ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.27.06.2017.T.03.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ

ИСМАИЛОВ ОТАБЕК МИРХАЛИЛОВИЧ

ИШЛАБ ЧИҚАРИШ МАЖМУАЛАРИ ҲИМОЯЛАНГАН ИНТЕГРИРЛАШГАН БОШҚАРИШ ТИЗИМЛАРИНИНГ АВТОМАТЛАШТИРИЛГАН ЛОЙИҲАЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.08 - Технологик жараёнлар ва ишлаб чиқаришларни автоматлаштириш ва бошқариш

ТЕХНИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент – 2019

УЎК 681.3

Фан доктори (DSc) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора наук (DSc)

Contents of dissertation abstract doctor of sciences (DSc)

ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.27.06.2017.T.03.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ ДАВЛАТ ТЕХНИКА УНИВЕРСИТЕТИ

ИСМАИЛОВ ОТАБЕК МИРХАЛИЛОВИЧ

ИШЛАБ ЧИҚАРИШ МАЖМУАЛАРИ ҲИМОЯЛАНГАН ИНТЕГРИРЛАШГАН БОШҚАРИШ ТИЗИМЛАРИНИНГ АВТОМАТЛАШТИРИЛГАН ЛОЙИҲАЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.08 - Технологик жараёнлар ва ишлаб чиқаришларни автоматлаштириш ва бошқариш

ТЕХНИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент – 2019

Фан доктори (DSc) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2018.4.DSc/T244 рақам билан рўйхатга олинган.

Докторлик диссертацияси Тошкент давлат техника университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгашнинг веб-саҳифасида (www.tdtu.uz) ҳамда «ZiyoNet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий маслаҳатчи:	**Юсупбеков Нодирбек Рустамбекович** техника фанлари доктори, профессор, академик
Расмий оппонентлар:	**Камилов Мирзаян Мирзаахмедович** техника фанлари доктори, профессор, академик
	Игамбердиев Хусан Закирович техника фанлари доктори, профессор, академик
	Каримов Мажит Маликович техника фанлари доктори, профессор
Етакчи ташкилот:	**Бухоро муҳандислик-технология институти**

Диссертация ҳимояси Тошкент давлат техника университети ҳузуридаги DSc.27.06.2017.T.03.02 рақамли Илмий кенгашнинг 2019 йил «____» _____ соат ___ даги мажлисида бўлиб ўтади. (Манзил: 100095, Тошкент шаҳри, Университет кўчаси, 2. Тел.: (99871) 246-46-00; факс: (99871) 227-10-32; e-mail: tstu_info@edu.uz).

Диссертация билан Тошкент давлат техника университетининг Ахборот-ресурс марказида танишиш мумкин (___ рақам билан рўйхатга олинган). Манзил: 100095, Тошкент шаҳри, Университет кўчаси, 2. Тел.: (99871) 246-03-41.

Диссертация автореферати 2019 йил «____» _____ куни тарқатилди.
(2019 йил «___» _____даги ____ рақамли реестр баённомаси).

Ф.Т.Адилов
Илмий даражалар берувчи
илмий кенгаш раиси ўринбосари,
техника фанлари доктори, профессор

У.Ф.Мамиров
Илмий даражалар берувчи илмий кенгаш
илмий котиби, техника фанлари бўйича
фалсафа доктори (PhD)

Х.З. Игамбердиев
Илмий даражалар берувчи
илмий кенгаш қошидаги илмий семинар раиси,
техника фанлари доктори, профессор, академик

КИРИШ (Фан доктори (DSc) диссертацияси аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурияти. Жаҳонда сўнгги вақтларда технологик жараёнлар ва ишлаб чиқаришларни автоматлаштириш соҳасида ишлаб чиқариш мажмуаларининг ҳимояланган интеграллашган бошқариш тизимлари (ИЧМ ҲИБТ)ни автоматлаштирилган лойиҳалаш усуллари ва алгоритмларини ишлаб чиқиш масалалари етакчи ўринни эгаллайди. Бу соҳада саноат тармоқларининг функционал ҳолатини мониторинг қилишни унификацияланган модел ва алгоритмлари ҳамда эҳтимолий таҳдидларни ўз вақтида бартараф этиш ва уларга реал вақт режимида адаптив таъсир кўрсатиш алгоритмларини ишлаб чиқишга алоҳида эътибор қаратилмоқда. Шу жиҳатдан саноат объектларининг ҳимояланганлигини мониторинг қилиш, идентификациялаш ва таъминлашнинг турли усулларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланмоқда.

