

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

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

НАЗАРОВ ФАЙЗУЛЛО МАХМАДИЯРОВИЧ

НОСТАЦИОНАР ТИЗИМЛАРНИ ТАШКИЛИЙ БОШҚАРИШДА
ТАҚСИМЛАНГАН РЕЕСТР МЕХАНИЗМЛАРИ АСОСИДА
МАЪЛУМОТЛАР ИШОНЧЛИЛИГИНИ ОШИРИШ УСУЛ ВА
АЛГОРИТМЛАРИ

05.01.02 – Тизимли таҳлил, бошқарув ва ахборотни қайта ишлаш

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD)
ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

**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**

Назаров Файзулло Махмадиярович

Ностационар тизимларни ташкилий бошқаришда тақсимланган реестр
механизмлари асосида маълумотлар ишончилигини ошириш усул ва
алгоритмлари.....3

Назаров Файзулло Махмадиярович

Методы и алгоритмы повышения достоверности информации на основе
механизмов распределенного реестра при организационном управлении
нестационарными системами.....21

Nazarov Fayzullo Makhmadiyarovich

Methods and algorithms for increasing the reliability of information based on the
mechanisms of the distributed register in the organizational management of non-
stationary systems.....39

Эълон қилинган ишлар рўйхати

Список опубликованных работ

List of published works.....43

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

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

НАЗАРОВ ФАЙЗУЛЛО МАХМАДИЯРОВИЧ

НОСТАЦИОНАР ТИЗИМЛАРНИ ТАШКИЛИЙ БОШҚАРИШДА
ТАҚСИМЛАНГАН РЕЕСТР МЕХАНИЗМЛАРИ АСОСИДА
МАЪЛУМОТЛАР ИШОНЧЛИЛИГИНИ ОШИРИШ УСУЛ ВА
АЛГОРИТМЛАРИ

05.01.02 – Тизимли таҳлил, бошқарув ва ахборотни қайта ишлаш

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD)
ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент – 2021

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида №В2020.2.PhD/Т1560 рақам билан рўйхатга олинган.

Диссертация Самарқанд давлат 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:

Ахатов Акмал Рустамович
техника фанлари доктори, профессор

Расмий оппонентлар:

Бабомурадов Озод Жураевич
техника фанлари доктори

Тухтаназаров Дилмурод Солижонович
техника фанлари бўйича фалсафа доктор

Етакчи ташкилот:

Тошкент давлат транспорт университети

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.Т.07.01 рақамли Илмий кенгашнинг 2021 йил «03» ИЮН соат 16:00 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 (202 рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2021 йил «21» май да тарқатилди.
(2021 йил «08» май даги 11 рақамли реестр баённомаси.)



Р. Х. Хамдамов
Илмий даражалар берувчи илмий кенгаш
раиси, техника фанлари доктори, профессор

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

А.В. Кабулов
Илмий даражалар берувчи илмий кенгаш
қошидаги илмий семинар раиси, техника
фанлари доктори, профессор

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳон тажрибаси шуни кўрсатадики, рақамли технологиялар асосида ижтимоий – иқтисодиёт тизимларни автоматлаштирилган ҳолда бошқаришни оптималлаштириш учун бошқариладиган тизим таркибидаги маълумотлар ишончилигини оширишга тўғри келади. Ҳозирда маълумотлар оқими ўзгарувчан бўлганлиги сабабли компьютер тармоқларидаги ахборот тизимларини бошқарув моделлари асосида бошқариш ҳамда маълумотлар ишончилигини оширишда тақсимланган реестрга асосланган блокчейн механизмларини қўллаш самарали усуллардан бири ҳисобланади. Шу сабабли, АҚШ, Буюк Британия, Германия, Франция, Италия, Испания Япония, Жанубий Корея, Россия Федерацияси, Хитой, Хиндистон ва дунёнинг бошқа мамлакатларининг олимлари сақланаётган маълумотларнинг ишончилигини таъминлашда тақсимланган реестрга асосланган блокчейн механизмларини қўллаш бўйича бир қанча тадқиқотлар олиб бормоқда. Бундай тадқиқотларда блокчейн технологиясини қўллаш асосан криптовалюта тизимларини ташкил қилиш ва пул айланишга асосланган бизнес – жараёнларини оптималлаштиришга қаратилган. Шу қаторда, бугунги кунда компьютер тармоқларидаги электрон ҳужжат айланиш, логистика, электрон коммунал тўловлар каби бошқарув тизимларининг маълумотлари ишончилигини ошириш учун тақсимланган реестр механизмларини қўллаш масалалари ўз ечимини етарли даражада топмаганлигини таъкидлаш мумкин.

Компьютер тармоқларидаги электрон ҳужжат айланиш, электрон коммунал тўловлар, логистика каби тизимларда қатъий чекланган муддатлар белгиланади, аммо маълумотларни қайта ишлаш жараёнида кечикиш ҳолатлари кузатилади ва ушбу кечикишларни бартараф этиш муаммоси муҳим масалалардан бири ҳисобланади. Келтирилган тизимлар ностационар табиатга эга эканлиги, кечикиш ҳолатларини тавсифлайдиган маълумотлар ишончилигини таъминлашда қўшимча муаммоларни келтириб чиқаради. Шу сабабли сўнгги йилларда бошқарувни оптималлаштириш учун, бошқарув назарияси усулларини қўллаш амалиёти асосида чекланган шартлардаги ностационар тизимларнинг маълумотлар ишончилигини ошириш усулларига қизиқиш ортиб бормоқда. Бошқарув тизимларида тақсимланган реестрга асосланган блокчейн технологиясини қўллаш маълумотлар ишончилигини оширишда янгича ёндашувни белгилаб беради. Демак, ностационар жараёнли бошқарув тизимларининг маълумотлар ишончилигини оширишда тақсимланган реестрга асосланган блокчейн механизмлари ёрдамида маълумотлар базасини шакллантиришнинг архитектура модели ва алгоритмларини ишлаб чиқиш ҳамда қўллаш долзарб тадқиқотлар мавзусини касб этади.

Республикамызда ахборот-коммуникацион технологияларни ривожлантириш билан бир қаторда ахборот тизимларининг бошқариш сифатини ва улардаги маълумотларнинг ишончилигини оширишга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. Ўзбекистон

Республикасини янада ривожлантириш бўйича ҳаракатлар стратегиясига кўра, илмий тадқиқот ва инновацион фаолиятни ривожлантириш, илмий ва инновацион ютуқларни амалиётга жорий этишнинг эффектив механизмларини яратиш масалаларига оид муаммоларни ҳал қилишга алоҳида эътибор қаратилган.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги ва 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари, 2018 йил 21 ноябрдаги ПҚ-4024-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти муайян 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. Ностационар жараёнларни динамик бошқариш бўйича хорижий олимлардан С.Р.Сутлер, В.Л.Рамакер, башоратлаш асосида бошқарувни моделлаштириш бўйича Ж.Ричалет, А.Раулт, Ж.Тестуд, Ж.Папон, Д.В.Кларке, Р.Скаттолини, Л.Чиски, Э.Моска, ностационар жараёнларини терминал бошқаришни математик моделлаштириш бўйича А.Пропое, А.Э.Красовский ва И.Е.Зубер тадқиқот ишларини олиб борган. Бошқариладиган тизимларга тақсимланган реестрга асосланган блокчейн механизмларини қўллаш бўйича М.М.Пряников, А.В.Чугунов, А.И.Власов, А.А.Карпунин, А.С.Теряева, А.С.Баева тадқиқот ишларини олиб борган. Блокчейн механизмлари таркибида криптографик алгоритмларни қўллаш бўйича Сатоши Накамото, Р.Маянк, Г.Данило, К.Катина, Л.Ванг, Х.Шен, Ж.Ли, Ж.Шао, Й.Янг, П.Й.Пириоу, Жеан Франсоис, Э.Дуффиелд, Х.Счинзел, Ф.Гутиеррез, К.В.Дам, Х.С.Лин тадқиқот ишлари олиб борган.

Шунингдек Ўзбекистонда М.М.Камилов, Т.Ф.Бекмуратов, М.М.Каримов, Р.Х.Хамдамов, Ш.Х.Фозилов, М.А.Исмаилов, Д.Т.Мухаммадиева, М.А.Рахматуллаев, О.Ж.Бабомуродов, Н.С.Маматовлар оптимал бошқарувга бағишланган илмий тадқиқотларга катта ҳиссаларини қўшган.

Юқорида келтирилган олим ва тадқиқотчиларнинг тадқиқот ишлари тизимли таҳлил қилиниш натижасида бошқарув жараёнлари чекланган шароитлардаги шартларда етарли даражада ўрганилмаган ҳамда бошқариладиган ахборот тизимларида тақсимланган реестр механизмлари асосида маълумотлар ишончлилигини ошириш ҳам етарли даражада

ўрганилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация иши Самарқанд давлат университети ва Тошкент ахборот технологиялари университети Самарқанд филиалининг А5-039-«Маълумотларни интеллектуал таҳлил қилишнинг параллел алгоритмларини қуриш дастурий воситаларини ишлаб чиқиш» (2015-2017) ва БА-А5-033-«Даволаш-профилактика муассасаларида маълумотларга ишлов бериш ва фаолият мониторинги автоматлашган тизимини яратиш» (2017-2018) мавзуларидаги лойиҳалар доирасида бажарилган.

Тадқиқотнинг мақсади чекланган шартли ностационар тизимларни башоратли бошқарув модели ҳамда тизимда маълумотлар ишончлилигини ошириш усул, алгоритмлари ва дастурий воситасини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

ностационар тизимларни бошқариш моделлари ва бошқариладиган тизим маълумотлар ишончлилигини ошириш усулларини тизимли таҳлил қилиш;

чекланган шартлардаги ностационар тизим маълумотлар ишончлилигини оширишнинг блокчейнга асосланган усул ва алгоритминини ишлаб чиқиш;

тақсимланган реестр механизмларига махфийлаштиришнинг динамик усулини қўллаш орқали бошқарув самарадорлигини ошириш алгоритминини ишлаб чиқиш;

чекланган шартлардаги ностационар тизимларни бошқаришнинг математик моделларини такомиллаштириш;

чекланган шартлардаги ностационар тизимлар бошқарувини оптималлаштириш дастурий мажмуасини лойиҳалаш, ишлаб чиқиш ва жорий қилиш.

Тадқиқотнинг объекти сифатида тўлов тизимлари шу жумладан, олий таълим шартнома тўловини амалга оширишда ва электрон хужжат алмашинув тизимида маълумотларга ишлов бериш жараёнлари қаралган.

Тадқиқотнинг предмети сифатида ностационар тизимларни ташкилий бошқариш ва тақсимланган реестр механизмлари асосида маълумотлар ишончлилигини оширишнинг усул ва алгоритмларидан иборат.

Тадқиқотнинг усуллари. Тадқиқот жараёнида тизимли таҳлил, бошқарув усуллар назарияси, математик моделлаштириш, нейрон тармоғи назарияси, тақсимланган реестр, яъни блокчейн механизмлари, ахборотни химоялаш усуллари, алгоритмлаштириш ҳамда маълумотлар ва билимлар базасини лойиҳалаштириш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

ностационар тизимларни чеклов шартлари асосида ташкилий бошқаришнинг башоратли модели ишлаб чиқилган;

чекланган шартлардаги ностационар тизимларни нейрон тармоғи асосида ташкилий бошқаришнинг оптималлаштириш модели ишлаб чиқилган;

ностационар тизимларда тақсимланган реестр механизмларининг консенсус алгоритми асосида маълумотлар ишончилигини ошириш усули ишлаб чиқилган;

ностационар тизим бошқарувини оптималлаштиришда блокчейнга асосланган махфийлаштиришнинг динамик усулини такомиллаштириш алгоритми ишлаб чиқилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

ностационар тизимларни чекланган шароитлардаги шартлар асосида бошқарув ва ностационар тизим маълумотлар ишончилигини тақсимланган реестр механизми асосида оширишнинг алгоритмик таъминоти ишлаб чиқилган;

тақсимланган реестр механизмлари асосида динамик калитли шифрлаш усулларни қўллаш жараёнининг алгоритмик таъминоти ишлаб чиқилган;

чекланган шароитлардаги ностационар тизимларни бошқариш ва маълумотлар ишончилигини оширишнинг дастурий модуллари яратилган ва бу дастурий модуллари олий таълим муассасаси шартнома тўлов ва электрон ҳужжат айланиш жараёнларига тадбиқ этилган.

Тадқиқот натижаларининг ишончилиги. Тадқиқот натижаларининг ишончилиги қўйилган муаммонинг математик жиҳатдан аниқ ифодаланиши, ностационар тизимлар учун чекланган шароитли шартларни эътиборга олиш усуллари, нейрон тармоғини башоратлаш моделлари асосида бошқариш, блокчейн механизмларини тармоқ тизимларига қўлланилиш усуллари, RSA шифрлаш усули билан интеграцияси, ишлаб чиқилган динамик калитли шифрлаш усулини криптобардошлилиги тажрибавий тадқиқотларнинг ижобий натижалари билан тасдиқланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти ишлаб чиқилган бошқарув моделлари, усуллари ва алгоритмлари ташкилий бошқариладиган иқтисодий жараёнлар параметрларини башоратлаш асосида бошқарувни оптималлаштириш ҳамда маълумотлар ишончилигини таъминлаш билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти шундан иборатки, ишлаб чиқилган усул ва алгоритмлар тўлов тизимларининг мавжуд маълумотлари асосида тўлов муддатларини белгилаш учун тавсиялар беради, тармоқ тизимларидаги ностационар тизим маълумотларини махфийлаштириш асосида маълумотлар ишончилигини ошириш, ташкилотларнинг электрон ҳужжат айланиш тизимларининг хавфсизлиги ва самарадорлигини ошириши билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Диссертация тадқиқотлари доирасида ностационар тизимларни ташкилий бошқаришда тақсимланган реестр механизми ёрдамида маълумотлар ишончилигини ошириш усули ва алгоритмларини ишлаб чиқиш бўйича олинган илмий натижалар асосида:

бошқариладиган ностационар тизимнинг кириш маълумотларини аниқлаш, консенсус алгоритмларини танлаш, тақсимланган реестрга асосланган блокчейн механизмлари асосида маълумотлар базаси архитектурасини ишлаб чиқиш алгоритмлари Самарқанд вилоят иқтисодий судига жорий қилинган (Ўзбекистон Республикаси Олий судининг 2020 йил 17 декабрдаги 08/УМ-727-20-сон маълумотномаси). Натижада тақсимланган реестрга асосланган блокчейн механизмлари асосида электрон хужжат айланиш тизими ташкил этишда хотира ҳажми ва маълумотлар ишончилиги самарадорлигини 1,5-2 баробар оширишга эришилган.

