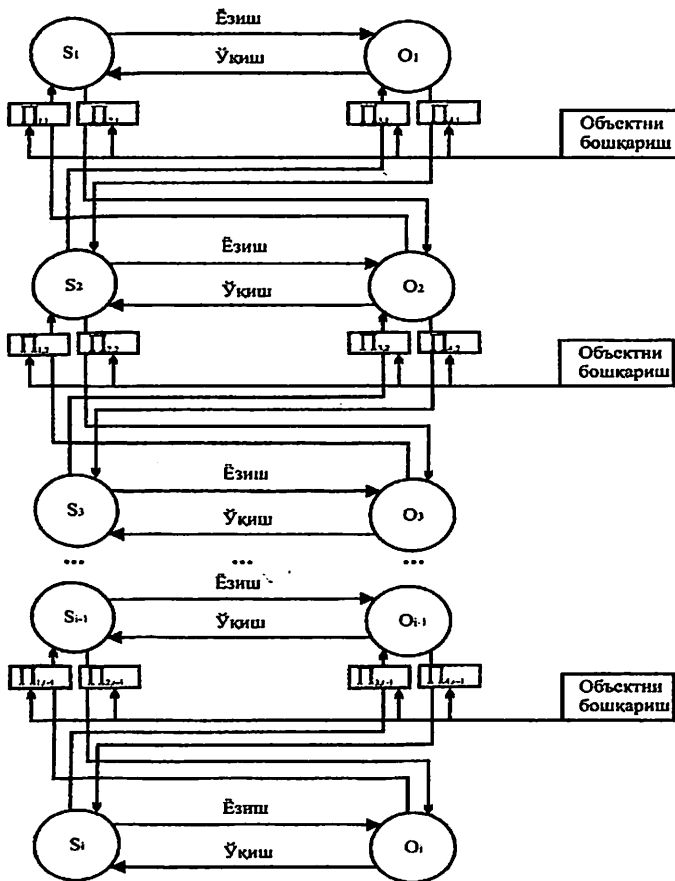


4.5-расм. Бошқариш объектига асосланган фойдаланишни бошқариш модели

Шундай қилиб, 4.5-расмда субъект ва объектларнинг ҳар кейинги махфий ахборотдан фойдаланиш ҳуқуқи олдинги субъект ва объектларнинг фойдаланиш ҳуқуқи даражасидан паст бўлиши кўрсатилган:

$$S_1 > S_2 \dots S_{i-1} > S_i;$$

$$O_1 > O_2 \dots O_{i-1} > O_i;$$



4.6-расм.  $i$  – ўлчовли шаклда эксперт қоидаларини ҳисобга олган ҳолда функцияларга асосланган фойдаланишни бошқариш модели

4.10-4.13 ёки 4.14-4.17 бинар функцияларни ечиш орқали олинган натижалар ахборотдан фойдаланиш бошқариш моделининг ишлашини кейинги босқичига ўтади.

Бошқариш объекти 4.10-4.13 функцияларидан олинган натижаларни қуйидаги шаклда бошқариш тизимига ўтказади:

$$\begin{aligned}
 F_{N_{\text{э.1}}}! &= \begin{cases} \omega_{1,1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{1,1}, F_0 = 1(t) \end{cases} \\
 F_{N_{\text{э.2}}}! &= \begin{cases} \omega_{2,1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{2,1}, F_0 = 1(t) \end{cases} \\
 F_{N_{\text{э.3}}}! &= \begin{cases} \omega_{3,1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{3,1}, F_0 = 1(t) \end{cases} \\
 F_{N_{\text{э.4}}}! &= \begin{cases} \omega_{4,1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{4,1}, F_0 = 1(t) \end{cases}
 \end{aligned} \tag{4.18}$$

4.14-4.17 ифодаларидан олинган бинар функцияларнинг натижаларини таққослаш учун тизим қуйидаги шаклда ифодаланилади:

$$\begin{aligned}
 F_{N_{\text{э.1},i-1}}! &= \begin{cases} \omega_{1,i-1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{1,i-1}, F_0 = 1(t) \end{cases} \\
 F_{N_{\text{э.2},i-1}}! &= \begin{cases} \omega_{2,i-1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{2,i-1}, F_0 = 1(t) \end{cases} \\
 F_{N_{\text{э.3},i-1}}! &= \begin{cases} \omega_{3,i-1}, F_0 = \text{а. қ} \\ 0, F_0 = 0(f) \\ \omega_{3,i-1}, F_0 = 1(t) \end{cases}
 \end{aligned} \tag{4.19}$$

$$F_{\text{№}4,i-1}! = \begin{cases} \omega_{4,i-1}, F_0 = \text{а. к.} \\ 0, F_0 = 0(f) \\ \omega_{4,i-1}, F_0 = 1(t) \end{cases}$$

бу ерда  $F_0 = \{f, t, \text{а. к.}\}$

бу ерда а.к. — аҳамиятсиз қиймат. Яъни, мисол учун, алоҳида омиллар мавжуд бўлиб, бу омилларнинг вужудга келиши комплекс ҳимоя тизимининг хавфсизлик сиёсатига катта таъсир ўтказмайди. Бундай омил ёки омиллар гуруҳи аҳамиятсиз қийматга эга бўлади;

бу ерда  $f = 0$ , яъни функция  $F_{\text{№}1}!$  нолга тенг қиймат қабул қилади, агар  $\omega$  бинар функция нолга тенг қийматни ўзлаштиради, бунинг учун тизимга таъсир этувчи омиллар бўлмаслиги керак;

бу ерда  $t = 1$ , яъни функция  $F_{\text{№}1}!$  бирга тенг қиймат қабул қилади, агар  $\omega$  бинар функция бирга тенг қийматни ўзлаштиради, бунинг учун тизимга таъсир этувчи камида битта омил бўлиши керак.

Шундай қилиб, 4.10-4.13 функцияларнинг қиймати таҳлил қилиш ва натижаларни таққослаш тизимига тушганда, яъни бошқариш объектида якуний босқич сифатида олинган маълумотлар таққосланади ва кейин натижада эксперт хулосаси шаклида тегишли қийматларни оламиз. Агар  $F_{\text{№}1}!$  функция  $\omega_{1.1} = 0$  қиймат қабул қилса, у ҳолда  $F_{\text{№}1}!$  натижа сифатида false қийматни ўзлаштиради, бунда тизим нормал режимда ишлаётлигини билдиради. Агар  $F_{\text{№}1}!$  функция  $\omega_{1.1} = 1$  қиймат қабул қилса, у ҳолда  $F_{\text{№}1}!$  натижа сифатида true қийматни ўзлаштиради, бунда тизимга номақбул омил таъсир этаётганини англатади, натижада биринчи тартиб рақамли ахборот оқими блокланади. Бунда юқори ваколат даражасига эга субъект  $S_{high}$  махфийлик даражаси паст  $O_{low}$  объектни ўқиш ҳуқуқи номақбул омил олиб ташланмагунича мавжуд бўлмайди.

Мавжуд Белл-Лападуланинг қатъий фойдаланишни бошқариш моделидан [13, 28] фарқли равишда таклиф этилган моделда омиллар гуруҳлари мажмуи тўлдирилиб борилиши мумкин ва бунинг натижасида моделни такомиллаштириш ва ривожлантириш имконияти пайдо бўлади. Моделнинг асосий афзаллиги бу мослашувчанлик бўлиб, таъсир этувчи омиллар асосида субъектлар ва объектлар орасидаги ахборот оқимларини блоклаш имкониятини яратади.

#### **4.4. Фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини ошириш моделини такомиллаштириш**

Ахборот ҳимояланганлигини ошириш моделини такомиллаштиришда ахборотни кластерлаш усулидан фойдаланилди [37, 38]. Бу усул таснифлашни ҳисоблаш процедураларини тартибларини кетма-кет бажарилишига имкон беради. У барча ҳимоя объектларини қамраб олади, яъни ахборотдан фойдаланишда ахборот тизимининг белгиланган хавфсизлик талабларини таъминлайди ва тизимда ҳар хил махфийлик даражасидаги ахборот ресурсларидан фойдаланишда йўқотишларсиз ва номувофиқликларсиз ишлаш мета тавсифи талабларини қондиради. Ахборотни ҳимоя қилишнинг барча объектлари маълумотларни тақдим этиш, сақлаш ва қайта ишлаш усулларида қатъий назар фойдаланувчиларнинг ахборотга бўлган эҳтиёжларининг тўплами кўринишида расмийлаштириш мумкин.

Тавсия этилаётган ёндашувда ахборотни моҳиятини босқичма-босқич таснифлаш орқали амалга оширувчи ҳимоя объектлари дарахт кўринишида қурилган, бунда иерархия даражалари ҳимоя қилиш субъектларини ўзаро боғлиқлигини акс этирувчи ҳимоя объектларининг эгалари мақомига эга бўлади. Ҳимоя қилиш объектларини дарахт тузилишида тасвирлаш субъектларнинг объектларга эгалик ҳуқуқи иерархияси орқали амалга оширилади. Ҳимоялаш объектлари ўртасидаги

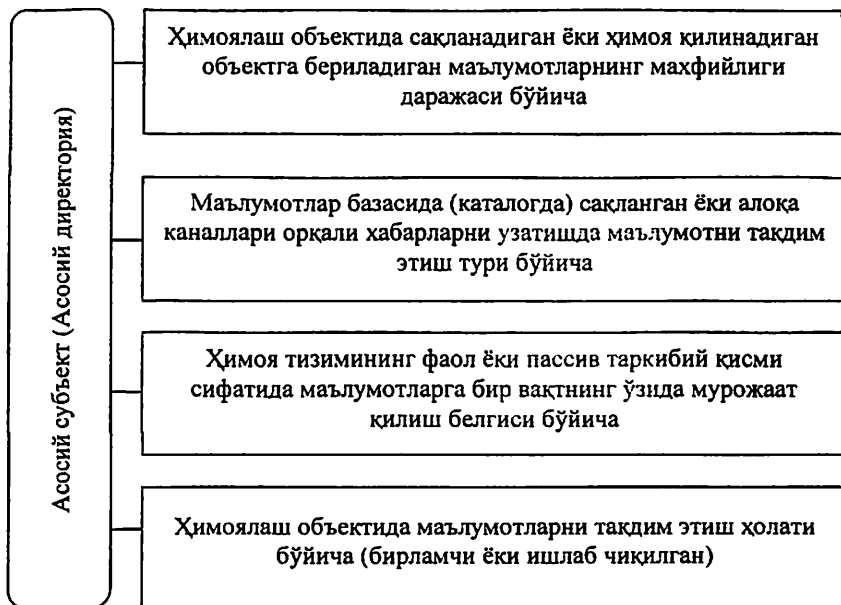
иерархик боғлиқлик маълумотларнинг махфийлик даражалари иерархияси ва объектларнинг эгалари бўлган субъектларни таснифлаш иерархияси орқали намоён бўлади. Объектлар дарахтининг танаси объектларга эгалик қиладиган субъектларнинг маълумотлардан фойдаланиш ҳуқуқлари даражасига қараб қурилади ва объектлар ўртасидаги алоқа ҳимоя объектларида сақланадиган ёки қайта ишланадиган маълумотларнинг махфийлигига қараб ўрнатилади.

Тармоқланиш субъектлар томонидан асосий каталогда янги объектларни яратилиши натижасида юзага келади. Бу жараён вакил объектларни яратиш деб аталади. Бундан ташқари, дарахтлар иерархиясининг ҳар бир сатҳида (4.7-расм) тўрт тоифага асосан ҳимоялаш объектларини батафсил таснифлаш амалга оширилади.

4.8-расмда фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини оширишнинг концептуал модели такомиллаштирилди.

Фойдаланувчининг предмет соҳасининг бошланғич ҳолатида, ажратилган ахборот объектлари структуравий ахборот элементлари сифатида тақдим этилади. Фойдаланувчиларнинг ахборотга бўлган талаблари маълумот сўровлари шаклида тақдим этилади. Тадқиқот соҳаси бўйича таҳлил натижалари ва маълумотлар базасини яратиш ва унинг хавфсизлигини таъминлашда хавфсизлик сиёсатининг асосий параметрларини аниқлашда ва асосий йўналишларда ҳимоя қилиш методлари тўплами сифатида куйидагилар кенг қўлланилади: фойдаланишни бошқариш, криптография, маълумотлар базасини тузилишини лойиҳалаш ва хавфсизликни бошқариш. Маълумотлар базаси ва унинг инфратузилмаси ресурслари устида бажариладиган амалларга хавфсизлик чекловлари ўрнатилади, фойдаланувчиларнинг барча амалий вазифалари аниқланади, бу эса барча хавфсизлик чораларини амалга ошириш орқали бутун ахборот тизимининг хавфсизлик даражасини таъминланади. Яратилаётган хавфсизлик тизимларида хавфсизлик

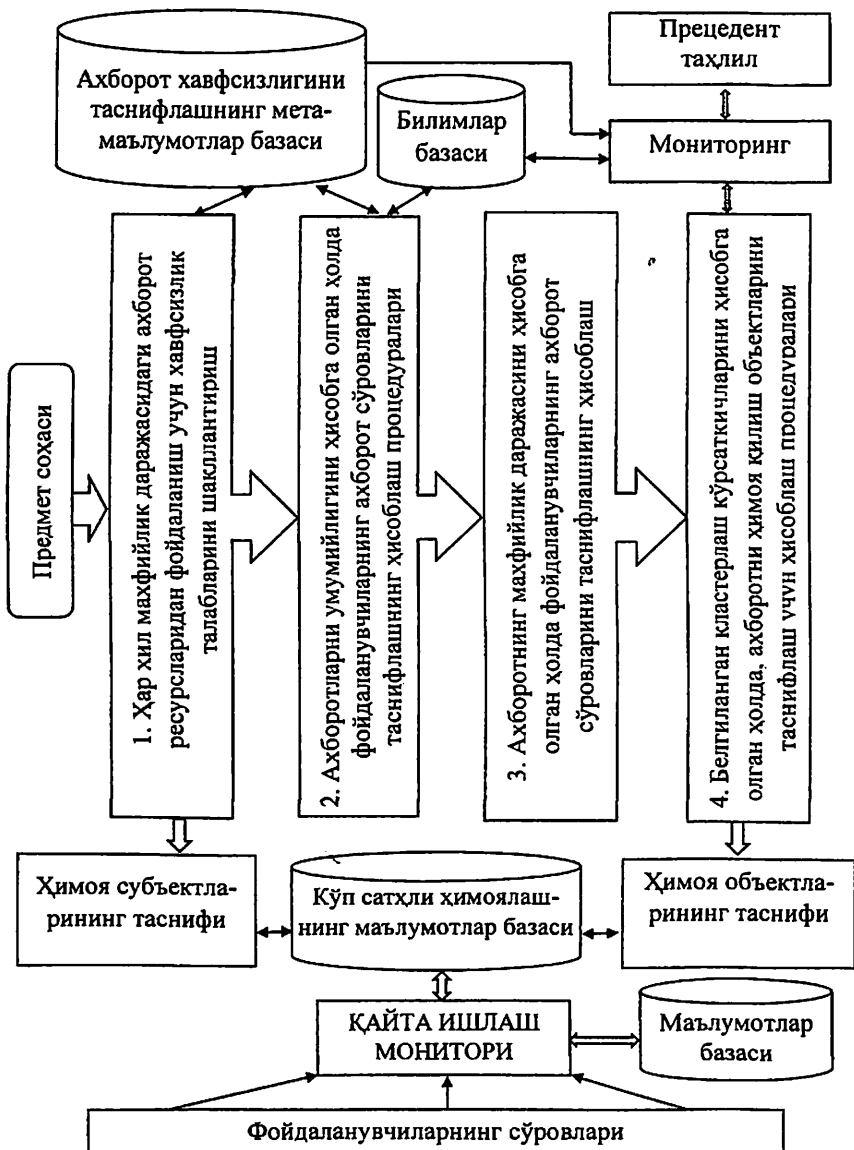
инфратузилмасини ва умуман тизимнинг ишлашини таъминлаш учун хавфсизлик талаблари бажарилиши қайд этилади.



4.7-расм. Иерархия даражасида ҳимоя қилиш объектларининг батафсил таснифи

Ахборотни ҳимоя қилиш учун етарли даражада воситалар ва ресурсларни ажратмаслик оқибатида келиб чиқиши мумкин бўлган йўқотишларни олдиндан ҳисоблаш керак бўлади. Фойдаланишни назорат қилиш тизими ва криптографик тизимлар механизмини танлашга асосланади. Хавфсизликнинг асосий талабларига мувофиқ хавфсизлик синфи бўйича ахборот-ҳисоблаш тизимини яратиш усулларига талаблар шакллантирилади. Ушбу асосий талаблар ҳимояланганликни тегишли синфи учун амалга ошириладиган хавфсизлик кўрсаткичлари орқали аниқланади.





**4.8-расм.** Фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот химояланганлигини оширишнинг концептуал модели

Кейин семантик ва инфор­мацион уланишларни ҳисобга олган ҳолда, бир-бири билан максимал ва минимал даражада боғлиқ бўлган маълумотлар кластерлари шакллантирилади [38]. Алоҳида фойдаланувчиларнинг предмет соҳаларининг умумийлик даражасининг миқдорий характеристикасини олиш учун автоматик таснифлаш назариясида қабул қилинган ўхшашлик ўлчови тушунчасидан фойдаланамиз [39]. Фойдаланувчиларнинг предмет соҳасини ахборот умумийлигини чегаравий қий­матини танлаш масаласи, ахборот алмашинуви ва ишлаб чиқарилаётган бошқарув тизимининг ўзига хос турини ҳисобга олган ҳолда алоҳида ҳал қилинади. Сўнгра, ҳар бир кластер ичида ҳар бир ахборот элементининг аҳамияти таҳлил қилинади ва таҳлил натижаларини ҳисобга олган ҳолда, энг яқин алоқада бўлган кластерлар ичида аниқланган аҳамият даражаларини муҳимлигига қараб бир нечта кластерларга бўлиш амалга оширилади.

Ахборот тўпламларини ҳимоя қилиш объектларининг яку­ний таснифини амалга ошириш учун интеллектуал процедура­лар ва билимлар базасидан фойдаланиб, иммунокомпьютеринг асосида мураккаб тизимларни комплекс баҳолаш учун ихтиёрий матрицаларни якка тартибда ажратиш усули орқали амалга оширилади [40].

Янги ҳисоблаш парадигмаси табиий иммун тизими формал механизмларига асосланган бўлиб, турли предмет соҳасида муайян амалий муаммоларни ечишда юқори самарадорлик, ишонччилик, мослашувчанлик ва ҳисоблаш тезлигига эришишга имкон беради [41, 42, 43]. Шу жумладан, ИКТ хавфсизлигини мониторинг қилиш ва маълумотларни ҳимоя қилишни таъмин­лаш вазифалари долзарб бўлган предмет соҳалари киради.

Имунокомпьютеринг ёндашув асосида таснифлаш ва клас­терлаш муаммоларини ҳал қилиш куйидаги вазифаларни бажа­ришни ўз ичига олади: эксперт орқали ўқитиш, мустақил ўрганиш, гуруҳлаш ва таснифлаш, ҳисоблаш натижаларини тимсоллар фазосида тақдим этиш.

Предмет соҳасининг дастлабки маълумотларга асосланиб, ўрганилаётган тизим тўғрисидаги фактографик маълумотларни ўз ичига олган маълумотлар базаси яратилади.

Билимлар базаси қуйидаги маълумотларни ўз ичига олади:

- янги билимларни олишга ва ўрганилаётган соҳанинг потенциал ҳолатини башорат қилишга имкон берадиган, кўриб чиқиладиган предмет соҳасида мавжуд бўлган қонуниятларини акс эттирувчи маълумотлар;

- маълумотлар базасининг таркиби ва мазмуни тўғрисидаги маълумотлар;

- алоқа воситалари ҳақидаги маълумотлар;

- билимларни ифодалаш ва қайта ишлаш усулларини белгилайдиган метабилимлар.

Билимлар базасига расмий маълумотлар ва ушбу предмет соҳаси экспертнинг билимлари, математик моделлар, иммунокомпьютеринг ҳисоблаш процедураларини амалга оширувчи алгоритмлари, гуруҳлаштириш натижалари ва автоматик таснифлаш, шунингдек, ҳисоблаш натижаларини талқин қилиш усуллари жойлаштирилади. Асосий ҳисоблаш процедуралари билимлар базасини шакллантиришга (эксперт орқали ўқитиш ва экспертсиз) ва автоматик таснифлашни амалга оширишга қаратилган. Бунда ҳисоблаш процедуралари иммунокомпьютеринг хуеусиятлари ва математик аппаратларига асосланган ҳолда амалга оширилади.

Ҳисоблашнинг интеллектуал процерадураларининг функционал мақсади хавфсизлик мониторинги орқали амалга оширилади, бу эса қуйидагини таъминлайди:

- ўқитиш – ўқув матрицаларини шакллантириш, бунда матрицалар ясси ёки OLAP-куб кўринишида нуқтали ёки интервал элементлардан ташкил топган бўлиши мумкин. Матрицаларни якка тартибда ажратиш усулидан фойдаланилади.

Прецедент таҳлилда ечимни қидириш аналогия (ўхшашлик) тушунчасига асосланади. Прецедент ва жорий ҳолат объектлар кўринишида ифодаланилади ва ушбу прецедентга тегишли

бўлган фактларни узатиш орқали ўхшашликлар топилади ва кўриб чиқиладиган инцидент бўйича хулосалар чиқарилади.

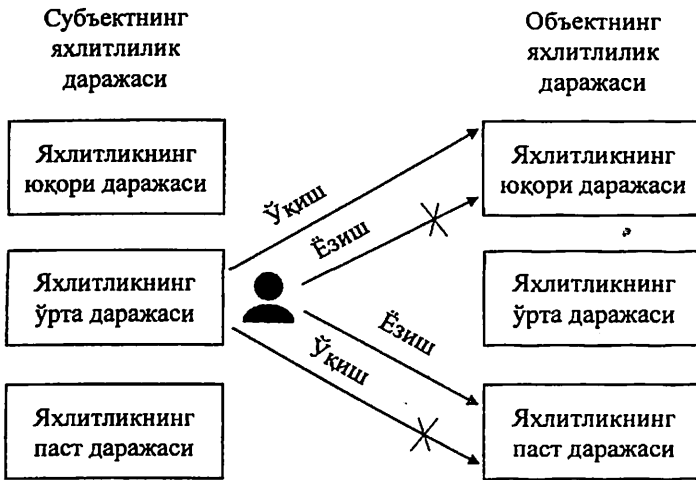
Мониторинг давомида мета маълумотларнинг базасида ҳимоялаш таснифи ва билимлар базаси асосида ахборот хавфсизлиги тизимида инцидентлар юзага келишини олдиндан тахмин қилиши керак. Шунингдек, уларни амалга оширишдан бўлган зарарни баҳолаши керак бўлади.