Жаҳонда ҳимояланган саноат мажмуаларини лойиҳалашга бўлган эҳтимолий таҳдидларга қарши курашиш, тизим узлуксиз ишлашини таъминлаш ва турли таҳдидлар шароитида объектларни адаптив бошқариш масалаларини ҳал қилишга қаратилган универсал ёндашувни яратиш бўйича илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, жумладан, миссиоцентрик ёндашув тушунчалари асосида ИЧМ ҲИБТни автоматлаштирилган лойиҳалаш усуллари ва алгоритмларини такомиллаштириш, дискрет маълумотлар оқимига эга бўлган ИЧМ ҲИБТдаги тармоқ трафигини статистик ва фрактал таҳлил қилиш усуллари ва алгоритмларини ишлаб чиқиш ва дастурий таъминотини яратиш муҳим вазифалардан бири хисобланилади. Шу билан бирга ишлаб чиқариш мажмуаларини ташқи ва ички таҳдидлардан ҳимояланган интеграллашган бошқариш тизимларини ҳавсизлигини таъминловчи самарали усуллар ва алгоритмларни яратиш зарур ҳисобланади.

Республикамизда технологик жараёнлар ва ишлаб чиқаришларни узлуксиз ишлашини таъминловчи ИЧМ ҲИБТни автоматлаштириш ва бошқариш ҳамда лойиҳалаш йўналишларига катта эътибор қаратилмоқда. 2017–2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «... иқтисодиётда энергия ва ресурслар сарфини камайтириш, ишлаб чиқаришга энергия тежайдиган технологияларни кенг жорий этиш, қайта тикланадиган энергия манбаларидан фойдаланишни кенгайтириш, иқтисодиёт тармоқларида меҳнат унумдорлигини ошириш, ... иқтисодиёт, ижтимоий соҳа, бошқариш тизимига ахборот-коммуникация технологияларини жорий этиш»[1] вазифалари белгилаб берилган. Мазкур вазифаларни амалга ошириш, жумладан ишлаб чиқариш мажмуаларининг интеграллашган бошқариш тизимлари (ИЧМ ИБТ) ҳимоясини оширишга имкон берувчи замонавий

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

усуллар ва алгоритмларни ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги Фармони, 2017 йил 27 июлдаги ПҚ-3151-сон «Олий маълумотли мутахассислар тайёрлаш сифатини оширишда иқтисодиёт соҳалари ва тармоқларининг иштирокини янада кенгайтириш чора-тадбирлари тўғрисида»ги, 2012 йил 21 мартдаги ПҚ-1730-сон «Замонавий ахборот-коммуникация технологияларини янада жорий этиш ва ривожлантириш чора-тадбирлари тўғрисида»ги, 2018 йил 27 апрелдаги ПҚ-3682-сонли «Инновацион ғоялар, технологиялар ва лойихаларни амалий жорий қилиш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Қарорлари ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти муайян даражада ҳизмат қилади.

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

Диссертация мавзуси бўйича хорижий илмий тадқиқотлар шарҳи[2]. Ишлаб чиқариш мажмуаларини ҳимояланган интегралашган бошқариш тизимларининг автоматлаштирилган лойиҳалаш усуллари ва алгоритмларини яратиш ҳамда такомиллаштиришга йўналтирилган илмий тадқиқотлар жаҳоннинг етакчи илмий марказлари ва олий таълим муассасалари, жумладан «Honeywell», Rockwell Automation Inc., University of California, Massachusetts Institute of Technology (АҚШ), «Check Point Software Technologies» (АҚШ, Исроил), Technical University Munich, Karlsruhe Institute of Technology, Technical University Darmstadt (Германия), Imperial College London, The University of Edinburgh (Буюк Британия), Linksping University (Швеция), University of Chemical Technology in Prague (Чехия), The University of Tokyo, Tokyo Institute of Technology (Япония), Seoul National University, Korea Advanced Institute of Science and Technology (Жанубий Корея), Автоматика институти (Хитой), «Станкоинформзащита» илмий-техник маркази, Н.Э.Бауман номидаги Москва давлат техника университети, Санкт-Петербург информатика ва автоматлаштириш институти, Самара давлат университети (Россия), Турин политехника университети, Тошкент давлат техника университети, Тошкент аҳборот технологиялари университети (Ўзбекистон)да олиб борилмоқда.

