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

ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ

КАДИРОВ МИР-ХУСАН МИРПУЛАТОВИЧ

ИНФОКОММУНИКАЦИОН ТИЗИМЛАРДА АХБОРОТ ҲИМОЯЛАНГАНЛИГИНИ ОШИРИШНИНГ УСУЛ ВА ВОСИТАЛАРИНИ ТАКОМИЛЛАШТИРИШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2020

УДК: 004.056.53

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

Contents of dissertation abstract of the doctor of philosophy (PhD) on technical sciences

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

ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ

КАДИРОВ МИР-ХУСАН МИРПУЛАТОВИЧ

ИНФОКОММУНИКАЦИОН ТИЗИМЛАРДА АХБОРОТ ҲИМОЯЛАНГАНЛИГИНИ ОШИРИШНИНГ УСУЛ ВА ВОСИТАЛАРИНИ ТАКОМИЛЛАШТИРИШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2020

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2020.3.PhD/T308 рақам билан рўйхатга олинган.

Диссертация Тошкент давлат техника университетида бажарилган.

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

Илмий раҳбар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
Расмий оппонентлар:	**Абдурахимов Бахтиёр Файзиевич** физика-математика фанлари доктори, профессор
	Ганиев Абдухалил Абдужалилович техника фанлари номзоди, доцент
Етакчи ташкилот:	**«UNICON.UZ» – фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.01 Илмий кенгашнинг 2020 йил «08» сентябрь соат 14-00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (2619 рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-ўй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2020 йил «25» сентябрь да тарқатилди.
(2020 йил «24» августдаги 14 рақамли реестр баённомаси.)

Р.Х. Хамдамов
Илмий даражалар берувчи илмий кенгаш раиси, т.ф.д., профессор

Ф.М. Нуралиев
Илмий даражалар берувчи илмий кенгаш илмий котиби, т.ф.д., доцент

С.К. Ганиев
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, т.ф.д., профессор

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. 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. 2020 йилнинг биринчи чорагида киберинцидентлар сони тез суръатлар билан ошиб борди ва бунинг натижасида ахборот тизимларга бўладиган ҳужумлар сони 2019 йилга нисбатан 22,5% га ошганини яққол кўриш мумкин. Шунингдек жорий йилнинг ўзида мақсадли ҳужумлар сони 67% фоизни ташкил этди[1]. Бу борада хорижий мамлакатларда, жумладан, АҚШ, Нидерландия, Германия, Буюк Британия, Франция, Италия, Россия Федерацияси ва бошқа давлатларда инфокоммуникацион тизимларининг ҳимояланганлигини таъминловчи ахборотдан рухсатсиз фойдаланишни ҳимоялашнинг дастурий-аппарат воситаларини ишлаб чиқиш муҳим аҳамият касб этмоқда.

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 мандат ва ролли хавфсизлик моделини ишлаб чиқиш долзарб масала ҳисобланади.

Республикамизда давлат ва хўжалик бошқарув органларида инфокоммуникацион тизимларини ривожлантириш ҳамда шу тизимларда маълумотларни сирқиб чиқишини ва ахборотдан 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 қаршилик кўрсатиш»[2] вазифалари белгиланган. Мазкур вазифаларни амалга ошириш, жумладан, инфокоммуникацион тизимларда ахборотдан рухсатсиз фойдаланишни чекловчи хавфсизлик моделларини замонавий талаблар асосида такомиллаштириш муҳим масалалардан бири ҳисобланади.

---

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/

[2] Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 21 ноябрдаги ПҚ-4022-сон «Рақамли иқтисодиётни ривожлантириш мақсадида рақамли инфратузилмани янада модернизация қилиш чора-тадбирлари тўғрисида»ги қарори, 2019 йил 14 сентябрдаги ПҚ-4452-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштиришга оид қўшимча чора-тадбирлар тўғрисида»ги қарорлари ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти маълум даражада хизмат қилади.

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

Муаммонинг ўрганилганлик даражаси. Жаҳон миқёсида илмий-тадқиқотлар натижасида ахборотнинг ҳимояланганлигини оширишда ахборотдан рухсатсиз фойдаланишни чеклашнинг усул, модел ва воситаларини ривожлантиришга: D. Elliott Bell, Leonard J. LaPadula, R.S. Sandhu, D. Richard Kuhn, Zoran Stojanovich, Ajantha Dahanayake, 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 ҳисса қўшишган.

Ахборотдан фойдаланишни чекловчи хавфсизлик сиёсатларини бирлаштириш усуллари ва алгоритмлари билан боғлиқ муаммолар Rivera Sanchez, C.E. Phillips, Mustafa Kocatürk, Taflan Gündem, П.Н. Девянин каби хорижий олимларнинг илмий ишларида тадқиқ этилган.

Ушбу йўналишнинг Республикамизда ривожланишига Т.Ф. Бекмуратов, С.К. Ганиев, М.М. Каримов, А.А.Ганиев, Д.Я. Иргашева, А.А. Сулима, О.М. Исмоилов ва бошқалар ўзларининг муҳим ҳиссаларини қўшишган.

Шу билан бирга ахборотдан фойдаланишни чекловчи хавфсизлик моделларини бирлаштириш усулларининг назарий соҳасида натижаларга эришилганига қарамасдан, уларни амалий жиҳатдан инфокоммуникацион тизимларда қўллаш усуллари ва алгоритмлари етарлича тадқиқ этилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент давлат техника университетининг илмий-тадқиқот ишлари режасининг №А-5-48 «Ахборот коммуникация тизимларида яратилаётган файл объектларга назоратли мурожаатда ахборотни ҳимоялашни ошириш усуллари» (2015-2017) ва ЁОТ-Атех-2018-168 «Компьютер тармоқларида ҳужумларни аниқлаш усуллари ва воситаларини такомиллаштириш» (2018-2019) мавзусидаги илмий лойиҳалар доирасида бажарилган.

Тадқиқотнинг мақсади инфокоммуникацион тизимларда фойдаланишни чеклаш моделлари асосида ахборотни ҳимояланганлик даражасини оширишнинг усул ва воситаларини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

инфокоммуникацион тизимларда фойдаланишни чеклашни хавфсизлик моделини такомиллаштириш;

ахборотни махфийлиги ва яхлитлигини таъминловчи мандатли хавфсизлик сиёсатини қуриш усулини такомиллаштириш;

операцион тизимларда фойдаланишни бошқаришнинг бирлаштирилган мандат ва ролли моделини такомиллаштириш;

ахборотдан рухсатсиз фойдаланишдан ҳимоя қилиш алгоритми ва дастурий мажмуасини ишлаб чиқиш.

Тадқиқотнинг объекти инфокоммуникацион тизимларида ахборот оқимлари қаралган.

Тадқиқотнинг предмети сифатида ахборотдан рухсатсиз фойдаланишни чеклаш қаралган.

Тадқиқотнинг усуллари. Тадқиқот жараёнида ахборотни ҳимоялаш усуллари, математик моделлар, алгебраик панжара назарияси, графлар назарияси ва объектга йўналтирилган дастурлашдан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

ахборотдан фойдаланишни назоратлаш усули асосида турли фойдаланувчилар маълумотларини бошқарув функцияларининг бир-бири билан кесишмаслигини таъминловчи ташкилотнинг хавфсизлик модели такомиллаштирилган;

ахборотдан фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини оширишнинг концептуал модели ишлаб чиқилган;

иккита қийматли панжаранинг декарт кўпайтмасини тузиш орқали маълумотларни махфийлиги ва яхлитлигини таъминлаш имконини берувчи мандатли хавфсизлик сиёсатини қуриш усули такомиллаштирилган;

фойдаланувчининг қайд маълумотларининг ваколатли ролларини ва фойдаланиш ҳуқуқларининг вазифаларини белгилаш орқали фойдаланишни бошқаришнинг мандат ва ролли модели такомиллаштирилган;

Де-юре ва Де-факто қоидалари ва ахборотдан фойдаланишни бошқариш қоидаларини шакллантириш асосида тизим ҳимояланганлик ҳолатини оширувчи алгоритм ишлаб чиқилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

инфокоммуникацион тизимларда ахборотдан рухсатсиз фойдаланишни чекловчи усуллар, моделлар ва алгоритмлар ишлаб чиқилган;

инфокоммуникацион тизимларини лойиҳалаш босқичларида ахборотдан рухсатсиз фойдаланишдан таҳдидларни амалга оширишга уринишлар сонини ҳисоблаш имконини берувчи усул таклиф этилган;

инфокоммуникацион тизимларининг ҳимояланганлик коэффициенти асосида рухсатсиз фойдаланишдан ахборотнинг ҳимояланганлигини миқдорий баҳолаш модели ва ахборотдан рухсатсиз фойдаланишни чекловчи

дастурий мажмуа ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги инфокоммуникацион тизимларида ахборотдан рухсатсиз фойдаланишни чеклашда ишлаб чиқилган усуллар ва рухсатсиз фойдаланишдан ахборотнинг ҳимояланганлигини миқдорий баҳолаш модели ҳамда дастурий мажмуани амалга оширишда ишлаб чиқилган алгоритмлар бўйича ўтказилган тажрибаларнинг натижалари билан шарҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти.

Тадқиқот натижаларининг илмий аҳамияти ишлаб чиқилган ахборотдан рухсатсиз фойдаланишни чекловчи усуллар, моделлар ва алгоритмлар ташкилотда хавфсизлик моделини яратишга асос бўлиб хизмат қилади.

Тадқиқот натижаларининг амалий аҳамияти шундан иборатки, инфокоммуникацион тизимларининг ҳимояланганлик коэффициенти ҳисобига ахборот хавфсизлигини бошқариш самарадорлигини ҳамда мандат ва ролли фойдаланиш асосида ишлаб чиқилган дастурий мажмуа инфокоммуникацион тизимларда ахборот ҳимояланганлик даражасини ошириш имконини беради.