бошқариладиган ностационар тизимларга шифрлаш усулларни тақсимланган реестр механизмлари билан интеграциялаш асосида яратилган алгоритм ва механизмлар Қишлоқ қурилиш банкига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 2 декабрдаги 33-8/7344-сон маълумотномаси). Натижалар электрон хужжат айланиш тизимининг маълумотлар базасида маълумотлар ишончилиги самарадорлигини 1,5-2 баробар ошириш имконини берган;

ностационар тизимларнинг ташкилий бошқаришнинг чекланган шартларни ҳисобга олган ҳолда ишлаб чиқилган бошқарувнинг башоратли, адаптив-статистик ва нейрон моделлари ҳамда тақсимланган реестр механизмлари асосида яратилган алгоритм ва механизмлар Самарқанд давлат университети ва ТАТУ Самарқанд филиалига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 2 декабрдаги 33-8/7344-сон маълумотномаси). Натижада олий таълим шартнома тўлов жараёнида чекланган шартдаги бошқарув моделлари асосида тавсия этилган янги муддатлардаги тўловларнинг ҳажмини 7-8% га оширишга эришилган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари, жумладан, 5 та халқаро ва 5 та республика илмий амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Тадқиқот мавзуси бўйича жами 22 та илмий иш чоп этилган, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертациялар асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 8 та илмий мақола, 4 таси хорижий ва 4 таси республика журналларида нашр қилинган, шунингдек, 4 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 110 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Киришда диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг республика фан ва технологиялари тараққиётининг устувор йўналишларига мослиги кўрсатилган. Тадқиқотнинг мақсад ва вазифалари белгилаб олинган ҳамда тадқиқот объекти ва предмети

аниқланган, олинган натижаларнинг ишончилиги асослаб берилган, уларнинг назарий ва амалий аҳамияти кўрсатилган, тадқиқот натижаларини амалиётга жорий қилиш ҳолати, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг «**Ностационар тизимларни бошқариш ва маълумотлар ишончилигини оширишнинг масалалари**» деб номланган биринчи боби, учта параграфдан иборат бўлиб, унда ностационар тизимларни бошқариш масаласининг замонавий ҳолати, чекланган шароитларда ечиш усулларининг таҳлили, бошқарувни оптималлаштиришда маълумотлар ишончилигини ошириш бўйича тақсимланган реестр механизмларининг ютуқ ва камчиликлари қайд этилган. Тизимдаги чекловлар сифатида автоматлаштирилган тизимларда топшириқлар ва вазифаларни бажариш жараёнида қаътий чекланган муддатлар белгиланади. Тадқиқотда қуйиладиган вазифалар ижро этилиш вақтида ушбу муддатларнинг кечикиш ҳолатлари ҳам мавжуд деб қабул қилинади. Электрон ҳужжат айланиш, таълим шартнома тўлов, коммунал тўловларни мониторинг қилиш, махсулотлар логистикаси ва шу каби бошқа тизимлар буларга мисол қилиб хизмат қилади. Шу муносабат билан, белгиланган вақт ичида вазифаларни бажарилмаслик ҳамда кечикишлар билан ишлов бериш ҳолатлари кузатилаётган тизимларни чекланган шартлардаги ностационар тизимлар деб номлаймиз (ЧШНТ). Ностационар тизимларни бошқариш бўйича маълумотлар ишончилигини оширишнинг усул ва алгоритмларини ўрганиш асосида тадқиқотнинг ушбу йўналишни ривожлантириш муаммолари ва уларни ҳал этиш йўллари аниқланган ҳамда тадқиқот иши масаласининг қўйилиши шакллантирилган. Ностационар тизимлар объектлари, кузатиш соҳаси ва бошқарилувчи чиқиш модели мос равишда қуйидаги (1)-(3) муносабатлар билан ифодаланади:

$$\begin{cases} x_{t+1} = A_t x_t + B_t u_t + z_t \\ x_{t|t=0} = x_0 \end{cases} \quad (1)$$

$$\lambda_t = H_t x_t + q_t \quad (2)$$

$$y_t = L_t x_t \quad (3)$$

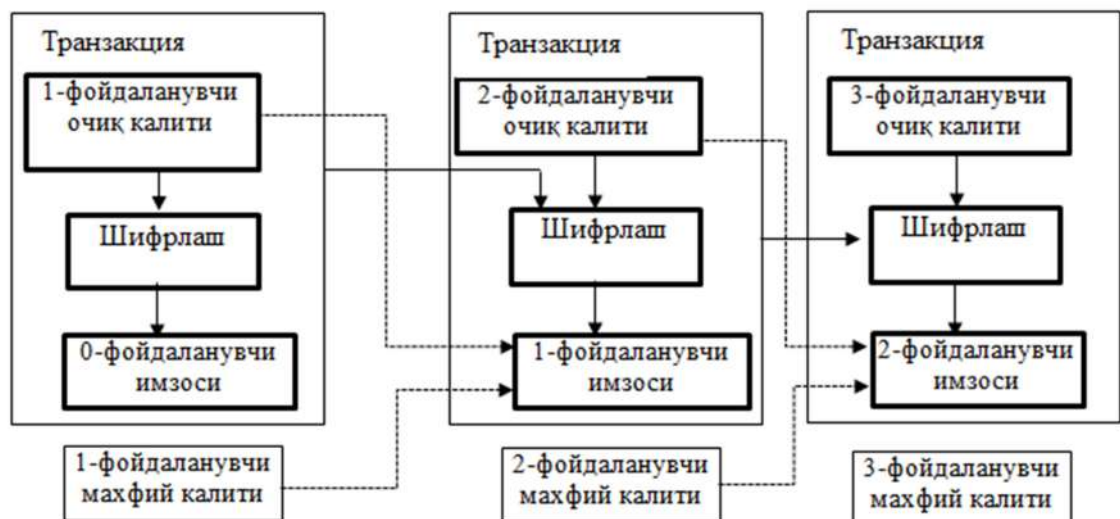
Бу ерда $x_t \in R^n$ - ностационар объектнинг ҳолати, $u_t \in R^m$ - бошқарувчи таъсир (маълум киришлар), $\lambda_t \in R^l$ - кузатишлар, назорат системасининг чиқиши, $y_t \in R^n$ - бошқарилувчи чиқишлар, A_t, B_t, H_t, L_t - тегишли параметрлар ўлчамларнинг матрицалари сифатида қаралади. Қаралаётган объект ҳолатининг назорат қилиш системаси (2) тенглама билан берилган. Фараз қиламизки, z_t тасодифий кўзғалишлар ва ўлчамнинг хатоликлари q_t ўзаро корреляцияланмаган ва ўртачаси 0 га тенг ва Z, Q ковариацияларга эга Гаусс тақсимотига бўйсинади. Чекланишлар қуйидаги тенгсизликлар кўринишида ифодаланади.

$$\alpha_1(t) \leq D_1 x_1 \leq \alpha_2(t) \quad (4)$$

$$\varphi_1(x_i, t) \leq D_2 u_i \leq \varphi_2(x_i, t) \quad (5)$$

Бу ерда D_1 ва D_2 чекланишларга қўйиладиган x_i ва u_i векторлар компоненталарини аниқловчи ноллар ва бирлардан иборат тўлиқ рангдаги структурали матрицалар; $\alpha_1(t), \alpha_2(t), \varphi_1(x_i, t), \varphi_2(x_i, t)$ - берилган векторлар ўлчовларининг вектор функциялари ҳисобланади. Масала шундан иборатки λ_i кузатишлар бўйича шундай бошқарув стратегиясини ишлаб чиқиш керакки, унда y_i системалар чиқиш вектори (4) - (5) чекланишларни ҳисобга олган ҳолда берилган \bar{y}_0 векторига яқин бўлиш керак. Юқорида қўйилган масаланинг оптимал ечимларини аниқлаш, ишончли маълумотларга таянган ҳолда амалга оширилади. Бунинг учун тақсимланган реестр механизмлари асосида маълумотлар ишончилигини оширишнинг тамоиллари, усул ва алгоритмларининг қиёсий таҳлили батафсил келтирилган.

Диссертациянинг «**Чекланган ностационар тизимларнинг маълумотлар ишончилигини ошириш алгоритмлари**» деб номланган иккинчи боби, тўртта параграфдан иборат. Ностационар тизимларни бошқаришда тақсимланган реестр механизмлари асосида маълумотлар ишончилигини ошириш усул ва алгоритмлари ишлаб чиқилган. Бошқарувни оптималлаштириш учун тақсимланган реестр механизмлари асосида маълумотлар базаси архитектура модели, консенсус алгоритмлари ва шифрлаш усулларини такомиллаштириш алгоритмлари таклиф этилган. Блокчейн технологиялари “тақсимланган реестр технологияси” (англ: Distributed ledger technology - ДЛТ) деб аталадиган алоҳида архитектуралар синфига киритилган. Бундан келиб чиқиб маълумотлар базасининг структурасини шифрланган маълумотлар занжири кўринишида ишлаб чиқилган. Ёпиқ транзакцияларни шифрлаш учун, очик транзакцияларни фиксациялаш учун мўлжалланган иккита криптографик калитлардан иборат жамланмани фойдаланувчилар тармоқга киришда ва ишчи станцияга зарур дастурий таъминотни ўрнатиш натижасида амалга оширадилар. Ҳар бир бажарилган транзакцияларни 1-расм кўринишидаги модел орқали тасдиқлаш амалга оширилади.



1- расм. Транзакция тўғри бажарилганлигини тасдиқлаш схемаси

Ҳар бир тармоқ таркибидаги фойдаланувчи кейинги фойдаланувчига транзакцияларни юбораётган вақтда, олдинги транзакция хешини ва кейингисининг очиқ калитини имзолайди ва бу ахборотни транзакция охирига қўшади. Бу схемага асосан ҳар бир навбатдаги маълумотлар блоки олдинги блок хешига асосланган бўлади. Назарий жиҳатдан тармоқнинг ички таркибига блокни қўшиш мумкин, лекин блокни қўшиш учун энг биринчи ҳосил қилинган блоккача барча олдинги блоklar хешини очишни таълаб этади. Бу эса амалий жиҳатдан олдиндан боғлиқ бўлмаган блокни қўшишнинг мумкин эмаслик хоссасини таъминлайди, яъни тақсимланган реестр асосида тармоқни қуришнинг концептуал принципи тасдиқланади. Тақсимланган реестр механизмларидан фойдаланишда, албатта консенсус алгоритмларидан бирини танлаш таълаб этилади. Консенсус алгоритмлари тақсимланган реестр технологияси таркибидаги маълумотларни ҳаққонийлигини тасдиқлаш учун фойдаланилади. Proof of Stake (Pos) алгоритмининг ишлаш принципи блокчейнга асосланган тизимларда кенг тарқалган ва у бажарилган ишлар улушларни тасдиқлаш алгоритми асосида яратилган услублар ва ечимлардан иборат бўлади. Консенсус алгоритмларининг тадқиқи натижасида Pos алгоритми ЧШНТлар учун энг самарали усул эканлиги аниқланди. Pos алгоритми қўлланилишида бошқарув тизимларидаги ҳар бир маълумот улуш сифатида қабул қилинади ва тасдиқланган криптографик калит орқали махфийлаштирилади. Тақсимланган реестр механизмлари асосида яратилган маълумотлар базасининг ҳар бир блоки узидан олдинги блок таркибидаги маълумотнинг параметри бўйича махфийлаштирилган ҳисобланади. Юқоридаги механизм бўйича тармоқдаги ахборот тизимларининг маълумотлар базаси блокчейн асосида қуйидаги алгоритм бўйича шакллантирилади:

1-қadam. Маълумотларнинг шакли ва турига асосан консенсус алгоритмлари танланади;

2-қadam. Криптографик усул асосида криптографик функция шакллантирилади;

3-қadam. Дастлабки маълумотлар блоки шакллантирилади;

4-қadam. Ҳар бир n -блок калити, $(n-1)$ -блок таркибидаги маълумотнинг параметри бўйича шакллантирилади;

5-қadam. Ҳар бир блок таркибига сақланадиган маълумот, яратилган калит асосида криптографик усул билан махфийлаштирилади;

6-қadam. Шифрланган маълумот блок таркибига жойлаштирилади.

Юқоридаги алгоритм, маълумотларни занжир шаклида динамик калитли криптографик усул билан сақлашни ташкил қилади. Тизим таркибига математик-криптографик ахборот ҳимоясини таъминлаш бўйича, RSA криптографик усулини тақсимланган реестр механизмлари асосида такомиллаштириб Pos алгоритми бўйича динамиклаштирилган калитли криптографик RSA алгоритми таклиф этилган.