[2] Диссертация мавзуси бўйича илмий тадқиқотлар шарҳи https://www.honeywell.com, https://www.rockwellautomation.com/site-selection.html, https://www.universityofcalifornia.edu, http://web.mit.edu, https://www.checkpoint.com, https://www.tum.de, https://www.kit.edu, https://www.tu-darmstadt.de, http://www.imperial.ac.uk, https://www.ed.ac.uk, https://liu.se, https://www.vscht.cz/?jazyk=en, https://www.u-tokyo.ac.jp/en/index.html, https://www.titech.ac.jp/english, http://en.snu.ac.kr, http://www.kaist.edu, http://english.ia.cas.cn, https://www.ntcsiz.ru, http://www.bmstu.ru, http://www.spiiras.nw.ru, https://polito.uz, http://tdtu.uz, https://tuit.uz ва бошқа манбалар асосида ишлаб чиқилган.

Технологик жараёнлар ва ишлаб чиқаришларни автоматлаштириш соҳасида ИЧМ ҲИБТни автоматлаштирилган лойиҳалаш усуллари ва алгоритмларини ишлаб чиқиш ҳамда ҳимоя тизимларини такомиллаштиришга оид жаҳонда олиб борилган тадқиқотлар натижасида қатор, жумладан қуйидаги илмий натижалар олинган: ИЧМ ҲИБТнинг қуйи поғоналаридаги мосламаларни ҳимоялаш усуллари ва алгоритмлари яратилган («Honeywell», University of California, Massachusetts Institute of Technology, George Mason University, АҚШ; Россия Фанлар Академияси Бошқариш муаммолари институти, Россия); ИЧМ ИБТни бошқариш объектлари (тўғридан-тўғри бошқариш буйруқлари, режим параметрлари ва уларни ўлчов қийматларини ўзгариши ҳамда авариялларга қарши ҳимоялар)га бўлган рухсатсиз киришдан ҳимоялаш алгоритмлари ишлаб чиқилган («Истиқболли тадқиқотлар жамғармаси», Россия); ИЧМ ҲИБТни муҳим инфратузилмаларини (SCADA серверлари, операторлик панеллари, муҳандислик ишчи станциялари, тармоқ уланишлари ва ахборот инфратузилмасининг бошқа муҳим тизимлари) барқарор ишлашини таъминлаш бўйича алгоритмлар ва аппарат-дастурий мажмуалар ишлаб чиқилган (Massachusetts Institute of Technology, АҚШ; Linksping University, Швеция; «Modcon Systems», Буюк Британия; Seoul National University, Жанубий Корея; Н.Э.Бауман номидаги Москва давлат техника университети, Санкт-Петербург информатика ва автоматлаштириш институти, Россия); автоматлаштирилган бошқариш тизимларининг техник воситалари (датчиклар, микроконтроллерлар, микропроцессорлар ва бошқалар)ни технологик носозликларини назорат қилиш усуллари ва алгоритмлари ишлаб чиқилган («Honeywell», АҚШ; Seoul National University, Жанубий Корея; Tokyo Institute of Technology, Япония; «Станкоинформзащита» илмий-техника маркази, Россия); ишлаб чиқаришнинг нефть-газ, кимё, биотехнология тармоқларида интеграллашган бошқариш тизимларини лойиҳалаш усуллари ва алгоритмлари ишлаб чиқилган («Honeywell», АҚШ; «Станкоинформзащита» илмий-техника маркази, Россия); ишлаб чиқаришнинг электрэнергетика ва транспорт тармоқларида бошқариш тизимларини автоматик сигнализациялаш, блокалаш ва мониторинг қилишнинг дастурий-техник мажмуалари ишлаб чиқилган («Honeywell», АҚШ; Linksping University, Швеция; «Станкоинформзащита» илмий-техника маркази, Россия).