Тадқиқот натижаларининг жорий қилиниши. Инфокоммуникацион тизимларида ахборотдан рухсатсиз фойдаланишни чекловчи усуллар, моделлар ва алгоритмлар бўйича олинган илмий натижалар асосида:

фойдаланувчининг қайд маълумотларининг ваколатли ролларини ва фойдаланиш ҳуқуқларининг вазифаларини белгилаш имконини берувчи фойдаланишни бошқаришни такомиллаштирилган мандат ва ролли модели асосида ишлаб чиқилган тизим ҳимояланганлигини оширувчи дастурий мажмуа – «Тошкент» Республика фонд биржаси АЖга жорий қилинган (Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 17 августдаги 33-8/4721-сон маълумотномаси). Илмий тадқиқот натижасида ишлаб чиқилган дастурий мажмуа ташкилот ходимларининг ишлаш жараёнларида махсус роллар асосида субъектнинг махфийлик даражасига қараб бошқариш, ходимларнинг мониторингини олиб бориш ва тизим ахборотидан рухсатсиз фойдаланишни олдини олиш имконини берган;

Де-юре ва Де-факто қоидалари ва ахборотдан фойдаланишни бошқариш қоидаларини шакллантириш бўйича тизим ҳимояланганлик ҳолатини оширишга имкон берувчи алгоритм ва дастурий мажмуа – «Trans New Millenium» МЧЖга жорий этилган (Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 17 августдаги 33-8/4721-сон маълумотномаси). Натижада, ишлаб чиқилган автоматлаштирилган тизим ҳимояланганлигини оширувчи дастурий мажмуаси «MK Universal» турли ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситалари ишлаши унумдорлигини баҳолаш бўйича энг яхши кўрсаткичга эга «Dallas Lock» дастурий мажмуасидан 7% га ва энг паст кўрсаткичга эга «Secret Net» дастурий мажмуасидан 18% га юқори унумдор ишлаш имконини берган;

инфокоммуникацион тизимларда фойдаланишни бошқариш усули

асосида ташкилотнинг хавфсизлик модели ва мижоз-сервер архитектураси орқали амалга оширилган дастурий мажмуа «UNF Universal» МЧЖга жорий этилган (Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 17 августдаги 33-8/4721-сон маълумотномаси). Натижада, мижоз-сервер архитектураси асосида ишлаб чиқилган дастурий мажмуа фойдаланувчилар маълумотларини бошқарув функцияларининг бир-бири билан кесишмаслигини таъминлаш ҳисобига роллар иерархиясини қуришга ва ташкилот тизим ахборотидан рухсатсиз фойдаланишни бартараф этишга ҳамда корхона раҳбарининг ўз ходимларини иш жараёнида бошқариш орқали ташкилотнинг иш унумдорлигини 13% фоиз оширишга имкон берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари, жумладан, 7 та халқаро ва 2 та республика илмий амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Тадқиқот мавзуси бўйича жами 28 та илмий иш чоп этилган, Ўзбекистон Республикаси Олий аттестация коммисиясининг докторлик диссертациялари асосий натижаларини чоп этиш тавсия этилган илмий нашрларда 13 та мақола, 11 таси хорижий ва 2 таси республика журналларида нашр қилинган, шунингдек, 6 та ЭҲМ учун яратилган дастурий воситаларни қайд қилиш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертациянинг ҳажми 118 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурати асосланган, тадқиқотнинг мақсад ва вазифалари, объект ва предмети тавсифланган, тадқиқотнинг Ўзбекистон Республикаси фан ва технологиялари ривожланишининг устувор йўналишларига мослиги асосланган, тадқиқотнинг илмий янгилиги ва амалий натижалари баён қилинган, олинган натижаларнинг илмий ва амалий аҳамияти очиб берилган, тадқиқот натижаларини амалиётга жорий қилиш, тадқиқот натижаларини апробацияси, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг **«Инфокоммуникацион тизимларда ахборотнинг ҳимояланганлигини ошириш усул ва воситаларини таҳлили»** деб номланган биринчи боби инфокоммуникацион тизимларнинг ҳимояланганлиги муаммолари, ахборот хавфсизлиги таҳдидлари ва хавф-хатарлари ҳамда ахборотнинг ҳимояланганлигини ошириш усулларига бағишланган. Шунингдек бу бўлимда инфокоммуникацион тизимларда ахборотнинг ҳимояланганлигини ошириш моделларининг қиёсий таҳлили ўтказилган. Инфокоммуникацион тизимларда ўтказилган қиёсий таҳлил асосида ахборотнинг ҳимояланганлик моделларининг умумий камчилик ва афзалликлари келтирилган. Инфокоммуникацион тизимлар ресурсларидан

фойдаланишни чеклаш моделларининг асосий характеристикаларининг қиёсий таҳлили 1-жадвалда келтирилган.

1-жадвал

Фойдаланишни чеклаш моделларининг характеристикаларини таққослаш

	Дискрецион	Мандат	RBAC
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
Тизим хавфсизлигининг формал исботи	Тўлиқ эмас	Тўлиқ	Тўлиқ эмас
Тармоқда хавфсизликни таъминлаш	Таъмин-ламайди	Таъмин-ламайди	Таъминлайди
Ахборотни сирқиб чиқиб кетишини назорат қилиш	Тўлиқ эмас	Тўлиқ	Тўлиқ эмас

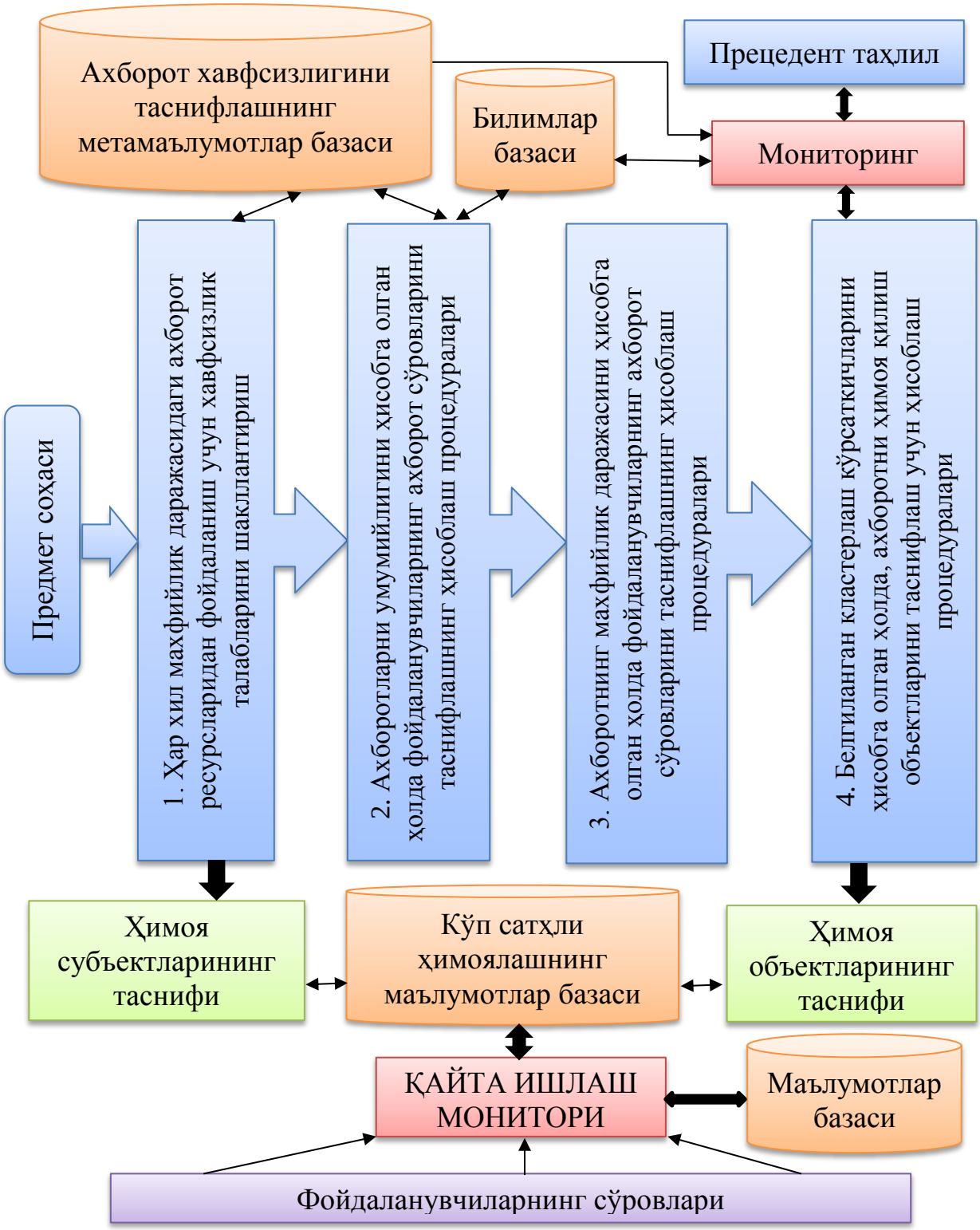
Таъкидлаш лозимки, янги усулларни ҳамда тизимнинг юқори хавфсизлигини таъминловчи модификацияланган ахборотнинг ҳимояланганлигини ошириш моделларини яратиш долзарб ҳисобланади.

Диссертациянинг **«Инфокоммуникацион тизимларда ахборот хавфсизлигини ошириш усул ва моделлари»** деб номланган иккинчи бобида ахборот ҳимояланганлигини оширишда мандат ва ролларга асосланган фойдаланишни чеклаш усуллари келтирилган ва ишлов бериладиган маълумотларнинг хавфсизлик даражасини рухсатсиз пасайтиришдан ҳимоялаш усули тавсифланган. Ташкилотларда ролларга асосланган фойдаланишни бошқариш усули қўлланилган ва фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини оширишнинг концептуал модели такомиллаштирилган. Ҳамда яратилаётган файл объектларидан фойдаланишни бошқариш тизимининг модели таклиф этилган.

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.

1-расмда фойдаланишни чеклашни мандатли бошқариш сиёсати

ёрдамида ахборот ҳимояланганлигини оширишнинг концептуал модели тақдим этилган.



1-расм. Фойдаланишни чеклашни мандатли бошқариш сиёсати ёрдамида ахборот ҳимояланганлигини оширишнинг концептуал модели

Фойдаланувчининг предмет соҳасининг бошланғич ҳолатида, ажратилган ахборот объектлари структуравий ахборот элементлари сифатида тақдим этилади. Фойдаланувчиларнинг ахборотга бўлган талаблари маълумот сўровлари шаклида тақдим этилади.

Диссертация ишининг **«Ахборотдан фойдаланишни чекловчи хавфсизлик сиёсатларини бирлаштириш усул ва алгоритмлари»** номли учинчи бобида инфокоммуникацион тизимларида маълумотлар махфийлиги ва яхлитлиги талаб қилинадиган иккита қийматли панжарани киритиш йўли билан мандатли хавфсизлик сиёсатини бирлаштириш усули такомиллаштирилган. Панжара графига асосланган мандат ва ролли хавфсизлик сиёсатини бирлаштириш усули ҳамда операцион тизимларда мандат ва ролли фойдаланиш бошқариш модели таклиф этилган. Де-юре ва Де-факто қоидаларига асосланган мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми ишлаб чиқилган.

Иккита мандатли хавфсизлик сиёсатини бирлаштириш зарурияти бир вақтнинг ўзида маълумотлар махфийлигини ва яхлитлигини талаб қиладиган тизимларда пайдо бўлади. Шу билан бирга тизимни бошқариш вазифаси жуда кўп вақт талаб этади, чунки ҳар бир ахборотдан фойдаланиш иккита мустақил қоидага мувофиқ текширилади. Бунинг учун ташкилотнинг ягона қийматлар панжарасини бўлимлар кесимида декарт кўпайтмаси орқали амалга ошириш мумкин.