Натижада бу усул криптобардошликни, икки марта оширади ва ёпиқ калитни бузиш ёки топишга уриниш $2 \cdot 2^N = 2^{N+1}$ комбинацияларнинг комбинациясига олиб келади. Ишлаб чиқилган алгоритмлар асосида

такомиллаштирилган RSA криптографик усулини криптобардошлик даражасини аниқланган. RSA криптографик усул учун қуйидаги (6) формула билан тавсифланадиган баҳо келтирилган.

$$L_{RSA}(n, r, \alpha) = O\left(e^{((\alpha+o(1))[\ln(n)]^r [\ln \ln(n)]^{1-r})}\right) \quad (6)$$

Юқорида келтирилган (6) формуладаги n – бу туб сон $n \geq 2^N$, бунда берилган кластернинг умумий ҳисоблаш қуввати $G=93014,6$ ТФлон/сга тенг. RSA алгоритмининг барқарорлигини йил, ой, кун, 12 соат, 8 соат, 4 соат, 2 соат ва бир соат бўйича маълумотлари таҳлил қилинган. Натижада ишлаб чиқилган RSA криптографик алгоритм, ЧШНТларнинг маълумотлар ишончилигини оширишга хизмат қила олиши исботланган.

Диссертациянинг «Чекланган ностационар тизимлар бошқарувини оптималлаштириш модел ва алгоритмлари» деб номланувчи учинчи боби тўртта параграфдан иборат. Бунда ЧШНТлар учун Кальман экстраполятори ва нейрон тармоқ асосида башоратлаш моделлари орқали оптимал бошқарув моделларини ишлаб чиқишга бағишланган. Қўйилган масалани, z_t тасодикий кўзғалишлар ва q_t ўлчаш хатолигидаги Гаусс тақсимотиға эга бўлгани учун Калман экстраполяторидан фойдаланиб объект ва чиқиш вектори ҳолатини башоратлаш асосида оптимал бошқариш мумкин. $\hat{x}_{i|j}$ ва $\hat{y}_{i|j}$ – i вақт моментидан бошлаб $j \leq i$ маълумот берувчи j вақт моментидаги ҳолат ва чиқиш вектори баҳолари ҳисобланади. Яъни

$$\hat{x}_{t+1|t} = A_t \hat{x}_{t|t-1} + B_t u_t + K_t (\lambda_t - H_t \hat{x}_{t|t-1}), \hat{x}_{0|-1} = \bar{x}_0, \quad (7)$$

$$\hat{y}_{t+1|t} = L_t \hat{x}_{t+1|t}, \quad (8)$$

$$K_t = A_t B_t H_t^T (H_t P_t H_t^T + Q_t)^{-1}, \quad (9)$$

$$P_{t+1} = Z_t + A_t P_t A_t^T - A_t P_t H_t^T (H_t P_t H_t^T + Q_t)^{-1} H_t P_t A_t^T, P_0 = P_{x_0} \quad (10)$$

P_t учун (10) тенглама дискрет вақтли Риккати айирмали тенгламаси сифатида аниқланади, P_{x_0} – дисперсион матрицани бошланғич қиймати. Башоратланувчи бошқарув моделини амалда қўллаш учун (7)-(10) тенгламалардан $\hat{x}_{t+1|t}$ ни $t+1, t+2, \dots, t+N$ моментлар учун оптимал баҳолар олинади. Башоратловчи бошқарув моделини синтезлаш жараёнинида мақсад функцияси сифатида қуйидаги (11) кўринишидаги критерияни оламиз:

$$J(\hat{x}_{t+1|t}, U_t) = \frac{1}{2} \sum_{k=1}^N \|\hat{y}_{t+k|t} - \hat{y}_{t+k}\|_{F_t}^2 + \frac{1}{2} \sum_{k=1}^M \|\hat{u}_{t+k|t} - \hat{u}_{t+k-1|t}\|_{D_t}^2 \quad (11)$$

бу ерда \hat{y}_{t+k} – $t+k$ вақт моментидаги кузатиловчи сигнал қийматлари вектори F_t ва D_t – симметрик мусбат аниқланган матрицалар. Адаптив моделлаштириш усулларини қўллашга имкон берувчи динамик тасодикий вақтли қаторлар асосида башоратли бошқарув моделлари тадқиқ этилган.

$$x_{t+1} = Ax_t + bu_t, \quad x_0, x_t \in R^n \quad t = 0, 1, \dots, \quad u_t = \varphi \cdot x_t, \quad (12)$$

Бошқарувни оптималлаштиришда кўзатишлар параметрини ўзгаришлар тенденцияси қуйидаги кўринишида аниқланади.

$$\bar{\varphi}_t = \alpha_0 + \alpha_1 \cdot t + \frac{\alpha_2}{2!} \cdot t^2 + \frac{\alpha_3}{3!} \cdot t^3 + \dots + \frac{\alpha_p}{p!} \cdot t^p \quad (13)$$

Бу ерда a – силлиқлаш параметри учун башоратлаш даражаси коэффициентини. Силлиқлаш параметри коэффициентини a қийматини танлаш чекловга боғлиқ равишда кечикишларни характерловчи кўрсаткични ўзгариш тенденциясининг акс этишига таъсир кўрсатади. Силлиқлаш параметри аниқлиги ва баҳосини аниқлашнинг ишлаб чиқилган алгоритми қуйидаги қадамлардан иборат:

1. (13) тенгламадаги параметрларнинг аниқлаш тавсифи;

2. Экспоненциал ўртачаларнинг бошланғич қийматларини қуйидаги (14) формула орқали аниқлаш

$$S_1^0 = \alpha_0 - \frac{1-a}{a} \alpha_1 \quad (14)$$

3. Параболик модел учун экспоненциал ўртачалар

$$S_1^1 = \alpha_0 - \frac{1-a}{a} \alpha_1 + \frac{(1-a)(2-a)}{2a^2} \alpha_2$$

$$S_1^i = \alpha_0 - \frac{i(1-a)}{a} \alpha_1 + \frac{(1-a)(i+1-i \cdot a)}{2a^2} \alpha_2 \quad (15)$$

(15) формулалар бўйича танланади;

4. Башоратловчи функция параметрларини топиш

$$\bar{\alpha}_0 = 2S_1^1 - S_1^2, \quad \bar{\alpha}_1 = \frac{a}{1-a} (S_1^1 - S_1^2)$$

5. $t+l$ момент учун ўзгарувчининг башорат қийматини аниқлаш (16) қуринишида

$$\hat{\varphi}_{t+l} = \bar{\alpha}_0 + \bar{\alpha}_1 (t+l) \quad (16)$$

параболик модел учун (17) қуринишида

$$\hat{\varphi}_{t+l} = \bar{\alpha}_0 + \bar{\alpha}_1 \cdot t_1 + \frac{\bar{\alpha}_2}{2!} (t+l)^2 \quad (17)$$

бу ерда l - қисқа муддатли ўртача, узоқ муддатли ёки бошқа типда прогноз ($l = 1, 2, \dots$) учун давр кўрсаткичи;

6. $t = 2, \dots, n$ лар учун экспоненциал ўртачаларни

$$S_t^1 = a \cdot \varphi_t + (l-a) \cdot S_{t-l}^1$$

$$S_t^2 = a \cdot S_t^1 + (l-a) \cdot S_{t-l}^2$$

формулалар билан ҳисоблаш;

7. Башоратловчи функция экспоненциал ўртачалари ва параметрларини t нинг қолган бошқа қийматлари учун ҳисоблашлар 4-бандга ўтиш билан амалга оширилади ва $t \leq n$ бўлгунча цикл бажарилади;

8. $t=n$ даги модел учун $\hat{\varphi}_{t+l}$ қийматлар башоратлаш қиймати каби қайд қилинади.

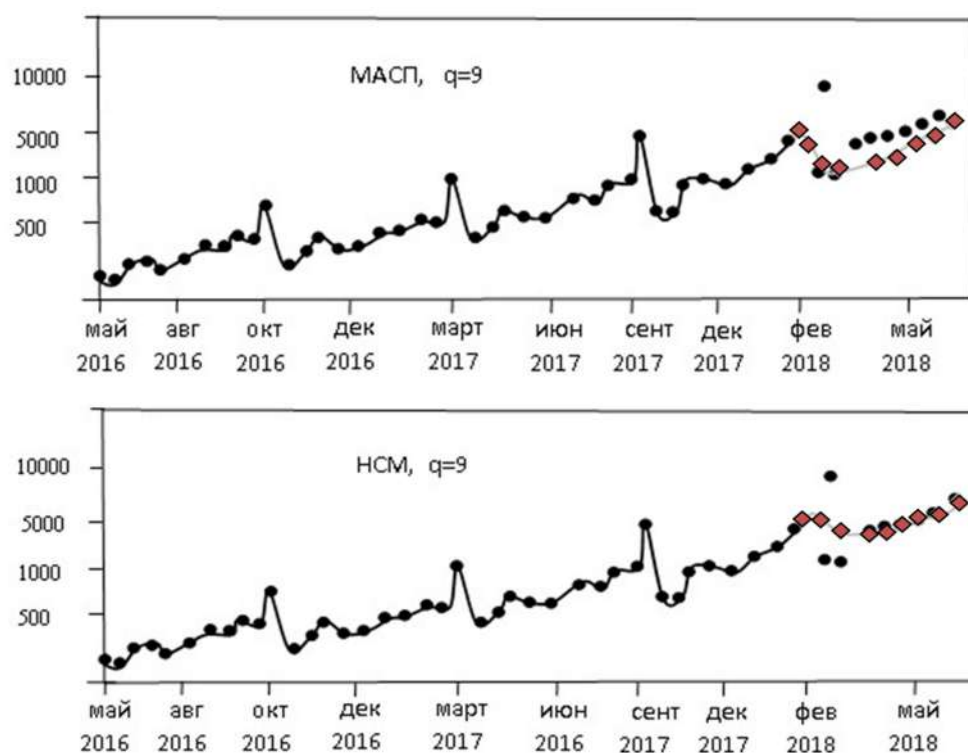
9. Тамом.

Ишлаб чиқилган адаптив модел асосида олинган маълумотларни нейрон тармоқ моделига қўлланилган ва натижалар олинган. Фойдаланаётган усулнинг афзаллик даражасини аниқлаш учун башоратланувчи қисмида башорат қийматининг ўртача четланиши қабул қилинган. Бу ҳолда σ бошланғич баъзи коэффициентларининг ўртача йўл қуйиладиган четланиш.

$$\gamma = \frac{1}{N-k} \sum_{i=k+1}^N \left| \frac{\sigma_i - \hat{\sigma}_i}{\sigma_i} \right|, \quad (18)$$

$\hat{\sigma}_i$ –тегишли усул билан топилган баҳо. Бу (18) формуладаги услубга кўра башоратнинг юқори аниқлиги $\gamma < 0,1$ қийматларда, яхши аниқлиги $0,1 < \gamma < 0,2$, қониқарли $0,2 < \gamma < 0,5$ ва қониқарсиз аниқлиқ $\gamma > 0,5$ да еришилади.

Мос равишда уч ой ($q=3$) ва тўққиз ой ($q=9$) муддатларда, шартнома тўлов мисолида иккита қиймат учун 2-расм кўринишида ҳисоблашлар амалга оширилган.

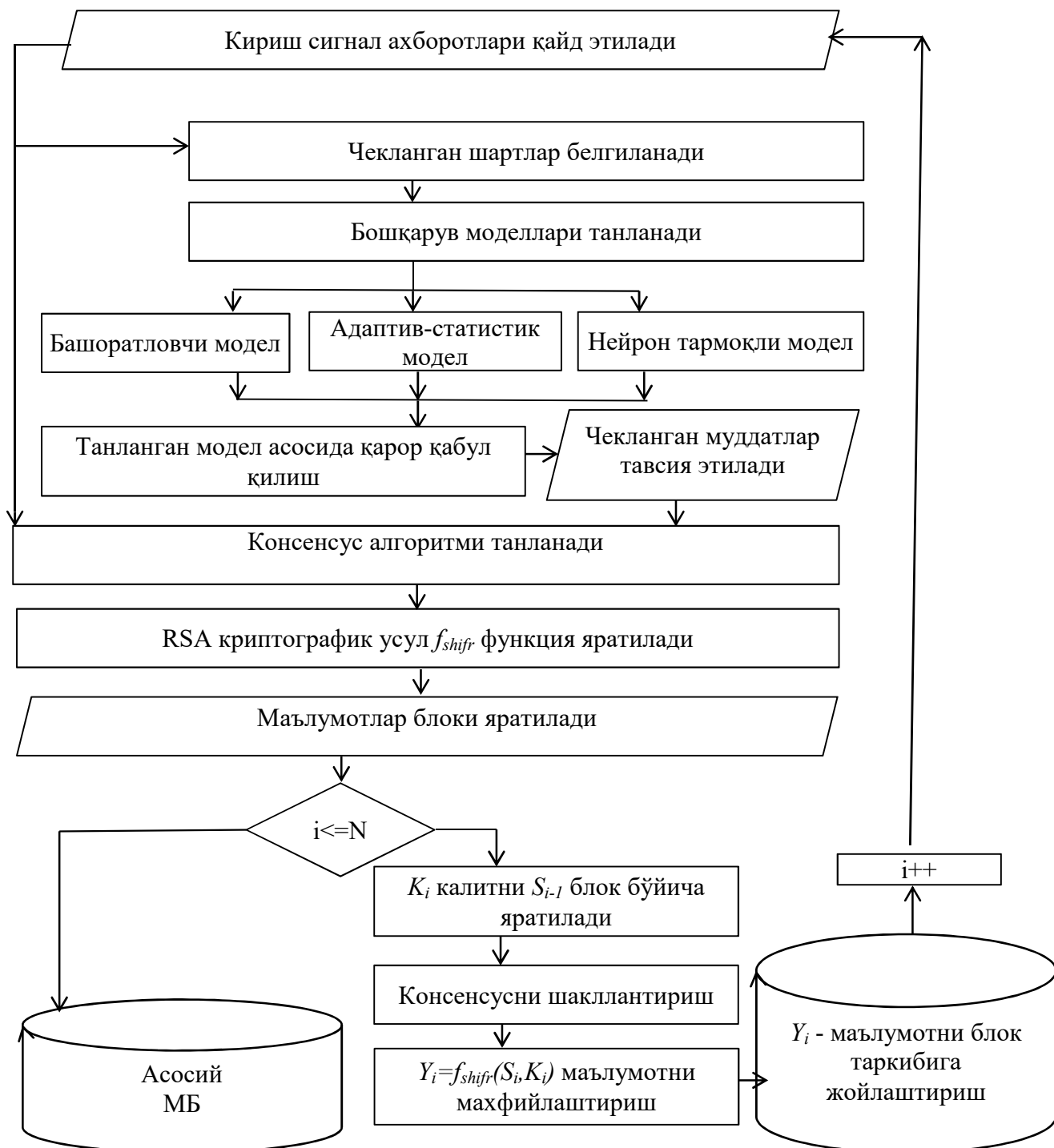


2-расм. Университет ҳисоб рақамига шартнома тўловларни тушиш суммасининг(млн.сумларда) графиги

МАСП–адаптив статистик башоратлаш усули, НСМ – нейрон тармоқли башоратлаш усули. Автоматлаштирилган бошқарув жараёнларида, адаптив-статистик модел ҳам фойдали ҳисобланади, лекин нейрон тармоқли модел самарадорлиги анчагина юқоридир.