Жаҳонда ИЧМ ҲИБТни лойиҳалашни автоматлаштириш масалаларини ечиш учун ишлаб чиқилаётган усуллар ва алгоритмларни такоминлаштиришга доир қатор, жумладан қуйидаги устувор йўналишларда илмий тадқиқотлар олиб борилмоқда: мураккаб динамик жараёнларга эга бўлган тизимлардаги таҳдидларни аниқлаш, хатарларни баҳолаш ва бошқаришни такомиллаштириш; бошқариш объектларига ва ресурсларига рухсатсиз киришларни бошқариш; саноат объектларининг ишлашида ностандарт вазиятларни мониторинг қилиш ва хабардор қилиш тизимлари; адаптив бошқариш ва таҳдидларга қарши курашиш тизимларини ишлаб

чиқиш; ташқи ва ички қўзғатувчи таъсирларга боғлиқ бўлмаган бошқариш тизимларининг ишлашини таъминловчи моделларни ишлаб чиқиш.

Муаммонинг ўрганилганлик даражаси. ИЧМ ИБТнинг автоматлаштирилган лойиҳалаш усуллари, моделлари ва алгоритмларини ишлаб чиқиш бўйича кўплаб хорижлик олимлар, жумладан: J.C.Smith, D.J.Howard, R.N.Selin, R.Lippmann, R.Kwitt, A.Ghosh, E.Eskin, N.Cristianini, M.Salem, H.Amstrong, P.Barford, J.Kline, H.J.Kim, P.Casas, В.А.Артамонов, Д.Ю.Гамаюнов, Ю.В.Писецкий, С.Гордейчик, В.Дубровин, В.И.Маркоменко, Р.В.Базаев, В.А.Конявский, В.А.Галатенко ва бошқалар ҳамда мамлакатимиз олимлари, жумладан А.А.Абдуқодиров, Б.М.Азимов, О.П.Ахмедова, Т.Ф.Бекмуратов, Ш.М.Ғуломов, И.И.Жуманов, О.О.Зарипов, Х.З.Игамбердиев, А.А.Кадиров, Н.З.Камалов, М.М.Камилов, М.М.Каримов, А.Р.Марахимов, Т.Р.Нурмухамедов, М.А.Рахматуллаев, О.Х.Расулова, И.Х.Сиддиқов, Ш.Х.Фозилов, Н.Р.Юсупбеков ва бошқалар ўзларининг улкан ҳиссаларини қўшишган.

Хорижлик ва мамлакатимиз олимлари ишларининг таҳлили, улар томонидан таклиф қилинаётган ахборот хавфсизлигини таъминлаш усуллари асосан хавфсизликнинг кўп босқичли моделини қуриш ва ИЧМ ИБТ ҳимоясини ташкиллаштиришга бўлган эшелонлаштирилган ёндашувга йўналтирилганлигини ёки криптографик ҳимоя каби масалаларни ечиш билан чекланганлигини кўрсатди. Хусусан, О.П.Ахмедова, О.Х.Расулов, М.М.Каримовлар ахборот тизимларидаги маълумотларни ҳимоя қилишга имкон берувчи маълумотларни кодлашнинг турли аппарат-дастурий воситаларини таклиф қилганлар.

Соҳага оид тадқиқотлар таҳлили шуни кўрсатадики, ишлаб чиқариш мажмуаларининг ҳозирги босқичида ҳимояланган интеграллашган бошқариш тизимларидаги маълумотларни узлуксиз қайта ишлаш, маълумотлар бутунлигини таъминлаш учун саноат тизимлари таҳдидларини аниқлаш ва уларга қарши курашишнинг адаптив тизимларини яратиш, маълумотлар узатиш каналларини ҳимоя қилишнинг илғор усулларини тадқиқ қилиш, саноат корхоналарида адаптив тизимлар ва ҳимоя технологияларини яратиш масалалари етарли даражада ўрганилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент давлат техника университети илмий-тадқиқот ишлари режаларининг №Ф-4-56–«Мураккаб технологик объектларни интеллектуал бошқариш тизимлари норавшан тўпламлари асосида тузилмавий-параметрик синтезнинг назарий асослари ва усулларини ишлаб чиқиш» (2012-2016); №А-5-42–«Априор ноаниқлик шароитида технологик объектларни автоматлаштирилган мониторинги ва бошқаришни интеллектуаллаштиришнинг дастурий инструментал воситаси» (2015-2017); №ОТ-Ф4-78–«Идентификацион ёндашув асосида динамик объектларни адаптив бошқариш системалари синтезининг назарий асослари ва мунтазам усулларини ишлаб чиқиш» (2017-2020); №ОТ-Ф7-88–«Тоза маҳсулотлар олишнинг энергия ва ресурстежамкор иссиқлик-масса алмаштириш