Ҳимояланган объектларни таҳлил қилиш ва таснифлаш учун такомиллаштирилган усул қайта ишланаётган маълумотларнинг махфийлигини ҳисобга олган ҳолда минимал даражада ўзаро боғланган кластерларни иерархик шакллантиришга имкон беради.

#### **4.5. Бибанинг яхлитлик модели**

Биба модели фойдаланишни бошқаришнинг формал модели ҳисобланади. Биба модели ахборотнинг яхлитлигини ҳимоялаш учун фойдаланилади [27].

Биба модели Белл-Лападула модели каби субъектлар ва объектларга асосланади, улар иерархик тарзда ташкил этилган даражаларга бўлинади. Белл-Лападула моделидан фарқли равишда Биба моделида маълумотлар махфийлиги даражасини ўрнига яхлитлик даражаси киритилади (4.9-расм). Объектнинг яхлитлик даражаси қанча юқори бўлса, унга кўп ишонч билдирилади ва бу объектнинг аниқ маълумот сақлаши даражаси эҳтимолиги юқори бўлади, шунингдек, бу объектдан фойдаланиш учун субъектларга фойдаланиш қоидалари қаттиқ назоратга олинади. Субъектнинг даражаси қанча юқори бўлса, унга ишонч даражаси юқори бўлади ва бу субъектга объектлардаги маълумотларни модификация (ўзгартириш) қилиш имконияти ишониб топширилади.



4.9-расм. Биба моделининг қоидалари

Биба моделида субъектларнинг объектларга ва субъектлардан фойдаланишнинг қуйидаги ҳолатлари мавжуд:

*modify* – субъектнинг объектни модификация (ўзгартириш) ҳуқуқи (Белл-Лападула моделида *write* ҳуқуқининг аналоги);

*invoke* – субъектнинг субъектга мурожаати (ёзиш);

*observe* – субъектнинг объектни ўқиш ҳуқуқи (Белл-Лападула моделида *read* ҳуқуқининг аналоги);

*execute* – бажариш ҳуқуқи;

Биба моделининг асосий элементлари қуйидагилар ҳисобланади:

*S* – субъектлар мажмуи;

*O* – объектлар мажмуи;

$(L, \leq)$  – яхлитлик даражалари панжараси, масалан:

$LI = \{I(\text{important}), VI(\text{very important}), C(\text{crucial})\}$ , бу ерда  $I < VI < C$ ;

$RI = \{modify, invoke, observe, execute\}$  фойдаланиш турлари ва фойдаланиш ҳуқуқи турлари мажмуи

$B = \{b \subseteq S \times O \times R\}$  – тизимда эҳтимолий кўплаб жорий фойдаланишлар мажмуи.

$(i_s, i_o, i_c) \in I = LI^S \times LI^O \times LI^S$  бу ерда  $(i_s, i_o, i_c)$  функциялар учталиги бўлиб, улар куйидагиларни амалга оширади:  $i_s: S \rightarrow LI$  субъектларнинг яхлитлик даражаси;  $i_o: O \rightarrow LI$  объектларнинг яхлитлик даражаси;  $i_c: S \rightarrow LI$  субъектларнинг жорий ҳолатининг яхлитлик даражаси; бунда ҳар бир  $s \in S$  учун  $i_c(s) \leq i_s(s)$  шарт бажарилади.

$V = B \times I$  – тизим ҳолатларининг мажмуи;

Биба моделида Белл-Лападуланинг классик модели каби субъектлар ва объектларнинг яхлитлик даражасини маъмураш масалалари таҳлил этилмайди.

Белл-Лападуланинг классик моделидаги хавфсизлик талабларидан фарқли равишда Биба моделида хавфсизлик талаблари динамик ҳисобланади ва уларни тавсифлашда тизимнинг жорий ва кейинги ҳолати элементлари куйидагича бўлади:

*Изоҳ 4.1.*  $(s, o, r) \in S \times O \times RI$  нинг фойдаланиш талаблари *low – watermark* [13, 27] сиёсати талабларига субъектлар учун  $i = (i_s, i_o, i_c) \in I$  га нисбатан мос келади, агар куйидаги талаблар бажарилса:

- $r = execute$ ;
- $r = modify$  ва  $i_s(s) \geq i_o(o)$ ;
- $r = invoke$ ,  $o \in S$  ва  $i_s(s) \geq i_c(o)$ ;
- $r = observe$  ва  $i'_c(s) = i_c(s) \otimes i_o(o)$  тизимнинг кейинги ҳолати учун фойдаланиш ҳуқуқини олиш, бу ерда  $\otimes$  –  $(LI, \leq)$

панжара элементларининг энг юқори пастки чегараси;  $i'_c(s)$  – субъектнинг жорий яхлитлик даражаси функцияси қиймати.

*Изоҳ 4.2.*  $(s, o, r) \in S \times O \times RI$  нинг фойдаланиш талаблари *low – watermark* [13, 27] сиёсати талабларига объектлар учун  $i = (i_s, i_o, i_c) \in I$  га нисбатан мос келади, агар куйидаги талаблар бажарилса:

- $r \in \{execute, invoke, observe\}$ ;
- $r = modify$  ва  $i'_o(o) = i_c(s) \otimes i_o(o)$  тизимнинг кейинги ҳолати учун фойдаланиш ҳуқуқини олиш, бу ерда  $i'_o(o)$  – объектнинг жорий яхлитлик даражаси функцияси қиймати.

Субъект ёки объектнинг яхлитлик даражасидаги функцияларини динамик ўзгариши *low – watermark* сиёсати қоидаларини такомиллаштиришни талаб қилиш мумкин. Масалан, агар тизимда субъект томонидан бир нечта сўровларни жўнатишга рухсат берилса, у ҳолда натижа сўровларнинг бажарилиш кетма-кетлиги боғлиқ бўлиши мумкин. Агар субъект бир вақтнинг ўзида *observe* ва *modify* сўровларини жўнатса, унда *observe* фойдаланиш ҳуқуқи субъектнинг яхлитлик даражасининг пасайишига олиб келиши мумкин, бундан келиб чиқадиги, *modify* фойдаланиш ҳуқуқини олишни имконсиз бўлади. Бундан ташқари, *modify* фойдаланиш ҳуқуқида объектнинг яхлитлик даражасини пасайиши, яхлитлик даражаси паст бўлган субъект томонидан юқори даражадаги яхлитликга эга маълумотни ўзгартиришга (модификация) олиб келиши мумкин.

*low – watermark* сиёсати қоидаларини такомиллаштириш усули сифатида  $(i_s, i_o, i_c)$  функцияларнинг қийматларини барча субъект ва объектлар тизимнинг ҳар қандай ҳолати учун ўзгаришсиз қолиш талабани бажариш ҳисобланади. Бу ҳолда  $i_s = i_c$  тенглик тўғри бўлади.

Изоҳ 4.3.  $(s, o, r) \in S \times O \times RI$  нинг фойдаланиш талаблари *low – watermark* сиёсати талабларига  $(i_s, i_o)$  функциянинг ўзгармас қийматларига нисбатан мос келади, агар қуйидаги талаблардан бири бажарилса:

- $r \in \{execute, observe\}$ ;
- $r = modify$  ва  $i_s(s) \leq i_o(o)$ ;
- $r = invoke, o \in S$  ва  $i_s(s) \geq i_s(o)$ ;

$(i_s, i_o)$  функциянинг ўзгармас қийматлари асосида *low – watermark* сиёсати талабларини бажарилиши яхлитлик даражаси паст субъектнинг яхлитлик даражаси юқори бўлган объектни ўзгартиришни (модификация) олдини олишни имконини беради. Бир вақтнинг ўзида *observe* фойдаланиш ҳуқуқига чекловларнинг йўқлиги яхлитлик даражаси паст субъектнинг яхлитлик даражаси юқори бўлган объектга маълумот оқимини амалга ошириш имконини беради. Бундай турдаги маълумот оқимини пайдо бўлиш хавфини бартараф этиш учун  $(i_s, i_o)$  функциянинг

ўзгармас қийматлари асосида *low – watermark* қатъий сиёсатидан фойдаланиш мақсадга мувофиқ ҳисобланади.

Изоҳ 4.4.  $(s, o, r) \in S \times O \times RI$  нинг фойдаланиш талаблари *low – watermark* қатъий сиёсати талабларига  $(i_s, i_o)$  функциянинг ўзгармас қийматларига нисбатан мос келади, агар қуйидаги талаблардан бири бажарилса:

- $r = execute$ ;
- $r = modify$  ва  $i_s(s) \geq i_o(o)$ ;
- $r = invoke, o \in S$  ва  $i_s(s) \geq i_s(o)$ ;
- $r = observe$  ва  $i_s(s) \leq i_o(o)$ ;

Биба моделида тизимнинг ҳар қандай ҳолати учун *low – watermark* сиёсати талабларини аниқлаш мумкин бўлади.



## У БОБ. РОЛЛАРГА АСОСЛАНГАН ФЙДАЛАНИШНИ БОШҚАРИШ МОДЕЛИ

### 5.1. Ролларга асосланган фойдаланишни бошқариш моделининг ташкил этувчилари

Ролларга асосланган фойдаланишни бошқариш модели (Role-based Access Control (RBAC)) [44, 45] субъектларнинг белгиланган фаолият тури билан боғлиқ хатти-ҳаракатлари ва мажбуриятларининг бирикмасига мувофиқ тизим субъектларининг объектлардан фойдаланишни назорат қилади. Бундай ваколатлар ўзи билан фойдаланишни чеклаш модели асосида ётадиган, субъектларнинг роли деб аталувчи семантик конструкцияларни тақдим этади. Ролларга асосланган фойдаланишни бошқариш модели дискрецион фойдаланишни бошқариш моделининг такомиллаштирилган варианты ҳисобланади ва роллар, аниқ шахсларга ўзларининг мажбуриятларини бажаришлари учун зарур бўлган даражада фойдаланишларга эга бўлишлари учун имкон беради.

Ролларга асосланган фойдаланишни бошқариш моделининг асосий элементлари қуйидагилар ҳисобланади:

$U$  — фойдаланувчилар мажмуи;

$R$  — роллар мажмуи;

$P$  — ИКТ объектларидан фойдаланиш ҳуқуқи мажмуи;

$S$  — фойдаланувчилар сессиясига фойдаланиш ҳуқуқи тўпламини киритадиган функциялар мажмуи;

$PA: R \rightarrow 2^P$  — ҳар бир рол учун фойдаланиш ҳуқуқи мажмуини киритадиган функция; бунда ҳар бир фойдаланиш ҳуқуқи  $p \in P$  учун  $p \in PA(r)$  каби бўлган рол  $r \in R$  мавжуд;

$UA: U \rightarrow 2^R$  — ҳар бир фойдаланувчи учун авторизация қилиниши мумкин бўлган кўплаб ролларни белгилайдиган функция;

$user: S \rightarrow U$  — унинг номидан активация қилинган ҳар бир фойдаланувчи сессияси учун киритадиган функция;

$roles: S \rightarrow 2^R$  — мазкур сессияда авторизациядан ўтган фойдаланувчи учун роллар мажмуи киритадиган функция, бунда

ҳар бир вақт мобайнида ҳар бир  $S \in s$  сессия учун  $Roles(S) \subseteq UA(user(s))$  шarti бажарилади.

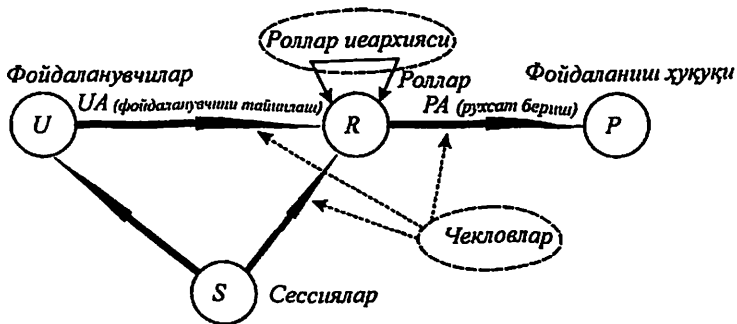
Таъкидлаб ўтиш лозим, шундай роллар учрайдики, унда ҳеч қандай фойдаланувчи авторизация қилинмаган бўлиши мумкин.

Ролларга асосланган фойдаланишни бошқаришда  $U, R, P$  мажмуалар ва  $PA, UA$  функциялар вақтнинг ўтиши билан ўзгармайди.

Ушбу сессияда кўплаб ролларга авторизация қилган фойдаланувчиларни фақатгина фойдаланувчининг ўзи ўзгартириши мумкин. Бунда бир сессия бошқа сессияни активлаштириш хусусияти мавжуд эмас. Барча сессиялар фойдаланувчи томонидан активлаштирилади.

Ролларга асосланган фойдаланишни бошқариш модели тизимдаги субъектларни улар томонидан бажариладиган алоҳида вазифаларга нисбатан фойдаланишни чеклаш имконини беради ва бунда тенг қийматли объектларга фойдаланишни чеклаш учун инструментларни тақдим этади. Бундан ташқари, фойдаланувчининг фойдаланиш ҳуқуқи доимий ҳисобланмайди ва фойдаланувчининг қайси рол билан авторизация қилинганлигига қараб ўзгариши мумкин [46].

Ролларга асосланган фойдаланишни бошқариш моделининг элементларининг тузилиши 5.1-расмда кўрсатилган.



5.1- расм. Ролларга асосланган фойдаланишни бошқариш моделининг элементларининг тузилиши

## 5.2. Ролларга асосланган фойдаланишни бошқаришни маъмурлаш модели

Ролларга асосланган фойдаланишни бошқаришнинг таянч моделида  $U, R, P$  мажмуалар ва  $PA, UA$  функциялар вақтнинг ўтиши билан ўзгармайди, ёки хавфсизлик офицери – ягона роли мавжуд бўлади ва у берилган мажмуа ва функцияларни ўзгартириш имконига эга бўлади [22, 47]. Бир вақтнинг ўзида юзлаб ва минглаб фойдаланувчилар ишлаши мумкин бўлган КТларда роллар структураси ва фойдаланиш ҳуқуқлари жуда мураккаб бўлиши мумкин. Бундай тизимларда маъмурлаш жуда муҳим аҳамиятга эга ҳисобланади ва масалани ечишда ролларга асосланган фойдаланишни бошқаришнинг таянч моделига асосланган маъмурлаш моделидан фойдаланилади.

Таянч моделининг элементларига кўшимча сифатида ролларга асосланган фойдаланишни бошқаришни маъмурлаш моделида қуйидагилар кўрилади:

$AR$  – маъмурлаш роллари мажмуи ( $AR \cap R = \emptyset$ );

$AP$  – маъмурлашда фойдаланиш ҳуқуқи мажмуи ( $AP \cap P = \emptyset$ );

$APA: AR \rightarrow 2^{AP}$  – маъмурлаш ролларига маъмурлашда фойдаланиш ҳуқуқи мажмуини киритадиган функция. Бунда ҳар бир  $p \in P$  фойдаланиш ҳуқуқига  $r \in AR$  рол мавжуд ва  $p \in APA(r)$ .

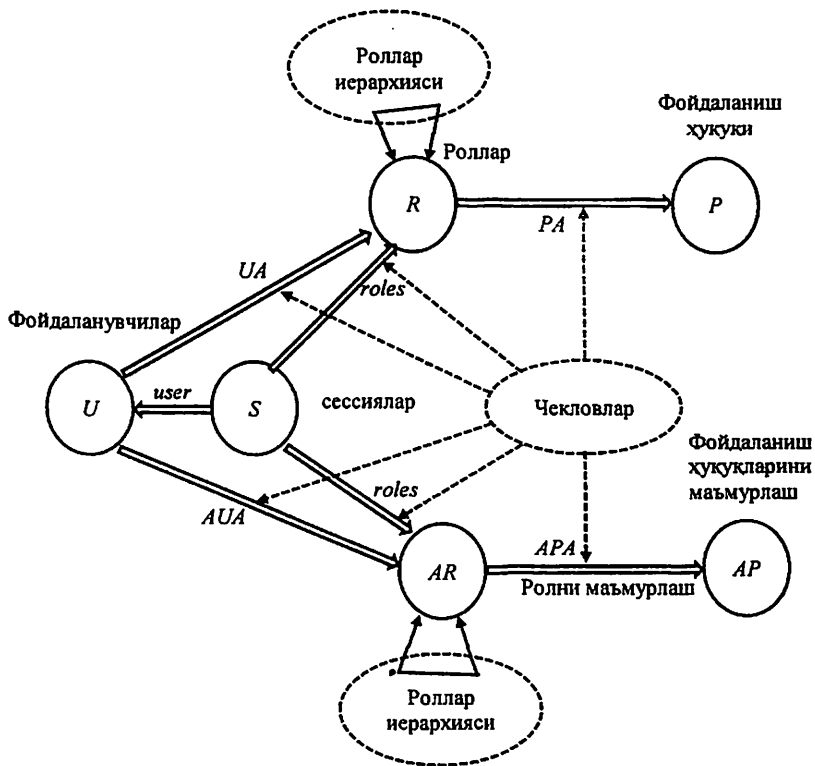
$AUA: AR \rightarrow 2^{AP}$  – авторизациядан ўтган ҳар бир фойдаланувчига маъмурлаш роллари мажмуини киритадиган функция.

Бундан ташқари функция қайта аниқланади:

$roles: S \rightarrow 2^R \cup 2^{AR}$  – мазкур сессияда авторизациядан ўтган фойдаланувчи учун роллар мажмуи киритадиган функция, бунда ҳар бир вақт мобайнида ҳар бир  $S \in s$  сессия учун  $Roles(S) \subseteq UA(user(s)) \cup AUA(user(s))$  шarti бажарилади.

Таянч модел каби ролларга асосланган фойдаланишни бошқаришни маъмурлаш моделида ҳам ролларни маъмурлаш ва чеклаш механизмлари иерархия кўринишида амалага оширилади.

Ролларга асосланган фойдаланишни бошқаришни маъмур-  
лаш моделининг элементларининг тузилиши 5.2-расмда кўрсатилган.



5.2-расм. Ролларга асосланган фойдаланишни бошқаришни маъмурлаш моделининг элементларининг тузилиши

Маъмурлаш вазифаларини уч гуруҳга ажратиш мумкин:

- 1) авторизациядан ўтган фойдаланувчилар мажмуини маъмурлаш;
- 2) роллар эга бўлган фойдаланиш ҳуқуқи мажмуини маъмурлаш;
- 3) роллар иерархиясини маъмурлаш;

Одатда, ҳар бир маъмурий ролга роллар иерархиясининг роллар тўплами тайинланади, ушбу маъмурлаш роли созлан-маларни ўзгартириш имконига эга бўлади.

### 5.3. Ахборот хавфсизлигини оширишда ролли моделни формаллаштириш

Ролларга асосланган усул тизимнинг алоҳида объектларига мурожаат қилмасдан, умуман тизимдаги ҳаракатларнинг рухсат этилиши ёки таъқиқланишига асосланади [13, 48]. Умуман олганда, усул ваколатлар концепциясидан фойдаланиб амалга оширилади. Ваколат бу тизим маълумотларидан фойдаланиш бирлиги. Тизим маълумотлари турли хил  $O$  объектлар кўринишида тақдим қилинади. Рол бу номланган ваколатлар тўплами, яъни тизим объектларидан фойдаланишнинг рухсат берилган ҳар хил турларнинг тўплами. Тизим объектларига фойдаланишнинг барча мумкин бўлган турларининг тўплामини  $A$  орқали белгилаймиз.

*Таъриф 5.1.* Ваколат сифатида  $(x, m)$  жуфтликни назарда тутамиз, бу ерда  $x$  — тизим объекти ( $x \in O$ ) ва  $m$  — фойдаланиш турларининг ( $m \in A$ ) ноаниқ тўпламидир.

*Таъриф 5.2.* Рол бу номланган ваколатлар тўплами, улар кейинчалик  $(rname, rpset)$  жуфтлик сифатида акс эттирилади, бу ерда  $rname$  — ноёб идентификатор,  $rpset$  — ваколатлар тўплами.

Агар  $r$  рол аниқланса, унда унинг номи  $gname$  ва ваколатлар тўплами  $gpset$  бўлади. Икки тўпламни киритамиз:  $R$  — тизимнинг роллар тўплами,  $P$  — барча мумкин бўлган ваколатлар тўплами. Шунингдек, ролларга асосланган фойдаланишни бошқариш тизимларини муҳим функцияси сифатида  $\Psi: R \rightarrow 2^{P^1}$  киритамиз. Ушбу функцияда ролнинг ваколатлари кўрсатилади. Унинг моҳияти куйидагича  $\Psi(r) = r.rpset$ . Рол концепцияси орқали тизим маълумотларидан фойдаланиш амалга оширилади.  $UID$  — фойдаланувчилар идентификаторлар

тўплами,  $GID$  — фойдаланувчилар гуруҳининг идентификаторлар тўплами, ролларга асосланган фойдаланишни бошқаришни амалга оширадиган идентификаторларнинг умумий тўплами  $ID = UID \cup GID$ . Ролларга асосланган фойдаланишни бошқариш тизимлари учун авторизация жараёни муҳим рол ўйнайди [45]. Бундай ҳолларда икки хил ҳолат бўлиши мумкин. Биринчи ҳолатда «Рол-ваколат» авторизация қилиш ушбу рол учун ваколатлар тўпламида кўрсатилган имтиёзни ўз ичига олади, яъни агар  $r$  рол  $p$  ваколатга авторизация қилинган бўлса, у ҳолда  $p \in r.rset$ .

Иккинчи ҳолатда «Рол-рол» авторизация қилиш битта ролнинг ваколатларини бошқа ролнинг ваколатлари тўпламига кўшилишини англатади. Яъни, агар  $r_1$  рол  $r_2$  авторизация қилинган бўлса, у ҳолда  $r_2.rpset \subseteq r_1.rpset$ .