Диссертациянинг «**Бошқариш ва маълумотлар ишончлилигини оширишнинг дастурий мажмуасини яратиш ва амалиётга қўлланилиши**» деб номланувчи тўртинчи боби учта параграфдан иборат, унда маълумотларни бошқаришни оптималлаштириш ва бу маълумотлар

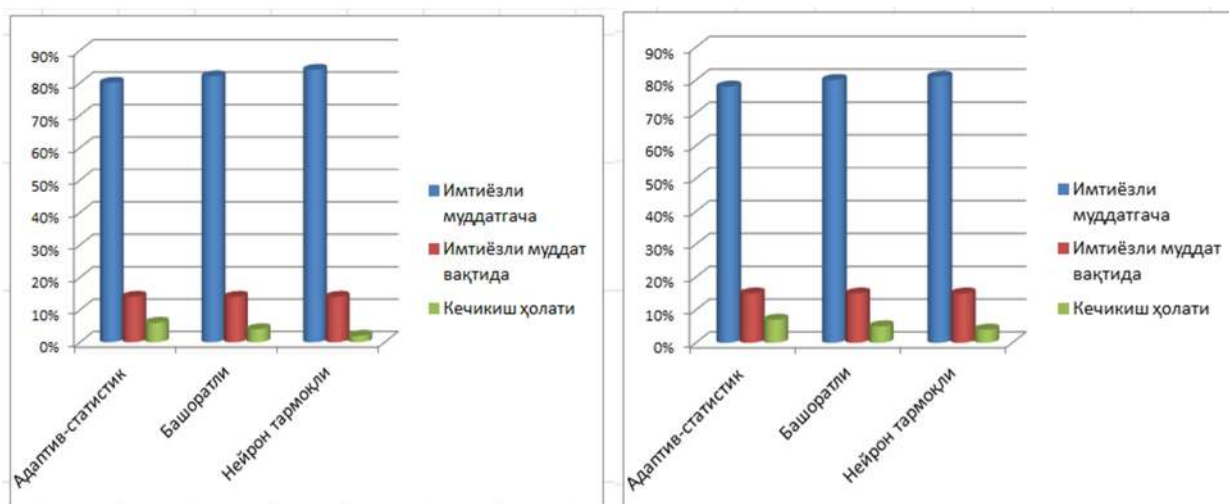
ишончилигини оширишнинг дастурий модуллари ҳамда дастурий мажмуанинг умумий структураси ишлаб чиқилган. Дастурий мажмуа 3-расмда кўрсатилган схема орқали белгиланган вазифаларни амалга оширади.



3-расм. Бошқарувни оптималлаштириш ва маълумотлар ишончилигини ошириш дастурий мажмуасининг умумий схемаси

Дастурий мажмуа таркибида ишлаб чиқилган башоратли, адаптив-статистик ва нейрон моделлари асосида, талабаларнинг тўлов тарихи маълумотлари бўйича чекланган муддатларни белгилаш учун тавсиялар берилган. Дастурий мажмуа, Самарқанд давлат университети ва ТАТУ

Самарқанд филиалининг шартнома тўловларини мониторинг қилиш ва электрон хужжат айланиш жараёнига тадбиқ этилган. Дастурий мажмуа ёрдамида тажриба натижалари олинди, тажрибада чекланган имтиёзли муддатлар давомида талабаларнинг тўлов миқдорларини келиб тушиши таҳлил этилди. Таҳлил натижалари асосида нейрон тармоқли модел оптималлиги аниқланган ва у 4-расм кўринишида келтирилган.



4-расм. СамДУ ва ТАТУ СФ маълумотлари бўйича бошқарув моделлари асосидаги тўлов миқдорларининг кўрсаткичларининг диаграммаси

Талабаларнинг одатий чекланган муддат ва бошқарув моделлари асосида берилган имтиёзли муддатларда шартнома тўлов миқдорларининг кечикиш кўрсаткичлари 1-жадвал кўринишида бўлади.

1-жадвал.

Чекланган муддат ва бошқарув моделлари асосида берилган имтиёзли муддатларда шартнома тўлов миқдорларининг кечикиш кўрсаткичлари

Вақт / Модел	Адаптив – статистик (СамДУ)	Адаптив – статистик (ТАТУ СФ)	Башоратли (СамДУ)	Башоратли (ТАТУ СФ)	Нейро-тармоқли (СамДУ)	Нейро-тармоқли (ТАТУ СФ)
Чекланган муддатда кечикиш	7%	9%	6%	5%	4%	6%
Имтиёзли муддатда кечикиш	6%	7%	4%	5%	2%	4%

Хулоса қилиб айтганда ишда таклиф этилган бошқарув моделларини қўллаганда, дастлабки белгиланган муддатга нисбатан дастурий тизим тавсия этган муддатлардаги тўловлар 7-8% га ошиши кузатилган. Ишлаб чиқилган

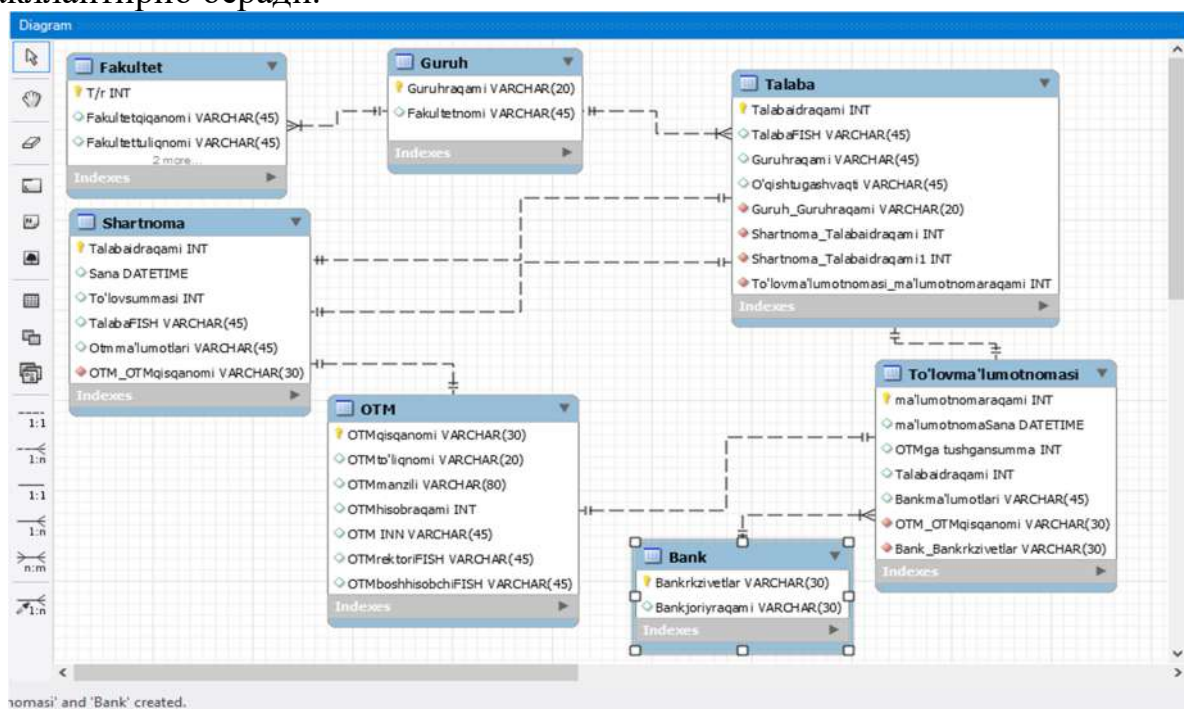
бошқарув моделларини тўлов тизимлари билан боғлиқ бошқа жараёнларга ҳам қўллаш мумкин.

Ишлаб чиқилган тақсимланган реестр механизмлари асосида маълумотлар ишончилигини ошириш усул ва алгоритмлари, Самарқанд вилоят иқтисодий суди ва Қишлоқ қурилиш банк Самарқанд филиалининг электрон ҳужжат айланиш тизимларида қўлланилди.

Ишлаб чиқилган тақсимланган реестр механизмлари асосида маълумотлар ишончилигини ошириш усул ва алгоритмлари, Самарқанд вилоят иқтисодий суди ва Қишлоқ қурилиш банк Самарқанд филиалининг электрон ҳужжат айланиш тизимларида қўлланилиш натижасида маълумотлар ишончилиги самарадорлигини 1,5-2 баробар ошириш имконини берди.

Олий таълим шартнома тўловларини мониторинг қилиш тизим маълумотлар базаси архитектураси, инфологик ва даталогик модели ҳамда дастурий мажмуанинг модуллари ишлаб чиқилган.

Шартнома тўлов маълумотлар базасининг инфологик ва даталогик модели MySQL Workbench интеллектуал дастури асосида ишлаб чиқилган. MySQL Workbench дастури маълумотларни инфологик моделдаги тузилиш бўйича боғланишлар муносабатлар схемасини қуйидаги 5-расм кўринишида шакллантириб беради.



5-расм. Маълумотлар базасининг боғланишлар ва муносабатлар схемаси

Маълумотлар базаси архитектураси, инфологик ва даталогик модели асосида олий таълим шартнома тўлов тизимининг дастурий мажмуаси яратилган. Дастурий мажмуа орқали тўлов жараёнларини мониторинг қилиш имкони яратилди.

ХУЛОСА

«Ностационар тизимларни ташкилий бошқаришда тақсимланган реестр механизмлари асосида маълумотлар ишончилигини ошириш усул ва алгоритмлари» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Чекланган шартлардаги ностационар тизимларнинг бошқариш ва бошқариладиган тизим маълумотлар ишончилигини тақсимланган реестр механизмлари асосида ошириш механизмларининг ўрганилганлик даражаси тизимли таҳлил қилинди.

2. Бошқарув жараёнларининг математик моделлари асосида чекланган шартлари аниқланди ва ЧШНТларни бошқаришни оптималлаштириш учун бошқаришнинг математик моделлари ишлаб чиқилди, бошқариладиган тизим маълумотлар ишончилигини ошириш мақсадида тақсимланган реестр яъни блокчейн технологиясининг механизмлари таклиф этилди.

3. Тақсимланган реестр механизмнинг асосий тамоиллари, ривожланиш истиқболлари, хавфсизлик даражаси ўрганиб чиқилди ва маълумотлар ишончилигини ошириш параметрлари аниқланди. Тақсимланган реестр яъни блокчейн механизмлари асосида ностационар тизимлар маълумотлар базаси архитектурасини ишлаб чиқишнинг умумий алгоритми яратилди.

4. Бошқариладиган ахборот тизимларининг маълумотлар ишончилигини ошириш учун маълумотлар базаси архитектурасини блокчейн модели асосида ишлаб чиқилди. Блокчейн механизмларидан фойдаланиш учун консенсус алгоритмлари таҳлил қилиниб ЧШНТлар учун Pos алгоритмидан фойдаланиш усули таклиф этилди.

5. Маълумотлар ишончилигини, тақсимланган реестр механизмлари асосида шифрлаш усулининг динамик калитлари орқали ошириш алгоритмлари ишлаб чиқилди.

6. Чекловлар мавжуд ностационар тизимлар маълумотларини башоратлаш асосида бошқарув модели, ўзгармас параметрли система орқали башоратловчи бошқарув моделлари ишлаб чиқилди. Ишлаб чиқилган моделлар маълумотларни қабул қилиш, сақлаш ва фойдаланувчига етказиш тизимига қўлланилди. Амалий масалаларга қўлланиш асосида ишлаб чиқилган модел ва алгоритмларнинг натижадорлиги аниқланди.

7. Ностационар тизимларнинг вақтли қаторли адаптив-статистик башоратли модели ишлаб чиқилди. Вақтли қаторли башоратли моделни нейрон тармоғи билан интеграцияланган модели таклиф этилди ва тажриба натижалари олинди. Тажриба натижаларида тез, ишончли ва олдиндан башоратлаш асосида автоматлаштирилган бошқарув тизимларида нейрон тармоқли моделнинг қўллаш самарали эканлиги аниқланди.

8. Бошқарув жараёнларини оптималлаштириш ва маълумотлар ишончилигини оширишнинг дастурий мажмуасини умумий схемаси ва модуллари ишлаб чиқилди. Ишлаб чиқилган бошқарувни оптималлаштиришнинг моделлари тажриба синовдан ўтказилди, тажриба

натижалари асосида 7-8% иқтисодий самарадорлик аниқланди. Маълумотлар ишончлилигини ошириш мақсадида ишлаб чиқилган тақсимланган реестр механизмлари тажриба синовдан ўтказилди, тажриба натижаларида тақсимланган реестр механизмлари ва шифрлаш усуллари асосида 1,5-2 баробар самарадорлик аниқланди.

9. Шартнома тўловларини мониторинги тизимининг маълумотлар базасини реляцион инфологик, даталогик моделлари ишлаб чиқилди. MySQL Workbench интеллектуал дастури асосида шартнома тўловларни мониторинги тизимининг маълумотлар базаси архитектураси ишлаб чиқилди. Ишлаб чиқилган модел ва алгоритмлар дастурий мажмуада жорий этилди ва синовдан ўтказилди.