жараёнларининг истиқболни мураккаб кимё-технологик тизимларининг назорати асосларини такоминлаштириш» (2017-2020) мавзуларидаги илмий лойиҳалари доирасида бажарилган.

Тадқиқотнинг мақсади ишлаб чиқариш мажмуаларини ташқи ва ички таҳдидлардан ҳимояланган интегралашган бошқариш тизимларининг автоматлаштирилган лойиҳалаш усуллари ва алгоритмларини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

ахборот ва саноат технологияларини унификация қилиш шароитида ишлаб чиқариш мажмуаларининг ҳимояланган интегралашган бошқариш тизимларини лойиҳалаш концепцияси ва методологиясини ишлаб чиқиш;

мураккаб технологик жараёнлар ва ишлаб чиқариш объектларининг бошқариш тизимлари структурасини синтезлаш ҳамда таҳдид ва заифликларини таҳлил қилиш алгоритмларини ишлаб чиқиш;

ишлаб чиқариш мажмуаларидаги тармоқ трафиги аномалликларини таҳлил қилишнинг математик моделлирни ишлаб чиқиш;

интегралашган бошқариш тизимлари тармоқ трафигидаги аномалликларни идентификациялаш алгоритмларини ишлаб чиқиш;

ишлаб чиқариш мажмуаларида интегралашган бошқариш тизимининг ҳимояланганлигини ошириш алгоритмларини ишлаб чиқиш;

интегралашган бошқариш тизимига бўлган киберҳужумни аниқловчи гибрид алгоритм ва дастурий мажмуаларни ишлаб чиқиш;

саноат мажмуаларидаги малумотлар омборини сақлаш ва заҳиралаш тизимларининг талофатсиз ишлашини таъминловчи алгоритмларни ишлаб чиқиш.

Тадқиқотнинг объекти сифатида ишлаб чиқариш мажмуаларида интегралашган бошқариш тизимининг ахборот ресурсларига электрон таъсир кўрсатиш жараёни олинган.

Тадқиқотнинг предмети ИЧМ ҲИБТга бўлган электрон таҳдидларга қарши курашиш бўйича чоралар, моделлар, алгоритмлар, маълумотлар омбори ва дастурий мажмуаларини ишлаб чиқиш ва такомиллаштиришдан иборат.

Тадқиқотнинг усуллари. Тадқиқот жараёнида тизимли-қиёсий ва тизимли-функционал ёндашувлар, бошқариш тизимларини таҳлил қилиш, бошқариш тизимларини структуравий-параметрик синтезлаш, вақт қаторларини статистик ва фрактал таҳлил қилиш, моделлаштириш ва башоратлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

ахборот ва саноат технологияларини унификация қилиш шароитида ишлаб чиқариш мажмуаларининг ҳимояланган интегралашган бошқариш тизимини лойиҳалашнинг асосий принциплари аниқланган ҳамда концепцияси ва услубияти ишлаб чиқилган;

тадқиқ қилинаётган объект хусусиятларини ҳисобга олиб, мураккаб ишлаб чиқариш технологик объектларини бошқариш тизимлари таҳдидлари ва заиф томонларини таҳлил қилган ҳолда ишлаб чиқариш мажмуаларининг

ҳимояланган интеграллашган бошқариш тизимини структураси ишлаб чиқилган;

статистик таҳлил концепцияси асосида дискрет маълумотлар оқимига эга бўлган ишлаб чиқариш мажмуаларининг ҳимояланган интеграллашган бошқариш тизимидаги тармоқ трафигини мониторинг қилишни модернизация қилинган математик моделлари ишлаб чиқилган;