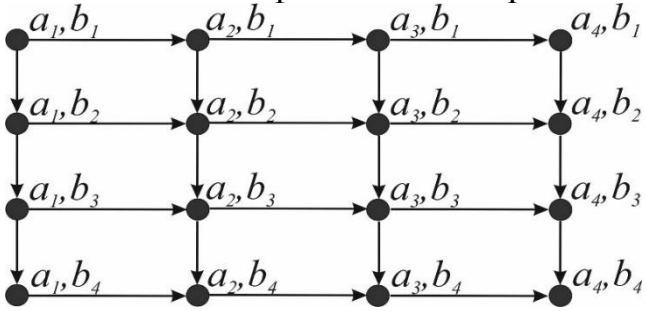
$$L_1 \times L_2$$

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 $(a_1 < a_2 < a_3 < a_4)$ 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.

Натижада 2-расмда 16 та хавфсизлик белгисига эга бўлган бирлаштирилган ташкилотнинг хавфсизлик панжараси ҳосил бўлади.

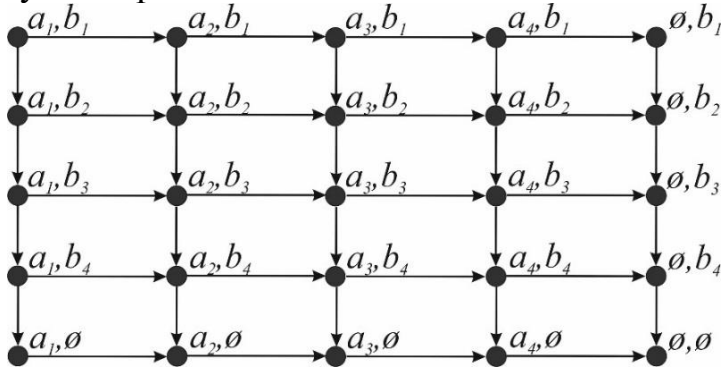


2-расм. Бирлаштирилган ташкилотнинг хавфсизлик панжараси

a_4, b_4 панжаранинг энг паст даражаси ҳар бир бўлимнинг ахборотдан фойдаланишини ўз ичига олади, бу эса ахборот сирқиб чиқишини пайдо қилиши мумкин. Бундай вазиятни олдини олиш учун янги хавфсизлик панжарасини қўшимча хавфсизлик даражалари билан тўлдириш керак бўлади. Бунинг учун ҳар қандай панжарани бўш элемент ёки ноль элементи билан тўлдирадиган элементар ўзгартириш киритиш керак бўлади. Юқоридаги ёндашув асосида натижавий панжара 25 элементдан иборат бўлади. $L^{\emptyset}$ панжарасининг диаграммаси 3-расмда кўрсатилган.

$L = L_1 \times L_2$ 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. Бундан ташқари, $L^{\emptyset}$ панжарасида яна иккита қуйи панжарани ажратиш мумкин, уларнинг ҳар бири ахборот алмашинувисиз бўлимларнинг ишлашини имитация қилади.



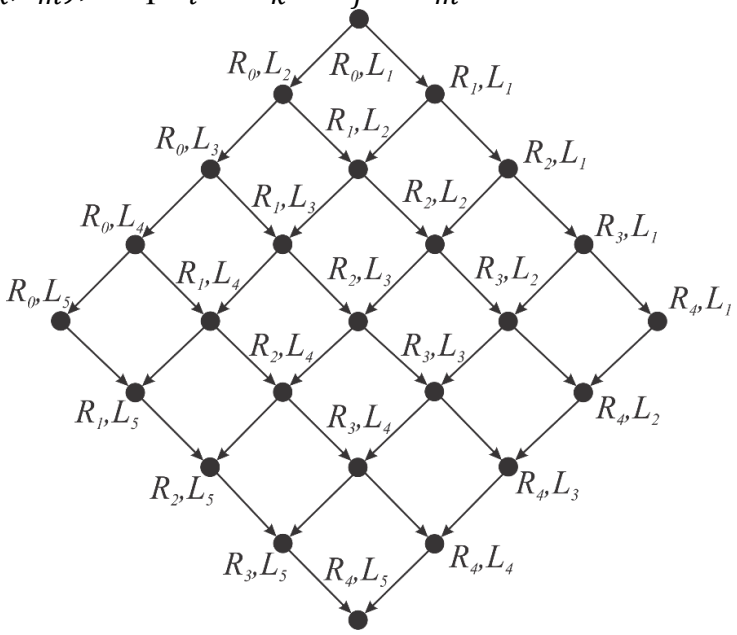
3-расм. Бирлаштирилган тизимнинг хавфсизлик панжараси

Ролли ва мандатли фойдаланишни бошқариш моделларини бирлаштириш усулида ролларга асосланган хавфсизлик сиёсати олтита роллар билан берилади, улардан бири (r_0) “Бўш”, яъни ҳеч қандай имтиёзларга эга эмас ва бошқа ҳар қандай ролларга бўйсунади. Мандатли хавфсизлик сиёсати L панжараси билан аниқлансин, унинг элементлари l_1, l_2, l_3, l_4 тугунлар, бунда тартиб қуйидагича берилади $l_1 \geq l_2 \geq l_3 \geq l_4$.

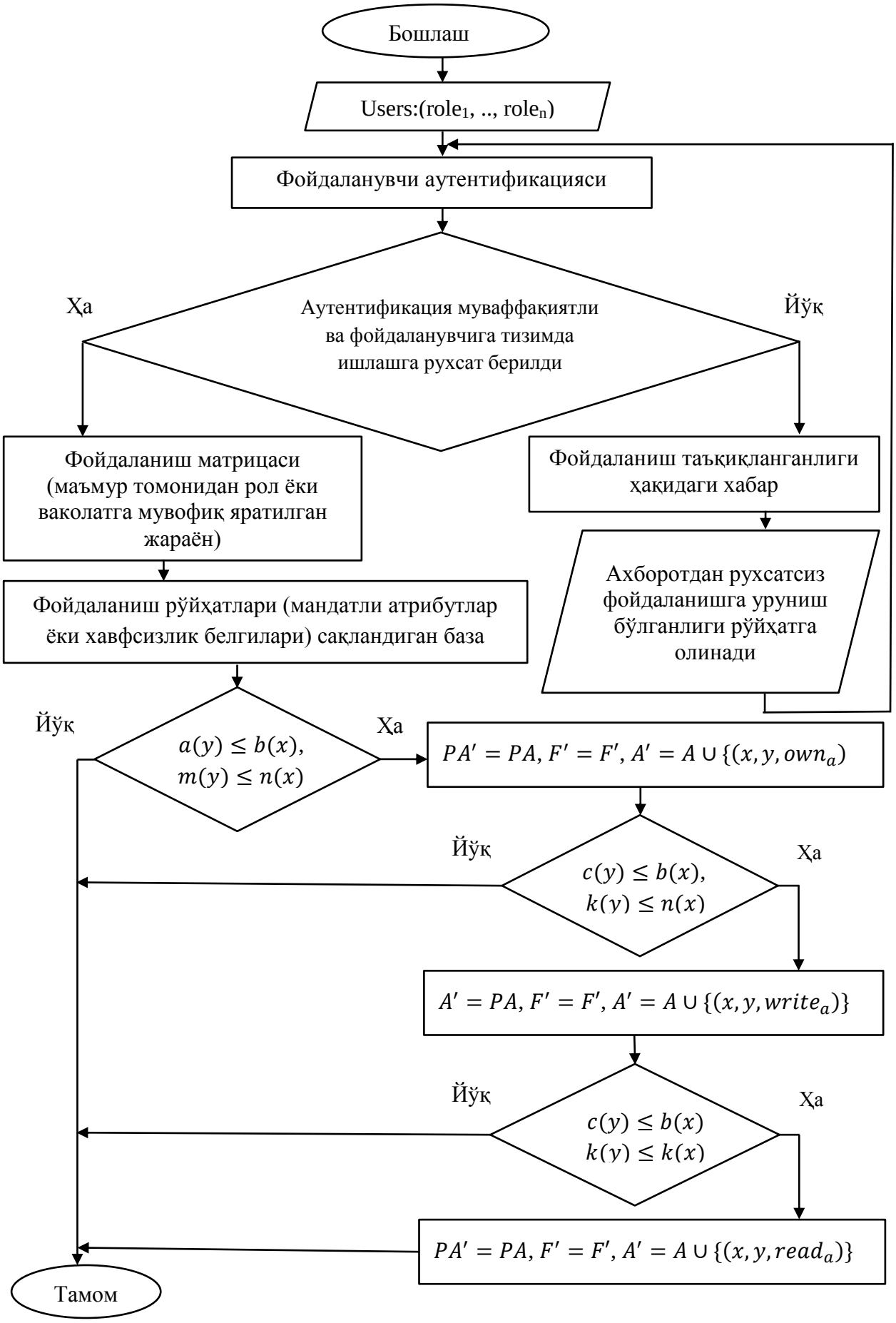
Ролларга асосланган хавфсизлик сиёсати мандатли хавфсизлик сиёсати билан бир-бирига зид бўлмаган ҳолда бирлашади. Бунинг учун R ва L панжараларининг декарт кўпайтмаси бўлган $R \times L$ панжарасини қуриш керак, бу ерда $R -$ панжара графи билан аниқланадиган панжара.

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

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



4-расм. Ролли ва мандатли хавфсизлик сиёсатини бирлаштириш панжараси



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

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

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.

Де-юре ва Де-факто қоидалари асосида ишлаб чиқилган мандат ва ролли фойдаланишни бошқаришни амалга ошириш алгоритми ахборотдан фойдаланишни бошқариш қоидаларини шакллантириш орқали ахборот тизимининг ҳимояланганлигини ошириш имконини беради (5-расм).

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

Диссертациянинг **«Инфокоммуникацион тизимларида ахборот ҳимояланганлигини баҳолаш воситалари»** номли тўртинчи бобида инфокоммуникацион тизимларини лойиҳалаш босқичларида рухсатсиз фойдаланишдан зарар эҳтимоли ва хавфсизликка таҳдидларни амалга оширишга уринишлар сонини ҳисоблаш имконини берувчи ёндашув ва рухсатсиз фойдаланишдан ахборотнинг ҳимояланганлигини миқдорий баҳолаш модели таклиф қилинган ҳамда инфокоммуникацион тизимларида рухсатсиз фойдаланишни чекловчи дастурий мажмуа ишлаб чиқилган.

Инфокоммуникацион тизимларини лойиҳалаш босқичларида ахборотдан рухсатсиз фойдаланишдан зарар эҳтимоллигини камайтириш, баҳолаш ва таҳдидларни амалга оширишга уринишлар сонини ҳисоблаш имконини берувчи усул асосида 2-жадвалда турли хил бошланғич параметрларга эга компьютер тизимлари учун P_x ва P_y ҳимояланганликни баҳолашни сон жиҳатидан фарқи кўрсатилган. P_x ва P_y ахборотдан рухсатсиз фойдаланишнинг эҳтимолини пастки ва юқори чегараларини беради.