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

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

НАЗАРОВ ФАЙЗУЛЛО МАХМАДИЯРОВИЧ

**МЕТОДЫ И АЛГОРИТМЫ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ
ИНФОРМАЦИИ НА ОСНОВЕ МЕХАНИЗМОВ
РАСПРЕДЕЛЕННОГО РЕЕСТРА ПРИ ОРГАНИЗАЦИОННОМ
УПРАВЛЕНИИ НЕСТАЦИОНАРНЫМИ СИСТЕМАМИ**

05.01.02 – Системный анализ, управление и обработка информации

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

Ташкент– 2021

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за №B2020.2.PhD/T1560.

Диссертация выполнена в Самаркандском государственном 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: Ахатов Акмал Рустамович
доктор технических наук, профессор

Официальные оппоненты: Бабомурадов Озод Жураевич
доктор технических наук

Тухтаназаров Дилмурод Солижонович
доктор философии технических наук


Ведущая организация: Ташкентский государственный транспортный университет


Защита диссертации состоится «03» сентября 2021 г. в 16.00 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 № 202). (Адрес: 100202, г.Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «2» мая 2021 года.
(протокол рассылки № 11 от «04» мая 2021 г.).




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


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


А.В.Кабулов
Председатель ~~научного семинара~~ при научном совете по
присуждению ученых степеней, доктор технических наук,
профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации.

Мировой опыт показывает, что для оптимизации автоматизированного управления социально-экономическими системами на основе цифровых технологий необходимо повышение достоверности информации в управляемой системе. В настоящее время, в связи с переменной природой потоков данных, управление информационными системами в компьютерных сетях на основе моделей управления и использования распределенных механизмов блокчейна на основе реестра для повышения достоверности информации является одним из наиболее эффективных способов. В связи с этим, ученые США, Великобритании, Германии, Франции, Италии, Испании, Японии, Южной Кореи, Российская Федерация, Китая, Индии и других стран проводят ряд исследований по использованию механизмов блокчейна на основе распределенного реестра для обеспечения достоверности хранимых данных. Использование блокчейн в этих исследованиях в основном ориентировано на организацию криптовалютных систем и оптимизацию бизнес-процессов с денежными потоками. В то же время, можно констатировать, что на сегодняшний день задачи использования механизмов распределенного реестра для повышения достоверности информации в системах управления, таких как электронный документооборот, логистические системы, электронные коммунальные платежи в компьютерных сетях, не нашли своего окончательного решения.

В системах, подобных электронному документообороту, электронным коммунальным платежам, логистическим системам, функционирующим в компьютерных сетях, устанавливаются жесткие сроки ограничения исполнения, однако при обработке данных зачастую выявляются запаздывания по срокам и задача преодоления таких запаздываний является одной из важнейших проблем. Тот факт, что эти системы нестационарны по своей природе, создает дополнительные проблемы для обеспечения достоверности данных, описывающих состояния запаздываний. Поэтому в последние годы растет интерес к методам повышения достоверности информации в нестационарных систем в условиях ограничений, основанных на практике применения методов теории управления для оптимизации управления. Поэтому, в последние годы, исходя из практики применения методов теории управления, растет интерес к способам обеспечения и повышения достоверности информации нестационарных систем в условиях ограничений. Использование технологии блокчейн на основе распределенного реестра в системах управления определяет новый подход к повышению достоверности информации. Таким образом, повышение достоверности информации на основе разработки и применения модели архитектуры и алгоритмов формирования базы данных с использованием механизмов распределенного реестра представляет собой актуальную тему исследований.

Наряду с развитием информационно-коммуникационных технологий в нашей республике принимаются широкомасштабные меры по повышению качества управления информационными системами и достоверности информации в них. В Стратегии действий по дальнейшему развитию Республики Узбекистан особое внимание уделяется решению проблем по созданию эффективных механизмов развития научно-исследовательской и инновационной деятельности, внедрению научных и инновационных достижений.

Данное диссертационное исследование в определенной степени послужит выполнению задач, установленных в Указами Президента Республики Узбекистан от 7 февраля 2017 года №УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан» и от 19 февраля 2018 года №УП-5349 «О мерах по дальнейшему совершенствованию информационных технологий и связи», постановлении №ПП-4024 от 21 ноября 2018 года «О мерах по контролю за внедрением информационных технологий и коммуникаций, совершенствованию системы их защиты».

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Это исследование реализуется в рамках приоритетного направления IV.«Развитие информатизации и информационно-коммуникационных технологий».

Степень изученности проблемы. Теория и практика динамического управления многомерными процессами исследованы такими зарубежными всемирно известными учеными, как С.Р.Сутлер, В.Л.Рамакер, моделирование управлением на основе прогнозирования исследовано Ж.Ричалетом, А.Раултом, Ж.Тестудом, Ж.Папоном, Д.В.Кларке, Р.Скаттолини, Л.Чиски, Э.Моска, математическое моделирование терминального управления нестационарными процессами исследовано А.Пропое, А.Э.Красовским, И.Е.Зубером. Исследования по применению механизмов блокчейн на основе распределенного реестра к системам управления исследовано зарубежными учеными, такими как М.М.Пряников, А.В.Чугунов, А.И.Власов, А.А.Карпунин, А.С.Теряева, А.С.Баева. Использование криптографических алгоритмов в механизмах блокчейн исследовано Сатоши Накамото, Р.Маянк, Г.Данило, К.Катина, Л.Ван, Х.Шен, Дж.Ли, Дж.Шао, Ю.Ян, П.Ю.Пириу, Жан Франсуа.

Среди ученых Узбекистана М.М.Камилов, Т.Ф.Бекмуратов, М.М.Каримов, Р.Х.Хамдамов, Ш.Х.Фозилов, М.А.Исмаилов, Д.Т.Мухаммадиева, М.А.Рахматуллаев, О.Ж.Бабомуродов, Н.С.Маматов внесли значительный вклад в исследованиях, посвященных оптимальному управлению.

Системный анализ исследований перечисленных выше ученых позволил выявить, что исследования по оптимизации процессов управления в условиях ограничений и задачи повышения достоверности информации на основе механизмов распределенного реестра в информационных системах управления недостаточно изучены.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного и научно-исследовательского учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках проектов А5-039-«Разработка программных средств построения параллельных алгоритмов интеллектуального анализа данных» (2015-2017) и БА-А5-033-«Обработка данных в медицинских учреждениях по созданию автоматизированной системы выдачи и мониторинга деятельности» (2017-2018) Самаркандского государственного университета и Самаркандского филиала Ташкентского университета информационных технологий.

Цель исследования. Состоит в разработке методов, алгоритма и программного средства прогнозной модели управления и повышения достоверности информации нестационарной системы в условиях ограничений.

Задачи исследования:

системный анализ моделей управления нестационарными системами и способов повышения достоверности информации управляемой системы;

разработка метода и алгоритма на основе блокчейна для повышения достоверности информации нестационарной системы в условиях ограничений;

разработка алгоритмов повышения эффективности управления за счет применения динамического метода шифрования к механизмам распределенного реестра;

совершенствование математических моделей управления нестационарными системами в условиях ограничений;

проектирование разработка и внедрение программного комплекса оптимизации управления нестационарной системы в условиях ограничений.

Объектом исследования являются процессы обработки данных при оплате контрактов на высшее образование и система электронного документооборота.

Предмет исследования методы и алгоритмы повышения достоверности информации на основе организационного управления нестационарными системами и механизмами распределенного реестра.

Методы исследования. В исследовании использовались системный анализ, теория управления, математическое моделирование, теория нейронных сетей, распределенный реестр, механизмы блокчейна, методы защиты информации, алгоритмы и методы проектирования баз данных и знаний.

Научная новизна исследования:

разработана прогнозная модель организационного управления, основанная на ограничительных условиях нестационарных систем;

разработана модель оптимизации организационного управления нестационарными системами в условиях ограничений на основе нейронной сети;

разработан метод повышения достоверности информации нестационарных систем на основе алгоритма консенсуса механизмов распределенного реестра;

разработан улучшенный алгоритм динамического метода шифрования на основе блокчейна для оптимизации управления нестационарными системами.

Практические результаты исследования:

разработано алгоритмическое обеспечение управления нестационарными системами в условиях ограничений и повышения достоверности информации нестационарных систем на основе механизмов распределенного реестра;

разработана алгоритмическая поддержка процесса применения методов динамического шифрования ключей на основе механизмов распределенного реестра;

разработанные программные модули управления нестационарными системами в условиях ограничений и повышения достоверности информации реализованы в системах оплаты контрактов и электронного документооборота высшего учебного заведения.

Достоверность результатов исследования. Математическая точность задачи, методы учета ограничительных условий нестационарных систем, управление нейронными сетями на основе прогнозных моделей, методы применения механизмов блокчейна к сетевым системам, интеграция с шифрованием RSA, криптостойкость разработанного динамического метода шифрования с ключом подтверждена положительными результатами.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования заключается в том, что разработанные модели, методы и алгоритмы управления служат основой для оптимизации управления и обеспечения достоверности информации на основе прогнозирования параметров организационно управляемых экономических процессов.

Практическая значимость результатов исследования заключается в том, что разработанные методы и алгоритмы дают рекомендации по определению условий оплаты на основе существующих данных платежных систем, повышают достоверность информации на основе секретности данных нестационарных систем в сетевых системах, повышают безопасность и эффективность систем электронного документооборота.

Внедрение результатов исследования. В рамках диссертационного исследования на основе полученных научных результатов по разработке методов и алгоритмов повышения достоверности информации с помощью механизмов распределенного реестра в организационном управлении нестационарными системами:

алгоритмы и механизмы, созданные на основе идентификации входных данных управляемой нестационарной системы, выбора алгоритмов консенсуса, разработки архитектуры базы данных на основе распределенных реестров внедрены в Самаркандском областном экономическом суде

(Справка Верховного Суда Республики Узбекистан №08/УМ-727-20 от 17 декабря 2020 г.). В результате при организации работы системы электронного документооборота на основе механизмов распределенного реестра достигнуто повышение эффективности использования объема памяти и достоверности информации в 1,5-2 раза;

алгоритмы и механизмы, созданные на основе интеграции методов шифрования с механизмами распределенного реестра внедрены в Кишлок курилиш банка (Справка Министерства информационных технологий и коммуникаций Республики Узбекистан от 2 декабря 2020 года №33-8/7344). Результаты позволили достигнуть повышения достоверности информации в базе данных системы электронного документооборота в 1,5-2 раза;

алгоритмы и механизмы на основе прогнозных, адаптивно-статистических и нейронных моделей управления а также механизмы распределенного реестра, разработанные с учетом ограниченных условий организационного управления нестационарными системами внедрены в Самаркандского государственного университета и Самаркандского филиала ТУИТ (Справка Министерства информационных технологий и коммуникаций Республики Узбекистан от 2 декабря 2020 года №33-8/7344). В результате достигнуто увеличение объемов выплаты контрактов на 7-8% за счет новых сроков, рекомендованных на основе моделей управления в условиях ограничений.

Апробация результатов исследования. Результаты этого исследования обсуждались в том числе на 5 международных и 5 республиканских научных конференциях.

Опубликованность результатов исследования. По теме диссертации опубликовано 22 научные работы, из которых 8 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов диссертаций, в том числе 4 в зарубежных и 4 в республиканских журналах, также получены 4 свидетельства о регистрации программных продуктов для ЭВМ Агентства интеллектуальной собственности РУз.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 110 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

В введении обоснована актуальность и важность темы диссертации, соответствие приоритетам развития науки и технологий республики. Определены цели и задачи исследования, определены объект и предмет исследования, обоснована достоверность полученных результатов, указана их теоретическая и практическая значимость, состояние внедрения результатов исследования, опубликованные работы и структура диссертации.

Первая глава диссертации, озаглавленная «**Задачи управления нестационарными системами и достоверность информации**», состоит из

трех параграфов, в которых обсуждается текущее состояние управления нестационарными системами, анализ решений в условиях ограничений, преимущества и недостатки механизмы распределенного реестра для повышения достоверности информации. В качестве ограничений в системе принимаются устанавливаемые в автоматизированных системах жесткие сроки исполнения. Для задач, поставленных в исследовании также принимается, что существуют состояния запаздывания по этим срокам. Примерами этому служат системы электронного документооборота, оплаты контрактов на обучение, мониторинга коммунальных услуг, материально-технического обеспечения и другие. В связи с этим, нестационарными системами в условиях ограничений (НСУО) назовем такие системы, в которых наблюдается процесс невыполнения задач и запаздываний в указанное время. На основе изучения методов и алгоритмов повышения достоверности информации по управлению нестационарными системами выявляются проблемы развития данного направления исследований и пути их решения, а также формируется задача исследовательской работы. Объекты нестационарных систем, поле наблюдения и модель управляемого выхода представлены соответственно следующими (1)-(3) соотношениями:

$$\begin{cases} x_{t+1} = A_t x_t + B_t u_t + z_t \\ x_{t|t=0} = x_0 \end{cases} \quad (1)$$

$$\lambda_t = H_t x_t + q_t \quad (2)$$

$$y_t = L_t x_t \quad (3)$$

Здесь $x_t \in R^n$ - состояние нестационарного объекта, $u_t \in R^m$ - управляющий эффект (известные входы), $\lambda_t \in R^l$ - наблюдения, выходные данные системы управления, $y_t \in R^n$ - управляемые выходы, A_t, B_t, H_t, L_t - соответствующие параметры рассматриваются как матрицы размерностей. Система управления рассматриваемым объектом задается уравнением (2). Предположим, что z_t случайные движения и q_t размерные ошибки не взаимокоррелируют и со средним значением 0 и подчиняются Гауссовскому распределению и ковариациями Z, Q .