дискрет маълумотлар оқимига эга бўлган ишлаб чиқариш мажмуаларини ҳимояланган интеграллашган бошқариш тизимидаги тармоқ трафигини фрактал таҳлилининг такомиллаштирилган алгоритмлари ва моделлари ишлаб чиқилган;

ишлаб чиқариш объектларини интеграллашган бошқариш тизимларида ахборотни мажмуавий криптографик ҳимоялаш алгоритмлари ишлаб чиқилган;

ишлаб чиқариш мажмуаларининг ҳимояланган интеграллашган бошқариш тизимларидаги исталмаган оқимларни мониторинг қилиш ва идентификациялашнинг қисман ўз-ўзини ўқитиш қобилиятига эга бўлган гибридли алгоритмлари ишлаб чиқилган;

ишлаб чиқаришни интеграллашган бошқариш тизимларида маълумотлар базасини носозликларга чидамлилигини ошириш усуллари ва алгоритмлари ишлаб чиқилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

жараён кечиши давомида технологик режимларни мониторинг қилиш ва носозликларини аниқлашга имкон берувчи қўрғошин чиқиндиларини қайта ишлаш ва қоришмаларни тайёрлаш технологик жараёнлари тармоқларидаги номақбул трафикларни таниб олиш алгоритмлари ишлаб чиқилган.

аккумлятор ишлаб чиқаришда қўрғошин чиқиндиларини қайта ишлаш ва қоришмаларни тайёрлаш технологик жараёнининг интеграллашган бошқариш тизимлари маълумотлар базасининг носозликларга чидамлилигини ошириш усуллари ва алгоритмлари ишлаб чиқилган;

қўрғошин чиқиндиларини қайта ишлаш ва қоришмаларни тайёрлаш технологик жараёнлар мажмуасида ахборотларни криптографик ҳимоялаш алгоритмлари ишлаб чиқилган;

қўрғошин чиқиндиларини қайта ишлаш ва қоришмаларни тайёрлаш технологик жараёнларидаги ишлаб чиқариш мажмуалари тармоқларини мониторинг қилишнинг ҳимояланган интеграллашган бошқариш тизимларида таҳдидларни идентификациялаш масалаларини ечишга мўлжалланган дастурий мажмуа ишлаб чиқилган;

Тадқиқот натижаларининг ишончлилиги. Олинган тадқиқот натижаларининг ишончлилиги услубий жихатдан асосланган назарий ҳисоб-китобларни амалга оширилиши, бошқариш тизимларини синтез қилишнинг структуравий-параметрик, замонавий бошқариш назариясининг амаллий синовдан ўтган усуллари ва алготималарини ишлатилиши, вақт қаторларининг статистик ҳамда фрактал таҳлил усуллари ва алгоритмларини ишлатилиши, назарий ва амалий тадқиқотларнинг олинган натижалари ва уларнинг ўзаро мувофиқлиги билан таъминланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти ишлаб чиқариш жараёнларини ишончлилиги ва хавфсизлигини оширишга имкон берувчи ишлаб чиқариш мажмуалари ҳимояланган интеграллашган бошқариш тизимларини автоматлаштирилган лойиҳалашнинг конструктив усуллари, моделлари ва алгоритмларини ишлаб чиқиш билан изоҳланади.

Тадқиқот натижаларинг амалий аҳамияти таклиф этилган усуллар, моделлар, алгоритмлар ва дастурлар янги ишлаб чиқариш ҳамда турдош объектларни ҳимояланган интеграллашган бошқариш тизимларини ва уларнинг қисмларини лойҳалашни автоматлаштиришда файдаланилиш мумкинлиги билан изоҳланилади.