2-жадвал

Компьютер тизимларида ахборот ҳимояланганлигини баҳолаш

	КТ1	***КТ2***	***КТ3***	***КТ4***	***КТ5***	***КТ6***	***КТ7***
S	12	15	20	30	40	50	50
K	3	3	3	3	3	4	4
N_1	3	5	5	4	10	10	10
N_2	4	5	6	6	10	10	10
N_3	5	5	7	10	10	10	10
M_1	3	3	9	5	3	6	4
M_2	4	3	3	2	3	6	5
M_3	2	3	6	9	3	6	9
P_1	0,066	0,055	0,037	0,040	0,030	0,021	0,022

P_2	0,063	0,055	0,047	0,045	0,030	0,021	0,023
P_3	0,071	0,055	0,042	0,034	0,030	0,021	0,020
U_1	0,187	0,248	0,172	0,151	0,265	0,197	0,205
U_2	0,227	0,248	0,254	0,243	0,265	0,197	0,209
U_3	0,309	0,248	0,257	0,296	0,265	0,197	0,186
P_x	0,251	0,248	0,232	0,251	0,265	0,197	0,198
P_y	8,411	1,481	1,772	5,371	2,782	3,091	3,282

Ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситаларининг мезонларини объектив қийматлар асосида ҳисоблаш жараёни амалга оширилган.

1. MK- Universal:

$$\sum_{i=1}^{15} F_{i1}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j1}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*1+1*0+0{,}9*0+0{,}8*0+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*1+0{,}6*1+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*1) = 5{,}8$$

2. Secret Net:

$$\sum_{i=1}^{15} F_{i2}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j2}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*1+1*1+0{,}9*1+0{,}8*0+0{,}7*0+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*4) = 4$$

3. КРИПТОН-ЩИТ:

$$\sum_{i=1}^{15} F_{i3}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j3}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*0+1*1+0{,}9*0+0{,}8*1+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*2) = 4{,}6$$

4. Страж NT:

$$\sum_{i=1}^{15} F_{i4}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j4}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*0+1*1+0{,}9*0+0{,}8*1+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*3) = 4{,}1$$

5. Dallas Lock:

$$\sum_{i=1}^{15} F_{i5}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j5}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*0+1*1+0{,}9*1+0{,}8*1+0{,}7*1+0{,}5*1+0{,}2*1 \\ +0{,}9*0+0{,}6*1+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*5) = 5{,}1$$

6. InfoWatch EndPoint Security:

$$\sum_{i=1}^{15} F_{i6}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j6}^{-} \cdot P_j^{-} =$$

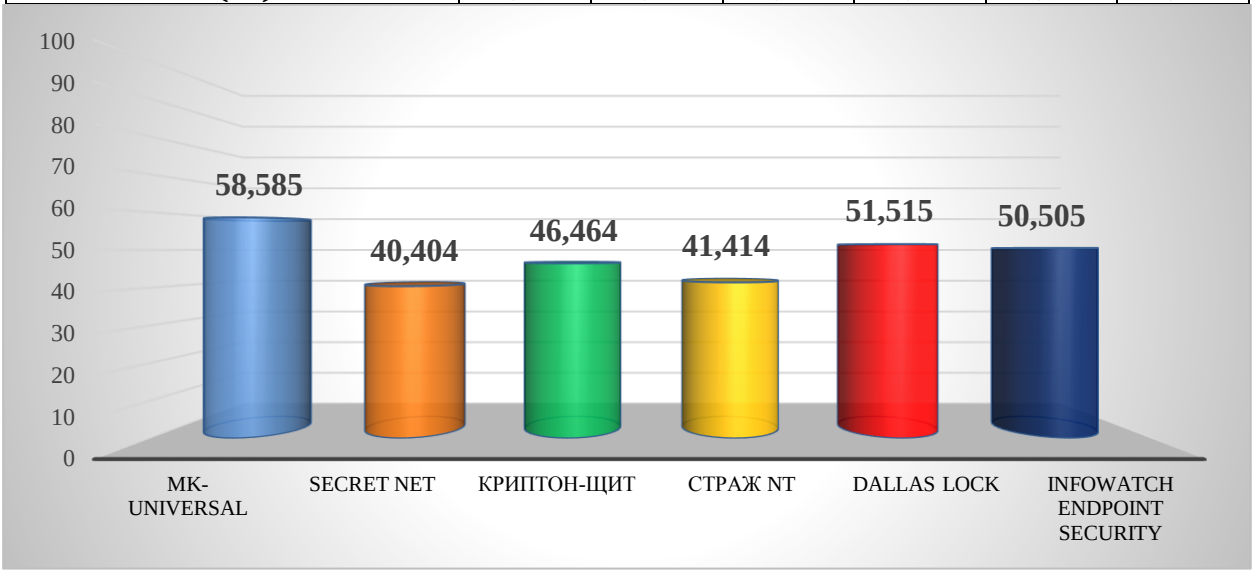
$$\begin{pmatrix} 1*1+1*1+1*1+0{,}9*0+0{,}8*1+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*0+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix} - (0{,}5*3) = 5$$

Диссертацияда такомиллаштирилган моделлар, усуллар ва алгоритмлар асосида автоматлаштирилган тизим ҳимояланганлигини оширувчи дастурий мажмуаси ишлаб чиқилган ҳамда ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситаларини ишлаш унумдорлигини қиёсий баҳолаши ўтказилган (3-жадвал ва 6-расм).

3-жадвал

Автоматлаштирилган тизим ҳимояланганлигини оширувчи дастурий мажмуасининг турли ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситалари билан ишлаши унумдорлигини баҳолаш натижалари

Ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситалари / Кўрсаткичлар	MK- Universal	Secret Net	КРИПТОН-ЩИТ	Страж NT	Dallas Lock	InfoWatch EndPoint Security
s	5,8	4	4,6	4,1	5,1	5
s_{max}	9,9	9,9	9,9	9,9	9,9	9,9
$U(\%)$	58,585	40,404	46,464	41,414	51,515	50,505



6-расм. Ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситаларининг унумдорлигини қиёсий таҳлили гистограммаси

Қиёсий таҳлил натижаларига кўра, автоматлаштирилган тизим ҳимояланганлигини оширувчи дастурий мажмуаси «MK Universal» турли ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситалари ишлаши унумдорлигини баҳолаш бўйича энг яхши кўрсаткичга эга «Dallas Lock» дастурий мажмуасидан 7% ва энг паст кўрсаткичга эга «Secret Net» дастурий мажмуасидан 18% юқори унумдорликка эга.

ХУЛОСА

«Инфокоммуникацион тизимларда ахборот ҳимояланганлигини оширишнинг усул ва воситаларини такомиллаштириш» мавзусидаги диссертация бўйича қуйидаги хулосалар тақдим этилди:

1. Ролларга асосланган фойдаланишни бошқариш усули асосида ташкилотнинг хавфсизлик модели таклиф этилган. Таклиф этилган модел турли фойдаланувчилар маълумотларини бошқарув функцияларининг бир-бири билан кесишмаслигини таъминлаш ҳисобига роллар иерархиясини қуришга имкон яратади.
2. Иккита қийматли панжаранинг декарт кўпайтмасини тузиш орқали маълумотларни махфийлиги ва яхлитлигини таъминлаш имконини берувчи мандатли хавфсизлик сиёсатини қуриш усули такомиллаштирилган.
3. Операцион тизимларда фойдаланишни бошқариш хусусиятларига асосланиб фойдаланишни бошқаришнинг мандат ва ролли модели такомиллаштирилган. Такомиллаштирилган модел фойдаланувчиларнинг қайд маълумотларининг ваколатли ролларини, жорий субъект-сеанси ва фойдаланувчи ҳуқуқининг жорий ролларини тақдим этишга имкон беради.
4. Де-юре ва Де-факто қоидаларидан фойдаланиб мандат ва ролларга асосланган фойдаланишни бошқариш алгоритми ишлаб чиқилди. Ишлаб чиқилган алгоритм ахборотдан фойдаланишни бошқариш қоидаларини шакллантириш орқали ахборот тизимининг ҳимояланганлигини ошириш имконини беради.
5. Инфокоммуникацион тизимларида ахборотдан рухсатсиз фойдаланишдан ҳимоя қилишни баҳоловчи усул таклиф этилган. Таклиф этилган усул ахборотдан рухсатсиз фойдаланишдан зарар эҳтимоллигини камайтириш, тизим ҳимояланганлигини баҳолаш ва уларга бўладиган таҳдидларни амалга оширишга уринишлар сонини ҳисоблашга имкон беради.
6. Автоматлаштирилган тизим ҳимояланганлигини оширувчи «MK Universal» - дастурий мажмуа ишлаб чиқилган. Ўтказилган ҳисоблаш тажриба натижалари бўйича ишлаб чиқилган дастурий мажмуа турли ахборотдан рухсатсиз фойдаланишни чекловчи ҳимоя қилиш воситалари ишлаши унумдорлигини баҳолаш бўйича энг яхши кўрсаткичга эга «Dallas Lock» дастурий мажмуасидан 7% ва энг паст кўрсаткичга эга «Secret Net» дастурий мажмуасидан 18% юқори унумдор ишлашга имкон беради.

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

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

КАДИРОВ МИР-ХУСАН МИРПУЛАТОВИЧ

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ И СРЕДСТВ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ**

Ташкент-2020

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2020.3.PhD/T308.

Диссертация выполнена в Ташкентском государственном техническом университете.

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

Научный руководитель:	**Каримов Маджит Маликович** доктор технических наук, профессор
Официальные оппоненты:	**Абдурахимов Бахтиёр Файзиевич** доктор физико-математических наук, профессор
	Ганиев Абдухалил Абдужалилович кандитат технических наук, доцент
Ведущая организация:	**«UNICON.UZ» – центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «08» октября 2020 года в 14[00] часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №1619). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «25» сентября 2020 года.
(протокол рассылки №14 от «24» августа 2020 года.)

Р.Х. Хамдамов
Председатель научного совета по присуждению ученых степеней, д.т.н., профессор

Ф.М. Нуралиев
Ученый секретарь научного совета по присуждению ученых степеней, д.т.н., доцент

С.К. Ганиев
Председатель научного семинара при Научном совете по присуждению ученых степеней, д.т.н., профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В мире особое внимание уделяется на обнаружение и устранение несанкционированного доступа к информации в инфокоммуникационных системах, оценке защищенности систем, а также на создание и совершенствование средств защиты от несанкционированного доступа. В цифровой экономике эффективность всех секторов увеличивается за счет использования информационных технологий. Это создает определенные риски для проблемы информационной безопасности. В первом квартале 2020 года количество киберинцидентов быстро увеличивалось, в результате чего количество атак на информационные системы увеличилось на 22,5% по сравнению с 2019 годом. Также количество целевых атак только в этом году составило 67%[1]. По данному направлению в развитых странах, таких как США, Нидерланды, Германия, Великобритания, Франция, Италия, Российская Федерация и других государствах уделяется особое внимание разработке программно-аппаратных средств, обеспечивающих защиту инфокоммуникационных систем от несанкционированного доступа к информации.