Ограничения выражаются в виде следующих неравенства.

$$\alpha_1(t) \leq D_1 x_t \leq \alpha_2(t) \quad (4)$$

$$\varphi_1(x_t, t) \leq D_2 u_t \leq \varphi_2(x_t, t) \quad (5)$$

Здесь D_1 и D_2 полноцветные структурные матрицы x_t и u_t состоящие из нулей и единиц, определяющие компоненты векторов; $\alpha_1(t), \alpha_2(t), \varphi_1(x_t, t), \varphi_2(x_t, t)$ – вектор-функции заданных векторных измерений.

Задача состоит в разработке стратегии управления на основе наблюдений, в которой выходной вектор систем y_i должен быть близок к заданному вектору \bar{y}_0 с учетом ограничений (4)-(5). Определение оптимальных решений вышеперечисленных проблем осуществляется на основе достоверных данных. С этой целью в работе приведены результаты сравнительного анализа принципов, методов и алгоритмов повышения достоверности информации на основе механизмов распределенного реестра.

Вторая глава диссертации «**Алгоритмы повышения достоверности информации ограниченных нестационарных систем**» состоит из четырех параграфов. Разработаны методы и алгоритмы повышения достоверности информации на основе механизмов распределенного реестра при управлении нестационарными системами.

Для оптимизации управления предложены архитектура базы данных, алгоритмы консенсуса и алгоритмы модификации методов шифрования на основе механизмов распределенного реестра. Технологии блокчейн включены в отдельный класс архитектуры, называемый технологией распределенного реестра (англ: Distributed ledger technology - ДЛТ). Разработка структуры базы данных в виде цепочки зашифрованных данных. Для шифрования закрытых транзакций набор из двух криптографических ключей, предназначенных для фиксации открытых транзакций, выполняется пользователями при доступе к сети и установке необходимого программного обеспечения на рабочую станцию. Проверка каждой завершенной транзакции выполняется с использованием модели, показанной на рис. 1.

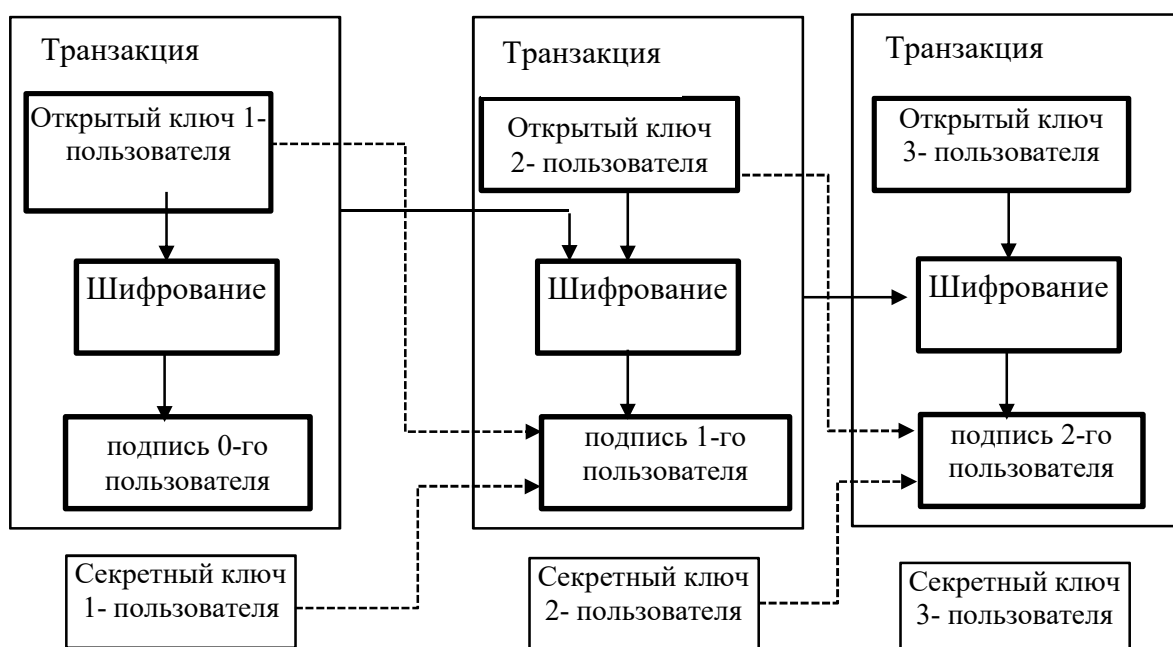


Рис. 1. Схема подтверждения правильного выполнения транзакции

Когда пользователь в каждой сетевой структуре отправляет транзакцию следующему пользователю, он подписывает хэш предыдущей и открытый ключ следующей транзакции и добавляет эту информацию в конец транзакции. Согласно этой схеме каждый последующий блок данных будет

основан на хэше предыдущего блока. Теоретически можно добавить блок во внутреннее содержимое сети, но для добавления блока требуется открытие хэша всех предыдущих блоков до первого сгенерированного блока. Тем самым обеспечивается невозможность добавления практически не подключенного заранее блока, т.е. утверждается концептуальный принцип построения сети на основе распределенного реестра. Алгоритмы консенсуса используются для проверки данных, содержащихся в технологии распределенного реестра. Принцип работы алгоритма Proof of Stake (Pos) широко распространен в системах на основе блокчейна и состоит из методов и решений, основанных на алгоритме подтверждения доли выполненных работ. Исследование алгоритмов консенсуса позволило сделать вывод, что алгоритм POS является наиболее эффективным методом для НСОУ. При применении алгоритма POS в системе управления каждая информация принимается как доля и шифруется с использованием аутентифицированного криптографического ключа. Каждый блок базы данных, созданный на основе механизмов распределенного реестра, считается зашифрованным по параметру информации, содержащейся в предыдущем блоке. Согласно указанному выше механизму база данных информационных систем в сети формируется на основе блокчейна по следующему алгоритму:

1-шаг. Алгоритмы консенсуса выбираются в зависимости от формы и типа данных;

2-шаг. Криптографическая функция формируется на основе криптографического метода;

3-шаг. Формируется блок исходных данных;

4-шаг. Каждый n -блочный ключ формируется согласно параметру информации, содержащейся в $(n-1)$ -блоке;

5-шаг. Информация, хранящаяся в каждом блоке, зашифрована криптографическим методом на основе сгенерированного ключа;

6-шаг. Зашифрованная информация помещается в блок.

Вышеупомянутый алгоритм организует хранение данных в виде цепочки криптографическим методом с динамическим ключом. Алгоритм RSA был предложен для улучшения криптографического метода RSA на основе механизмов распределенного реестра для обеспечения защиты математической и криптографической информации в системе.

Это удваивает криптоустойчивость, а попытка взломать или найти закрытый ключ приводит к числу комбинаций $2 \cdot 2^N = 2^{N+1}$. На основе разработанных алгоритмов улучшенный криптографический метод RSA определил уровень криптостойкости. Оценка для криптографического метода RSA задается следующей формулой (6).

$$L_{RSA}(n, r, \alpha) = O\left(e^{((\alpha+o(1))[\ln(n)]^r [\ln \ln(n)]^{1-r})}\right) \quad (6)$$

В приведенной выше формуле (6), n – простое число $n \geq 2^N$, определяемое общей вычислительной мощностью кластеров G=93014,6

ТФлоп/с. Устойчивость RSA алгоритмов проанализирована за год, месяц, день, 12 часов, 8 часов, 4 часа, 2 часа и 1 час. Полученный криптографический алгоритм RSA может служить для повышения достоверности информации.

Третья глава диссертации «**Модели и алгоритмы оптимизации управления ограниченными нестационарными системами**» состоит из четырех параграфов, посвященных разработке моделей оптимального управления для НСОУ с помощью экстраполятора Кальмана и модели прогнозирования на основе нейронных сетей. Поскольку поставленная задача имеет Гауссовское распределение z_t случайных движений и q_t погрешность измерения, оптимальное управление может быть получено на основе предсказания состояния объекта и выходного вектора с использованием экстраполятора Калмана. $\hat{x}_{i|j}$ и $\hat{y}_{i|j}$ - оценки вектора состояния и выхода в момент времени j , который дает информацию с момента времени i ($j \leq i$). То есть

$$\hat{x}_{t+1|t} = A_t \hat{x}_{t|t-1} + B_t u_t + K_t (\lambda_t - H_t \hat{x}_{t|t-1}), \hat{x}_{0|-1} = \bar{x}_0, \quad (7)$$

$$\hat{y}_{t+1|t} = L_t \hat{x}_{t+1|t}, \quad (8)$$

$$K_t = A_t B_t H_t^T (H_t P_t H_t^T + Q_t)^{-1}, \quad (9)$$

$$P_{t+1} = Z_t + A_t P_t A_t^T - A_t P_t H_t^T (H_t P_t H_t^T + Q_t)^{-1} H_t P_t A_t^T, P_0 = P_{x_0} \quad (10)$$

Уравнение (10) определяется для P_t как дифференциальное уравнение Риккати с дискретным временем, P_{x_0} - начальное значение дисперсионной матрицы. Чтобы применить прогнозируемую модель управления на практике, $\hat{x}_{t+1|t}$ из уравнений (7)-(10) используются для получения оптимальных значений для моментов $t+1, t+2, \dots, t+N$. В процессе синтеза модели прогнозного управления мы получаем следующие критерии в виде (11) как целевую функцию:

$$J(\hat{x}_{t+1|t}, U_t) = \frac{1}{2} \sum_{k=1}^N \left\| \hat{y}_{t+k|t} - \hat{y}_{t+k} \right\|_{F_t}^2 + \frac{1}{2} \sum_{k=1}^M \left\| \hat{u}_{t+k|t} - \hat{u}_{t+k-1|t} \right\|_{D_t}^2 \quad (11)$$

где \hat{y}_{t+k} - $t+k$ -векторы наблюдаемых значений сигнала в момент времени, а F_t и D_t - симметричные положительно определенные матрицы.

Изучены модели прогнозного управления на основе динамических случайных временных рядов, позволяющие применять методы адаптивного моделирования.

$$x_{t+1} = A x_t + b u_t, \quad x_0, \quad x_t \in R^n \quad t = 0, 1, \dots, \quad u_t = \varphi \cdot x_t, \quad (12)$$

Тенденция изменения параметра наблюдения при оптимизации управления определяется следующим образом.

$$\bar{\varphi}_t = \alpha_0 + \alpha_1 \cdot t + \frac{\alpha_2}{2!} \cdot t^2 + \frac{\alpha_3}{3!} \cdot t^3 + \dots + \frac{\alpha_p}{p!} \cdot t^p, \quad (13)$$

где a – коэффициент прогнозируемого уровня для параметра измельчения. Выбор значения коэффициента параметра шлифования a влияет на отражение тенденции изменения показателя, характеризующего запаздываний в зависимости от ограничения. Разработанный алгоритм определения точности и значения параметра шлифования состоит из следующих шагов:

1. Описание в определении параметров в уравнении (13);

2. Начальные значения экспоненциальных средних определяются по формуле (14)

$$S_1^0 = \alpha_0 - \frac{1-a}{a} \alpha_1 \quad (14)$$

3. Для параболической модели экспоненциальные средние (15) выбираются по формулам;

$$S_1^1 = \alpha_0 - \frac{1-a}{a} \alpha_1 + \frac{(1-a)(2-a)}{2a^2} \alpha_2$$

$$S_1^i = \alpha_0 - \frac{i(1-a)}{a} \alpha_1 + \frac{(1-a)(i+1-i \cdot a)}{2a^2} \alpha_2 \quad (15)$$

4. Определение параметров функции прогнозирования.

$$\bar{\alpha}_0 = 2S_1^1 - S_1^2, \bar{\alpha}_1 = \frac{a}{1-a} (S_1^1 - S_1^2)$$

5. Определите прогнозируемое значение переменной для момента $t + l$ в виде (16).

$$\hat{\varphi}_{t+l} = \bar{\alpha}_0 + \bar{\alpha}_1 (t+l) \quad (16)$$

в виде (17) для параболической модели

$$\hat{\varphi}_{t+l} = \bar{\alpha}_0 + \bar{\alpha}_1 \cdot t_1 + \frac{\bar{\alpha}_2}{2!} (t+l)^2 \quad (17)$$

где l – среднесрочная средняя, долгосрочная перспектива или другие типы ($l=1,2, \dots$) для индекса периода;

6. Расчет по формулам экспоненциальных средних для $t=2, \dots, n$

$$S_t^1 = a \cdot \varphi_t + (l-a) \cdot S_{t-l}^1$$

$$S_t^2 = a \cdot S_t^1 + (l-a) \cdot S_{t-l}^2$$

7. Расчет экспоненциальных средних и параметров функции прогнозирования, расчет для остальных других значений t выполняется переходом к пункту 4 и цикл выполняется до тех пор, пока $t \leq n$;

8. Значения для модели при $t=n$ записываются как прогнозируемые значения.

9. Конец.

Данные, полученные на основе разработанной адаптивной модели, были применены к модели нейронной сети и были получены результаты. Для определения степени преимущества используемого метода было принято среднее отклонение прогнозируемого значения в прогнозируемой части. В

данном случае σ – это среднее допустимое отклонение некоторых начальных коэффициентов.

$$\gamma = \frac{1}{N-k} \sum_{i=k+1}^N \left| \frac{\sigma_i - \hat{\sigma}_i}{\sigma_i} \right|, \quad (18)$$

где $\hat{\sigma}_i$ – оценка, найденная соответствующим методом.

Согласно методу этой формулы (18) высокая точность прогноза достигается при значениях $\gamma < 0,1$, хорошая точность – при $0,1 < \gamma < 0,2$, удовлетворительная – при $0,2 < \gamma < 0,5$ и неудовлетворительная точность – при $\gamma > 0,5$. На рис. 2 показаны результаты расчетов на примере оплаты контрактов, выполненных для периодов в три ($q=3$) и девять ($q=9$) месяцев для двух значений.