Тадқиқот натижаларининг жорий қилиниши. Ишлаб чиқариш мажмуалари ҳимояланган интеграллашган бошқариш тизимларининг автоматлаштирилган лойиҳалаш усуллари ва алгоритмларини яратиш бўйича ишда олинган илмий натижалар асосида:

исталмаган оқимларни мониторинг қилиш ва таниб олишнинг қисман ўз-ўзини ўқитиш қобилиятига эга бўлган гибридли алгоритмлар, ишлаб чиқаришнинг интеграллашган бошқариш тизимларида ахборотни мажмуавий криптографик ҳимоялаш ва маълумотлар базасини носозликларга чидамлилигини ошириш усуллари ва алгоритмлари Ўзбекистон Республикаси Марказий банки ахборотлаштириш Бош марказида жорий қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 28 февралдаги 33-8/1449-сон маълумотномаси). Натижада тармоқ трафигини таҳлил қилиш тизимининг ишлаш унумдорлигини 12 % га ошириш имконини берган;

статистик таҳлил концепцияси асосида дискрет маълумотлар оқимига эга бўлган ИЧМ ҲИБТдаги тармоқ трафигини мониторинг қилишнинг модернизация қилинган математик моделлари ва дискрет маълумотлар оқимига эга бўлган ИЧМ ҲИБТдаги тармоқ трафигининг фрактал таҳлилини такомиллаштирилган алгоритмлари ва моделлари «Жиззах аккумулятор заводи» АЖ да жорий қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 28 февралдаги 33-8/1449-сон маълумотномаси). Ишлаб чиқилган математик моделлар ва саноат тармоқларини мониторинг қилиш тизимини такомиллаштириш алгоритмлари ИЧМ ҲИБТни тўхтовсиз ишлаш имконини берган;

ахборот ва саноат технологияларини унификация қилиш шароитида ИЧМ ҲИБТни лойиҳалашнинг аниқланган асосий принциплари ҳамда ишлаб чиқилган концепцияси ва услубияти Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ахборот ва жамоатчилик хавфсизлиги Маркази ҳамда «UNICON.UZ» ДУКда жорий қилинган (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 28 февралдаги 33-8/1449-сон маълумотномаси). Натижада ИЧМ ҲИБТдаги

трафикни мониторинг қилиш тизими самарадорлигини 15 % га ошириш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқотнинг назарий ва амалий натижалари 3 та халқаро ва 5 та республика илмий-амалий анжуманларида маъруза қилинган ва муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертация мавзуси бўйича 26 та илмий иш, жумладан Ўзбекисон Республикаси Олий аттестация комиссиясининг докторлик диссертациялари асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 13 та мақола, 10 таси республика журналларида ва 3 таси хорижий журналларда, нашр қилинган, ҳамда 3 та ЭҲМ учун яратилган дастурий воситаларни қайд қилиш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация кириш, бешта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 184 бетни ташкил қилади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг мақсад ва вазифалари, объект ва предмети тавсифланган, тадқиқотнинг республика фан ва технологиялари ривожланишини устувор йўналишларига мослиги кўрсатилган, тадқиқотнинг илмий янгилиги ва амалий натижалари баён қилиган, олинган натижаларнинг ишончлилиги асослаб берилади, олинган натижаларнинг илмий ва амалий аҳамияти очиб берилган, тадқиқот натижаларини амалиётга жорий қилиш, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг «**Ҳимояланган интегралашган бошқариш тизимларини лойиҳалаш усулларини ривожлантиришнинг замонавий ҳолати**» деб номланган биринчи бобида ИЧМ ИБТ тузилишини синтез қилиш бўйича тадқиқот натижалари келтирилган, мавжуд таҳдидлар, АХ заифликлари ва хатарлари, муаммолари ҳамда мураккаб ишлаб чиқариш технологик объектлари инфратузилмасига бўлган салбий электрон таъсирлардан ҳимояланиш ва уларга қаршилик кўрсатиш бўйича истиқболли воситалар таҳлил қилинади.

Замонавий ИЧМ ИБТ кўп босқичли одам-машина бошқариш тизимидан иборатдир. Корхона барча қисм-тизимлари ўртасидаги ўзаро алоқа саноат тармоғи асосида юз беради.

Кўп босқичли саноат тармоғини вазнлаштирилган қирралар ва учларга эга бўлган йўналтирилган мультиграф $G = (D, S)$ кўринишида ифодалаймиз. G граф ёйларининг йўналиши трафик узатиш йўналишини кўрсатади.

Бу ерда $D = \{d_i, i = 1,..., n_d\}$ – турли қурилмалар (датчиклар, контроллерлар, коммутаторлар, компьютерлар ва ҳок.) – ИЧМ ИБТ саноат тармоғига уланган тармоқ объектларидан ташкил топган учлар тўплами.