«Рол-рол» авторизацияси кўплаб ролларда ўзаро бинар муносабатларни келтириб чиқаради. Бу муносабатни  $r_1 \rightarrow r_2$  орқали белгилаймиз, агар  $r_1$  рол  $r_2$  авторизация қилинган бўлса.

$\Psi$  функцияси монотон равишда  $\rightarrow$  амалга нисбатан ошиб боради, яъни  $r_1 \rightarrow r_2$ , у ҳолда  $\Psi(r_2) \subseteq \Psi(r_1)$ .

Занжирнинг кўриниши  $r_i \rightarrow r_{i1} \rightarrow \dots \rightarrow r_{in} \rightarrow r_j$ ,  $r_i \rightarrow^+ r_j$  орқали ( $n > 0$  учун) ва  $r_i \rightarrow^* r_j$  ( $n > 0$  учун) белгиланади.

*Таъриф 5.3.*  $r_i$  ва  $r_j$  роллари орасидаги  $p(r_i, r_j)$  ролнинг йўналиши  $r_i \rightarrow^* r_j$  занжири деб номланади.

Роллар тўпламига берилган муносабат учун мос келадиган граф ҳосил қилишимиз мумкин. Бунда  $(r_1, r_2)$  учун ёй мавжуд бўлади, агар  $r_1$  рол  $r_2$  ролга авторизация қилинган бўлса. Кўриниб турибдики,  $p(r_i, r_j)$  роллар йўли мос келадиган диаграммада  $r_i$  учидан  $r_j$  учигача бўлган йўналишга изоморфдир.

*Таъриф 5.4.* Рол йўли эскирган ҳисобланади, агар битта ролдан иборат бўлган рол йўли ноль узунликдаги масофага тенг бўлса.

*Таъриф 5.5.*  $r_1$  — роли  $r_j$  — ролдан устунлик қилади,  $r_j$  — роли  $r_i$  — ролига бўйсунди, агар  $p(r_i, r_j)$  рол йўли мавжуд бўлса, ёки график кўринишида  $r_i$  — чўққиси,  $r_j$  — чўққисидан устун,

$r_j$  — чўққиси  $r_i$  — чўққисига бўйсунди, агар йўналтирилган  $p(r_i, r_j)$  рол йўли мавжуд бўлса.

Бир ролнинг бошқасига нисбатан устунлиги муносабати  $R$  роллар тўпламида берилади. Шунини таъкидлаб ўтиш керакки, ролларга асосланган хавфсизлик сиёсатини маъмурлаш принципига кўра икки хил ҳолат бўлиши мумкин. Биринчи ҳолатда ваколатлари мос келадиган роллар учраши мумкин. Ундай бўлса роллар ўртасидаги муносабатлар қатъий ҳисобланмайди. Аммо бундай ёндашув ролларга асосланган хавфсизлик сиёсатини шакллантиришда фақат вақтинчалик чора сифатида қабул қилинади. Сўнгги шаклланган ролларнинг иерархиясида бир хил ваколатларга эга бўлган иккита ролнинг мавжудлиги маъносиздир. Иккинчи ҳолат бир хил ваколатларга эга бўлган иккита ролнинг мавжудлигини истисно қилади. Ушбу ёндашув учун роллар ўртасидаги муносабатлар қатъий ҳисобланади. Иккинчи ёндашув ролларни оптимал бошқаришни имконини беради. Бунда  $r_i$  ролнинг  $r_j$  ролдан устунлигини  $r_i \geq r_j$  ( $r_j \leq r_i$  ёки) нисбат орқали белгиланади.

Ролларга асосланган фойдаланишни бошқариш модели фойдаланишни дискрецион бошқариш моделининг ривожлантирилган кўриниши бўлиб, тизим субъектнинг объектга бўлган ваколатларини фойдаланишнинг ўзига хос хусусиятларини ҳисобга олган ҳолда фойдаланиш ҳуқуқларини беради. Ролларга асосланган фойдаланишни бошқариш усули тизимнинг ишлаш жараёнида динамик равишда ўзгариб турадиган фойдаланишни бошқариш қоидаларини амалга ошириш имконини беради.

#### **5.4. Ахборот ҳимояланганлигини оширишда ролларга асосланган фойдаланишни бошқариш усули**

Бир вақтнинг ўзида кўплаб фойдаланувчилар ишлайдиган реал инфокоммуникацион тизимларда роллар тузилиши ва фойдаланиш ҳуқуқларини жуда мураккаб бўлиши маъмурлаш жараёнини аҳамиятини оширади. Турли ташкилий-технологик

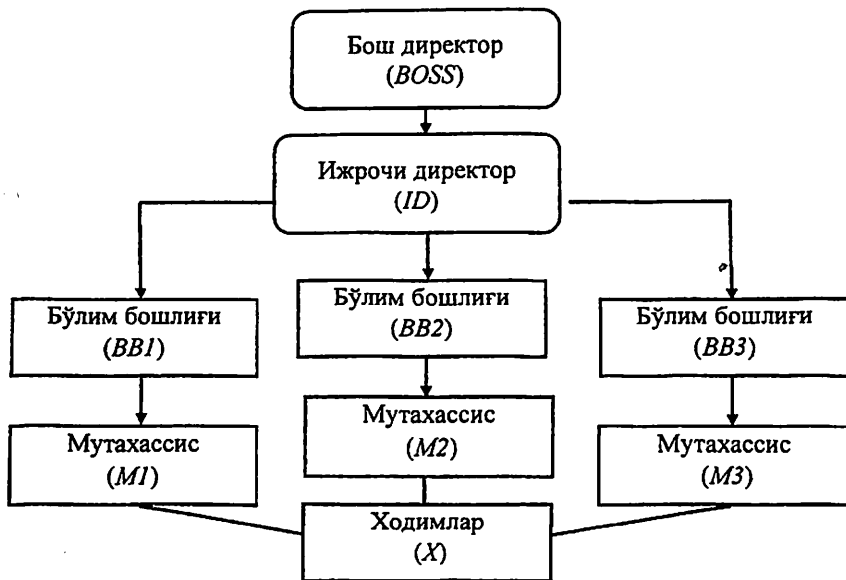
ва бошқарув-технологик схемаларнинг тахлили шуни кўрсатадики [49, 50, 51], реал ҳаётда корхоналар ва муассасалар ходимлари муайян функционал вазифаларини шахсий номидан эмас, балки маълум бир лавозим доирасида бажарадилар. Лавозимни муайян рол сифатида талқин қилиш мумкин, бунда бу тушунча мавҳум ва умумлаштирилган моҳиятни, яъни маълум вазифа турини ва ходимнинг ҳолатини ифодалайди. Шундай қилиб, реал ҳаётда, аксарият ташкилий-технологик схемаларда ҳуқуқ ва ваколатлар маълум бир ходимга шахсан берилмайди, балки у маълум бир лавозимга (ролга) тайинланиши орқали, у муайян ҳуқуқ ва ваколатлар тўпламини олади. Ролларга асосланган фойдаланишни бошқариш усули тизим субъектининг объектга бўлган ваколатларини фойдаланишнинг ўзига хос хусусиятларини ҳисобга олган ҳолда фойдаланиш ҳуқуқларини роллар орқали беради [4].

Ролларга асосланган фойдаланишни бошқаришнинг асосий усули қуйидаги тўплamlарни ўз ичига олади:  $U$  – фойдаланувчилар тўплами,  $R$  – роллар тўплами,  $P$  – тизимда ишлаш учун ҳуқуқлар тўплами. Ролларни акс эттиришда  $PA: R \rightarrow 2^P$  муҳим аҳамиятга эга бўлиб, бу берилган рол учун фойдаланиш ҳуқуқларининг тўпламини белгилайди ва ҳар бир  $p \in P$  учун  $r \in R$  бўлган  $p \in PA(r)$  мавжуд.

Ишлаб чиқиш ва техник хизмат кўрсатиш функцияларини ташқи ташкилотларда қўллаш ҳолатларини кўриб чиқамиз. Бунинг учун ижро этувчи, маъмурий ва бошқарув функциялари нисбатларини аниқлаш керак.

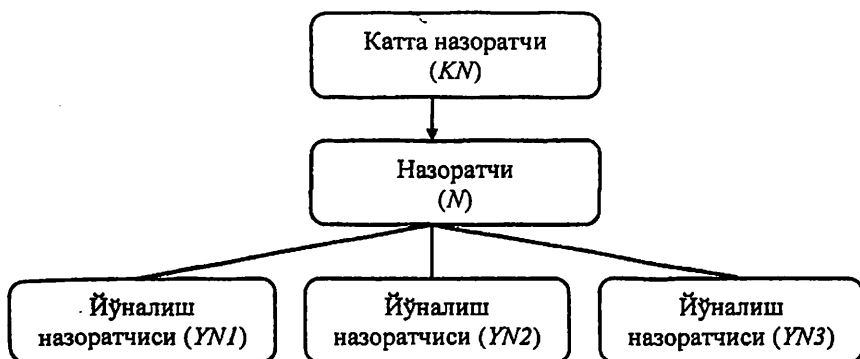
Яққол мисол сифатида корхонанинг хавфсизлик модели ишлаб чиқилган. Бу ерда ижро этувчи ролларнинг иерархияси (5.3-расм), назорат ролларнинг иерархияси (5.4-расм), маъмурий ролларнинг иерархияси (5.5-расм), ишлаб чиқиш роллар иерархияси (5.6-расм) ва техник хизмат кўрсатиш роллари иерархияси (5.7-расм).





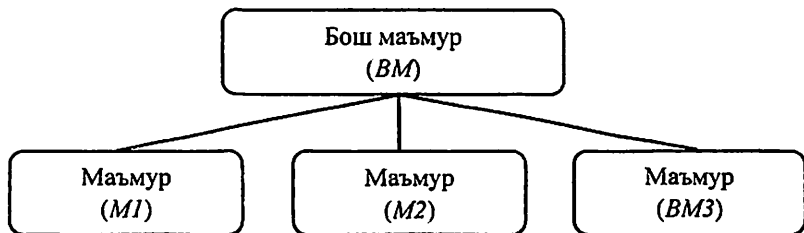
5.3-расм. Ижро этувчи ролларнинг иерархияси

Бошқарувчи BOSS бу иерархиядаги максимал рол, минимал рол  $X$  ходим ҳисобланади. Ҳар бир фаолият йўналишида ижрочи директорнинг ( $ID$ ) максимал даражадаги роли аниқланади, йўналишнинг минимал рол  $X$  ходим ҳисобланади.



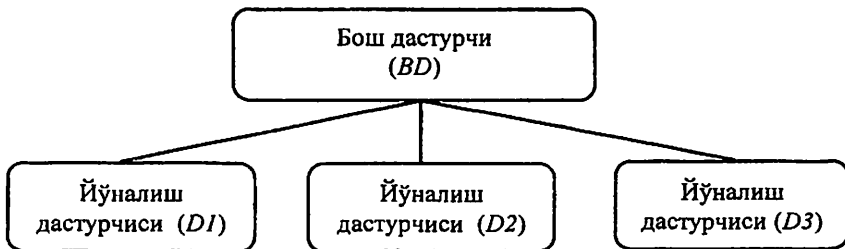
5.4-расм. Назорат ролларнинг иерархияси

YN1, YN2, YN3 йўналиш назоратчилари хар бир ижро этувчиларни назорат қилиш функциясини амалга оширади. Назорат бўлим бошлиқларидан тортиб, тегишли йўналиш маъмурлари, тегишли йўналишлар бўйича кўмаклашиш мутахассислари, шунингдек, тегишли йўналиш ишлаб чиқувчилари, бунда YN1, YN2, YN3 учун бошқариш функциялари бир-бири билан кесишмайди. YN1 йўналиш назоратчиси YN2 йўналиш назоратчисини ва YN3 йўналиш назоратчисини фаолиятини бошқара олмайди. Ўз-ўзидан YN2 йўналиш назоратчиси YN1 йўналиш назоратчисини ва YN3 йўналиш назоратчисини фаолиятини бошқара олмайди. Бу жараён YN3 йўналиш назоратчисига ҳам тегишли.



5.5-расм. Маъмурий ролларнинг иерархияси

Бош маъмур BM KN, N, BD ва QQBM учун ҳамда BOSS дан бошланган барча ижрочилар учун маъмурий функцияларни амалга оширади. M1, M2 ва M3 маъмурлари фаолият йўналишлари устидан маъмурий функцияларни амалга оширади.



5.6-расм. Дастурчи роллар иерархияси

Бош дастурчи BD ижро этувчиларга ишлаб чикувчи вази-  
фасини бажаради, бунга таъсисчи BOSS, ҳамда QQBM ва  $N$  лар  
киради. D1, D2 ва D3 ишлаб чиқиш функциялари ўзаро кесиш-  
майди. D1 дастурчиси фақат биринчи йўналиш фаолияти учун  
ишлаб чиқиш функциясини бажаради. Ўз-ўзидан D2 ва D3 дас-  
турчиси мос йўналиш фаолияти учун ишлаб чиқиш функция-  
сини бажаради.



5.7-расм. Техник хизмат кўрсатиш роллари иерархияси

QQBM бош мутахассиси ижрочилар учун таъсисчи BOSSдан  
бошлаб, шунингдек, VM, BD, KN учун қўллаб-қувватлаш функ-  
цияларини бажаради. QQM1, QQM2 ва QQM3 қўллаб-қувватлаш  
функциялари ўзаро кесишмайди, яъни QQM1 қўллаб-қувватлаш  
мутахассиси фақат биринчи йўналиш фаолияти учун қўллаб-  
қувватлаш функциясини бажаради. Ўз навбатида QQM2 ва  
QQM3 мутахассиси мос йўналиш фаолияти учун қўллаб-қувват-  
лаш функциясини бажаради.

Қуйида бошқарувчи ролларни ва уларга боғлиқ ижро рол-  
лари тўпламлари ўртасидаги муносабатни, шунингдек, маъмурий  
хуқуқлар ва уларга тайинланган бошқариш роллари тўпламлари  
ўртасидаги муносабатни тавсифловчи жадваллар келтирилган.

**Назорат қилувчи ролларни ижро этувчи роллар билан  
ўзаро боғлиқлиги**

Назорат қилувчи рол	Роллар тўплами
<i>YN1</i>	<i>[M1, BB1]</i>
<i>YN2</i>	<i>[M2, BB2]</i>
<i>YN3</i>	<i>[M3, BB3]</i>
<i>N</i>	<i>[BB1, BB1]</i>
<i>N</i>	<i>[BB2, BB2]</i>
<i>N</i>	<i>[BB3, BB3]</i>

**Маъмурий ролларнинг назорат қилувчи роллар билан  
ўзаро боғлиқлиги**

Маъмурий роллар	Роллар тўплами
<i>M1</i>	<i>[YN1, N]</i>
<i>M2</i>	<i>[YN2, N]</i>
<i>M3</i>	<i>[YN3, N]</i>
<i>BM</i>	<i>[N, N]</i>

Бошқа ролларнинг тўпламлари ўртасидаги муносабатларни акс эттириш учун юқоридаги жадвалларга ўхшаш жадвалларни тузиш мумкин.

ИКТда барқарор ишлаш имкониятини берувчи ролларга асосланган хавфсизлик сиёсатини қуриш учун қуйидаги амалларни бажариш керак:

1) Тизимдаги барча фойдаланиш ҳуқуқларини ижро этувчи, маъмурий ва бошқарувчиларга бўлиб чиқиш керак, бунда битта ҳуқуқ фақат битта тўплагга тегишли бўлиши мумкин, яъни тўпламлар ўзаро кесишмайди.

2) Ҳар бир ижро этувчи ҳуқуқи учун назорат ҳуқуқларининг тўпламини аниқлаш керак, яъни ушбу ҳуқуқдан фойдаланишни тўлиқ назорат қилиш учун ҳуқуқга эгалик қилиши керак.

3) Ҳар бир ижро этувчи рол билан ишлайдиган ижро этувчи ҳуқуқлар тўплами учун бошқарувчи роллар мажмуини аниқлаш керак, яъни уларнинг ҳар бири бошқариладиган ролнинг ижро этувчи ҳуқуқларини назорат қилувчи ролларнинг тўплами.

4) Ҳар бир назорат ҳуқуқи учун маъмурий ҳуқуқлар тўпламини аниқлаш керак, яъни бу рол ҳуқуқини назоратини таъминлаш учун маъмур эга бўлиши керак бўлган ҳуқуқлар мажмуи.

## **VI БОБ. АХБОРОТДАН ФЙДАЛАНИШНИ ЧЕКЛОВЧИ ХАВФСИЗЛИК СИЁСАТЛАРИНИ БИРЛАШТИРИШ УСУЛ ВА АЛГОРИТМЛАРИ**

### **6.1. Икки қийматли панжарага асосланган мандатли хавфсизлик усули**

Иккита мандатли хавфсизлик сиёсатини бирлаштириш зарурияти бир вақтнинг ўзида маълумотлар махфийлигини ва яхлитлигини талаб қиладиган тизимларда пайдо бўлиши мумкин. Махфийлик ёки юқори даражали ахборотни паст даражали фойдаланувчиларга сирқиб чиқмаслиги, ахборот оқимини юқоридан пастга таъқиқланиши орқали кафолатланади, яъни қийматлар панжарасида субъектнинг ишонч даражаси объектнинг махфийлик даражасидан устун бўлиши керак [52, 53].

Агар қийматлар панжарасида субъектнинг даражаси объектнинг даражасидан юқори бўлмаган фойдаланишларга рухсат берилган бўлса, яхлитлик кафолатланади [13]. Шундай қилиб, бир қийматли панжарада бир вақтнинг ўзида ҳам махфийликни ҳам яхлитликни таъминлаш қарама-қарши қоидаларга олиб келади. Натижада маълумотни фақат битта даражада бошқа жойга кўчириш имконияти пайдо бўлади, лекин турли даражадаги ваколатларга эга бўлган субъектлар ўртасида ахборот алмашилиш имкониятига эга бўлмайди.

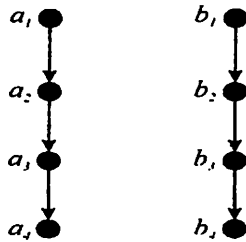
Ушбу қарама-қаршилиқ иккита қийматли панжарани кириштириш йўли билан ҳал қилинади, бунда бир панжара махфийликни таъминлаш учун, иккинчи панжара яхлитликни таъминлаш учун хизмат қиладди [54]. Шу билан бирга, тизимни бошқариш вазифаси жуда кўп вақт талаб этади, чунки ҳар бир ахборотдан фойдаланиш иккита мустақил қоидага мувофиқ текширилади. Бу муаммони ечиш учун иккита бўлимнинг мандатга асосланган хавфсизлик сиёсатини амалга ошириш орқали кўриб чиқилади. Бунинг учун ташкилотнинг ягона қийматлар панжарасини бўлимлар кесимида декарт кўпайтмаси орқали амалга ошириш мумкин [55, 56]:

$$L_1 \times L_2$$

Бундай ёндашувда тизимдаги ҳар бир объект  $(m_1, m_2)$  ( $m_1 \in L_1, m_2 \in L_2$ ) хавфсизлик белгилари билан тавсифланади.

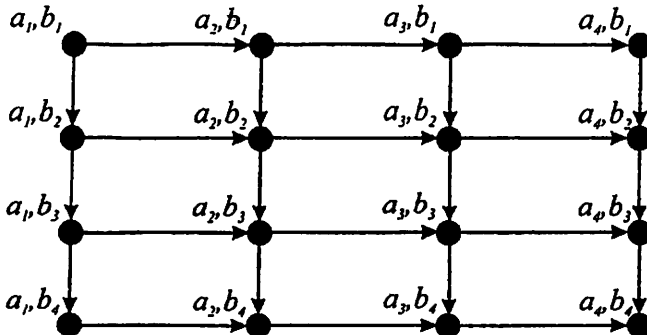
$D_1$  бўлимда  $L_1 = a_1, a_2, a_3, a_4$  чизиқли қийматлар панжарасида ( $a_1 \leq a_2 < a_3 < a_4$ ) тўртта хавфсизлик даражаси амал қилсин.

$D_2$  бўлимда  $L_2 = b_1, b_2, b_3, b_4$  чизиқли қийматлар панжарасида ( $b_1 < b_2 < b_3 < b_4$ ) тўртта хавфсизлик даражаси амал қилсин (6.1-рasm).



6.1-рasm. Чизиқли қийматлар панжараси

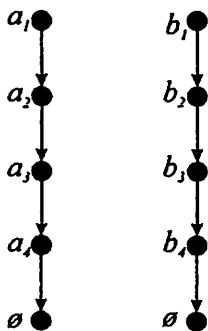
6.2-рasmда 16 та хавфсизлик белгисига эга бўлган бирлаштирилган ташкилотнинг хавфсизлик панжараси кўрсатилган.



6.2-рasm. Бирлаштирилган ташкилотнинг хавфсизлик панжараси

Агар  $D_1$  бўлимининг  $L_1$  панжарасидаги хабарнинг хавфсизлик белгиси  $D_2$  панжарасига киритилмаган бўлса,  $D_2$  бўлимининг ҳеч бир субъекти бундай хабарни ўқий олмайди то унга ахборотдан фойдаланиш учун тегишли ваколоти берилмагунича, яъни  $L_1 \times L_2$  декарт кўпайтмалар панжарасидан янги хавфсизлик белгиси қўшилмагунча.

Шу билан бирга, баъзи турли хил бўлимларнинг субъектлари ўртасида алмашилиши мумкин бўлмаган вазият юзага келади, бу эса декарт кўпайтмалар панжарасидан олинган янги хавфсизлик белгисининг ҳеч бири мос келмаслигини англатади. Акс ҳолда, ахборот сирқиб чиқиши пайдо бўлади, чунки олинган янги панжаранинг  $a_4, b_4$  энг паст даражаси ҳар бир бўлимнинг ахборотдан фойдаланишини ўз ичига олади. Бундай вазиятни олдини олиш учун янги хавфсизлик панжарасини қўшимча хавфсизлик даражалари билан тўлдириш керак, улар янги панжаранинг остки панжараси бўлади. Бунинг учун ҳар қандай панжарани бўш элемент ёки ноль элементи билан тўлдирадиган элементар ўзгартириш киритиш керак.  $L_1$  қийматлар панжараси чизиқли бўлганлиги учун минимал элемент  $a_4$  эмас  $\{0\}$  бўлади.  $L_2$  қийматлар панжарасига ҳам шундай мулоҳазани қўллаш мумкин. Натижада  $L_1 \cup \{0\} = L_1^\emptyset$  ва  $L_2 \cup \{0\} = L_2^\emptyset$  панжараларини оламиз.