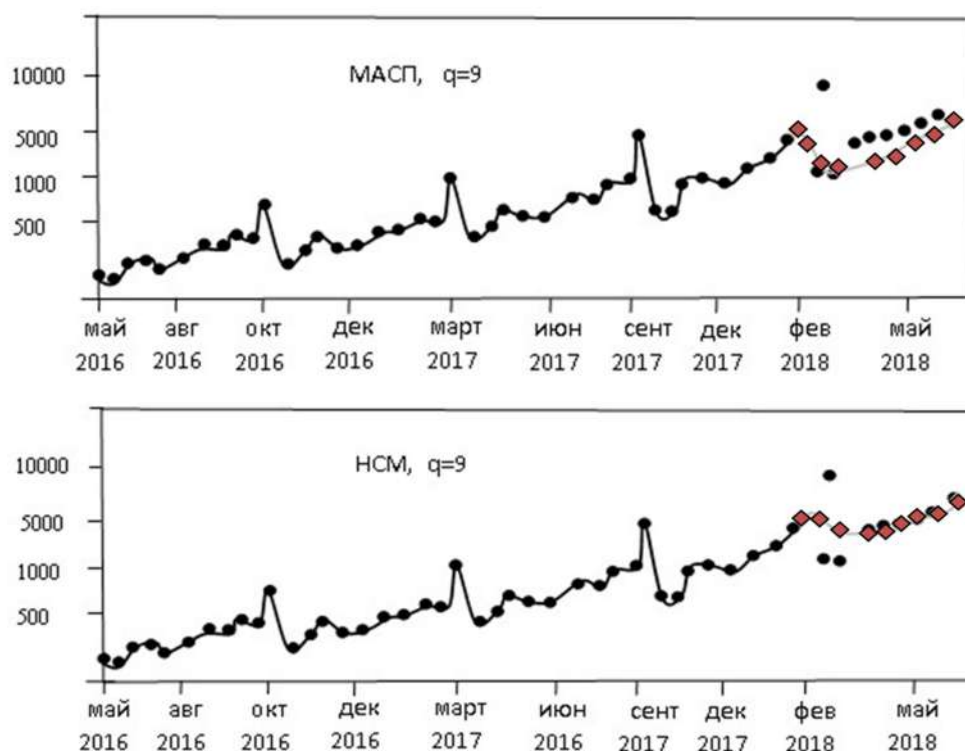


Рис. 2. График суммы контрактных платежей на расчетный счет университета (в миллионах сумов)

МАСП - метод адаптивного статистического прогнозирования, НСМ - метод прогнозирования нейронной сети. В автоматизированных процессах управления также полезна адаптивно-статистическая модель, но эффективность нейросетевой модели намного выше.

Четвертая глава диссертации «Создание и внедрение программного обеспечения для управления и повышения достоверности информации» состоит из трех параграфов, в которых изложены результаты разработки программных модулей для оптимизации управления данными и повышения достоверности этих данных, а также общая структура программного обеспечения. Для определения достоверности управляемых данных был разработан процесс оплаты контракта на получение докторской степени с

высшим образованием. Программный комплекс выполняет задачи, определенные схемой, показанной на рис. 3.

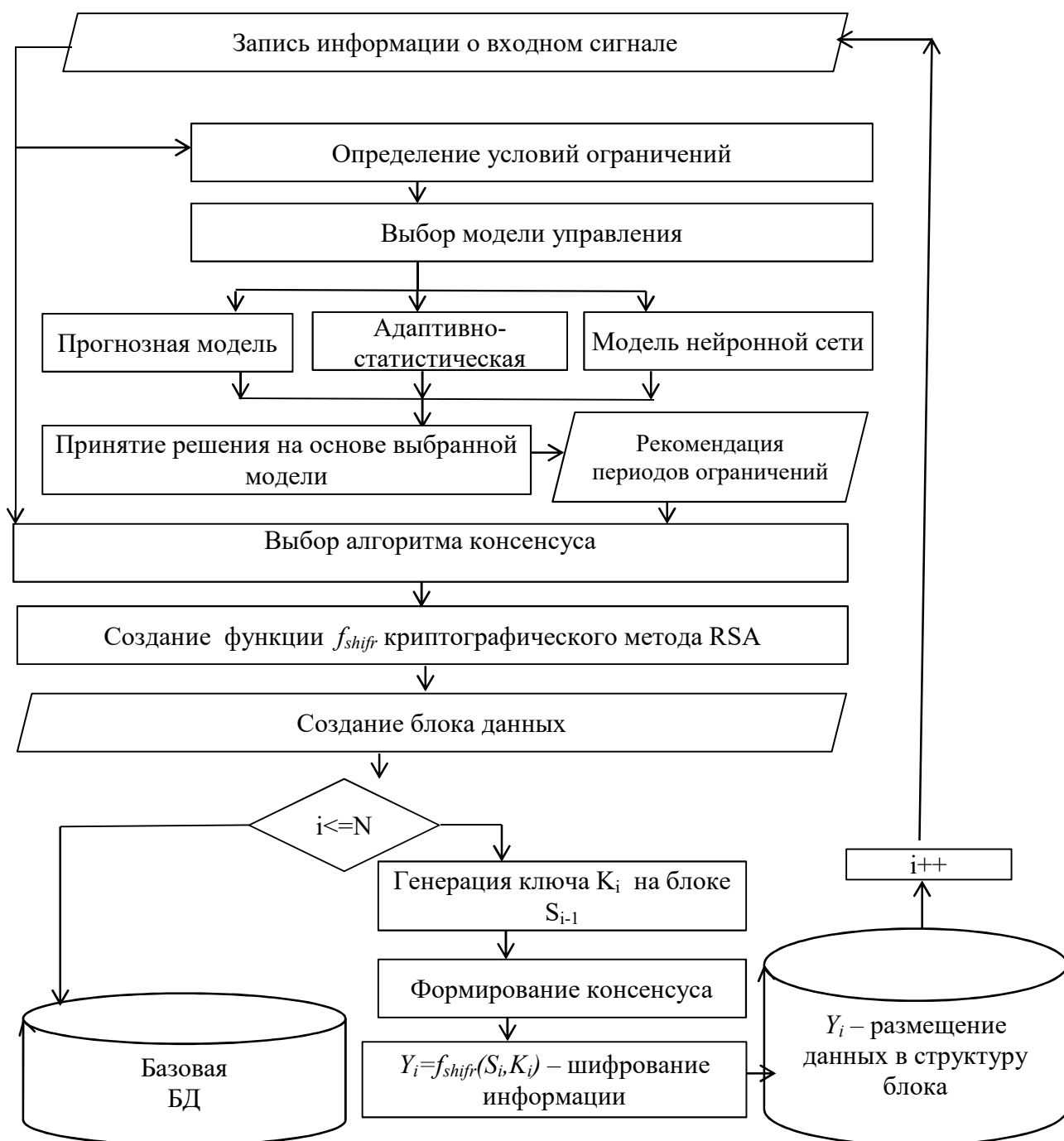


Рис. 3. Общая схема программного комплекса для оптимизации управления и повышения достоверности информации

На основе прогнозных, адаптивно-статистических и нейронных моделей, разработанных в программном пакете, даются рекомендации по установке ограниченных периодов на основе данных истории платежей студентов. Программный комплекс внедрен в процесс мониторинга и электронного документооборота контрактных платежей Самаркандского государственного университета и Самаркандского филиала ТУИТ. С помощью программного комплекса были получены результаты эксперимента и в ходе эксперимента

было проанализировано получение студенческих платежей в течение ограниченного льготного периода. По результатам анализа определена оптимальность модели нейросети, которая представлена на рис. 4.

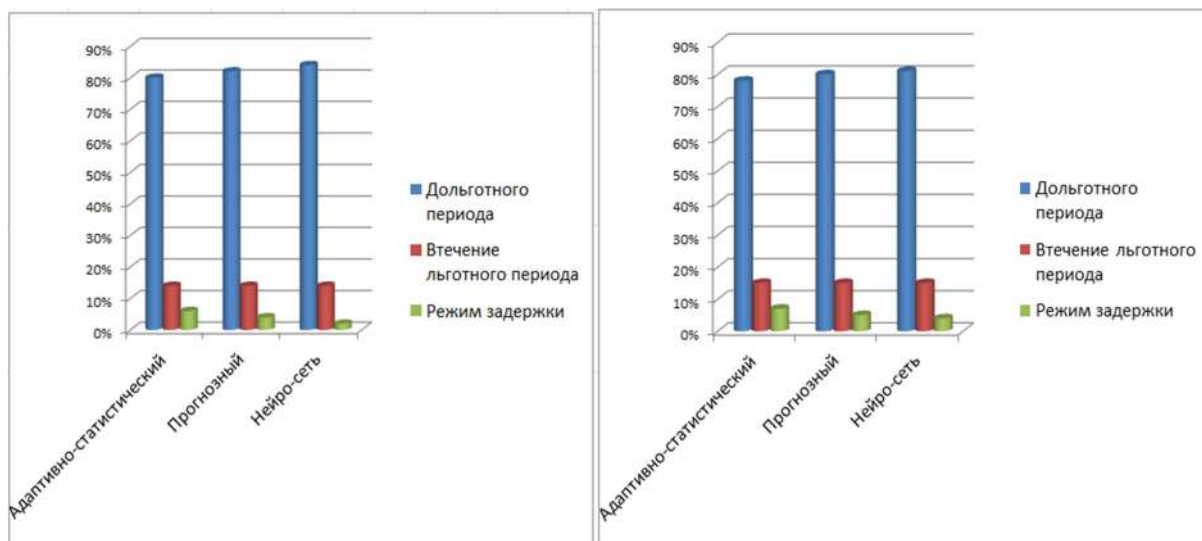


Рис. 4. Диаграмма показателей сумм платежей на основе моделей данных СамГУ и СФ ТУИТ.

В таблице 1 приведены показатели запаздывания выплат контрактов по льготным условиям, предоставленным студентам на основе моделей обычных ограничений по времени и управления.

**Таблица 1.
Запаздывание выплат по контракту по льготным условиям, предоставленным на основе моделей ограничений по времени и управления**

Время / Модель	Адаптивно-статистический (СамГУ)	Адаптивно-статистический (СФ ТУИТ)	Прогноз-ный (СамГУ)	Прогноз-ный (СФ ТУИТ)	Нейрон-ные сети (СамГУ)	Нейрон-ные сети (СФ ТУИТ)
Запаздывание на ограниченное время	7%	9%	6%	5%	4%	6%
Отсрочка льготного периода	6%	7%	4%	5%	2%	4%

В результате применения предложенных в работе моделей управления наблюдается увеличение уровня платежей на 7-8% в рекомендуемые программной системой сроки относительно первоначально установленных сроков. Разработанные модели управления могут быть применены к другим процессам, связанным с платежными системами.

В системах электронного документооборота Самаркандского областного экономического суда и Самаркандского филиала Кишлок курилиш банка использованы методы и алгоритмы повышения достоверности информации на основе разработанных механизмов распределенного реестра.

В результате применения разработанных методов и алгоритмов повышения достоверности информации, основанных на механизмах распределенного реестра, в системах документооборота Самаркандского областного экономического суда и филиала Кишлок курилиш банк, достоверность информации повысилась в 1,5-2 раза.

Разработаны архитектура базы данных системы, инфологическая и даталогическая модели данных, а также модули программного комплекса для мониторинга оплаты по контрактам высшего образования.

Инфологическая и даталогическая модели базы данных договоров на оплату разработаны на основе интеллектуальной программы MySQL Workbench. Программа MySQL Workbench форматирует структурные отношения в инфологической модели, как показано на рис. 5.

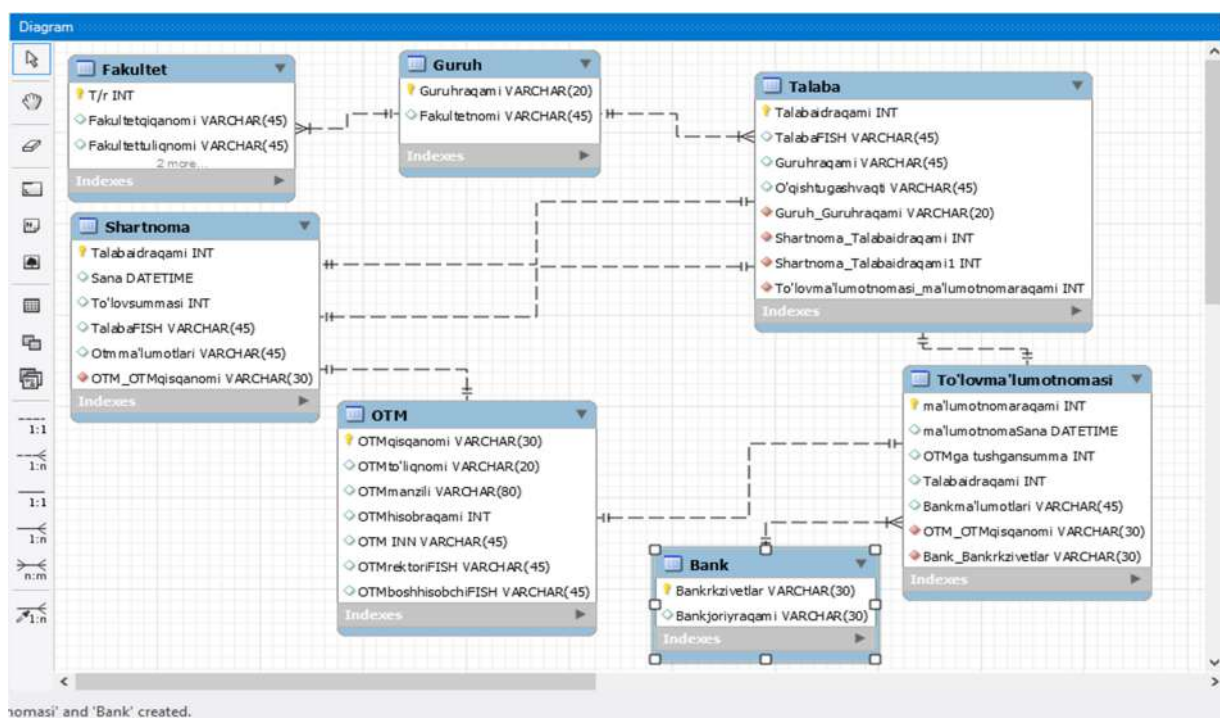


Рис. 5. Схема взаимосвязей и отношений базы данных

На основе архитектуры базы данных, инфологической и даталогической модели данных создан программный комплекс контрактной системы оплаты высшего образования. С помощью программного комплекса можно отслеживать платежные процессы.