В мире системы обработки и хранения информации представляют собой совмещение нескольких специализированных информационных сервисов. Для специализированных информационных сервисов разработана своя математическая модель. В связи с этим объединение нескольких моделей безопасности в одну систему в настоящее время является одной из важных задач. Однако объединение нескольких сервисов в одну систему без изменения моделей безопасности может привести к снижению работоспособности системы. Следовательно, разработка усовершенствованной модели управления политикой безопасности мандатно-ролевого разграничения доступа является актуальной для осуществления управления на основе ролей и повысит конфиденциальность систем управления базами данных в инфокоммуникационных системах.

В нашей Республике, наряду с развитием инфокоммуникационных систем в органах государственного и хозяйственного управления, особое внимание уделяется широкому применению методов и средств защиты информации, утечке информации и несанкционированному доступу к информации в этих системах. В стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 годах определены задачи, в том числе, «…совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[2]. Для решения этих задач одним из важных вопросов является совершенствование политик безопасности, ограничивающих несанкционированный доступ к информации в инфо-коммуникационных системах в соответствии с современными требованиями.

---

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/

[2] Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

Данное диссертационное исследование, в определенной степени, служит выполнению задач, предусмотренных указом Президента Республики Узбекистан № УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», Постановлением Президента Республики Узбекистан № ПП-4022 от 21 ноября 2018 года «О мерах по дальнейшей модернизации цифровой инфраструктуры в целях развития цифровой экономики», № ПП-4452 от 14 сентября 2019 года «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», а также в других нормативно-правовых документах, принятых в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствии с приоритетным направлением развития науки и технологий Республики IV. «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. В рамках мировых исследований по разработке методов, моделей и средств разграничения доступа от несанкционированного доступа к информации большой вклад внесли следующие зарубежные ученые: D. Elliott Bell, Leonard J. LaPadula, R.S. Sandhu, D. Richard Kuhn, Zoran Stojanovich, Ajantha Dahanayake, 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 и др.

Совместная реализация методов и алгоритмов разграничения доступа к информации исследованы в научных трудах зарубежных ученых, таких как Rivera Sanchez, C. E. Phillips, Mustafa Kocatürk, Taflan Gündem, П.Н. Девянин.

В развитие этого направления в нашей Республике внесли свой вклад Т.Ф. Бекмуратов, С.К. Ганиев, М.М. Каримов, А.А. Ганиев, Д.Я. Иргашева, А.А. Сулима, О.М. Исмоилов и др.

Несмотря на достаточный уровень теоретических исследований в области объединения моделей контроля доступа к информации, недостаточно исследованы методы и алгоритмы их практической реализации, связанные с формализацией в инфокоммуникационных системах.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках научных проектов согласно плану научно-исследовательских работ Ташкентского государственного технического университета №А-5-48 «Способы повышения защищенности информации при контроле доступа к создаваемым файловым объектам в инфокоммуникационных системах» (2015-2017) и ЁОТ-Атех-2018-168 «Совершенствование методов и средств обнаружения атак в компьютерных сетях» (2018-2019).

Целью исследования является разработка методов и средств на основе моделей разграничения доступа для повышения уровня защищенности инфокоммуникационных систем.

Задачи исследования:

совершенствование модели безопасности для разграничения доступа в инфокоммуникационных системах;

совершенствование метода построения мандатной политики безопасности, обеспечивающей конфиденциальность и целостность информации;

совершенствование объединенной мандатной и ролевой модели контроля доступом в операционных системах;

разработка алгоритма и программного комплекса для защиты от несанкционированного доступа к информации.

Объектом исследования являются информационные потоки в инфокоммуникационных системах.

Предметом исследования являются разграничения доступа от несанкционированного доступа к информации.

Методы исследования. В процессе исследования использованы методы защиты информации, математические модели, теория алгебраических решеток, теория графов и объектно-ориентированное программирование.

Научная новизна исследования заключается в следующем:

усовершенствована модель безопасности организации на основе метода контроля доступа к информации, гарантирующая, не пресечение функции управления различных пользовательских данных.

разработана концептуальная модель повышения защищенности информации с мандатной политикой разграничения доступа;

усовершенствован метод построения мандатной политики безопасности на основе декартова произведения решетки двух ценностей, который позволит обеспечить конфиденциальность и целостность данных;

усовершенствована мандатно-ролевая модель управления доступом, позволяющая задать функции авторизованных ролей учетных записей пользователей и прав доступа;

разработан алгоритм повышающий уровень защищенности системы в соответствии с правилами Де-юре и Де-факто и на основе формирования правил управления доступом к информации.

Практические результаты исследования заключаются в следующем:

разработаны методы, модели и алгоритмы защиты от несанкционированного доступа к информации в инфокоммуникационных системах;

предложен метод, позволяющий рассчитать количество попыток реализации угроз от несанкционированного доступа к информации на этапах проектирования инфокоммуникационных систем;

разработана модель количественной оценки защищенности инфо-коммуникационных систем от несанкционированного доступа на основе коэффициента защищенности и программный комплекс для разграничения

несанкционированного доступа к информации.

Достоверность результатов исследования. Достоверность результатов исследования подтверждается разработанными методами ограничения несанкционированного доступа к информации в инфокоммуникационных системах, моделью количественной оценки защищенности инфокоммуникационных систем от несанкционированного доступа, а также результатами проведенных экспериментов по разработанным алгоритмам при реализации программного комплекса.

Научная и практическая значимость результатов исследования.

Научная значимость результатов исследования заключается в том, что разработанные модели, методы и алгоритмы, ограничивающие несанкционированный доступ к информации, служат основой для создания модели безопасности в организации.

Практическая значимость полученных результатов исследования заключается в том, что эффективность управления информационной безопасностью за счет коэффициента защищенности инфокоммуникационных систем, а также разработанный программный комплекс на основе использования мандатного и ролевого разграничения доступа позволяют повысить уровень защищенности в инфокоммуникационных системах.

Внедрение результатов исследования. На основе полученных научных методов, моделей и алгоритмов, ограничивающих несанкционированный доступ к информации в инфокоммуникационных системах:

программный комплекс, повышающий защищенность автоматизированных систем на основе усовершенствованной мандатно-ролевой модели управления доступом, позволяющая задать функции авторизованных ролей учетных записей пользователей и прав доступа, внедрен деятельности в АО республиканской фондовой бирже «Тошкент» (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 17 августа 2020 года №33-8/4721). Программный комплекс, разработанный в результате научных исследований, позволил управлять уровнем конфиденциальности субъекта на основе ролей в рабочих процессах организации, мониторинга сотрудников и предотвращать несанкционированное использование системной информации;

разработанный алгоритм и программный комплекс, позволяющий повысить уровень защищенности системы в соответствии со сформированными правилами Де-юре и Де-факто, также на основе формирования правил управления доступом к информации внедрен в деятельность ООО «Trans New Millenium» (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 17 августа 2020 года №33-8/4721). В результате, разработанный программный комплекс, повышающий защищенность автоматизированных систем «MK Universal» работает на 7% производительнее, чем средство защиты информации от несанкционированного доступа «Dallas Lock», и на 18% производительнее, чем программный комплекс «Secret Net»;

предложенная модель безопасности организации на основе метода

контроля доступа защищенности информации и разработанный программный комплекс на основе клиент-серверной архитектуры, внедрен в деятельность ООО «UNF Universal», (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 17 августа 2020 года №33-8/4721). В результате разработанный программный комплекс, основанный на архитектуре клиент-сервера, позволил построить иерархию ролей, гарантируя, что функции управления пользовательскими данными не пересекаются, предотвращен несанкционированный доступ к системной информации организации, также за счет управления сотрудниками в рабочем процессе производительность организации повысилась на 13%.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 7 международных и 2 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме исследования опубликованы всего 28 научных работ, из них 13 статей в журнальных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 11 – в международных и 2 – в республиканских журналах, а также получены 6 свидетельств о регистрации программных продуктов для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 118 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и востребованность темы диссертации, сформулированы цель и задачи, выявлены объект и предмет исследования, определено соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, изложены научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыты научная и практическая значимость полученных результатов, приведены перечень внедрений в практику результатов исследования, список апробации результатов работы, сведения по опубликованным работам и структура диссертации.

Первая глава диссертации, озаглавленная как **«Анализ методов и средств повышения защищенности информации в инфокоммуникационных системах»**, посвящена проблемам защищенности инфокоммуникационных систем, анализу угроз и рисков информационной безопасности, а также методам повышения защищенности информации. Также был произведен сравнительный анализ моделей повышения защищенности информации в инфокоммуникационных системах. На основе сравнительного анализа представлены общие недостатки и преимущества моделей информационной безопасности. В таблице 1 приведено сравнение

основных характеристик моделей разграничения доступа к ресурсам инфокоммуникационных систем.

Таблица 1

Сравнение характеристик моделей разграничения доступа

	Дискреционная	Мандатная	RBAC
Сложность реализации	Средняя	Высокая	Высокая
Защищенность	Средняя	Высокая	Высокая
Сложность использования	Средняя	Высокая	Средняя
Производительность	Задействует не много ресурсов	Задействует не много ресурсов	Задействует много ресурсов
Формальное доказательство безопасности системы	Не полное	Полное	Не полное
Обеспечение безопасности в сети	Не обеспечивает	Не обеспечивает	Обеспечивает
Контроль утечки информации	Не полное	Полное	Не полное

Следует отметить, что актуальным является создание новых методов и модифицированных моделей повышения защищенности информации, обеспечивающих высокую защищенность системы.

Во второй главе диссертации **«Способы и модели повышения защищенности информации в инфокоммуникационных системах»** приведены способы повышения защищенности информации от нарушения конфиденциальности посредством защиты от несанкционированного понижения, а также приведены мандатные и ролевые методы разграничения доступа. Построена модель политики безопасности организации на основе ролевого доступа и предложена концептуальная модель повышения защищенности информации с мандатной политикой разграничения доступа. Также, построена модель системы управления доступа к создаваемым файловым объектам.

В предлагаемом подходе поэтапной классификации информационных сущностей строится дерево объектов защиты, уровни иерархии которого отражают взаимосвязь субъектов защиты, имеющих статус владельцев объектов защиты. Древовидная структура представления объектов защиты реализуется через иерархию прав владения субъектов объектами. Иерархическая зависимость между объектами защиты проявляется через иерархию степеней секретности информации и иерархию классификации субъектов-владельцев объектов.

На рисунке 1 представлена усовершенствованная концептуальная модель

повышения защищенности информации с мандатной политикой разграничения доступа.