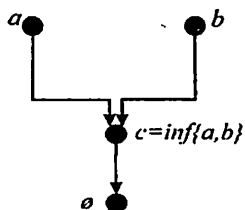


6.3-расм.  $L_1 \cup \{0\} = L_1^\emptyset$  ва  $L_2 \cup \{0\} = L_2^\emptyset$  панжаралари



Агар қийматлар панжараси ночизиқли бўлса, унда панжара таърифи бўйича ҳар қандай иккита элемент учун аниқ қуйи чегараси бўлади, ҳар қандай панжарада энг кичик элемент бўлади. Бу шуни англатадики, панжарага бўш элементни қўшиш мумкин ва бунда панжара хусусиятлари бузилмайди. 3.4-расмда ночизиқли панжарани ноль элементи билан тўлдирилган ҳолат тасвирланган.

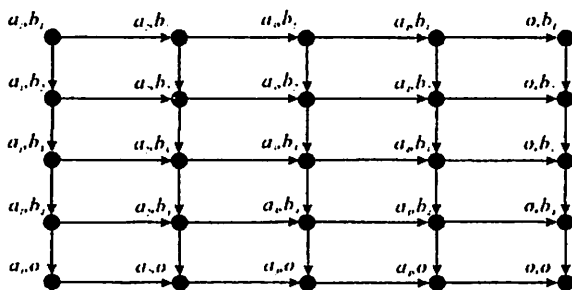
Бўш элемент қўшиш орқали бирлаштирилган панжараларни декарт кўпайтмаси орқали  $L^\emptyset = L_1^\emptyset \times L_2^\emptyset$  амалга оширилиши мумкин.



6.4-расм. Ночизиқли панжарани ноль элементи билан тўлдирилиши

бу ерда  $a$  ва  $b$  даражалари  $c$  бирлашади ва ҳар бир бўлимнинг энг паст даражасидаги субъект ахборотдан фойдаланиши имконияти мумкин бўлади.

6.5-расмда юқоридаги ёндашув асосида натижавий панжара 25 элементдан иборат бўлади.  $L^\emptyset$  панжарасининг диаграммаси 6.5-расмда кўрсатилган.



6.5-расм. Бирлаштирилган тизимнинг хавфсизлик панжараси

$L^\emptyset$  панжарасининг 25 элементи пастки панжарани ташкил этади.  $L = L_1 \times L_2$  панжараси  $D_1$  ва  $D_2$  бўлимлари ўртасида ахборот алмашинувини таъминлаш воситаси сифатида ҳисобланади, бунда ахборот алмашинуви хавфсиз бўлади, чунки ҳар бир ўзаро таъсир учун хавфсизликнинг махсус даражаси мавжуд [57]. Бундан ташқари,  $L^\emptyset$  панжарасида яна иккита қуйи панжарани ажратиш мумкин, уларнинг ҳар бири ахборот алмашинувисиз бўлимларнинг ишлашини имитация қилади.

Иккита бўлим ёки ташкилотларнинг мандатли хавфсизлик сиёсати асосида ҳар бир бўлимнинг ва улар ўртасида хавфсиз ахборот алмашинувини амалга ошириш учун қуйидагиларни бажариш керак:

- Ҳар бир бўлимнинг мандатли хавфсизлик сиёсатини бўш элемент билан тўлдирилиши керак, яъни хавфсизлик белгисини киритиш керак, бу белгига ҳеч қандай ваколат ва ймтиёз берилмайди. Бундай ҳолда, хавфсизлик белгилари тўплами панжара бўлиб қолади.

- Икки панжарадан иборат декарт кўпайтмасини тўпламини олиш керак, яъни иккита бўлимда мавжуд бўлган жуфтлик хавфсизлик белгиларини олиб ташлаш керак, бунда жуфтликга ҳар бир бўлимдан биттадан хавфсизлик белгилари киради. Панжаранинг декарт кўпайтмалар тўплами панжара бўлганлиги сабабли, олинган кўплаб жуфтликлар чўққисида мандатли хавфсизлик сиёсатини куриш мумкин бўлади: Натижада ҳосил бўлган хавфсизлик сиёсати орқали ҳар бир бўлим (бўш белгилар тўфайли) ва иккита бўлим ўртасида хавфсиз ахборот алмашинувини амалга ошириш мумкин.

- Қуйидаги қоидага мувофиқ  $\forall a_1, a_2 \in L_1, b_1, b_2 \in L_2$  хавфсизлик белгилари жуфтликлари  $(a_1, b_1) \geq (a_2, b_2) \leftrightarrow a_1 \geq a_2$  ва  $b_1 \geq b_2$  ўртасида қисман тартиб бўйича ўзаро алоқани тузиш. Бу ерда  $L_1, L_2$  лар  $D_1$  бўлим ва  $D_2$  бўлимларнинг хавфсизлик белгилари тўплами.

- Фойдаланувчи ва ресурсларга керакли хавфсизлик белгиларини ўрнатиш. Бундай ҳолда, агар ҳужжат бўлимлар ўртасида ахборот алмашинувида иштирок этмаса, жуфтликни ташкил

этувчи белгилардан бири бўш бўлади. Агарда хужжат ахборот алмашинувида қатнашса, унда бўш белги ушбу хужжат учун жуфтликни ташкил этувчи белгилар тўпламига тушмайди.

## **6.2. Ролли ва мандатли хавфсизлик сиёсатини бирлаштириш усули**

Бугунги кунда ресурслардан фойдаланишни ташкил қилиш учун маълумотлар базасини бошқариш тизимларидан фойдаланиш кенг қўлланилади. Кўпгина замонавий маълумотлар базалари фойдаланувчига ресурсдан фойдаланиш учун роллар тушунчасидан фойдаланадилар, шу орқали ролли фойдаланишни чеклашни амалга оширади [30, 58]. Шу билан бирга, бир қатор ташкилотлар, хусусан, ҳимояланган хужжат алмашинуви билан боғлиқ ташкилотлар мандатли фойдаланишни бошқаришга асосланган хавфсизлик белгиларидан фойдаланилади. Ахборотдан фойдаланишни чекловчи хавфсизлик сиёсатларини бирлаштириш усуллари [59, 61, 62] кўриб чиқилган.

Мандатли фойдаланишни бошқаришда рухсат этишлар аниқ берилмаган бўлиб, унда объектлар учун махфийлик даражаси ва КТнинг субъектлари учун ишонч даражаси шаклида ўрнатилади. Фойдаланиш тўғрисидаги қарор махфийлик даражаси ва ишонч даражасини таққослаш йўли билан қабул қилинади [62]. Роллар концепциясидан фойдаланилганда, фойдаланиш рухсат этилган тизим операциялари кўшимча объектлар – рухсат этилган фойдаланишлар тўпламига эга роллар орқали белгиланади. Фойдаланишга рухсат бериш тўғрисидаги қарор таққосланган рол асосида қабул қилинади. Ролларга асосланган хавфсизлик сиёсатини шакллантириш 5.1 бобда кўриб чиқилган. Ролларга асосланган хавфсизлик сиёсати алоҳида тизим объектларига мурожаат қилмасдан тизимдаги ресурслардан фойдаланиш ёки ҳаракатларни тақиқлашга асосланган. Умуман олганда, ушбу ёндашув имтиёзлар концепциясидан фойдаланган ҳолда амалга оширилади. Рол моҳиятидан келиб чиқиб тизим маълумотларидан фойдаланиш амалга оширилади.

*Мандатли хавфсизлик сиёсатини шакллантириш.* Мандатли хавфсизлик сиёсати ахборотнинг махфийлик даражаси ва фойдаланувчига ишонч даражаси тушунчаларига асосланиб ишлаб чиқилади. Ахборотнинг махфийлик даражасини аниқлаш учун турли хил ёндашувлар мавжуд [63, 64, 65]. Бундай ёндашувлардан бири қийматлар панжарасига асосланган.

*Таъриф 6.1.* Панжара бу қисман тартибланган тўпلام бўлиб, унда ҳар бир икки элементли осткитўпلامда аниқ юқори (*sup*) ва аниқ пастки (*inf*) чегараларига эга.

*Таъриф 6.2.*  $A, B$  учун  $C = \sup(A, B)$  элементи аниқ ёки энг кичик юқори чегараси деб номланади, агар шарт бажарилса:

1.  $A \leq C, B \leq C$ .
2.  $\forall D: D \leq A, D \leq B \Rightarrow C \leq D$ .

*Таъриф 6.3.*  $A, B$  учун  $E = \inf(A, B)$  элементи аниқ ёки энг юқори пастки чегараси деб номланади, агар шарт бажарилса:

1.  $E \leq A, E \leq B$ .
2.  $\forall D: D \leq A, D \leq B \Rightarrow D \leq E$ .

Тизимнинг ҳар бир объекти ва субъекти панжара элементи бўлган «Хавфсизлик белгилари» билан солиштирилади. Субъект объектдан фойдаланиш учун сўров жўнатганда хавфсизлик белгилари таққосланади. Агар субъектнинг хавфсизлик белгиси объектнинг хавфсизлик белгисидан юқори бўлса ахборотдан фойдаланишга рухсат берилади, бошқа ҳолларда фойдаланиш тақиқланади.

Ролларга асосланган фойдаланишни бошқаришнинг асосий тушунчалари графлар назарияси нуқтаи назаридан шакллантирилганлиги сабабли [66], мандатли фойдаланишни бошқариш учун шунга ўхшаш тушунчаларни киритамиз.

*Таъриф 6.4.* Панжарали графни йўналтирилган граф деб номлаймиз, унинг чўққилари панжарани ҳосил қилади. Шу билан бирга, тартиб муносабати граф чўққиси тўпламидаги устунлик билан белгиланади: агар  $\exists p(r_1, r_2)$  у ҳолда ( $r_1 \geq r_2$ ). Энг кичик юқори чегара  $\sup(r_1, r_2)$  энг яқин чўққи сифатида белгиланади,  $r_1$  ва  $r_2$  устидан устунлик қилади. Энг юқори

пастки чегара  $\inf(r_1, r_2)$  энг яқин чўққи сифатида белгиланади,  $r_1$  ва  $r_2$  устидан устунлик қилади.

Йўналтирилган графда энг кичик юқори ва энг юқори пастки чегара тушунчаларини расмий равишда аниқлаймиз [67]:

$$r = \sup(r_1, r_2) \Leftrightarrow$$

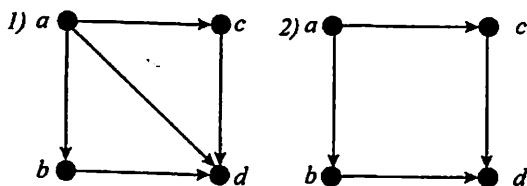
1.  $\exists p(r, r_2) \& p(r_2, r)$ , бунда  $r$  юқори чегараси ҳисобланади.
2. Агар  $\exists p(r', r_2) \& p(r', r)$ , унда  $\exists p(r', r)$ , бунда  $r$  барча юқори чегаралар орасида минимал ҳисобланади.

$$r = \inf(r_1, r_2) \Leftrightarrow$$

1.  $\exists p(r_1, r) \& p(r_2, r)$ , бунда  $r$  пастки чегараси ҳисобланади.
2. Агар  $\exists p(r_1, r') \& p(r_2, r')$ , унда  $\exists p(r, r')$ , бунда  $r$  барча пастки чегаралар орасида максимал ҳисобланади.

**Таъриф 6.5.** Ихтиёрий панжара учун унга изоморф бўлган панжара графи мавжуд бўлади.

Панжара графи учун берилган изоморф панжараси ягона эмас [67]. Дарҳақиқат, масалан, 6.6-расмдаги графлар бир хил панжара  $(M, P)$  учун изоморф бўлиб, бу ерда  $M = \{a, b, c, d\}$  – панжара тугунлари тўплами,  $P = \{(a, b), (a, c), (a, d), (b, d), (c, d)\}$  – бу  $M$  – да берилган қисман тартиб муносабати.  $G_1$  ва  $G_2$  панжара графларини ( $G_1 \sim G_2$ ) билан эквивалент деб ҳисоблаймиз, агар улар бир хил панжара учун изоморф бўлса.



3.6-расм. Эквивалент панжара графи

**Таъриф 6.6.** Панжара графидаги манба ҳар қандай чўққидан устунлик қилади, оқим шу графнинг ихтиёрий чўққисига бўйсунди.

Тармоқдаги манба йўналишсиз цикларнинг ихтиёрий чўққилардан устун, оқим шу графнинг ихтиёрий чўққисига

бўйсунди.  $r$  йўналтирилмаган цикллар тармоқнинг ихтиёрий чўққиси,  $s$  — манба,  $t$  — оқим бўлсин. Йўналиш маршрутини курамиз,  $r$  чўққисидан бошлаб, ҳар қадамда биттадан ёй кўшиб борамиз. Тармоқда йўналтирилган циклларнинг йўқлиги сабабли, маршрутни куриш чекланган, охириги кўшилган ёй орқали ёй ҳосил қилинади, графга олиб борувчи ягона оқим бўлади. Шундан келиб чиқадики, тармоқда камида битта  $p(r, t)$  йўналтирилган маршрутга эга бўлади. Унда  $t$  оқим  $r$  чўққига бўйсунди.

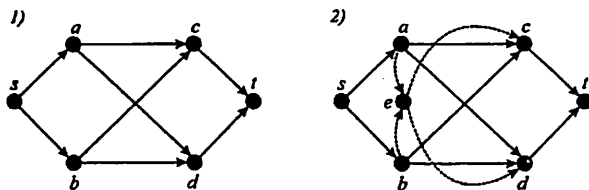
$p(s, r)$  йўналтирилган маршрутнинг мавжудлиги ўхшашлигини исботлайди, аммо унинг ташкил этилиши ёйларнинг йўналишига қарама-қарши йўналишда амалга оширилади.

Тармоқда йўналтирилмаган цикллар учун ҳар қандай жуфтликда камида битта юқори чегара (манба) ва пастки чегара (оқим) мавжуд. Аммо энг кичик юқори (энг катта пастки) чўққиларни танлаш, яъни чўққиларни таққослаш масаласи очиқлигича қолмоқда.

Графнинг «панжарасизлигини» куйидаги мисол билан тушунтириш мумкин: 6.7 расмда (1) граф - йўналтирмаган цикллар мавжуд тармоқ, аммо бу граф панжара ҳисобланмайди.  $a$  ва  $b$  чўққиларни солиштириб бўлмайдиган иккита  $c$  ва  $d$  пастки чегаралари мавжуд, ундан ташқари  $t$  пастки чегара шак-шубҳасиз  $c$  ва  $d$  дан кичик.  $c$  ва  $d$  чўққиларни солиштириб бўлмайдиган иккита  $a$  ва  $b$  юқори чегаралари мавжуд, яна битта  $s$  юқори чегара шак-шубҳасиз  $a$  ва  $b$  дан катта.

Тармоқда  $\{a, b, c, d\}$  (6.7-расм (1)) чўққилари тўпламининг оқибатида ҳосил бўлган остки граф каби, бир нечта оқимлари ёки манбалари бўлган остки графларнинг мавжуд эмаслиги панжара етарли шарт эмас.

$e$  (6.7-расм (2)) чўққини кўшиш кўриб чиқилаётган тармоқни панжара графига айлантиради:  $\inf(a, b) = e$  ( $c$  ва  $d$  ни солиштириб бўлмайдиган, лекин  $(e \geq c) \& (e \geq d)$ ) ва  $\sup(c, d) = e$  ( $a$  ва  $b$  ни солиштириб бўлмайдиган, лекин  $(e \geq a) \& (e \geq b)$ ).

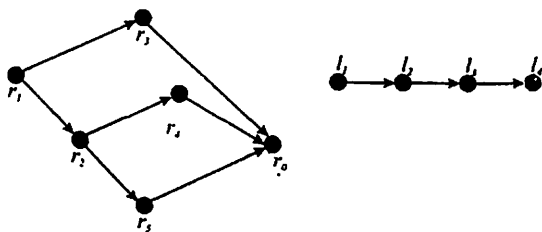


6.7-расм. (1) панжара графи бўлмаган тармоқ ва (2) панжара графи бўлган тармоқ

*Таъриф 6.7.* Агар роллар иерархияси графи панжара кўринишида бўлса ёки уни ўзгартириш ёрдамида кенгайтириш орқали панжара кўринишига келтириш мумкин бўлса, унда ролларга асосланган хавфсизлик сиёсати мандатли хавфсизлик сиёсати билан бир-бирига зид бўлмаган ҳолда бирлаштириш имконини беради.

Роллар иерархияси графини панжара графига кенгайтира- миз ва уни  $GM$  деб белгилаймиз. Мандатли хавфсизлик сиёсати  $L$  панжараси билан белгиланади.  $L$  панжара ва  $GM$  панжара графи чўққисида қурилган декарт кўпайтмасини оламиз.  $GM \times L$  билан белгиланган декарт кўпайтмаси панжара ҳисобланади [67].

Таклиф этилаётган усулни тушунарли кўринишда тасвир- лаш 6.8 -расмдан фойдаланилади, бунда ролларга асосланган хавфсизлик сиёсатини ва тўртта элементнинг чизиқли тўпламига асосланган мандатли хавфсизлик сиёсатини бирлаштирилади.



6.8-расм.  $R$  ролларга асосланган хавфсизлик сиёсати ва  $L$  қийматли панжара

Ролларга асосланган хавфсизлик сиёсати олти роллар билан берилган, улардан бири ( $r_0$ ) “Бўш”, яъни ҳеч қандай имтиёзларга эга эмас ва бошқа ҳар қандай ролларга бўйсунди.  $G$  графи тармоқ бўлсин, ундан оқимни ўчириб уни йўналтирилган иерархияга (дарахт кўринишига) айлантирамиз, унда  $G$  панжара бўлади. Бунда  $s$  — манба,  $t$  — оқим ва  $G\{t\} = T$  — бошланғич графдан оқимни ўчириб ташлаш орқали олинган иерархия (дарахт). Агар  $R - G$  графнинг чўққилар тўплами бўлса, у ҳолда  $R \setminus \{t\} - T$  дарахтнинг чўққилар тўплами ва  $s$  — дарахт илдизи. Бундан келиб чиқадики 6.8-расмда келтирилган граф панжара ҳисобланади.

Мандатли хавфсизлик сиёсати  $L$  панжараси билан аниқлансин, унинг элементлари  $l_1, l_2, l_3, l_4$  тугунлар, бунда тартиб куйидагича берилади  $l_1 \geq l_2 \geq l_3 \geq l_4$ .

Ролларга асосланган хавфсизлик сиёсати мандатли хавфсизлик сиёсати билан бир-бирига зид бўлмаган ҳолда бирлашади. Бунинг учун  $R$  ва  $L$  панжараларининг декарт кўпайтмаси бўлган  $R \times L$  панжарасини қуриш керак, бу ерда  $R - 6.7$ -расмда кўрсатилган панжара графи билан аниқланадиган панжара.

$R \times L$  панжара элементлари  $(r_i, l_j)$  жуфтликлари, бунда  $i = 0, \dots, 4$  ва  $j = 1, \dots, 5$ . Бундай ҳолда тартибланиш куйидагича белгиланади:

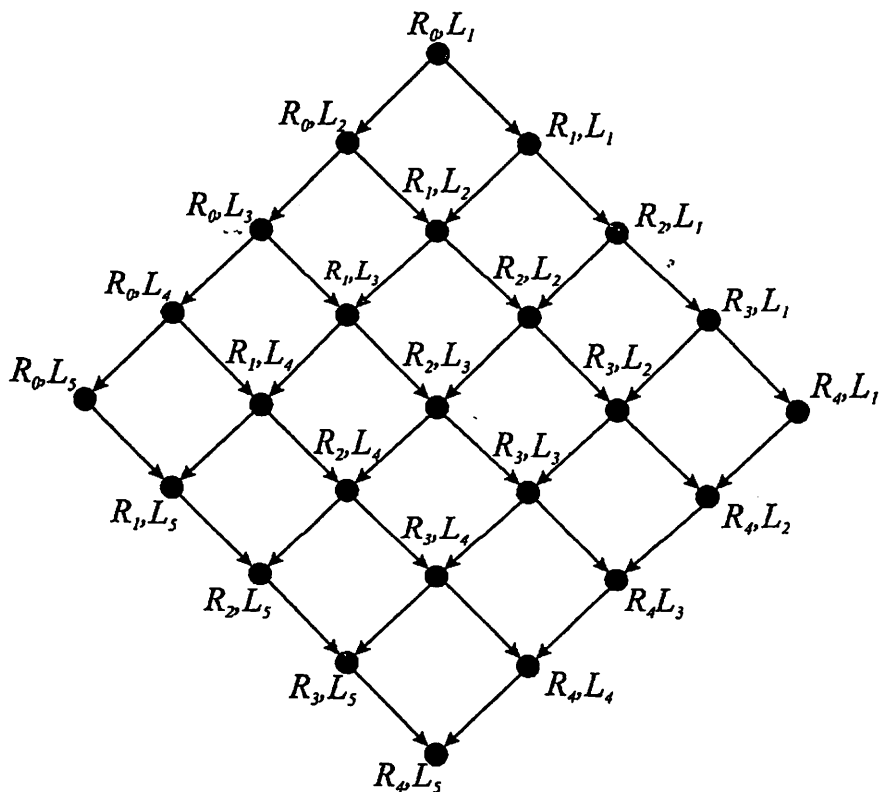
$$(r_i, l_j) \geq (r_k, l_m), \text{ агар } r_i \geq r_k \text{ ва } l_j \geq l_m.$$

Шуни таъкидлаш керакки,  $r_2$  ва  $r_3, r_4$  ва  $r_5, r_3$  ва  $r_4, r_3$  ва  $r_5$  тугунлари ўзаро жуфт таққосланмайди.