ЗАКЛЮЧЕНИЕ

Приведены следующие выводы в результате проведенных исследований по диссертационной работе на тему «Методы и алгоритмы повышения

достоверности информации на основе механизмов распределенного реестра при организационном управлении нестационарными системами»:

1. Систематически проанализирован уровень изученности механизмов управления нестационарными системами в условиях с ограничениями и повышения достоверности информации управляемой системы на основе механизмов распределенного реестра.

2. На основе математических моделей процессов управления определены условия с ограничениями и разработаны математические модели управления для оптимизации управления НСОУ, для повышения достоверности информации управляемой системы предложены механизмы распределенного реестра технологии блокчейн.

3. Изучены основные принципы механизма распределенного реестра, перспективы развития, уровень безопасности и определены параметры повышения достоверности информации. Создан общий алгоритм разработки архитектуры баз данных нестационарных систем на основе распределенного реестра или механизмов блокчейна.

4. Для повышения достоверности информации управляемых информационных систем разработана архитектура базы данных на основе модели блокчейна, проанализированы алгоритмы консенсуса в качестве механизмов технологии блокчейн и предложен метод использования алгоритма Pos для НСОУ.

5. Разработаны алгоритмы повышения достоверности информации на основе механизмов распределенного реестра с помощью динамических ключей метода шифрования.

6. На основе прогнозирования данных нестационарных систем с ограничениями была разработана модель управления, прогнозные модели управления с использованием постоянной параметрической системы. Разработанные модели были применены к системе приема, хранения и передачи данных пользователю. Определена эффективность разработанных моделей и алгоритмов на основе приложения к практическим задачам.

7. Разработана адаптивно-статистическая модель прогнозирования нестационарных систем на основе временных рядов. Предложена модель прогнозирования по временным рядам, интегрированная с нейронной сетью, и получены экспериментальные результаты. Результаты эксперимента показали, что применение модели нейронной сети в оперативных, надежных и прогнозирующих автоматизированных системах управления является эффективным.

8. Разработаны общая схема и модули программного комплекса для оптимизации процессов управления и повышения достоверности информации. Разработанные модели оптимизации управления апробированы экспериментально, по результатам экспериментов определена экономическая эффективность в 7-8%. Механизмы распределенного реестра, разработанные для повышения достоверности информации, протестированы экспериментально, и по результатам эксперимента выявлено улучшение

эффективности в 1,5-2 раза на основе механизмов распределенного реестра и методов шифрования.

9. Разработаны реляционные инфологические и даталогические модели базы данных системы мониторинга оплаты контрактных договоров. На основе интеллектуальной программы MySQL Workbench разработана архитектура базы данных системы мониторинга оплаты контрактных договоров. Создан и протестирован программный комплекс, реализующий разработанные модели и алгоритмы.

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

SAMARKAND STATE UNIVERSITY

NAZAROV FAYZULLO MAKHMADIYAROVICH

**METHODS AND ALGORITHMS FOR INCREASING THE RELIABILITY
OF INFORMATION BASED ON THE MECHANISMS OF THE
DISTRIBUTED REGISTER IN THE ORGANIZATIONAL
MANAGEMENT OF NON-STATIONARY SYSTEMS**

05.01.02 – System analysis, management and information processing

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

Tashkent-2021

The theme of doctor of philosophy (PhD) was registered at the Supreme Attestation Commission of the Cabinet of Ministers of the Republic of Uzbekistan under number №B2020.2.PhD/T1560.

The dissertation has been prepared at Samarkand State 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: Akhatov Akmal Rustamovich
Doctor of Technical Sciences, Professor

Official opponents: Babomuradov Ozod Jurayevich
Doctor of Technical Sciences
Tukhtanazarov Dilmurod Solijonovich
Doctor of Philosophy of Technical Sciences

Leading organization: Tashkent State Transport University

The defense will take place “03” June 2021 at 16:00 on 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 is available at the Information Resource Centre of the Tashkent University of Information Technologies (is registered under No. 202). (Address: 100202, Tashkent City, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

The abstract of dissertation is distributed on “21” may 2021 y.
(Protocol at the registr No. 11 on “08” may 2021 y.).



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

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

A.V. Kabulov
Chairman of the scientific seminar of the
scientific council awarding scientific degrees,
Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to consist in the development of methods, an algorithm and software for a predictive control model and an increase in the reliability of information from a non-stationary system under constraints.

The object of the research work these are the data processing processes for paying for higher education contracts and the electronic document management system.

The scientific novelty of the research work is as follows:

a predictive model of organizational management based on the restrictive conditions of non-stationary systems is developed;

a model for optimizing organizational management of non-stationary systems in limited conditions based on a neural network has been developed;

a method has been developed to improve the reliability of information from non-stationary systems based on the consensus algorithm of distributed ledger mechanisms;

an improved algorithm of the dynamic encryption method based on the blockchain has been developed to optimize the management of non-stationary systems.

Implementation of research results. Within the framework of the dissertation research on the basis of the obtained scientific results on the development of methods and algorithms for improving the reliability of information using distributed registry mechanisms in the organizational management of non-stationary systems:

algorithms and mechanisms created on the basis of identification of input data of a managed non-stationary system, selection of consensus algorithms, development of a database architecture based on distributed registries are applied in the Samarkand Regional Economic Court (Certificate of the Supreme Court of the Republic of Uzbekistan No. 08/UM-727-20 dated December 17, 2020). As a result, when organizing the work of an electronic document management system based on distributed registry mechanisms, an increase in the efficiency of memory usage and information reliability was achieved by 1.5-2 times;

algorithms and mechanisms created on the basis of integration of encryption methods with distributed registry mechanisms are applied in the Kishlok Kurilish Bank (Certificate of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan dated December 2, 2020 No. 33-8/7344). The results allowed us to achieve an increase in the reliability of information in the database of the electronic document management system by 1.5-2 times;

algorithms and mechanisms based on predictive, adaptive-statistical and neural management models, as well as distributed registry mechanisms developed taking into account the limited conditions of organizational management of non-stationary systems, are applied in the Samarkand State University and the Samarkand branch of TUIT (Certificate of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan dated December

2, 2020 No. 33-8/7344). As a result, an increase in the volume of payment of contracts by 7-8% was achieved due to the new terms recommended on the basis of management models in conditions of restrictions.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, four chapters, conclusion, the list of used literature and appendix. The volume of the dissertation 110 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим(I часть; I part)

1. Ахатов А., Назаров Ф.М. Разработка модели прогнозирования временных рядов нестационарных дискретных систем на основе нейронной сети // Проблем информатики. Федеральное государственное бюджетное учреждение науки, Институт вычислительной математики и математической геофизики Сибирского отделения РАН. Российская Федерация. 2018. №3(40). – С.34-50. (05.00.00; №67)
2. Nazarov F.M. Forecasting Non-Stationary Discrete Systems With Limitations On Condition And Management // International Journal of Advanced Research in Science, Engineering and Technology. National Institute of Science Communication and Information Resources. 2019.Volume 6, Issue 3, March, INDIA. – P. 8332-8337. (05.00.00; №8)
3. Ахатов А., Назаров Ф.М. Методы реализации блокчейн на основе криптографической защиты для системы обработки данных с ограничением и запаздыванием в электронном документообороте // Вестник компьютерных и информационных технологий. Москва. ООО Издательский дом «Спектр» 2019. №10. – С.3-13. (05.00.00; №12)
4. Akhatov A.R., Nazarov F.M, Meliyev F.F. Development of Models and Algorithms for Improving the Reliability of Transfer of Information Based on the Application of Cryptographic Methods to the Distributed Register Technology // International Journal of Control and Automation. 2020. Vol. 13, No.2, – P.1118–1129. (№3; Scopus; IF=0.1)
5. Ахатов А., Назаров Ф.М. Проектирование базы данных системы автоматизированного мониторинга, анализа и прогнозирования показателей процессов оплаты образовательных контрактов // Фан ва технологиялар тараққиёти. Бухоро муҳандислик технологиялари институти. Бухоро. 2018. № (4). – С.128-134. (05.00.00; №24)
6. Ахатов А., Назаров Ф.М. MySQL Workbench муҳитида таълим шартнома тўловларини мониторинг тизимининг маълумотлар базасини ишлаб чиқиш // ТАТУ хабарлари. Тошкент ахборот технологиялари университети. Тошкент. 2019. № 1(45). – С.115-124. (05.00.00; №31)
7. Ахатов А., Назаров Ф. Чекланган ва кечикиш шароитлардаги тизимларда, таксимланган реестр(блокчейн) технологиялари асосида маълумотлар ишончилигини таъминлаш // Муҳаммад ал-хоразмий авлодлари. Тошкент ахборот технологиялари университети. Тошкент. 2019. №(4)10. – С.10-14. (05.00.00; №10)
8. Akhatov A.R., Nazarov F.M., Meliyev F.F. Algorithms for data reliability based on a cryptographic distributed database (blockchain). Scientific journal Samarkand state university. Samarkand. 2020. №3(121). –P.98-104. (283/7.1-сон ОАК қарори. №32)

II бўлим(II часть; II part)

9. Ахатов А., Назаров Ф. Модель шифрования для обеспечения достоверности данных на основе технологии блокчейн в системах электронного документооборота // «GLOBAL SCIENCE AND INNOVATIONS 2018: CENTRAL ASIA» Международной научно-практической конференции. Республика Казахстан. 2018. –С. 602-605.

10. Akhatov A., Nazarov F. Optimization of management of nonstationary discrete systems by the account of terminal regulation of parameters of perturbing factors // Abstracts of the VI international scientific conference «Modern problems of the applied mathematics and information technology – Al-Khorezmiy 2018» NUUZ. 15-17-sent. Tashkent. 2018. – P.73.

11. Ахатов А, Назаров Ф. Чекланган ва кечикиш шароитлардаги тизимларда тақсимланган реестр технологиясини қўллаш алгоритмини ишлаб чиқиш // Международная научная конференция «Актуальные проблемы прикладной математики и информационных технологий», ЎзМУ. Ноябрь 14-15. Ташкент. 2019. – С. 184-185.

12. Назаров Ф.М. Жараёнларни бошқаришда тақсимланган реестр механизмлари орқали маълумотлар ишончлилигини таъминлаш // Инновацион ва замонавий ахборот технологияларини таълим, фан ва бошқарув соҳаларида қўллаш истиқболлари Халқаро илмий – амалий онлайн конференцияси материаллари. 2020 йил 14-15 май Самарқанд-2020. –С. 251-253.

13. Akhatov A., Nazarov F. Development Of Control Models Of Non-Stationary Systems In Limited Conditions. // International conference on information science and communications technologies. 4,5,6 November. ICISCT 2020(IEEE), art. no. 9351372. DOI: 10.1109/ICISCT50599.2020.9351372.

14. Akhatov A, Nazarov.F, Sayidqulov A. Optimization of relationship between databases of monitoring system of payment of educational contracts. // Zamonaviy informatikaning dolzarb muammolari: o'tmish tajribasi, istiqbollari Respublika ilmiy amaliy konferensiya matreallari. Toshkent. 2018. 23-aprel. –P. 132-134.

15. Ахатов А, Назаров Ф., Сайидкулов А. Особенности построения архитектуры базы данных ОЗ СЭД на основе технологии блокчейн // «Фан ва таълим-тарбиянинг долзарб масаллари» Республика илмий-назарий анжумани. Ажиниёз номидаги Нукус давлат педагогика институти. 2019 йил 27-28 март. Нукус 2019.–С. 322-324.

16. Назаров Ф. Чекловлар ва кечикиш шароитларидаги дискрет ностационар тизимлар ва уларнинг башоратлаш // Ахборот коммуникация технологиялари ва дастурий таъминот яратишда инновацион ғоялар. Республика илмий-техник анжуманининг маърузалар тўплами. ТАТУ СФ 16-17 апрел, Самарқанд. 2019. –С.266-269.

17. Назаров Ф. Тақсимланган реестр (блокчейн) механизмларини ташкилий бошқариладиган тизимларга қўллаш // Ахборот технологияларининг замонавий муаммолари ҳамда уларнинг ечимлари.

Республика илмий-амалий анжуман мақолалар тўплами.– ТАТУ УФ 05.06.2020. Урганч. 2020. –С. 267-268.

18. Жуманов И., Ахатов А, Назаров Ф. Тақсимланган реестр механизмларининг ишлаш алгоритмлари // Инновацион ёндашувлар илм-фан тараққиёти калити сифатида: ечимлар ва истиқболлар мавзусидаги Республика илмий-амалий конференцияси мақолалар тўплами. ЎзМУ ЖФ. 8-10 октябрь 2020 йил. Жиззах 2020.–С. 88-92.

19. Назаров Ф., Эштемиров С., Эштемиров Б. Онлайн шартнома тўлови дастурий таъминоти // Интеллектуал мулк агентлиги гувоҳнома №DGU 04512. 19.05.2017.

20. Ахатов А., Назаров Ф., Сайидкулов А. Чекловлар ва кечикиш шароитларида ностационар тизимларнинг кўрстакларини мониторинг тизими // Интеллектуал мулк агентлиги гувоҳнома №DGU 05189. 27.02.2018.

21. Назаров Ф., Сайидкулов А. Блокчейн асосида жойлаштирилган маълумотларни криптографик махфийлаштириш тизими // Интеллектуал мулк агентлиги гувоҳнома № DGU 06420. 04.04.2019.

22. Ахатов А., Назаров Ф. Ностационар тизимларни бошқариш ва тақсимланган реестр механизмлари асосида маълумотлар ишончилигини ошириш дастури // Интеллектуал мулк агентлиги гувоҳнома №DGU 08485. 09.07.2020.