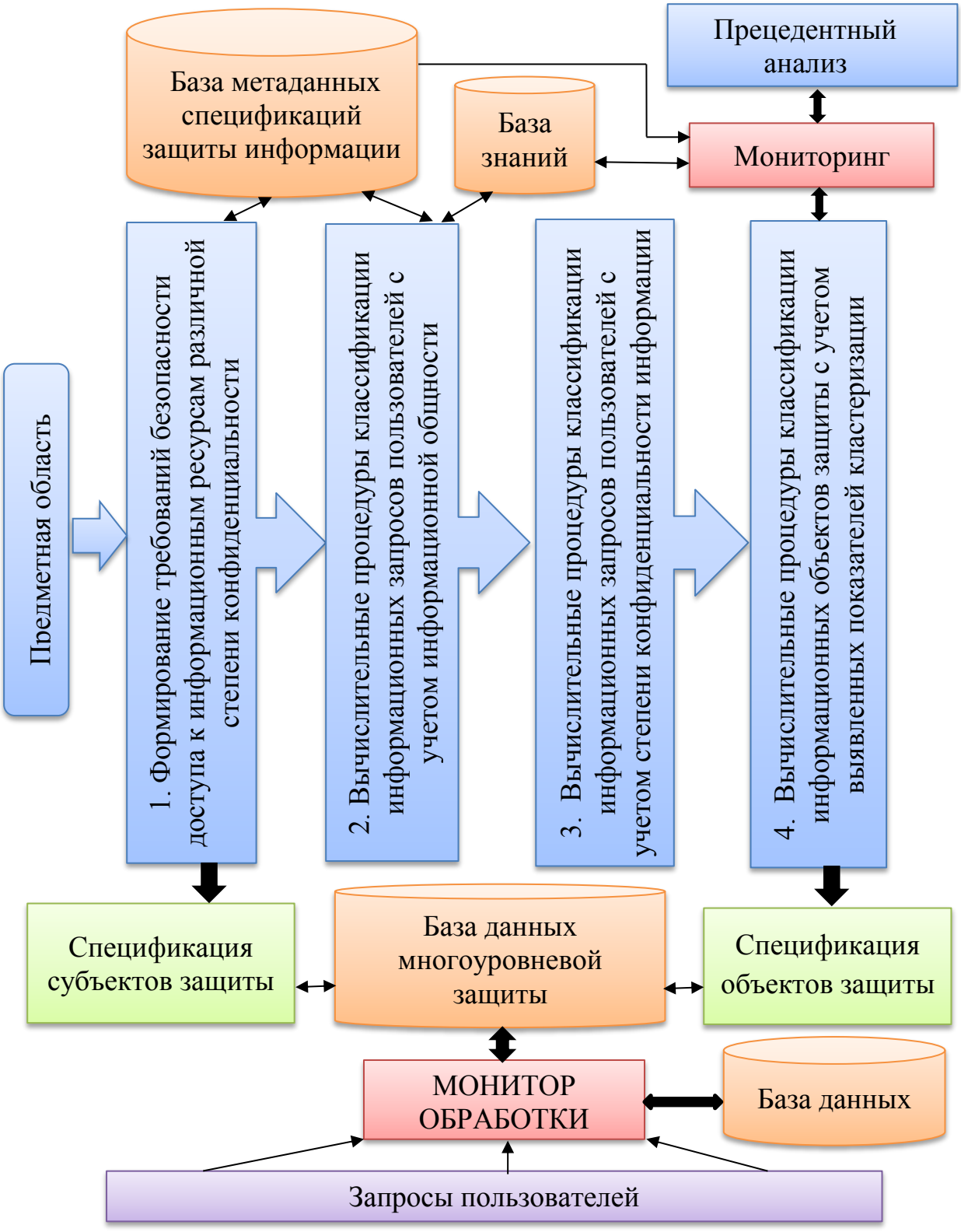


Рис.1. Концептуальная модель повышения защищенности информации с мандатной политикой разграничения доступа

В начале, на этапе предметной области пользователей, выделенные информационные сущности представляются в виде структурных информационных элементов, а информационные требования пользователей –

в виде информационных запросов.

В третьей главе диссертации **«Методы и алгоритмы совмещения политик безопасности разграничения доступа к информации»** усовершенствованы методики мандатной политики безопасности на основе двух решеток ценностей: конфиденциальности и целостности данных в инфокоммуникационных системах. Предлагается метод объединения мандатной и ролевой политики безопасности на основе решеточного графа, а также, мандатно-ролевая модель управления доступом в операционных системах. Представляется алгоритм реализации мандатного и ролевого управления доступом на основе Де-юре и Де-факто правил.

Необходимость совмещения двух мандатных политик безопасности может возникнуть в системах, требующих обеспечения конфиденциальности и целостности информации одновременно. При этом задача администрирования системы становится весьма трудоемкой, так как каждый доступ проверяется по двум независимым правилам. Наиболее простым решением задачи является построение единой решетки ценностей организации как декартова произведения решеток отделов:

$$L_1 \times L_2$$

При таком подходе каждый объект в системе будет характеризоваться парой меток безопасности (m_1, m_2) $(m_1 \in L_1, m_2 \in L_2)$.

Пусть в отделе D_1 действует линейная решетка ценностей $L_1 = a_1,\ a_2, a_3, a_4$ с четырьмя уровнями безопасности $(a_1 < a_2 < a_3 < a_4)$.

Во втором отделе D_2 пусть действует линейная решетка ценностей $L_2 = b_1, b_2, b_3, b_4$ с четырьмя уровнями безопасности $(b_1 < b_2 < b_3 < b_4)$.

На рис.2. приведен результат применения итоговой решетки безопасности объединенной организации, имеющий 16 меток безопасности.

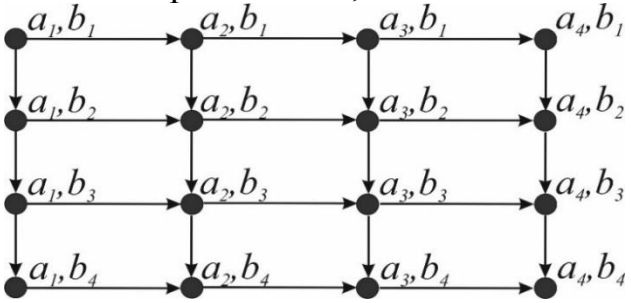


Рис.2. Итоговая решетка безопасности объединенной организации

Возможно возникновение утечки информации, поскольку в полученной новой решетке самый низкий уровень a_4, b_4 предполагает доступ к информации каждого из отделов. Для того чтобы избежать подобной ситуации, необходимо дополнить новую решетку безопасности дополнительными уровнями безопасности. Для этого необходимо ввести элементарное преобразование, которое будет дополнять любую решетку пустым элементом, или нулевым элементом. При таком подходе результирующая решетка будет состоять из 25-ти элементов. Диаграмма решетки $L^{\emptyset}$ представлена на рис. 3.

Решетка $L = L_1 \times L_2$ является инструментом обеспечения

информационного обмена между отделами D_1 и D_2, причем этот информационный обмен будет безопасным, поскольку для каждого вида взаимодействия предусмотрен специальный уровень безопасности. Кроме того, в решетке $L^{\emptyset}$ можно также выделить еще 2 подрешетки, каждая из которых будет имитировать работу отделов без информационного обмена.

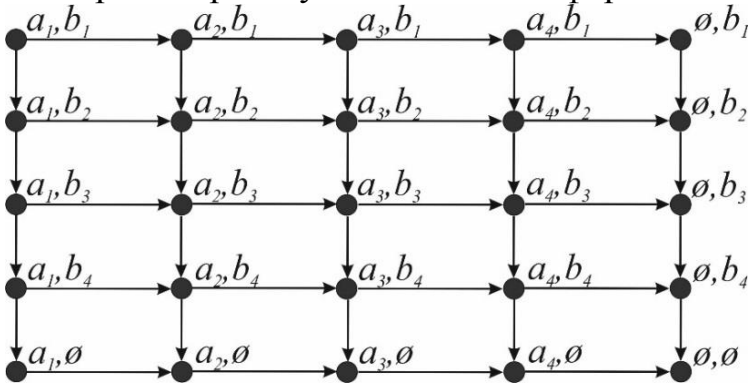


Рис.3. Решетка безопасности объединенных систем

Ролевая политика задается шестью ролями, одна из которых (r_0) является «пустой», то есть не обладающей какими-либо привилегиями и подчиненной любой другой роли. Пусть мандатная политика безопасности задается решеткой L, элементами которой являются узлы l_1, l_2, l_3, l_4 причем отношение порядка задано таким образом, что $l_1 \geq l_2 \geq l_3 \geq l_4$.

Ролевая политика безопасности допускает непротиворечивое совмещение с мандатной политикой безопасности. Для этого необходимо построить решетку $R \times L$, являющуюся декартовым произведением решеток R и L, где $R -$ решетка, определяемая решеточным графом.

Элементами решетки $R \times L$ являются пары (r_i, l_j), при $i = 0, \dots, 4$ и $j = 1, \dots, 5$. При этом отношение порядка задается следующим образом: $(r_i, l_j) \geq (r_k, l_m)$, если $r_i \geq r_k$ и $l_j \geq l_m$.