6.9-расмда келтирилган панжара графи  $R \times L$  панжарасига изоморф ҳисобланади. Олинган  $R \times L$  панжарасида мандатли хавфсизлик сиёсатини ўрнатиш мумкин. Ўз навбатида, олинган йўналтирилган графда ролларга асосланган хавфсизлик сиёсатини қуриш мумкин бўлади.

Шундай қилиб, ушбу икки ёндашувни бирлаштириш натижасини хавфсизлик белгиларига асосланган концепция кўринишида ва ролларнинг иерархияси кўринишида тақдим этилиши мумкин.





6.9-расм. Ролли ва мандат хавфсизлик сиёсатини бирлаштириш панжараси

Иккита бўлимнинг ролли ва мандатли хавфсизлик сиёсатининг бирлашишига асосланган мандатли хавфсизлик сиёсатини тузиш учун куйидаги жараёнларни амалга ошириш керак:

1. Ролларга асосланган хавфсизлик сиёсати учун ролли граф куриш ва ушбу граф панжара эканлигини текшириш керак. Агар рухсат этилган ўзгартиришдан кейин панжарали граф кўринишига келмаса, унда иккита сиёсат талабларни ўз ичига олган мандатли хавфсизлик сиёсатини тузиш мумкин эмас.

2. Панжара декарт кўпайтмаси панжара бўлганлиги сабабли, натижада олинган чўққилар жуфтлиги тўпламида мандатли хавфсизлик сиёсатини куриш мумкин, бунда пайдо бўлган хавфсизлик сиёсати иккита сиёсатнинг талабларига жавоб беради.

3. Роллар ва белгилар жуфтликлари орасидаги қисман тартиблаш муносабати қуйидаги қоидага асосан яратилади:

$$\forall r_i, r_k \in R \text{ ва } l_j, l_m \in L(r_i, l_j) \geq (r_k, l_m) \Leftrightarrow r_i \geq r_k \text{ ва } l_j \geq l_m.$$

4. Фойдаланувчилар ва ресурсларга лозим бўлган хавфсизлик белгиларини тайинлаш талаб этилади.

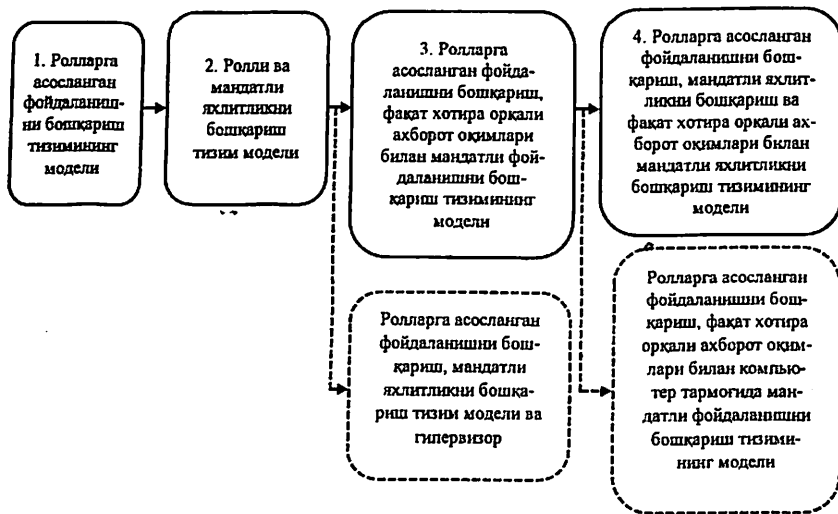
Иккита бўлимнинг роли ва мандатли хавфсизлик сиёсатининг бирлашишига асосланган мандатли хавфсизлик сиёсатини яратиш, рол графи панжара ёки панжара эмаслигини аниқлашга имкон беради. Агар ролли граф панжара бўлмаса, унда панжара графини олиш учун рухсат этилган ўзгартиришни амалга ошириб, панжара графи кўринишига келтириш керак.

### **6.3. Операцион тизимларда мандат ва ролли фойдаланиш бошқариш модели**

Ахборот махфийлигини ҳар хил турдаги таҳдидлардан ҳимоя қилишда мандатли фойдаланишни бошқариш модели ролли фойдаланишни бошқаришга асосланади.

Мандат ва ролли иерархик модел ҳар хил даражаларни ўз ичига олиши мумкин (6.10-расм).

Бундай ёндашув моделни таърифланишини босқичма-босқич мураккаблаштириш ва моделни тасдиқлашда унга мос келадиган кейинги даражадаги элементларни киритиш имконини беради [68]. Моделнинг ҳар бир пастки даражаси бу мавҳум тизим бўлиб, унинг элементлари юқори даражага тегишли бўлган янги элементларга боғлиқ эмас, бу эса ўз навбатида мерос қилиб олиш ва керак бўлганда пастки даражали элементларни тузатиш ёки тўлдириш имконини беради.



**6.10-расм.** Мандат ва ролли моделнинг иерархик кўриниши ва унинг кенгайтиш имкониятлари

Гипервизорнинг иерархик моделида қўшимча учинчи даража (ролларга асосланган фойдаланишни бошқариш, мандатли яхлитликни бошқариш тизим модели ва гипервизор) кўриб чиқилади, шунинг учун операцион тизимларда мандатли фойдаланишни бошқариш гипервизор томонидан амалга оширилмаслиги керак ва операцион тизимлар учун гипервизор мандатли яхлитликни бошқаришни функциясини тўғри ишлашини таъминлаши керак [69]. Қўшимча учинчи даражадаги шаклда компьютер тармоғидаги ролларга асосланган фойдаланишни бошқариш модели тўртинчи даражадаги иерархик мандат ва ролли моделини муқобили ҳисобланади, бу моделда мандатли яхлитликни бошқариш ва хотира орқали ахборот оқимларини мандатли фойдаланишни бошқариш тизими муҳим аҳамиятга эга.

Ролли фойдаланишни бошқаришнинг таянч моделига асосланган мандатли фойдаланишни бошқаришни амалга оширадиган ёндашув кўриб чиқилади:

Куйидаги белгилардан фойдаланилади:

$O$  – объектлар тўплами;

$(L, \leq)$  – махфийлик даражасининг панжараси;

$(LI, \leq)$  – махфийлик яхлитлиги панжараси;

$ci: U \rightarrow L$  – фойдаланувчиларнинг фойдаланиш даражаси ва яхлитлилик функцияси;

$ci: O \rightarrow L$  – объектларнинг махфийлик ва яхлитлилик даражалари функцияси;

$A = \{read, write\}$  – фойдаланиш турлари.

Қатъий мандатли фойдаланишни бошқариш учун  $(s, o, r) \in S \times P$  фойдаланиш хавфсиз ҳисобланади, агар қуйидаги шартлардан бири бажарилса:

-  $r = read$  ва  $ci(user(s)) \geq ci(o)$ ;

-  $r = write$  ва агар фойдаланиш мавжуд бўлса  $(s, (o', read)) \in S \times P$ , у ҳолда  $ci(o) = ci(o')$  (қатъий \*- хосса).

Ролларга асосланган фойдаланишни бошқариш тизимини курамиз. Бунда

$R = \{xi\_read | xi \in LI\} \cup \{xi\_write | xi \in LI\}$  – роллар тўплами;

$P = \{(o, read) | o \in O\} \cup \{(o, write) | o \in O\}$  – фойдаланиш ҳуқуқлар тўплами.

$R$  роллар тўпламига иерархияни ўрнатамиз, бу ерда тўпламлардаги роллар иерархияси  $\{xi\_read | xi \in LI\}$  ва  $\{xi\_write | xi \in LI\}$  мустақил бўлади.

Қатъий мандатли фойдаланишни бошқариш талабларига мувофиқ  $R$  роллар тўплами иерархияси « $\leq$ » қисман тартиб нисбати бўлиб, унда роллар  $r, r' \in R$  учун  $r \leq r'$  тенгсизлик адолатли, агар қуйидаги шартлардан бири бажарилса:

-  $r = xi\_read, r' = xi'_read$  ва  $xi \leq xi'$ ;

-  $r = xi\_write, r' = xi'_write$  ва  $xi = xi'$  ( $xi\_write$  шаклининг ҳар бир роли фақат ўзи билан таққосланади).

Ролларга асосланган фойдаланишни бошқариш модели қатъий мандатли фойдаланишни бошқариш талабларига мувофиқ бўлади [4], қачонки  $R$  роллар тўплами иерархияси юқоридаги талабларга жавоб берса ва қуйидаги чекловлар қондирилганда:

-  $UA$  – функциясини чеклаш  $u \in U$  ҳар бир фойдаланувчи роли  $xi\_read = \oplus(UA(u) \cap \{yi\_read | yi \in LI\}) \in UA(u)$  (бу ерда  $xi = ci(u)$ ) ва  $\{yi\_write | yi \in LI\} \subset UA(u)$ ;

- ҳар бир сессия  $s \in S$  учун  $roles$  – функциясини чеклашда тенглик адолатли  $roles(s) = \{xi\_read, xi\_write\}$ ;

-  $PA$  – функциясини чеклаш учун куйидагилар бажарилиши керак:

• ҳар бир  $xi \in L$  фойдаланиш учун  $(o, read) \in PA(xi\_read)$  ва фақат фойдаланиш  $(o, write) \in PA(xi\_write)$ ;

• ҳар бир фойдаланиш учун  $(o, read) \in P$  фақат битта рол мавжуд  $xi\_read: (o, read) \in PA(xi\_read)$  (бу ерда  $xi = ci(o)$ ).

Шундай қилиб, ролларга асосланган фойдаланишни бошқариш моделлари учун қатъий мандатли фойдаланишни бошқаришнинг мувофиқлик талаблари ҳаммасида мос келади,  $roles$  функциясига чекловлар ва тегишли роллар иерархиясига қўйиладиган талаблар бундан мустасно.

Агар ролларга асосланган фойдаланишни бошқариш модели қатъий мандатли фойдаланишни бошқариш талабларига жавоб берса, унда ҳар қандай объект  $o, o' \in O$  учун шундай  $c(o) > c(o')$ ,  $o$  дан  $o'$  гача бўлган ахборот оқимининг пайдо бўлиши мумкин эмас.

Ахборотнинг махфийлиги ва яхлитлигини таҳдидлардан ҳимоялашга йўналтирилган фойдаланишни бошқаришнинг мандат ва ролли тизимини кураамиз. Бунда

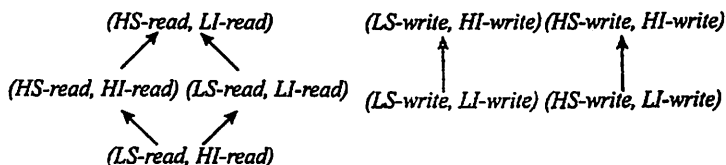
$$R = (\{x\_read | x \in L \times \{xi\_read | xi \in LI\}\} \cup \{x\_write | x \in L\}) \times$$

$\times \{xi\_write | xi \in LI\}$  – роллар тўплами.

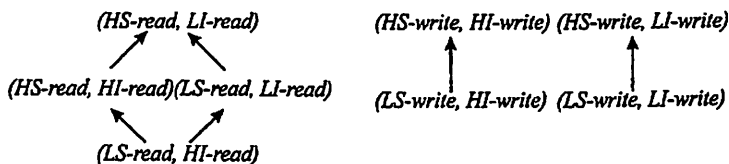
$R$  роллар тўпламига иерархияни ўрнатамиз, бу ҳолда қатъий мандатли фойдаланишни бошқариш ёки қатъий яхлитликни назорат қилиш ролларининг иерархиясини ихтиёрий бирлаштириш мумкин.

Тўпламдаги роллар иерархияси  $\{x\_read | x \in L \times \{xi\_read | xi \in LI\}\}$  ва  $\{x\_write | x \in L\} \times \{xi\_write | xi \in LI\}$  боғлиқ эмас.

6.11 ва 6.12-расмларда махфийлик даражалари  $(L, \leq) = \{LS, HS\}$  ва яхлитлилик даражалари  $(L, \leq) = \{LI, HI\}$  панжаралари учун иккита мумкин бўлган бирикмалари учун роллар иерархияларини либерал ва қатъий мандатли фойдаланишни бошқариш билан мандатли либерал ва қатъий яхлитликни назорат қилиш тақдим этилган.



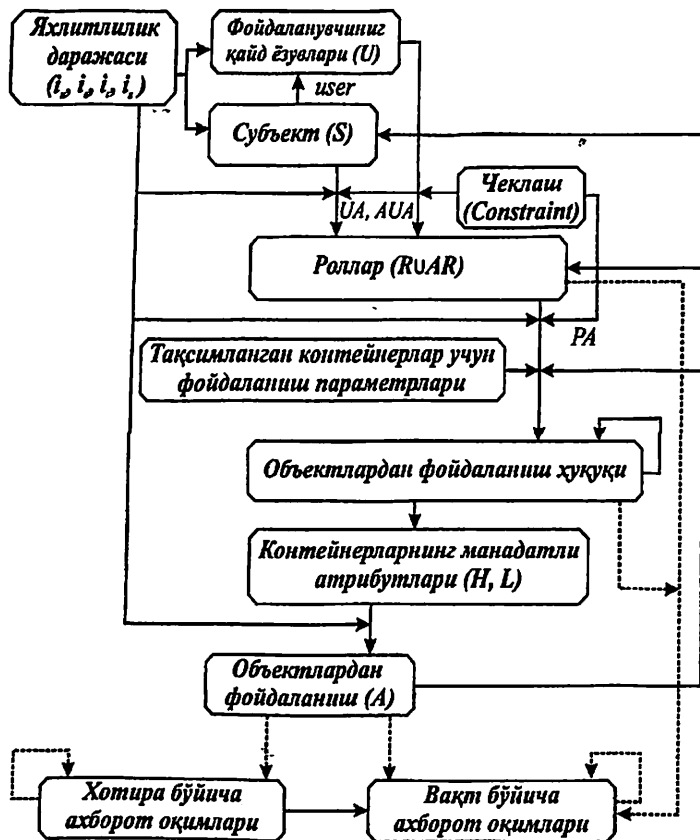
6.11-расм. Қатъий мандатли фойдаланишни бошқариш ва либерал яхлитликни назорат қилиш



6.12-расм. Либерал мандатли фойдаланишни бошқариш ва қатъий яхлитликни назорат қилиш

Ролли фойдаланишни бошқаришнинг таянч моделига асосланган мандатли фойдаланишни бошқариш моделини қўллаш орқали фойдаланиш ҳуқуқларини узатиш шартларини таҳлил қилиш, хотира ёки вақт бўйича ахборот оқимларини амалга ошириш мумкин. Ушбу модел доирасида роллардан ташқари, ролларнинг фойдаланиш ҳуқуқлари ва субъектнинг аниқ эгалик қиладиган ҳаракатларини амалга ошириш имкониятлари кўриб чиқилади. Шунингдек, ҳақиқий роллар, ролларнинг аниқ фойдаланиш ҳуқуқлари ва бошқа субъектлар устидан назоратни қўлга киритиш орқали ушбу субъектнинг ҳаракатларни амалга оширишнинг ҳақиқий имкониятлари кўриб чиқилади. Ушбу моделда ҳолатни ўзгартиришнинг монотон қоидалари

қўлланилади [70]. 6.13-расмда мандат ва ролли моделнинг шартларининг боғлиқлик ҳолати схемаси таклиф этилган.



6.13-расм. Мандат ва ролли моделнинг шартларининг боғлиқлик ҳолати схемаси

Ишлаб чиқилган схема хотира ва вақт бўйича тегишли ахборот оқимида иерархиядаги барча объектларни ўқиш ва ёзишни амалга ошириш учун субъектга фойдаланиш имкониятини беради.

#### **6.4. Мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми**

Ахборот тизимидаги субъектлар фойдаланиш имкони бўлган маълумотларнинг яхлитлигини ҳимоя қилиш, ахборот тизимини формал мантикий мандат ва ролли фойдаланишни бошқаришнинг хавфсизлик модели ва ахборот оқимларини ва яхлитлигини назорат қилиш орқали таъминланади:

- ҳар бир ролга яхлитлик даражаси белгиланади, фақат иерархияда бўйсунадиган ролларнинг яхлитлик даражасидан ошмаслиги керак;

- ҳар бир ролга субъектга ёки объектга эгалик ёки ёзиш ҳуқуқи белгиланади, фақат агар объектнинг яхлитлик даражаси ролнинг яхлитлик даражасидан юқори бўлмаганида;

- субъектга ролдан фойдаланиш ҳуқуқи берилади, агар ролнинг яхлитлик даражаси субъектнинг ҳозирги яхлитлик даражасидан ошмаса.

Ҳимояланган ахборот тизимининг хавфсизлик моҳияти тўпламига субъектлар, объектлар, контейнерлар ва роллар киради, шунингдек, уларнинг хавфсизлик параметрларининг таркиби ва уларнинг хавфсизликка таъсири ҳимояланган ахборот тизимининг муҳити бўлган операцион тизим тури ва версиясига қараб белгиланади. Ундан ташқари қуйидаги моҳият ва хавфсизлик параметрларни ўз ичига олади:

- ишончли ва ишончсиз фойдаланувчиларнинг қайд ёзувлари;

- файл тизимининг элементлари, шу жумладан, дисклар, каталоглар, файллар ва ҳаволалар;

- реестр элементлари, график интерфейс дарчалари, тармоқ интерфейслари;

- жараёнлар, оқимлар, драйверлар, қурилмалар, хизматлар, синхронизация объектлари;

- субъектлар ёки объектлардан фойдаланишда ролларнинг ваколатлари ва ҳуқуқлари рўйхати, бўлинадиган контейнерлар белгилари;



- махфийлик ва яхлитлик фойдаланиш даражалари белгилари, контейнерларнинг ичидаги маълумотлардан фойдаланиш учун CCR- белгилари;

- моҳият иерархиялари, шу жумладан, роллар ва субъектлар.

Расмий равишда, ушбу усулни амалга оширишда,  $\Sigma(G^*, OP)$  ахборот тизимидан фойдаланамиз, унинг барча ҳолатлари тўпламини  $G^*$  ва ҳолатларни ўзгартириш қоидаларини  $OP$  орқали белгилаймиз. Шу билан бирга  $\Sigma(G^*, OP)$  ахборот тизимининг ҳар бир ҳолати  $(PA, A, F)$  билан намойиш этилади ва унинг тавсифи қуйидаги элементларни қамраб олади:

-  $E = O \cup C$  – моҳиятлар тўплами, бу ерда  $O$  – объектлар тўплами (масалан, файллар),  $C$  – контейнерлар (масалан, каталоглар) ва  $O \cup C = \emptyset$ ;

-  $S \subseteq E$  – субъектлар тўплами, фойдаланувчининг қайд ёзувлари номидан фаолият олиб боради;

-  $R_r = \{read_r, write_r, execute_r, own_r\}$  – фойдаланиш ҳуқуқлари турларининг тўплами, бунда  $read_r$  – ўқиш учун фойдаланиш ҳуқуқи,  $write_r$  – ёзиш учун фойдаланиш ҳуқуқи,  $execute_r$  – бажариш учун фойдаланиш ҳуқуқи,  $own_r$  – эгалик фойдаланиш ҳуқуқи;

$R_a = \{read_a, write_a, own_a\}$  – фойдаланиш турларининг тўплами, бунда  $read_a$  – ўқиш учун фойдаланиш,  $write_a$  – ёзиш учун фойдаланиш,  $own_r$  – эгалик қилиш учун фойдаланиш;

$R_f = \{write_m, write_t\}$  – ахборот оқимларининг турларининг тўплами (хотира ва вақт бўйича);

$P \subseteq (E \cup R) \times R_r$  – моҳият ва роллардан фойдаланиш ҳуқуқлари тўплами;

$A \subseteq S \times (E \cup R) \times R_a$  – субъектларнинг моҳият ва роллардан фойдаланиш тўплами;

$F \subseteq (E \cup R) \times (E \cup R) \times R_f$  – ахборот оқимларининг тўплами;

$PA: R \rightarrow 2^P$  – моҳият ва роллардан фойдаланиш ҳуқуқлари функцияси, шу билан бирга ҳар бир фойдаланиш ҳуқуқи  $p \in P$  унда  $r \in P$  рол мавжуд, шартларни қаноатлантирадиган  $p \in PA(r)$  мавжуд;

$(LC, \leq)$  – махфийлик даражаларининг кўп даражали хавфсизлик даражаси (одатда, маълумотларнинг махфийлик даражаси чизиқли декрарт кўпайтмаси кўринишида);

$a: E \cup R \rightarrow LC$  – объект ёки рол учун махфийлик даражасини белгилайдиган функция;

$a: S \rightarrow LC$  – ҳар бир субъект учун жорий фойдаланиш даражасини белгилайдиган функция;

$(LI, \leq)$  – маълумотлар яхлитлигининг икки даражали чизиқли шкаласи, бу ерда  $LI = \{d_{low}, d_{high}\}$ ;

$m: E \cup R \rightarrow LI$  – ҳар бир объект ёки рол учун яхлитлик даражасини белгилайдиган функция;

$n: S \rightarrow LI$  – ҳар бир субъект учун жорий яхлитлик даражасини белгилайдиган функция.

$\Sigma(G^*, OP)$  ахборот тизимининг ҳар бир ҳолатида куйидаги шартлар бажарилиши таъминланади:

- ҳар бир ролда  $execute_r$ , – фойдаланиш ҳуқуқи бор, ҳар икки  $r, r' \in R$  рол учун  $(r, execute_r) \in PA(r')$  шарт бажарилади;

- контейнер объекти ёки роли таркибига кирадиган мантиқий объект ёки ролнинг махфийлик даражаси мос равишда унинг махфийлик даражасидан ошмайди: объектлар ёки роллар  $e, e' \in E \cup R$ , агар  $e \leq e'$ , унда  $a(e) \leq a(e')$ ;

- контейнер объекти ёки роли таркибига кирадиган мантиқий объект ёки ролнинг яхлитлик даражаси мос равишда унинг яхлитлик даражасидан ошмайди: объектлар ёки роллар  $e, e' \in E \cup R$ , агар  $e \leq e'$ , унда  $a(e) \leq a(e')$ ;

- Ролда объектлар ёки ролларга эгалик ёки ёзиш фойдаланиш ҳуқуқи бўлади, агар яхлитлик даражаси ўзиникидан юқори бўлмаса: рол учун  $r \in R$ , объект ёки рол учун  $e \in E \cup R$ , агар  $(e, \alpha_r \in PA(r))$ , унда  $m(e) \leq m(r)$ , бу ерда  $\alpha_r \in \{own_r, write_r\}$ .

$\Sigma(G^*, OP)$  ахборот тизимида куйидаги ҳолат ўзгартириш қоидалари (Де-юре қоидаси) амалга оширамиз, улардан ҳозирги ҳолатда фойдаланиш шартлари ва тизимнинг кейинги ҳолатида кўллаш натижалари 3.1-жадвалда келтирилган [70].

*Де-юре қоидалар.* Қоидалар ҳимояланган ахборот тизимларида фойдаланишни бошқариш механизмининг асосий қуйидаги функцияларини расмий равишда тавсифлашга мўлжалланган:

- роллар, маъмурий роллар, субъектлар, фойдаланувчининг қайд ёзувлари параметрларини олиш ёки ўзгартириш, яратиш, ўчириш, қайта номлаш;
- субъектларнинг объектлардан, роллардан ёки маъмурий роллардан фойдаланиш ҳуқуқига эга бўлиш;
- роллар ёки маъмурий ролларнинг объектлардан фойдаланиш ҳуқуқини ўзгартириш;
- объектлар, роллар ёки маъмурий ролларнинг махфийлик ёки яхлитлик даражалари иерархиясини ўзгартириш;

6.1-жадвал.

$\Sigma(G^*, OP)$  ахборот тизими ҳолатини ўзгартиришнинг  
Де-юре қоидалари

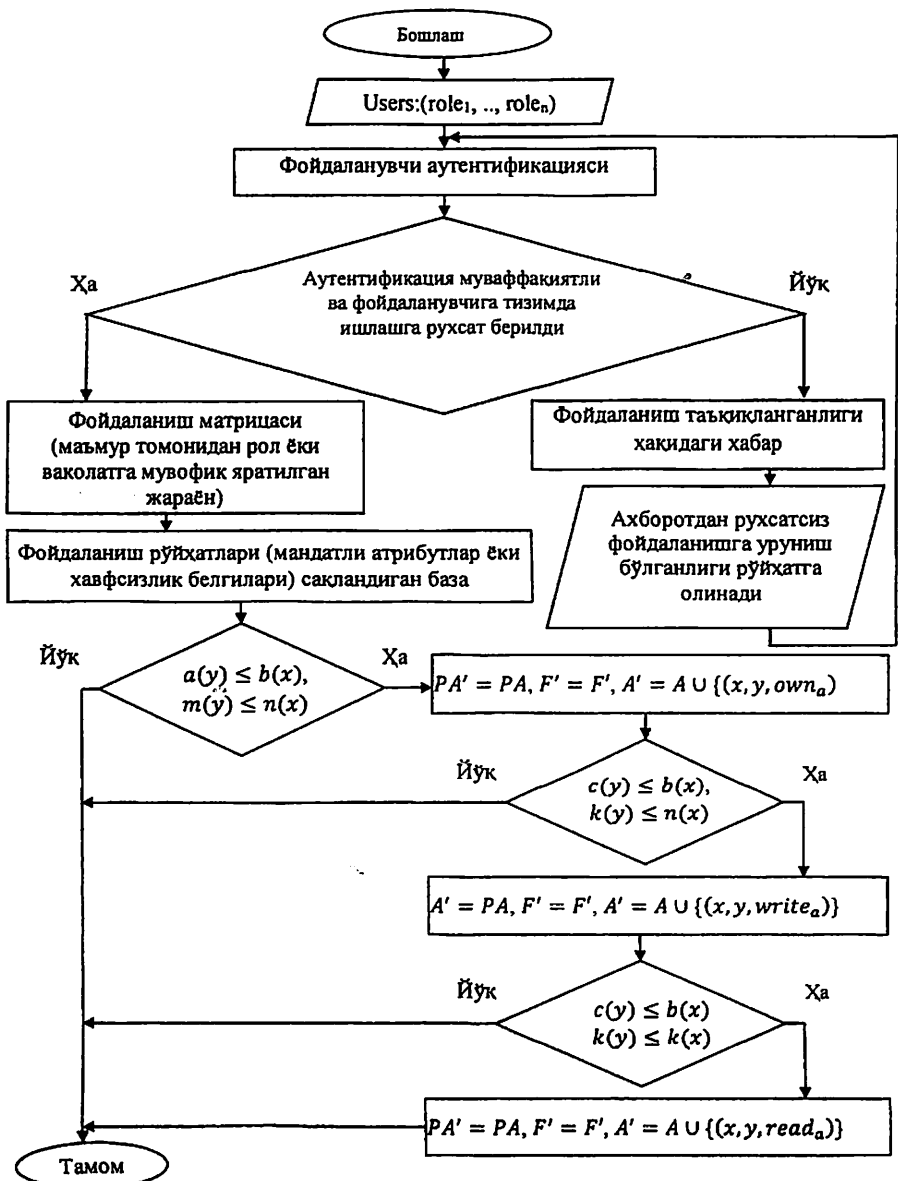
Қоида	Бошланғич ҳолат $G = (PA, A, F)$	Натижавий ҳолат $G' = (PA', A', F')$
$access\_own(x, y)$	$a(y) \leq b(x),$ $m(y) \leq n(x)$	$A'$ $= A$ $\cup \{(x, y, own_a)\}$
$aces\_write(x, y)$	$c(y) \leq b(x),$ $k(y) \leq n(x)$	$A'$ $= A$ $\cup \{(x, y, write_a)\}$
$access\_read(x, y)$	$c(y) \leq b(x),$ $k(y) \leq k(x)$	$A'$ $= A$ $\cup \{(x, y, read_a)\}$
$delete\_access(x, y, \alpha_a)$	$(x, y, \alpha_a) \in A$	$A' = A \setminus \{(x, y, \alpha_a)\}$
$grant\_rights(x, r, y, \alpha_a)$	$(x, r, write_a) \in A,$ $\alpha_r$ $\in \{own_r, write\}$	$A' = A, F' = F,$ $PA'(r') = PA(r')$
$remove\_rights(x, r, y, \alpha_r)$	$(x, r, write_a) \in A,$ $(x, y, own_a) \in A$	$A' = A, F' = F,$ $PA'(r') = PA(r')$

*Де-факто қоидалари.* Техник натижага эришишилганлигини асослаш учун  $\Sigma(G^*, OP)$  ахборот тизимининг ҳолатини ўзгартиришда куйидаги қоидалар қўлланилади [70], жорий ҳолатдаги фойдаланиш шартлари ва улардан фойдаланиш натижасида олинган натижаларни ахборот оқимларида қўлланилганлиги тизимнинг кейинги ҳолати 6.2-жадвалда келтирилган.

6.2-жадвал

$\Sigma(G^*, OP)$  ахборот тизими ҳолатини ўзгартиришнинг  
Де-факто қоидалари

Қоида	Бошланғич ҳолат $G = (PA, A, F)$	Натижавий ҳолат $G' = (PA', A', F')$
$flow\_memory\_access(x, y)$	$\alpha_a \in \{read_a, write_a\}$	$A' = A, \{(y, x, write_m)\}$
$flow\_time\_access(x, y)$	$R, (x, y, \alpha_a) \in A$	$F' = F \cup \{(y, x, write_t)\}$ $\{(x, y, write_a)\}$
$take\_flow(x, y)$	$(x, y, own_a) \in A$	$PA' = PA, F' = F, A' = A$ $\alpha \in \{write_m, write_t\}$
$find(x, y, z)$	$\alpha f, \beta f \in \{write_m, write_t\}$	$F'$ $= F \cup \{(x, z, write_m)\},$ $F' = F \cup \{(x, z, write_t)\}$
$post(x, y, z)$	$(x, y, \alpha f) \in F,$ $(z, y, \beta a) \in A$	$F'$ $= F \cup \{(x, z, write_m)\},$ $F' = F \cup \{(x, z, write_t)\}$
$pass(x, y, z)$	$(y, x, \alpha_a) \in A,$ $(y, z, \beta f) \in F$	$F'$ $= F \cup \{(x, z, write_m)\},$ $F' = F \cup \{(x, z, write_t)\}$



6.14-расм. Мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми

Юқоридаги Де-юре ва Де-факто қоидаларига асосланиб, 6.14-расмда мандат ва ролларга асосланган фойдаланишни бошқариш алгоритми келтирилган.

Шундай қилиб, ишлаб чиқилган мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми ахборотдан фойдаланишни бошқариш қоидаларини шакллантириш орқали ахборот тизимининг ҳимояланганлигини ошириш имконини беради.

«Де-юре» ҳолатни ўзгартириш қоидаларини  $\Sigma(G^*, OP)$  ахборот тизимига қўллаш орқали қуйидагиларни амалга ошириш мумкин:

- *access\_own(x, y)*, *access\_write(x, y)* ва *access\_read(x, y)* қоидаларида  $x$  субъектнинг  $y$  тизимнинг жорий ҳолатида  $r$  ролларда ўқиш ҳуқуқи мавжудлигини текширади;

- *access\_own(x, y)* ва *access\_write(x, y)* қоидалари  $y$  нинг махфийлик даражаси  $x$  нинг фойдаланиш ҳуқуқи даражаси тенглигини текширади ва  $y$  нинг яхлитлик даражаси жорий ҳолатдаги  $x$  нинг яхлитлик даражасидан ошмаслигини текширади;

- *access\_read(x, y)* қоида  $y$  нинг махфийлик даражаси жорий ҳолатдаги  $x$  нинг фойдаланиш ҳуқуқи даражасидан юқори эмаслигини текширади ва агар  $y$  нинг яхлитлик даражаси жорий ҳолатдаги  $x$  нинг яхлитлик даражасидан ошиб кетмайдиган  $y$  рол бўлса,  $y$  ҳолда тизим  $x$  га  $y$  га мос келувчи фойдаланиш ҳуқуқини беради;

- *delete\_access(x, y, \alpha\_a)* қоида  $y$  тизимнинг жорий ҳолатида  $x$  субъектнинг  $\alpha_a$  объекти ёки ролдан фойдаланиш ҳуқуқига эга эканлиги текширилади;

- *grant\_rights(x, r, y, \alpha\_a)* қоида  $y$  тизимнинг жорий ҳолатида  $x$  субъектнинг  $r$  ролга ёзиш ҳуқуқи мавжудлигини текширади ва объект ёки ролга эгалик ҳуқуқи мавжудлиги ва  $\alpha_a$  да ёзиш ва эгалик ҳуқуқи мавжуд бўлса,  $y$  нинг яхлитлилик даражаси  $r$  нинг яхлитлилик даражасидан юқори эмаслигини текширади ва муваффақиятли ўтса  $r$  га  $y$  дан  $\alpha_a$  фойдаланиш ҳуқуқини беради;

-  $remove\_rights(x, r, y, a_r)$  қондаси  $y$  тизимнинг жорий ҳолатида  $x$  субъектнинг  $r$  ролга ёзиш ва эгалик ҳуқуқи мавжудлигини текширади.

«Де-факто» ҳолатни ўзгартириш қондаларини  $\Sigma(G^*, OP)$  ахборот тизимига қўллаш орқали қуйидагиларни амалга ошириш мумкин:

-  $flow\_memory\_access(x, y)$  қондаси  $y$  тизимнинг  $x$  субъектнинг объектга ўқиш ёки ёзиш ҳуқуқи мавжудлигини текширади ва муваффақиятли ўтса  $F$  хотира бўйича ахборот оқимлар тўпламига киритади, ҳамда  $\alpha_a$  фойдаланиш ҳуқуқига кўра ўқиш ёки ёзиш ҳуқуқини беради;

-  $flow\_time\_access(x, y)$  қондаси  $y$  тизимнинг  $x$  субъектнинг объектга ёзиш ёки эгалик ҳуқуқи мавжудлигини текширади ва муваффақиятли ўтса  $F$  вақт бўйича ахборот оқимлар тўпламига киритади, ҳамда  $\alpha_a$  фойдаланиш ҳуқуқига кўра ёзиш ёки эгалик ҳуқуқини беради;

-  $take\_flow(x, y)$  қондасида  $y$  тизимнинг жорий ҳолатида  $x$  субъектнинг  $y$  субъектга эгалик ҳуқуқи мавжудлигини текширади ва муваффақиятли ўтса  $F$  ахборот оқимлар тўпламига киритади;

-  $find(x, y, z)$  қондаси тизимнинг жорий ҳолатида  $x$  субъектдан  $y$  субъектгача ва ундан  $z$  роллигача ахборот оқимларини мавжудлигини текширади, ҳамда муваффақиятли ўтса  $x$  дан  $z$  гача  $F$  ахборот оқимлар тўпламида хотира бўйича амалга оширади.

Шундай қилиб, тавсифланган усулни ахборот тизимида қўллаш мандат ва ролли фойдаланишни бошқаришнинг ягона механизмини амалга ошириш имконини беради ва натижада бузгунчи субъектларга роллар параметрларидан фойдаланиб тақиқланган ахборотдан фойдаланиш имконияти олди олинади.

6.3-жадвалда ахборотдан фойдаланишни чекловчи хавфсизлик сиёсатини бирлаштириш алгоритмларини таққослаш учун қуйидаги амалга оширувчи мезонлар гуруҳидан фойдаланилган.

**Ахборотдан фойдаланишни чекловчи хавфсизлик  
сиёсатини бирлаштириш алгоритмларини қиёслаш  
натижалари**

	Oracle Label Security қўлланилган алгоритм	CRUD алгоритми	Мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми
Амалга оширишнинг содаллиги	Ўрта	Ўрта	Ўрта
Ҳимояланганлик	Юқори	Юқори	Юқори
Фойдаланишни мураккаблиги	Паст	Ўрта	Ўрта
Унумдорлик	Ўрта	Ўрта	Ўрта
Тармоқда хавфсизликни таъминлаш	Юқори	Ўрта	Юқори
Ахборотни сирқиб чиқиб кетишини назорат қилиш	Юқори	Ўрта	Юқори

Ахборотдан фойдаланишни чекловчи хавфсизлик сиёсати-ни бирлаштириш алгоритмларини қиёслаш натижаларини баҳолаш учун сонли қаторлар йиғиндисидан фойдаланади, яъни  $\sum_{i=1}^n b_i$ .

бу ерда  $n$  — қаторлар сони;  $b_i$  — баҳолашнинг умумий аргументи. Баҳолаш учун қуйидаги аргументлар қабул қилинди:

$$b_1 = 2 \text{ (мавжуд эмас);}$$

$$b_2 = 3 \text{ (паст);}$$

$$b_3 = 4 \text{ (ўрта);}$$

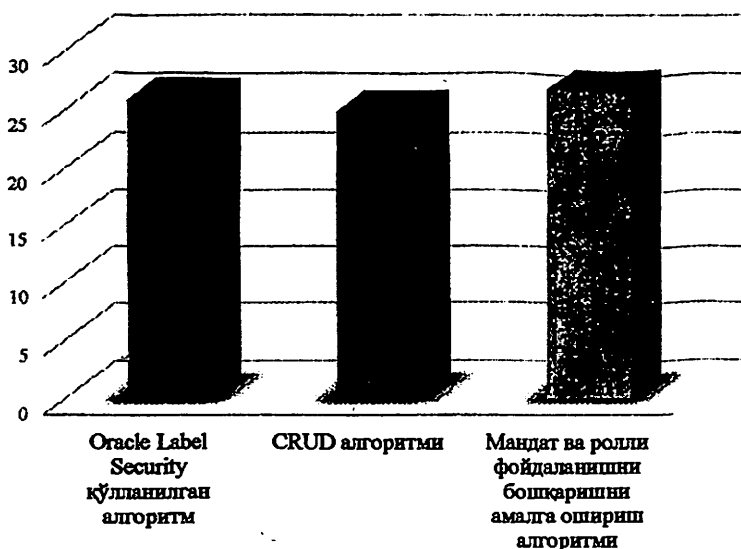


$b_4 = 5$  (юқори).

6.3-жадвалдан келиб чиққан ҳолда қуйидаги  $B$  матрица шакллантирилади:

$$B = \begin{pmatrix} 4 & 5 & 3 & 4 & 5 & 5 \\ 4 & 5 & 4 & 4 & 4 & 4 \\ 4 & 5 & 4 & 4 & 5 & 5 \end{pmatrix}$$

Юқоридаги  $B$  матрица натижалари асосида 3.15-расмда қиёсий таҳлили диаграммаси келтирилган.



6.15-расм. Мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритмлар қиёсий таҳлил диаграммаси

Қиёсий баҳолаш натижаларидан қуйидагича хулоса қилиш мумкинки, мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми мезонлари бўйича бошқа мавжуд CRUD алгоритми ва Oracle Label Security қўлланилган алгоритмга нисбатан юқори кўрсаткичга эга.

## VII БОБ. ИНФОКОММУНИКАЦИОН ТИЗИМЛАРИДА АХБОРОТ ҲИМОЯЛАНГАНЛИГИНИ БАҲОЛАШ

### 7.1. Ахборотдан рухсатсиз фойдаланишдан ҳимоя қилишни баҳолашга бўлган ёндашув

ИКТни нормал ишлашини, ахборотларнинг махфийлигини, яхлитлигини бузилишига ва ахборотни рухсатсиз ошкор бўлишига олиб келадиган ахборотлардан рухсатсиз фойдаланишни амалга ошириш учун, бузғунчи  $T_{арф}$  вақт сарфлайди [71, 72]. Бунда тахдидни амалга ошириш учун қуйидаги вақт оралиғи ифодаланилади:

$$T_{арф} = \sum_{i=1}^4 T_i$$

бу ерда  $T_1$  — аппарат-дастурий таъминотни заифликларини аниқлаш;  $T_2$  — ҳимоя қилиш тизимини ҳисобга олган ҳолда заифликлардан фойдаланиш имкониятини баҳолаш;  $T_3$  — ахборотдан рухсатсиз фойдаланишни амалга ошириш усулини танлаш;  $T_4$  — ахборотдан рухсатсиз фойдаланишни амалга ошириш.

Шунга асосланиб,  $T_i$  ошириш орқали ИКТларида ахборот хавфсизлигини бошқариш мумкин бўлади. Яъни,  $T_i$  ИКТларида ахборот хавфсизлигини баҳолаш мезони сифатида қабул қилиш мумкин. ИКТни лойиҳалашда  $T_{рухсат арф}$  бошланғич қийматини белгилаб,  $T_{арф} \leq T_{рухсат арф}$  шартни бажарилишини таъминлаш орқали, ИКТда чекланган ахборотдан рухсатсиз фойдаланишдан ҳимоя қилишни амалга ошириш мумкин бўлади [73, 74].

Бироқ, бу ёндашув ҳақиқий ҳолатни акс эттирмайди, чунки  $T_i$  вақт тасодифий ўзгарувчидир, вақтнинг тақсимотини ҳисоблаш қийин масала, сабаби у бузғунчининг имкониятларига қараб ўзгаради.

Бундан ташқари, бу ерда эксплуатациянинг асосий омилар ҳисобга олинмайди, масалан: ИКТга бўладиган ахборот хавфсизлигига турли тахдидлар, ИКТнинг эксплуатация вақти,

фойдаланиладиган ахборотни ҳимоя қилиш воситаларининг характеристикалари.

Ахборотдан рухсатсиз фойдаланиш шароитида ИКТларнинг максимал самарадорлигини таъминлаш учун ахборотларни ҳимоя қилиш воситаларининг мажмуасини ишлаб чиқиш куйидагича шаклга эга бўлади:

$$\begin{aligned} U_{\Sigma} &\rightarrow \min \\ C &= C_{opt} \end{aligned} \quad (7.1)$$

бу ерда  $U_{\Sigma}$  — умумий етказилган зарар;  $C$  — ахборотни ҳимоя қилиш воситалари мажмуасини лойиҳалаштириш харажатлари ёки

$$\begin{aligned} E_3 &\rightarrow \max, \quad \delta_3 \rightarrow \max, \\ C &= C_{opt} \quad C = C_{opt}. \end{aligned} \quad (7.2)$$

бу ерда  $E_3$  — ИКТнинг ишлаш самарадорлиги,  $\delta_3$  — ИКТнинг ишлашининг нисбий самарадорлиги.

Классик муаммони ечишнинг шаклининг соддалигига қарамай, амалиётда тақдим этилган натижалардан кам ҳолларда фойдаланиш мумкин бўлади. Бунинг сабаби, ахборотларни ҳимоя қилиш воситаларини мажмуасини лойиҳалаштириш харажатларида мумкин бўлган ахборотдан рухсатсиз фойдаланишни қисқартиришни математик тавсифлашнинг мураккаблиги билан боғлиқ. Агар хавфсизликни ҳимоя қилиш воситаларининг нархига боғлиқлигини бозорда мавжуд бўлган ушбу воситаларнинг техник ва иқтисодий хуёусиятлари билан олиш мумкин бўлса, ахборотдан рухсатсиз фойдаланишдан ҳақиқий зарарни баҳолаш жуда қийин [75, 76.], чунки бу зарар шунингдек, зарар етказиш эҳтимолига таъсир қилувчи қўплаб омилларга боғлиқ [77].

Ахборотни ҳимоя қилиш воситаларини танлаш энг яхши кўрсаткичлар билан амалга оширилади, шунинг учун хавфсизлик воситаларнинг нархининг самарадорликка таъсирини эътиборга олмаймиз, яъни агар  $C \ll U$  бўлса, у ҳолда:

$$U_{\Sigma} = \frac{U}{f(C)} \quad (7.3)$$

Бу ҳолда (7.1) ва (7.2) куйидаги шаклни олади:

$$\begin{aligned} U_{\Sigma} &\rightarrow \min \\ C &= C_{\text{рухсат}} \end{aligned} \quad (7.4)$$

ёки

$$\begin{aligned} E_3 &\rightarrow \max, \quad \delta_3 \rightarrow \max, \\ C &= C_{\text{рухсат}} \quad C = C_{\text{рухсат}}. \end{aligned} \quad (7.5)$$

бу ерда  $C_{\text{рухсат}}$  — химоя қилишга рухсат этилган харажатлар.

Шундай қилиб, ИКТда ахборотдан рухсатсиз фойдаланиш, фойдаланилаётган химоя воситаларига, ахборот хавфсизлигига бўладиган таҳдидлар сонига [78], химояланганлик даражасига ва ИКТнинг эксплуатация вақтига боғлиқ бўлади.