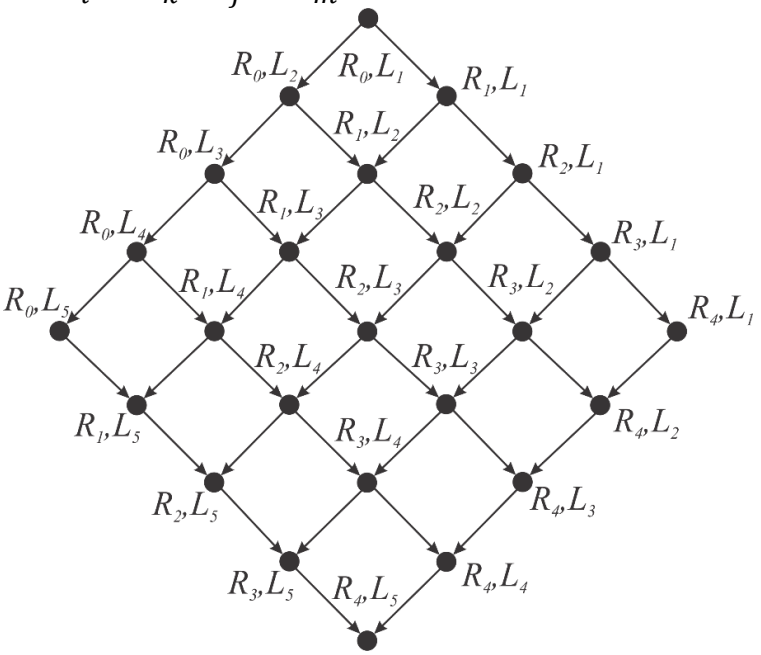


Рис.4. Совмещение ролевой и мандатной политик безопасности

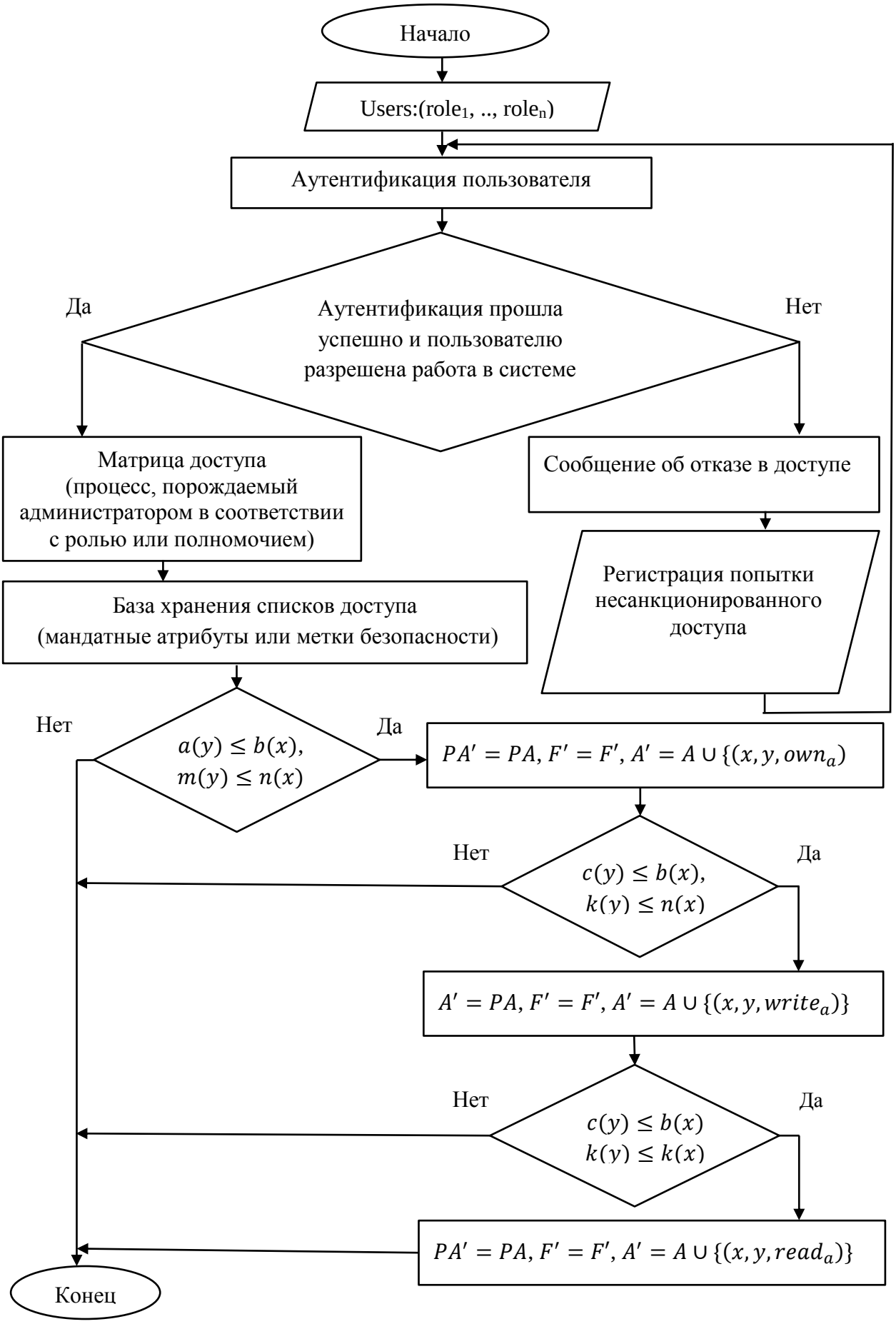


Рис.5. Алгоритм реализации мандатного и ролевого управления доступом

Решеточный граф, изоморфная решетка $R \times L$, представлена на рис.4. На полученной решетке $R \times L$ можно задать мандатную политику безопасности. В свою очередь, на полученном ориентированном графе можно построить ролевую политику безопасности.

Если граф иерархии ролей является решеточным, либо его можно с помощью допустимого преобразования расширить до решеточного, то ролевая политика безопасности допускает непротиворечивое совмещение с мандатной политикой безопасности.

Разработанный на основе Де-юре и Де-факто правил алгоритм реализации мандатно и ролевого управления доступом позволяет повысить защищенность информационной системы с учетом формирования правил управления доступом (рисунок 5).

Таким образом, при применении описанного способа в защищенной информационной системе реализуют единый механизм мандатного и ролевого управления доступом, и в результате предотвращают возможность использования субъектами-нарушителями параметров ролей для доступа к запрещенной информации.

В четвертой главе диссертации **«Средства оценки защищенности информации в инфокоммуникационных системах»** предложен метод, позволяющий рассчитать вероятность ущерба от несанкционированного доступа и количеств попыток реализации угроз безопасности на этапах проектирования инфокоммуникационных систем, а также модель количественной оценки защищенности информации от несанкционированного доступа в инфокоммуникационных системах. Разработан программный комплекс для разграничения несанкционированного доступа в инфокоммуникационных системах.

В таблице 2 показано, как численно различаются оценки защищенности P_x и P_y для компьютерных систем с разными исходными параметрами, на основе метода, который позволит на этапах проектирования инфокоммуникационных систем оценить и минимизировать вероятность ущерба от несанкционированного доступа, а также рассчитать количества попыток реализации угроз безопасности информации. P_x и P_y дают верхнюю и нижнюю границы вероятности несанкционированного доступа к информации.

Таблица 2

Оценка защищенности информации в компьютерных системах

	КТ1	***КТ2***	***КТ3***	***КТ4***	***КТ5***	***КТ6***	***КТ7***
S	12	15	20	30	40	50	50
K	3	3	3	3	3	4	4
N_1	3	5	5	4	10	10	10
N_2	4	5	6	6	10	10	10
N_3	5	5	7	10	10	10	10
M_1	3	3	9	5	3	6	4
M_2	4	3	3	2	3	6	5
M_3	2	3	6	9	3	6	9

P_1	0,066	0,055	0,037	0,040	0,030	0,021	0,022
P_2	0,063	0,055	0,047	0,045	0,030	0,021	0,023
P_3	0,071	0,055	0,042	0,034	0,030	0,021	0,020
U_1	0,187	0,248	0,172	0,151	0,265	0,197	0,205
U_2	0,227	0,248	0,254	0,243	0,265	0,197	0,209
U_3	0,309	0,248	0,257	0,296	0,265	0,197	0,186
P_x	0,251	0,248	0,232	0,251	0,265	0,197	0,198
P_y	8,411	1,481	1,772	5,371	2,782	3,091	3,282

Расчет критериев средств защиты информации от несанкционированного доступа к информации на основе объективных ценностей.

1. MK- Universal:

$$\sum_{i=1}^{15} F_{i1}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j1}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*1+1*0+0{,}9*0+0{,}8*0+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*1+0{,}6*1+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*1) = 5{,}8$$

2. Secret Net:

$$\sum_{i=1}^{15} F_{i2}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j2}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*1+1*1+0{,}9*1+0{,}8*0+0{,}7*0+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*4) = 4$$

3. КРИПТОН-ЩИТ:

$$\sum_{i=1}^{15} F_{i3}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j3}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*0+1*1+0{,}9*0+0{,}8*1+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*2) = 4{,}6$$

4. Страж NT:

$$\sum_{i=1}^{15} F_{i4}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j4}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*0+1*1+0{,}9*0+0{,}8*1+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*3) = 4{,}1$$

5. Dallas Lock:

$$\sum_{i=1}^{15} F_{i5}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j5}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*0+1*1+0{,}9*1+0{,}8*1+0{,}7*1+0{,}5*1+0{,}2*1 \\ +0{,}9*0+0{,}6*1+0{,}1*1+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix}$$
$$-(0{,}5*5) = 5{,}1$$

6. InfoWatch EndPoint Security:

$$\sum_{i=1}^{15} F_{i6}^{+} \cdot P_i^{+} - \sum_{j=1}^{1} F_{j6}^{-} \cdot P_j^{-} =$$

$$\begin{pmatrix} 1*1+1*1+1*1+0{,}9*0+0{,}8*1+0{,}7*1+0{,}5*0+0{,}2*1 \\ +0{,}9*0+0{,}6*0+0{,}1*0+0{,}2*1+0{,}9*1+0{,}9*0+0{,}7*1 \end{pmatrix} - (0{,}5*3) = 5$$

На основе моделей, методов и алгоритмов, усовершенствованных в диссертации, разработан программный комплекс, повышающий защищенность автоматизированных систем, а также произведена сравнительная оценка производительности функционирования разработанного программного комплекса с различными средствами защиты информации от несанкционированного доступа (таблица 3 и рисунок 6).

Таблица 3

Результаты оценки производительности функционирования программного комплекса с различными средствами защиты информации от несанкционированного доступа(НСД)

Средства защиты информации от НСД / Показатели	МК- Universal	Secret Net	КРИПТОН-ЩИТ	Страж NT	Dallas Lock	InfoWatch EndPoint Security
S	5,8	4	4,6	4,1	5,1	5
S_{max}	9,9	9,9	9,9	9,9	9,9	9,9
$U(\%)$	58,585	40,404	46,464	41,414	51,515	50,505

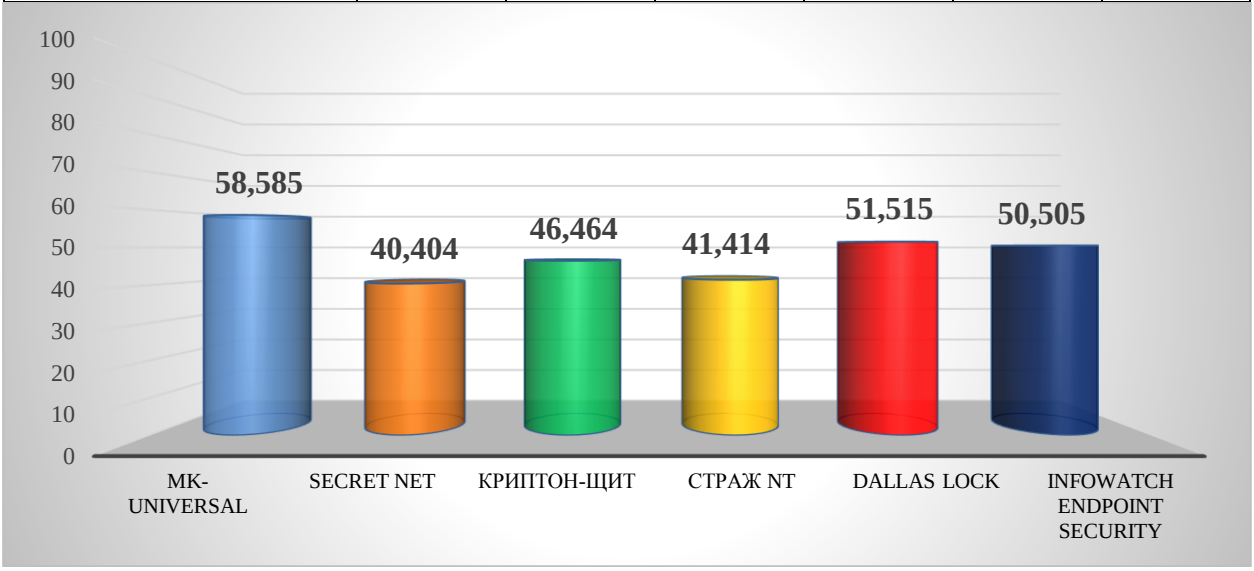


Рис.6. Гистограмма сравнительного анализа производительности функционирования средств защиты информации от несанкционированного доступа

По результатам сравнительного анализа, программный комплекс, повышающий защищенность автоматизированных систем «MK Universal» работает на 7% более производительно, чем средства защиты информации от несанкционированного доступа «Dallas Lock», и на 18% более производительно, чем средства защиты информации от несанкционированного доступа «Secret Net».