Ҳар бирида  $N_i, i = 1, 2, \dots, k$  ахборот хавфсизлигига таҳдидларни амалга ошириш мумкин бўлган  $k$  қисмларга эга ИКТни лойиҳалаштирамыз. ИКТ мумкин бўлган  $S$  хавфсизлик таҳдидларини ўз ичига олади,  $S = N_1 + N_2 + \dots + N_k = \sum_{i=1}^k N_i$ . Хавфсизлик таҳдидларини бартараф этиш ахборотни химоя қилиш воситалар мажмуаси таркибига киритилган ахборот хавфсизлик воситалари ёрдамида амалга оширилади. Ахборотни химоя қилиш воситалари химоя қилиш механизмлари, техник талаблар, бошқа химоя қилиш воситалари билан мувофиқлиги, иқтисодий ва эргономик хусусиятларига қараб химоя қилиш учун турли функционал имкониятларга эга.

Ахборотни химоя қилиш воситаларининг мажмуасини фарқлаш учун  $M_i, i = 1, 2, \dots, k$  аҳамиятли коэффицентларни киритамиз. Қайта ишланадиган ахборотларнинг махфийлик грифи қанчалик юқори бўлса, химоя қилишнинг техник талаблари ва характеристикаларига нисбатан қаттиқ талаблар қўйилади, шу асосида  $M_i$  коэффицентига кўп қиймат ўзлаштириш керак ва аксинча.

Ҳеч бўлмаганда битта хавфсизлик таҳдидини амалга ошириш орқали ахборотдан рухсатсиз фойдаланиш эҳтимоли  $P_x$  ва барча хавфсизлик таҳдидини амалга ошириш орқали ахборотдан рухсатсиз фойдаланиш эҳтимоли  $P_y$  тахмин қиламиз.

Кўриб чиқилаётган ИКТда мумкин бўлган  $S$  хавфсизлик таҳдидлари тенг тақсимланиш қонуни асосида тасодифий деб ҳисоблаймиз. Унда, муайян хавфсизлик таҳдидини амалга оширишда ахборотдан рухсатсиз фойдаланиш эҳтимоли ва ахборотни ҳимоя қилиш воситалари мажмуаларининг ахборотдан рухсатсиз фойдаланишдан ҳимояланганлиги қуйидагича аниқланади:

$$P_s = \frac{1}{S} \quad (7.6)$$

ИКТнинг қисмларини заиф томонларини ҳисобга олиш учун [79], (7.6) га  $M_i$  аҳамиятлилик коэффицентини киритиш керак, бунда  $i$  қисм учун ишлатиладиган ахборотни ҳимоя қилиш воситаларининг хусусиятларини ҳисобга олади:

$$P_{iS} = \frac{1}{M_i + S}. \quad (7.7)$$

Агар  $M_i = 0$  бўлса бу ҳимоя йўқлигини англатади ва (7.7) ифода (7.6) га айланади. Агар  $M_i$  ошиб борса, унда ахборотдан рухсатсиз фойдаланиш эҳтимоли камаяди, бу эса ҳодисанинг физикасини тўғри акс эттиради.

ИКТнинг ихтиёрий  $i$  — чи қисми учун  $N_i$  мумкин бўлган хавфсизлик таҳдидлари. Шундай қилиб,  $i$  — чи қисм учун мумкин бўлган хавфсизлик таҳдидлари  $N_i$  дан камида битта хавфсизлик таҳдидини амалга оширилганда  $U_i$  ахборотидан рухсатсиз фойдаланиш эҳтимоли учун қуйидаги ифода тўғри бўлади:

$$U_i = 1 - (1 - P_{iS})^{N_i}. \quad (7.8)$$

$k$  қисмларда бир хил турдаги хавфсизлик таҳдидлари мавжуд, бу ерда таҳдидларни амалга ошириш каналари ҳам пайдо бўлиши мумкин. Шунинг учун, барча  $k$  қисмларни ҳисобга олган ҳолда, камида битта хавфсизликка таҳдид амалга оширилганда, ахборотдан рухсатсиз фойдаланиш эҳтимоли учун, ҳодисаларнинг умумий эҳтимолини ҳисоблаш учун қуйидаги ифода тўғри бўлади:

$$P_x = \sum_{i=0}^k \eta_i U_i = \frac{N_i}{S} [1 - (1 - P_{iS})^{N_i}] \quad (7.9)$$

бу ерда  $\eta_i$  қиймати  $\eta_i = \frac{N_i}{S}$  муносабати билан аниқланади.

$P_x$  қиймати камида битта қисмда ҳеч бўлмаганда битта хавфсизлик таҳдиди амалга оширилганда ахборотдан рухсатсиз фойдаланиш эҳтимоли.

Агар қисмлар бир хил миқдордаги хавфсизлик таҳдидига эга бўлса, яъни,  $N_1 = N_2 = \dots = N_k$ ,  $S = N_1 + N_2 + \dots + N_k = k * N_i$  шундай экан, ифода  $\eta_i = \frac{N_i}{S} = \frac{N_i}{k \cdot N_i} = \frac{1}{k}$

ундан кейин (7.9) формула қуйидаги кўринишга келади:

$$P_x = \sum_{i=0}^k \eta_i U_i = \frac{1}{k} \sum_{i=1}^k [1 - (1 - P_{iS})^{N_i}] \quad (7.9.1)$$

(7.9 ва 7.9.1) формулалар ИКТнинг барча қисмлари учун камида битта мумкин бўлган хавфсизлик таҳдидлари амалга оширилганда ахборотдан рухсатсиз фойдаланиш эҳтимолини аниқлайди. Бу ҳолатда умумий етказилган зарар минимал бўлиши мумкин деб тахмин қиламиз. Бошқа томондан, камида битта хавфсизлик таҳдидини амалга ошириш пайтида ахборотдан рухсатсиз фойдаланиш эҳтимоли хавфсизлик хусусияти сифатида максимал қийматни олади, яъни ИКТдаги ахборотдан рухсатсиз фойдаланишни эҳтимолигининг юқори чегараси баҳолаш.

Максимал зарар барча мумкин бўлган хавфсизлик таҳдидларини амалга ошириш вақтида содир бўлади, яъни:

$$P_y = \prod_{i=1}^k P_{iS}^{N_i} \quad (7.10)$$

Шундай қилиб, ИКТнинг ҳимояланганлигини иккита  $P_x$  ва  $P_y$  орқали баҳолаймиз, улар ахборотдан рухсатсиз фойдаланишнинг эҳтимолини пастки ва юқори чегараларини беради, улар ИКТга зарар етказишнинг яхши ва ёмон ҳолатларига тўғри келади.

$T_a$  интервалнинг берилган қиймати учун ИКТнинг  $T$  объектини эксплуатация вақтида хавфсизликга таҳдидни амалга ошириш учун бўлган барча ёки камида битта уринишлар сонини  $R$  аниқлаш мумкин:

$$R = \frac{T}{T_a}, \quad (7.11)$$

бу ерда  $T$  — эксплуатация вақти,  $T_a$  — хавфсизликка таҳдидларни амалга ошириш босқичи.

$T$  — эксплуатация вақтида барча ёки ҳеч бўлмаганда битта хавфсизликка таҳдид амалга оширилганда ҳимояланган ахборотлардан рухсатсиз фойдаланиш эҳтимолигини баҳолаш мумкин:

$$P(t) = 1 - (1 - P_k)^R \quad (7.12)$$

бу ерда  $P_k$  — қиймати, хавфсизлик таҳдидларини амалга ошириш учун битта муваффақиятли уриниш эҳтимолини тавсифловчи маълум қиймат ва  $t = T$ .

Шуни таъкидлаш мумкинки, (7.12) ифода муайян КТ учун хавфсизликка таҳдидларнинг барча рўйхати бўйича ҳам, маълум бир йўналишни ташкил этувчи таҳдидлар учун ҳам ишлатилиши мумкин. Хусусан, амалга оширилиши мумкин бўлган ахборотнинг махфийлиги ва унинг яхлитлигини бузадиган хавфсизликка таҳдидларни ажратиб кўрсатиш мумкин.

Турли хил КТлар учун турли йўналишдаги хавфсизлик таҳдидларини амалга оширишдан етказилган зарар сезиларли даражада фарқ қилиши мумкин. Бу КТнинг бажарадиган функцияларининг хилма-хиллигига боғлиқ.

Моделаштириш орқали олинган миқдорий натижаларни жадвал ва график кўринишда тасвирлаш мумкин бўлади.

(7.12) ифода КТда ахборотдан рухсатсиз фойдаланиш эҳтимолини юқори чегарасини беради, яъни энг ёмон ҳолати учун бу эса, КТни лойиҳалашда муҳим бўлган кўрсаткичи ҳисобланади.

7.1-жадвалда турли хил бошланғич параметрларга эга КТ учун  $P_x$  ва  $P_y$  ҳимояланганликни баҳолашни сон жиҳатидан фарқи кўрсатилган.

7.2-жадвалда КТ4 ва КТ7 учун хавфсизликка таҳдидни амалга оширишга барча уринишлар сонини ва камида битта хавфсизликка таҳдидни амалга оширилганда ахборотдан рухсатсиз фойдаланиш эҳтимоли кўрсатилган.

7.1-жадвал

## КТда ахборот ҳимояланганлигини баҳолаш

	<i>КТ1</i>	<i>КТ2</i>	<i>КТ3</i>	<i>КТ4</i>	<i>КТ5</i>	<i>КТ6</i>	<i>КТ7</i>
<i>S</i>	12	15	20	30	40	50	50
<i>K</i>	3	3	3	3	3	4	4
<i>N<sub>1</sub></i>	3	5	5	4	10	10	10
<i>N<sub>2</sub></i>	4	5	6	6	10	10	10
<i>N<sub>3</sub></i>	5	5	7	10	10	10	10
<i>M<sub>1</sub></i>	3	3	9	5	3	6	4
<i>M<sub>2</sub></i>	4	3	3	2	3	6	5
<i>M<sub>3</sub></i>	2	3	6	9	3	6	9
<i>P<sub>1</sub></i>	0,066	0,055	0,037	0,040	0,030	0,021	0,022
<i>P<sub>2</sub></i>	0,063	0,055	0,047	0,045	0,030	0,021	0,023
<i>P<sub>3</sub></i>	0,071	0,055	0,042	0,034	0,030	0,021	0,020
<i>U<sub>1</sub></i>	0,187	0,248	0,172	0,151	0,265	0,197	0,205
<i>U<sub>2</sub></i>	0,227	0,248	0,254	0,243	0,265	0,197	0,209
<i>U<sub>3</sub></i>	0,309	0,248	0,257	0,296	0,265	0,197	0,186
<i>P<sub>x</sub></i>	0,251	0,248	0,232	0,251	0,265	0,197	0,198
<i>P<sub>y</sub></i>	8,411	1,481	1,772	5,371	2,782	3,091	3,282

7.2-жадвал

*R* га боғлиқ равишда КТдаги ахборот ҳимояланганлигини баҳолаш

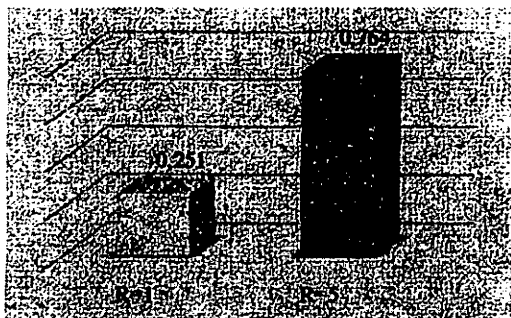
<i>R</i> уруниш- лар сони	<i>КТ4</i>		<i>КТ7</i>	
	<i>P<sub>x</sub></i>	<i>P<sub>y</sub></i>	<i>P<sub>x</sub></i>	<i>P<sub>y</sub></i>
0,20	0,056	3,2934	0,048	6,3673
0,25	0,069	8,2532	0,059	4,7470
0,33	0,092	1,2632	0,079	7,5869
0,5	0,134	5,4830	0,116	4,6767
1	0,251	5,3729	0,218	3,0865
2	0,439	7,2927	0,389	2,4562
3	0,580	2,6425	0,523	6,3760
4	0,685	1,2524	0,627	4,2557
5	0,764	9,8321	0,709	7,6753
6	0,823	5,3720	0,772	2,9251



Ҳеч бўлмаганда битта хавфсизликка таҳдид  $P_x$  амалга оширилганда ахборотдан рухсатсиз фойдаланиш эҳтимолигини миқдорий баҳолашнинг КТ эксплуатация параметрларига боғлиқлигини таҳлил қиламиз. Шундай қилиб, 7.1-жадвалда КТ№5 хавфсизликка таҳдидлар сони  $S = 40$  га тенг бўлганда  $P_x=0.265$  энг юқори қийматини қабул қилади.  $S$  нинг камроқ қийматларида  $P_x$  нинг қийматлар миқдори камаяди, яъни КТ№3 да  $S = 20$  га тенг бўлганда  $P_x=0.232$ , КТ№4 да сони  $S = 30$  га тенг бўлганда  $P_x=0.251$ , КТ№1 да сони  $S = 12$  га тенг бўлганда  $P_x=0.251$ , КТ№2 да сони  $S = 15$  га тенг бўлганда  $P_x=0.248$ .

$P_x=0.232$  нинг энг паст қиймати КТ№3да қабул қилинганлиги аниқланди, бу ерда ахборотларни ҳимоя қилиш воситаларининг мажмуасини қисмлари учун аҳамиятлилик коэффициентлари энг юқори кўрсаткичларга эга (9, 3, 6).

7.2-жадвални таҳлил қилиб, хавфсизликка таҳдидларни амалга оширишга уринишларнинг сонини ўсиши билан  $P_x$  сезиларли даражада ошади деган хулосага келишимиз мумкин. Шундай қилиб, КТ№4 хавфсизликка таҳдидларни амалга оширишга уринишларнинг сони битта бўлганда  $P_x = 0.251$  га тенг. Хавфсизликка таҳдидларни амалга оширишга уринишларнинг сони бешта бўлганда  $P_x = 0.764$  га тенг.



**7.1-расм.** Муайян ҳолат учун  $R$  га боғлиқ равишда КТдаги ахборот ҳимояланганлигини баҳолаш

Шундай қилиб, ишлаб чиқилган аналитик ҳисоб-китоблар ИКТни лойиҳалаш босқичларида ахборотдан рухсатсиз фойдаланиш эҳтимолининг юқори ва пастки чегараларини ва хавфсизликка таҳдидларни амалга оширишга урунишлар сонини ҳисоблаш имконини беради.

## **7.2. Рухсатсиз фойдаланишдан ахборотнинг ҳимояланганлигини миқдорий баҳолаш моделини ишлаб чиқиш**

Ҳозирги вақтда ИКТда ахборотдан рухсатсиз фойдаланишда ахборотларни ҳимоя қилишни ўрганиш ва тизимни баҳолаш билан боғлиқ бўлган ягона амал қилинадиган ҳужжатларнинг йўқлиги бироз қийинчилик келтиради. Ахборот ҳимояланганлигини миқдорий баҳолашнинг хорижий усуллари (ахборот хавфсизлигига бўладиган хавф-хатарларни таҳлилга асосланган ёндашув [80], Клементс-Хоффман хавфсизликни таъминлаш тизими моделига асосланган ёндашув [81, 82, 83] бир қатор камчиликлари мавжуд, хусусан:

- ИКТнинг реал тузилиши ҳисобга олинмайди;
- ахборотдан рухсатсиз фойдаланишдан етказилган зарар қиймати пул бирликларида баҳоланади, бу эса барча ИКТ учун мақбул эмас;

- ахборотдан рухсатсиз фойдаланишни амалга ошириш тартибининг ўзгарувчанлиги ва ахборотни ҳимоя қилиш жараёнининг динамик хусусиятлари тўлиқ ҳисобга олинмайди.

ИКТда ахборотдан рухсатсиз фойдаланишдан ҳимояланганлиги, бу унинг ресурсларининг ҳимояланганлиги билан белгиланади. Хавфсизликни баҳолаш учун комплекс кўрсаткичларидан фойдаланиш тавсия этилади, ИКТда ресурсларнинг хавфсизлигини бузиш жараёнлари, ҳамда тизимнинг ҳимояланган ҳолатини назорат қилиш ва тиклаш жараёнлари ҳисобга олинади. Шундай кўрсаткич сифатида ахборотдан рухсатсиз фойдаланишни олдини олиш учун ИКТда ахборот ҳимояланганлик коэффицентидан фойдаланиш таклиф этилади, бу ҳолат

ишончлилик назариясида тайёрлик коэффициентига ўхшаш [84, 85, 86].

ИКТда ахборотдан рухсатсиз фойдаланишда агар битта ресурснинг ҳимояланганлигини тиклаш мумкин бўлса, у ҳолда ахборотнинг ҳимояланганлик коэффициентини ҳисоблаш учун қуйидаги формуладан фойдаланиш мумкин:

$$K_{\text{х ИКТ}} = \frac{1}{\sum_{i=0}^{N_{\text{хр}}} A_{N_{\text{хр}}}^i \left( \frac{\lambda_{\text{хб}} i}{\mu_{\text{хт}} i} \right)} \quad (7.13)$$

Бу ерда  $N_{\text{хр}}$  — ҳимояланаётган ресурслар сони,  $A_{N_{\text{хр}}}^i = \frac{N_{\text{хр}}!}{(N_{\text{хр}}-i)!} N_{\text{хр}}$  — дан  $i$  гача жойлаштиришлар сони,  $\lambda_{\text{хб}}$  — ресурс хавфсизлигини бузиш интенсивлиги,  $\mu_{\text{хт}}$  — ресурс ҳимояланганлигини тиклаш интенсивлиги.

Ҳимояланган ресурсларни тиклашда шартли равишда чекланмаган имкониятлар мавжуд бўлса, у ҳолда қуйидаги формуладан фойдаланилади:

$$K_{\text{х ИКТ}} = \prod_{i=1}^{N_{\text{хр}}} \frac{\mu_{\text{хт}}}{\lambda_{\text{хб}} + \mu_{\text{хт}}} \quad (7.14)$$

Рухсатсиз фойдаланишда ахборот ҳимояланганлигини қийёсий тахлилини амалга ошириш учун урта КТ мисолида кўриб чиқамиз [87]. Бунда маҳаллий тармоқлар асосида қурилган кўлами ва имкониятлари ҳар хил бўлган ҳимоялаш тизимларидан фойдаланилади. Ташкилотнинг ҳар бир ходимида унинг фойдаланувчи маълумотлари жойлашган Windows 7 операцион тизимида ишловчи ишчи станцияси мавжуд бўлсин. Ишчи станциялар Windows 2008 Server операцион тизимига асосланган бир нечта серверлар ёрдамида компьютер тармоғига бирлаштирилган, уларда почта сервери, маълумотлар базасини бошқариш тизимлари, ташкилотнинг веб сервери, ходимлар учун тезкор хабарлар жўнатиш тизими ва бошқалар мавжуд. Биринчи корхонанинг ИКТда 100 та (10 та серверларда жойлаштирилган умумий ресурслар, 90 та ресурс уларнинг ишчи станцияларида жойлашган), иккинчи корхонанинг ИКТда 200 та (20 та серверларда жойлаштирилган умумий ресурслар, 180 та ресурс фойдаланувчилар маълумотлари) ва учинчи корхонанинг

ИКТда 300 та (30 та серверларда жойлаштирилган умумий ресурслар, 170 та ресурс фойдаланувчилар маълумотлари) муҳим ҳимояланган ресурсга эга бўлсин.

Энг ёмон ҳолатдан келиб чиқиб, бузғунчи “Мукамал” (юқори малакали, янги заифликларни пайдо бўлишини доимий равишда кузатиб боради, шунингдек, кўриб чиқилаётган ташкилотнинг ИКТда қайта ишланаётган маълумотларидан рухсатсиз фойдаланишда уларни амалга ошириш имкониятига эга) деб фараз қиламиз. Тажавузкор бундай моделдан фойдаланганда ИКТда ахборот ҳимояланганлиги бузилишларининг интенсивлиги дастурий таъминотдаги пайдо бўладиган заифликлар интенсивлигига мос келади. Windows операцион тизимида ишлайдиган ИКТда заифликларни аниқлаш бўйича статистик маълумотларга кўра, ўртача ҳимояланган ахборотни бузилиш интенсивлиги ойига 9 тани ташкил этади, яъни  $\lambda_{\text{хб}} = 0,013/\text{соат}$ . Одатда, ташкилотнинг ИКТ хавфсизлик маъмури бир вақтнинг ўзида фақатгина битта ресурснинг ҳимояланганлигини тиклаши мумкин. У ҳолда (7.13) формуладан фойдаланиб, бундай шароитда ИКТда ахборот хавфсизлиги коэффициентини ресурснинг ҳимояланганликни тиклаш интенсивлигига боғлиқлигини олиш мумкин (7.2-расм).



7.2-расм. Чекланган ресурсларда ресурс ҳимояланганлигини тиклаш интенсивлигига боғлиқлиги

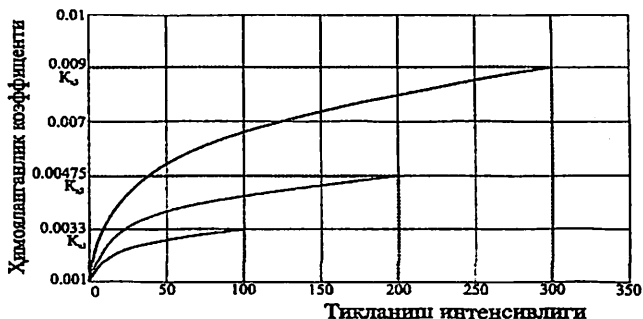
Айтайлик, ташкилотда ахборот ҳимояланганлигини тиклаш учун чекланмаган имкониятлар мавжуд. У ҳолда (7.14) формуладан фойдаланиб, ИКТда ахборот хавфсизлиги коэффициентини ресурсни ҳимояланганликни тиклаш интенсивлигига боғлиқлигини олиш мумкин (7.3-расм).



7.3-расм. Чекланмаган ресурсларда ресурс химояланганлигини тиклаш интенсивлигига боғлиқлиги

Ўрта корхонанинг хавфсизлик маъмури томонидан ИКТда ресурсларни ҳимояланганлигини тиклаш интенсивлиги қандай бўлишини кўриб чиқамиз. ИКТда ахборотдан рухсатсиз фойдаланишда ахборот химояланганлик коэффициенти куйидаги талаб этилган қийматлар асосида:  $K_{x_1 \text{ икт}} = 0.0033$ ,  $K_{x_2 \text{ икт}} = 0.00475$ ,  $K_{x_3 \text{ икт}} = 0.0099$ .

Корхонанинг ИКТ хавфсизлик маъмури томонидан ахборот химояланганлигини тиклаш учун чекланган ресурсга эга деб фараз қиламиз, унда ҳисоблаш учун (7.13) формуладан фойдаланамиз. Ҳисоблаш натижалари 7.4-расмда келтирилган.



7.4-расм.  $K_{x_1 \text{ ИКТ}} = 0.0033$ ,  $K_{x_2 \text{ ИКТ}} = 0.00475$ ,  $K_{x_3 \text{ ИКТ}} = 0.009$  да ресурс химояланганлигини тиклаш интенсивлиги

ИКТ хавфсизлик маъмури томонидан ресурсларни химояланганлигини тиклаш учун сарф қилинадиган вақтни ҳисоблаш натижалари қуйидаги жадвалда келтирилган.

7.3-жадвал

**Химояланганлик коэффициентининг талаб қилинган қийматларида химояланганликни тиклаш учун сарф этиладиган вақт**

$K_{x \text{ ИКТ}}$	$\mu_{\text{ИКТ}}$ , марта/соат	Ресурс химояланганлигини тиклаш учун сарфланган вақт
0,0033	100	0.0231 минут
0,00475	200	0.0475 минут
0,009	300	0.9 минут

ИКТда ахборот химояланганлигини назорат қилишни  $K_{\text{ИКТ}} \geq 0.99$  мувофиқлик мезони бўйича қуйидаги хулосаларини чиқариш мумкин:

- ИКТда рухсатсиз фойдаланишда маълумотларнинг хавфсизлик даражаси боғлиқлигини тиклашга ажратилган ресурсларнинг химояланганлигини тиклаш учун сарфланган вақт яққол ночизиқ характерга эга;

- керакли хавфсизлик даражасини таъминлаш учун қўшимча ва муқобил химоя воситаларидан фойдаланиш керак.

## Фойдаланилган адабиётлар

1. <https://www.ptsecurity.com/ru-ru/research/analytics/cyber-security-threatscape-2021-q3/>
2. Внуков А. А. Основы информационной безопасности: защита информации. - 2-е изд., испр. и доп. М.: Издательство Юрайт, 2019. – 240 с.
3. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности - Санкт-Петербург: НИУ ИТМО, 2014. - 173 с.
4. Kadirov M.M., Yuldasheva M., Akbarova Sh.A., Problems of Security of Infocommunication Systems. International Journal of Advanced Research in Science, Engineering and Technology (IJARSET), Vol. 6, Issue 2, India 2019, P.8026-8031.
5. Мухин В. Е., Волокита А. Н., Павленко Е. Н. Мониторинг состояний информационных ресурсов для реализации адаптивного управления защищенностью компьютерных систем // Искусственный интеллект. – Донецк: ИПИИ МОН Украины и НАН Украины. – 2005. – №. 3. – С. 670-680.
6. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. Москва: Ленанд, 2016. – 248 с.
7. Запечников С.В. Адаптивное управление механизмами защиты распределенных компьютерных систем // XIII Всероссийская научная конференция - Проблемы информационной безопасности, 2006 – с.48-49.
8. Gulomov Sh.R., Kadirov M.M., Tulyaganov Z.Ya. The methodology of the ways for increasing the efficiency of intrusion detection systems. International Journal of Engineering Innovation & Research Volume 5, Issue 5, ISSN: 2277 – 5668, India 2016, p.296-302.
9. Кадилов М.М. Современные системы обнаружения атак в беспроводных сетях. Вестник ТашГТУ, №1, Ташкент 2015, с.50-55.

10. O'zDStISO/IEC 27005:2013 – “Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлиги рискларини бошқариш”.
11. Щеглов А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры //М.: Издательство Юрайт. – 2020. – 309 с.
12. Богульская Н.А., Кучеров М.М. Модели безопасности компьютерных систем. Учебное пособие. – Красноярск: Сиб. федер. Ун-т, 2019. – 206 с.
13. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. – Горячая линия-Телеком, 2012. – 322 с.
14. Щеглов А. Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие //СПб: Университет ИТМО. – 2014. – 95 с.
15. Девянин П. Н. Обзорные лекции по моделям безопасности компьютерных систем //Прикладная дискретная математика. Приложение. – 2009. – №. 2.
16. Мухин В. Е., Волокита А. М. Разработка и реализация политики безопасности в распределенных компьютерных системах //Управляющие системы и машины. – 2010.
17. Ревнивых А. В., Федотов А. М. Обзор политик информационной безопасности //Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2012. – Т. 10. – №. 3.
18. Kadirov M.M., Tashmatova Sh.S., Ganiyeva T.I., Kurbonova K.E. Comparative analysis of information security models in computer networks. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 6, Issue 2, India 2019, p. 8198-8204.
19. Harrison M. A., Ruzzo W. L., Ullman J. D. Protection in operating systems //Communications of the ACM. – 1976. – Т. 19. – №. 8. – С. 461-471.



20. Karimov M.M., Kadirov M.M., Some features of the use of models discretionary access control for protection against malware // Журнал «Вестник ТашГТУ». –Ташкент, 2015. №2. –С. 28-34.

21. Harrison M. A., Ruzzo W. L., Ullman J. D. On protection in operating systems //Acm Sigops Operating Systems Review. – 1975. – Т. 9. – №. 5. – С. 14-24.

22. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М. : Горячая линия-Телеком, –2000. – 452 с.

23. Sandhu R. S. The typed access matrix model //IEEE Symposium on Security and Privacy. – 1992. – С. 122-136.

24. Kadirov M.M. Access Control Model and Policies for Collaborative Environments // International Journal of Advanced Research in Science, Engineering and Technology, Vol. 4, Issue 7, India 2017. –PP. 4223-4229.

25. Bishop M. Theft of information in the take-grant protection model //Journal of Computer Security. – 1995. – Т. 3. – №. 4. – С. 283-308.

26. Brechka D. Analysis of access in the Take-Grant model //arXiv preprint arXiv:1208.0108. – 2012.

27. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности: Учеб. Пособие для вузов. – М.: Радио и связь, 2000. – 192 с.

28. Bell D. E., La Padula L. J. Secure Computer System: Unified Exposition and Multics Interpretation. Bedford, MA 01730 - March, 1976. p 127.

29. Кадилов М.М., Тулаганов З.Я. Модель Белла-ЛаПадуды в управление доступом. Сборник статей международной научно-технической конференции “Радиоэлектроника, информационные и телекоммуникационные технологии: проблемы и развитие”, II том, Ташкент 2015, 188-190 стр.

30. Куликов С. С. Модели безопасности компьютерных систем: учеб. пособие [Электронный ресурс]. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015. – 178 с.

31. Щеглов К. А., Щеглов А. Ю. Непротиворечивая модель мандатного контроля доступа // Приборостроение. 2014. №4. – С. 12-15.

32. Кадилов М.М. Фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини ошириш моделини такомиллаштириш. “Ўзбекистонда илмий-амалий тадқиқотлар” мавзусидаги республика 14 - кўп тармоқли илмий масофавий онлайн конференция материаллари тўплами// 31.03.2020. Тошкент: Tadqiqot 2020. 160-163 бетлар.

33. Соколова С. П., Горковенко Е. В. Интеллектуальная система классификации с иерархической структурой множества объектов защиты в системах с мандатным разграничением доступа к информации //Актуальные проблемы экономики и управления. – 2015. – №. 1. – С. 93-106.

34. Белим С. В., Белим С. Ю., Бречка Д. М. Проблемы обработки и защиты информации. Модели политик безопасности компьютерных систем/ Омск: «ООО Полиграфический центр КАН». – 2010. – С 223.

35. Kadirov M.M. Development of mathematical model of system of information security at control of access to the created file objects // Журнал «Вестник ТашГТУ». –Ташкент, 2016. №1. –С. 62-68.

36. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 с.

37. Соколова С. П., Горковенко Е. В. Интеллектуальная система классификации с иерархической структурой множества объектов защиты в системах с мандатным разграничением доступа к информации //Актуальные проблемы экономики и управления. – 2015. – №. 1. – С. 93-106.

38. Kadirov M. M., Akbarova Sh.A., Vahidova G.R. Improving the model of information security with a mandatory access control policy // Materials of the XVI international scientific and practical conference science without borders – 2020: England, March 30 - April 7, 2020 Volume 14. –PP. 170-172.

39. Орлов А. И. Математические методы теории классификации // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2014. – №. – С 95-99.

40. Блюм В. С., Заболотский В. П. Социальная иммунная система и иммунокомпьютинг // Региональная информатика и информационная безопасность. – 2015. – С. 264-272.

41. Tarakanov A. O., Skormin V. A., Sokolova S. P. Immunocomputing: principles and applications. – Springer Science & Business Media. – 2013. – 204 p.

42. Melnikov Y., Tarakanov A. Immunocomputing model of intrusion detection // International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security. – Springer, Berlin, Heidelberg, 2003. – P. 453-456.

43. Kadirov M.M., Tulyaganov Z.Ya., Karimova N.A., Comparative analysis of modern security monitoring systems. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 5, Issue 8, India 2018, p. 6548-6553.

44. Sandhu R. S. et al. Role-based access control models // Computer. 1996. – Т. 29. – №. 2. – С. 38-47.

45. Ferraiolo D. F. et al. Proposed NIST standard for role-based access control // ACM Transactions on Information and System Security (TISSEC). – 2001. – Т. 4. – №. 3. – С. 224-274.

46. Kadirov M.M., Tulyaganov Z.Ya. Developing Software Module Based on TT-RBAC Model of Access Control. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 4, Issue 10, India 2017, p. 4664-4673.

47. Sandhu R. S. Role-based access control // Advances in computers. – Elsevier, 1998. – Т. 46. – С. 237-286.

48. Каримов М.М., Кадиров М.М. Сагатова С.М. Применение ролевой модели контроля доступа в защите информации. Международная научно-практическая конференция, “Инновация 2015”, Сборник научных статей, Ташкент 2015, 303-304 стр.

49. Ракицкий Ю. С. Импорт и экспорт ролевой политики безопасности в СУБД Oracle //Математические структуры и моделирование. – 2018. – №. 4 (48). – С. 147-153.

50. В. В. Скакун. Защита информации в базах данных и экспертных системах: пособие для студентов фак. радиофизики и комп. технологий / В.В. Скакун. – Минск: БГУ, 2015. – 140 с.

51. Ghazal R. et al. Intelligent Agent-Based RBAC Model to Support Cyber Security Alliance Among Multiple Organizations in Global IT Systems //17th International Conference on Information Technology–New Generations (ITNG 2020). – Springer, Cham, 2020. – P. 87-93.

52. Белим С. В., Ракицкий Ю. С. Объектно-ориентированная модель защищенного электронного документооборота //Вопросы защиты информации. – 2014. – №. 3. – С. 89-93.

53. Киреенко А. Е. Модели разграничения доступа в компьютерных системах: реализация, особенности, сравнительный анализ //Социальная политика и социология. – 2012. – №. 2. – С. 222-239.

54. Богаченко Н. Ф. Алгоритм определения основных характеристик решетки ценностей по графу доступов //Математическое и компьютерное моделирование: сборник. – 2018. – С. 188-190.

55. Kadirov M. M., Tojikhujueva N. Z., Kasimova G. I., Usmanbayev D. Sh. Methodology for Developing a Mandatory Security Policy Based on Two Value Chains // International Journal of Advanced Research in Science, Engineering and Technology, Vol. 6, Issue 11, India 2019. –PP. 11855-11859.

56. Kadirov M., Tulyaganov Z., Tojikhujueva N., Karimova N. Development of an Algorithm for Implementing Mandatory and Role-Based Access Control // International Journal of Emerging Trends in Engineering Research, Vol. 8, Issue 4, India 2020. –PP. 1027-1033.

57. Пог О. А. Многокритериальная модель решетки ценностей для реализации мандатных политик безопасности в системах

разграничения доступа //Информационное противодействие угрозам терроризма. – 2013. – №. 20. – С. 116-121.

58. Kadirov M., Tadjibaeva D., Rasulev A., Islomova F. Joint Implementation of Mandated and Role-Based Delimitation of Access to Information Flows in Infocommunication Systems // International Journal of Emerging Trends in Engineering Research, Vol. 8, Issue 5, India 2020. -PP. 1892-1896.

59. Sánchez Y. K. R., Demurjian S. A., Baihan M. S. A service-based RBAC & MAC approach incorporated into the FHIR standard //Digital Communications and Networks. – 2019. – Т. 5. – №. 4. – С. 214-225.

60. Phillips Jr C. E. et al. A service-based approach for RBAC and MAC security //Service-oriented software system engineering: Challenges and Practices. – IGI Global, 2005. – С. 317-339.

61. Kocatürk M. M., Gündem T. İ. A fine-grained access control system combining MAC and RBAC models for XML //Informatica. – 2008. – Т. 19. – №. 4. – С. 517-534.

62. Белим С. В., Богаченко Н. Ф., Фирдман И. А. Обратная задача построения мандатной политики безопасности //Математические структуры и моделирование. – 2010. – №. 1 (21). –С. 119-127.

63. Щеглов К. А., Щеглов А. Ю. Реализация метода мандатного доступа к создаваемым файловым объектам системы //Вопросы защиты информации. – 2013. – №. 103. – С. 16-20.

64. Щеглов А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры //М.: Издательство Юрайт. – 2020. – 309 с.

65. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. – 328 с.

66. Miraziz Sagatov, Durdon Irgasheva, Mirhusan Kadirov. Construction hardware protection infocommunication systems from network attacks. ICAICTSEE – 2015, November 13 – 14th, 2015, Sofia, Bulgaria. 271-277 стр.

67. Ракицкий Ю.С., Белим С.В. Возможность совместной реализации ролевой и мандатной политик безопасности // Решетневские чтения. 2009. №13. – С. 573-574.

68. Девянин П. Н. О результатах формирования иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. – 2016. – №. 9. –С. 84-87.

69. Алексеев А. Л., Красноперова Е. А., Вахрушева Е. А. Гипервизоры и виртуальные машины// Информационные технологии в науке, промышленности и образовании. – 2019. – С. 121-128.

70. Девянин П. Н. Ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux // Прикладная дискретная математика. – 2012. – №. 1 (15). –С. 64-77.

71. Kadirov M.M., Karimova D., Tojikhujajeva N.Z., Tulyaganov Z.Ya, Classification of modern security monitoring systems in computer systems and networks. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 8, Issue 6, India 2021, p. 6764-6769.

72. Михнев И. П., Капицына М. А., Зайцева В. А. Автоматизированная система радионуклидной спектрометрии: защита информации от несанкционированного доступа // Научные исследования: векторы развития. – 2018. – С. 110-114.

73. Kadirov M.M., Karimova N.A., Djurayeva Sh.T, Nosirjonova M. M., A model for assessing the security of information from unauthorized access when designing computer systems in a protected version. International Journal of Advanced Research in Science, Engineering and Technology (IJARSET), Vol. 6, Issue 3, India 2019, P.8426-8432.

74. Герасименко В. А. Защита информации в автоматизированных системах обработки данных // М.: Энергоатомиздат. – 1994. – Т. – С. 536.

75. Kadirov M.M. Approach to Assessing the Security of Information From Unauthorized Access // International Journal of

Advanced Research in Science, Engineering and Technology. ISSN: 2350-0328, India, Vol. 6, Issue 12, India 2019. –PP. 12182-12187.

76. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учеб. пособие. – М.: ИЦ Академия, 2009. – 416 с.

77. Дроботун Е. Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. – СПб.: Научно-технические технологии, 2017. – 120 с.

78. Гуломов Ш.Р, Кадиров М.М., Защита информации от сетевых атак// Монография, «Fan va texnologiya», ISBN 978-9943-6155-4-0, Ташкент – 2019, С – 172.

79. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: учеб. пособие для вузов. – М.: Радио и связь, 2003. – № 6. – 296 с.

80. Витенбург Е. А. Поддержка принятия решений при проектировании системы защиты информации на предприятии // Информационные технологии (IT) в контроле, управлении качеством и безопасности. – 2019. – С. 75-79.

81. Астахова Л.В. Теория информационной безопасности и методология защиты информации: учебное пособие. – Челябинск: Издательский центр ЮУрГУ, 2014. – 137 с.

82. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. №2 (4). – С. 42-48.

83. Янников И. М., Телегина М. В. Особенности реализации системы оценки защищенности критически важных и потенциально опасных объектов на основе метода Клементса-Хоффмана // Интеллектуальные системы в производстве. – 2018. – Т. 16. – №. 4. – С. 169-175.

84. Козленко А. В. и др. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. – 2012. – Т. 2. – №. 21. – С. 41-55.

85. Казарин О. В., Кондаков С. Е., Троицкий И. И. Подходы к количественной оценке защищенности ресурсов автоматизированных систем //Вопросы кибербезопасности. – 2015. – №. 2 (10). – С. 31-35.

86. Кондаков С. Е. К вопросу о количественной оценке защищенности информации от несанкционированного доступа в информационных системах //Труды Международного симпозиума «Надежность и качество». – 2015. – Т. 1. – С. 83-85.



## МУНДАРИЖА

<b>КИРИШ</b> .....	3
<b>I БОБ. ИНФОКОММУНИКАЦИОН ТИЗИМЛАРДА АХБОРОТНИНГ ҲИМОЯЛАНГАНЛИГИНИ ОШИРИШНИНГ УСУЛ ВА ВОСИТАЛАРИНИ ТАҲЛИЛИ</b>	
1.1. Инфокоммуникацион тизимларнинг ҳимояланган- лиги муаммоларининг таҳлили .....	7
1.2. Инфокоммуникацион тизимларида ахборот ҳимоя- ланганлигини ошириш усуллари таҳлили .....	10
<b>II БОБ. ИНФОКОММУНИКАЦИОН ТИЗИМЛАРИДА ФЙДАЛАНИЛАДИГАН ХАВФСИЗЛИК МОДЕЛЛАРИНИНГ АСОСИЙ ТУШУНЧАЛАРИ</b>	
2.1. Ахборотдан фойдаланишни назоратлашда фойдала- ниладиган асосий тушунчалар .....	14
2.2. Фойдаланишни назоратлаш усулининг умумлаш- тирилган схемаси .....	16
2.3. Ахборотдан фойдаланишни назоратлашда сиёсат турлари .....	17
<b>III БОБ. ФЙДАЛАНИШНИ БОШҚАРИШНИНГ ДИСКРЕЦИОН МОДЕЛИ</b>	
3.1. Харрисон-Руззо-Ульман фойдаланиш матрицаси моделли .....	23
3.2. Типик фойдаланиш матрицаси модели .....	25
3.3. Take-Grant фойдаланишни тарқатиш модели .....	28
<b>IV БОБ. ФЙДАЛАНИШНИ МАНДАТЛИ БОШҚАРИШ МОДЕЛИ</b>	
4.1. Фойдаланишни мандатли бошқаришга асосланган Белл-ЛаПадула модели .....	33
4.2. Ахборот ҳимояланганлик даражасини оширишда mandatли фойдаланишни чеклаш усули .....	35
4.3. ИКТда фойдаланишни бошқаришнинг математик моделини ишлаб чиқиш .....	38

4.4. Фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини ошириш моделини такомиллаштириш .....	49
4.5. Бибанинг яхлитлик модели .....	55

**V БОБ. РОЛЛАРГА АСОСЛАНГАН  
Фойдаланишни бошқариш модели**

5.1. Ролларга асосланган фойдаланишни бошқариш моделининг ташкил этувчилари .....	60
5.2. Ролларга асосланган фойдаланишни бошқаришни маъмурлаш модели .....	62
5.3. Ахборот хавфсизлигини оширишда ролли моделни формаллаштириш .....	64
5.4. Ахборот ҳимояланганлигини оширишда ролларга асосланган фойдаланишни бошқариш усули .....	66

**VI БОБ. АХБОРОТДАН Фойдаланишни  
Чекловчи хавфсизлик сиёсатларини  
бирлаштириш усули ва алгоритмлари**

6.1. Икки қийматли панжарага асосланган мандатли хавфсизлик усули .....	73
6.2. Ролли ва мандатли хавфсизлик сиёсатини бирлаштириш усули .....	78
6.3. Операцион тизимларда мандат ва ролли фойдаланиш бошқариш модели .....	85
6.4. Мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми .....	91

**VII БОБ. ИНФОКОММУНИКАЦИОН  
Тизимларида ахборот  
ҳимояланганлигини баҳолаш**

7.1. Ахборотдан рухсатсиз фойдаланишдан ҳимоя қилишни баҳолашга бўлган ёндашув .....	101
7.2. Рухсатсиз фойдаланишдан ахборотнинг ҳимояланганлигини миқдорий баҳолаш моделини ишлаб чиқиш .....	109
<b>Фойдаланилган адабиётлар</b> .....	114

# QAYDLAR UCHUN

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

**М. М. КАДИРОВ**

**ИНФОКОММУНИКАЦИОН ТИЗИМЛАРДА  
АХБОРОТДАН ФойДАЛАНИШНИ БОШҚАРИШ  
УСУЛ ВА МОДЕЛЛАРИ**

Монография

Тошкент – «Fan va texnologiyalar nashriyot-matbaa uyi» – 2022

Мухаррир:  
Тех. муҳаррир:  
Рассом:  
Компьютерда  
саҳифаловчи:

Ш.Кушербаева  
Ш.Мирқосимова  
У.Ортиқов  
Н.Раҳматуллаева



**E-mail: [tipografiyasnt@mail.ru](mailto:tipografiyasnt@mail.ru) Tel: 97-450-11-14, 93-381-22-07.**

**Босишга рухсат этилди 14.04.2022.**

**Бичими 60x84 <sup>1</sup>/<sub>16</sub>. «Times New Roman» гарнитураси.**

**Офсет босма усулида босилди.**

**Шартли босма табоғи 8,75. Нашриёт босма табоғи 8,0.**

**Тиражи 300. Буюртма № 47.**

**«Fan va texnologiyalar nashriyot-matbaa uyi»  
bosmaxonasiда chop etildi.  
Тошкент ш., Фозилтепа кўчаси, 22 б уй.**