ЗАКЛЮЧЕНИЕ

Представлены следующие выводы по теме диссертации «Совершенствование методов и средств повышения защищенности информации в инфокоммуникационных системах»:

1. Предложена модель безопасности организации, основанная на методе ролевого управления доступа. Предложенная модель позволяет построить иерархию ролей, гарантируя, что различные функции управления пользовательскими данными не пересекаются друг с другом.
2. Усовершенствован метод построения мандатной политики безопасности на основе декартова произведения решетки двух ценностей, который позволит обеспечить конфиденциальность и целостность данных.
3. Усовершенствована мандатно-ролевая модель управления доступом с учетом одной из особенностей реализации управления доступом в операционных системах. Усовершенствованная модель позволяет задать функции авторизованных ролей учетных записей пользователей, текущих ролей субъект-сессии и прав доступа.
4. Разработан алгоритм совмещения мандатной и ролевой политик безопасности с использованием Де-юре и Де-факто правил. Разработанный алгоритм позволяет повысить защищенность информационной системы с учетом формирования правил управления доступом.
5. Предложен метод оценки защищенности информации от несанкционированного доступа в инфокоммуникационных системах. Предлагаемый способ позволяет снизить вероятность ущерба от несанкционированного доступа, оценить уровень защищенности системы и дает возможность рассчитать количество реализации угроз безопасности информации.
6. Разработан программный комплекс «MK Universal», повышающий защищенность автоматизированных систем. В результате оценки производительности установлено, что разработанный программный комплекс защиты информации от несанкционированного доступа позволяет работать на 7% производительнее лучшего показателя «Dallas Lock», и на 18% производительнее худшего показателя «Secret Net».

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

TASHKENT STATE TECHNICAL UNIVERSITY

KADIROV MIR-KHUSAN MIRPULATOVICH

IMPROVING METHODS AND TOOLS OF INCREASING INFORMATION SECURITY ON INFOCOMMUNICATION SYSTEMS

05.01.05 – Methods and systems of information protection. Information Security.

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES

Tashkent-2020

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2020.3.PhD/T308.

The dissertation has been prepared at Tashkent State Technical University.

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

Scientific adviser:	**Karimov Madjit Malikovich** Doctor of Technical Sciences, Professor
Official opponents:	**Abdurakhimov Bakhtiyor Fayzievich** Doctor of Physical-Mathematical Sciences, Professor
	Ganiev Abdukhalil Abdujalilovich Doctor of Philosophy on Technical Sciences, Docent
Leading organization:	**Scientific-Engineering and Marketing researches Center «UNICON.UZ»**

The defense will take place "08" october 2020 at 14 ^{00} the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No2619). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on "25" september 2020 y.
(mailing report No. 14 on "24" august 2020 y.).

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

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

S.K. Ganiev
Chairman of the academic seminar under the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to develop methods and tools based on access control models to beef up the security level of infocommunication systems.

The object of the research work is information flows on infocommunication systems.

The scientific novelty of the research work is as follows:

the organization's security model based on the method of access control to information, which guarantees that the function of managing various user data is not interrupted is improved;

a conceptual model for increasing the security of information with a mandated access control policy is developed;

the method for constructing a mandatory security policy based on the Cartesian product of a lattice of two values, which will ensure the confidentiality and integrity of data is improved;

the mandatory-role model of access control, which allows to define the functions of the authorized roles of user accounts and access rights is improved;

an algorithm that increase the level of security of the system in accordance with the De jure and De facto rules and based on the formation of rules for controlling access to information are worked out.

Implementation of the research results. On the basis obtained scientific methods, models and algorithms restricting unauthorized access to information on infocommunication systems:

a software complex that increases the security of automated systems based on an improved mandate-role model of access control, which allows to set the functions of authorized roles for user accounts and access rights is implemented in the Republican Stock Exchange “Toshkent” JSC (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated August 17, 2020 No. 33-8/4721). As a result of scientific research the developed software complex in the work processes of employees of the organization allowed to manage the level of confidentiality of the subject, monitor employees and prevent unauthorized use of system information.

the developed an algorithm and software complex which allows to increase the level of system security in accordance with the formed rules De jure and De facto, also based on the formation of rules for managing access to information implemented into the activities of “Trans New Millenium” Ltd (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated August 17, 2020 No. 33-8/4721). As a result, the developed software complex “MK Universal” that increases the security of automated systems works 7% more efficiently than the tools of protecting information from unauthorized access “Dallas Lock”, and 18% more productive than the software complex “Secret Net”;

the proposed organization security model based on the information security access control method and the developed software complex based on the client-server architecture implemented into the activities of “UNF Universal” Ltd

(certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated August 17, 2020 No. 33-8/4721). As a result, the software complex based on the client-server architecture allowed to build a hierarchy of roles by ensuring that user data management functions do not overlap and eliminate unauthorized use of system information also increase the organization's productivity by 13% by managing its employees.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, four chapters, conclusion, references and appendix. The volume of the thesis is 118 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (Часть I; Part I)

1. 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. (05.00.00; №16)
2. 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. (05.00.00; №16)
3. 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. (05.00.00; №8)
4. 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. –PP. 4664-4673. (05.00.00; №8)
5. Kadirov M.M., Tojikhujaeva N.Z., Kasimova G.I. Classification of modern security monitoring systems in computer systems and networks // International Journal of Advanced Research in Science, Engineering and Technology, Vol. 5, Issue 9, India 2018. –PP. 6764-6769. (05.00.00; №8)
6. Kadirov M.M., Yuldasheva M., Akbarova Sh.A. Problems of Security of Infocommunication Systems // International Journal of Advanced Research in Science, Engineering and Technology, Vol. 6, Issue 2, India 2019. –PP. 8026-8031. (05.00.00; №8)
7. Kadirov M.M., Toshmatova Sh.S., Ganiyeva T.I., Kurbanova 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. –PP. 8197-8204. (05.00.00; №8)
8. 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, Vol. 6, Issue 3, India 2019. –PP. 8426-8432. (05.00.00; №8)
9. Sagatov M.V., Kadirov M.M., Karimova D., Tojikhujaeva N.Z., Khamdamova S.M. Software Implementation of the System of Additional Guaranteed Deletion of Created File Objects // International Journal of Advanced Research in Science, Engineering and Technology, Vol. 6, Issue 3, India 2019. –PP. 9078-9083. (05.00.00; №8)
10. Kadirov M. M., Tojikhujaeva 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. (05.00.00; №8)

11. Kadirov M.M. Approach to Assessing the Security of Information From Unauthorized Access // International Journal of Advanced Research in Science, Engineering and Technology, Vol. 6, Issue 12, India 2019. –PP. 12182-12187. (05.00.00; №8)

12. Kadirov M., Tulyaganov Z., Tojikhujaeva 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. (№3; Scopus; IF=0.3)

13. 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. (№3; Scopus; IF=0.3)

II бўлим (Часть II; Part II)

14. Кадиров М.М. Принципы построения комплексной системы защиты информации // Сборник статьей международной научно-технической конференции “Радиоэлектроника, информационные и телекоммуникационные технологии: проблемы и развитие”, II том, Ташкент 2015. –С.184-187.

15. Кадиров М.М., Тулаганов З.Я. Модель Белла-ЛаПадулы в управление доступом // Сборник статьей международной научно-технической конференции “Радиоэлектроника, информационные и телекоммуникационные технологии: проблемы и развитие”, II том, Ташкент 2015. –С.188-190.

16. 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. –С. 303-304.

17. Miraziz Sagatov, Durdona Irgasheva, Mirhusan Kadirov. Construction hardware protection infocommunication systems from network attacks // International conference on application of information and communication technology and statistics in economy and education, (ICAICTSEE – 2015), November 13 – 14th, 2015, Sofia, Bulgaria. – PP. 271-277.

18. Каримов М.М., Кадиров М.М. Ахборот хавфсизлигини оширишда файлларни назорат қилиш // “Ўзбекистон Республикаси ҳуқуқни муҳофаза қилиш органлари тизимларида локал компьютер тармоқларини амалда жорий этиш йўллари ва уларни хавфсизлигини таъминлаш” мавзусидаги республика илмий – амалий семинар. Тошкент – 10 май 2016 йил. Ўзбекистон Республикаси ички ишлар вазирлиги, Тошкент олий ҳарбий – техник билим юрти.

19. Кадиров М.М., Тожихужаева Н.З. Каримова Н.О. Подход к оценке защищенности информации от несанкционированного доступа // International scientific journal «Global Science and Innovations 2020: Central Asia» Hyp-

Султон, февраль-март 2020. № 3(3). 126-130 стр.

20. 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.

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

22. 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.

23. Каримов М.М., Кадиров М. М., Турдибоев Б. Й., Сагатов М. М. Тизимдаги фойдаланувчиларни ҳуқуқларини белгилаш орқали назорат қилиш/ ЭҲМ учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисидаги гувоҳнома №DGU04652, 16.06.2017 й.

24. Каримов М. М., Ташев К. А., Кадиров М. М., Ёриқулов М.Р., Сагатова С. М. Маълумотларни кафолатли ўчириш дастури / ЭҲМ учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисидаги гувоҳнома. № DGU 04845, 29.09.2017 й.

25. Кадиров М.М., Гуломов Ш. Р., Юсупов Б. К., Туляганов З.Я., Хамдамова С.М., Бозоров С.М. Компьютер тармоқларидаги ҳужумларни аниқловчи дастурий модул / ЭҲМ учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисидаги гувоҳнома. №DGU05742, 31.10.2018 й.

26. Кадиров М.М., Каримова Н.О., Тожихужаева Н.З., Акбарова Ш.А., Касимова Г.И., “SFOandCIAgent” иловаси / ЭҲМ учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисидаги гувоҳнома. № DGU 07713, 10.02.2020 й.

27. Кадиров М.М., Каримова Н.О., Тожихужаева Н.З., Акбарова Ш.А., Касимова Г.И., Мандат ва ролли моделларига асосланган фойдаланишни назорат қилувчи дастурий пакет / ЭҲМ учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисидаги гувоҳнома. № DGU 07736, 10.02.2020 й.

28. Каримов М.М., Гуломов Ш. Р., Юсупов Б. К., Равилов М.М., Туляганов З.Я. Автоматлаштирилган тизим ҳимояланганлигини оширувчи дастурий мажмуаси “MK Universal”/ЭҲМ учун яратилган дастурнинг расмий рўйхатдан ўтказилганлиги тўғрисидаги гувоҳнома. №DGU07714, 10.02.2020 й.

Автореферат “Муҳаммад ал-Хоразмий авлодлари” илмий журнали таҳририятида таҳрирдан ўтказилди ва ўзбек, рус ва инглиз тилларидаги матнларини мослиги текширилди.