$S = \{s_l, l = 1,..., n_s\}$ – барча қурилмаларни ягона тармоққа бирлаштирувчи алоқа каналлари билан ифодаланувчи қирралар тўплами. Бу ерда $S \subset D^2$ – қурилмалар ўртасидаги физик боғланишни характерловчи D тўпламдаги бинар муносабат. Унинг учун қуйидаги ўринли:

$$G = (D,S)^{def} =< D,S >,\ D \neq \varnothing \quad S \subset D^2 \ \& \ \forall s \in S(|s| = 2).$$

Интеграллашган бошқариш тизимларига (ИБТ) янги компьютер технологияларининг (IP тармоқлари/Ethernet) қўлланилиши билан ахборот технологияларининг (АТ) таҳдидлари ишлаб чиқариш объектларининг ишлашига салбий таъсир кўрсата бошлади.

Инцидентларга жавоб қайтариш Америка маркази ICS-CERT нинг компания томонидан АХ соҳасидаги 108 та инцидент бўйича маълумотлар таҳлил қилинган 2018 йил учун йиллик ҳисоботида энг кўп инцидентларнинг энергетика (27,4%), нефт ва нефт қазиб олиш саноатида (21,3%), кимё саноатида (11,4%), сув ресурсларини бошқариш (6,3%) ва бошқа ўта муҳим ишлаб чиқаришларда қайд этилганлиги таъкидланади.

ИБТ га бўлган янги таҳдидларга самарали қаршилик кўрсатиш учун АТ соҳасидаги техник ечимлар ИЧМ ИБТ га муваффақиятли қўлланилмоқда.

Бундай техник ечимлар таркибига ҳужумларни аниқлаш тизимлари (ҲАТ), антивируслар ёки суқилиб киришларнинг олдини олиш тизимлари (СКООТ) ҳам киради. ИЧМ ИБТ IP/Ethernet тармоқ инфратузилмасига уланган бир қатор компонентларга (қурилмалар, датчиклар) эга, бироқ антивируслар, ҲАТ ёки хост даражасидаги СКООТ каби ахборот хавфсизлигини (АХ) таъминлаш воситаларини улар учун ҳар доим ҳам ўрнатиб бўлмайди.

Шунинг учун ИЧМ ИБТ ҳимоясини оширишга имкон берувчи истиқболли усуллар, алгоритмлар ва технологияларни тадқиқ қилиш зарурияти юзага келади. Бундай ечимлардан бири сифатида ўрганилаётган объектнинг ўзига хос хусусиятларини ҳисобга олган ҳолда ишлаб чиқариш мажмуалари саноат тармоқлари тармоқ трафигини таҳлил қилиш тизимларини қўллашда кўринади.

Баён қилинганларни ҳисобга олган ҳолда Ўзбекистон Республикаси давлат ва тижорий корхоналари учун янги тизимларни ишлаб чиқиш ва ахборот муҳити ва ҳимоя тизимларини такомиллаштириш зарурияти долзарб ҳисобланади. Бунинг асосида ИЧМ ИБТ, ҳисоблаш техникаси, коммуникацион тизимлар ва жиҳозлар лойиҳаловчилари ва ишлаб чиқарувчилари бўлган етакчи компанияларнинг лойиҳалаш ва технологик ечимлар бўйича жаҳон тажрибаси ҳамда ушбу билимлар тармоғидаги мутахассисларнинг янги илмий натижалари ва таклифлари ётиши керак.

Шунинг учун ИЧМ ИБТ нинг самарали ҳимоясини таъминлаш учун саноат корхоналари компьютер тизимларини лойиҳалаш тизимларини мунтазам равишда такомиллаштириб ва модернизация қилиб бориш зарур. Шу туфайли танланган мавзу долзарб ва зарур ҳисобланади.

Диссертациянинг **«Ҳимояланган интеграллашган бошқариш тизимларини лойиҳалаш концепцияси ва методологиясини ишлаб**

чиқиш» деб номланган иккинчи боби ҳимояланган ИЧМ ИБТ ни лойиҳалаш масалаларига бўлган концептуал ёндашувларни ишлаб чиқиш, ҳимояланган ИБТ ни лойиҳалаш методологиясини ишлаб чиқиш, ИБТ ни лойиҳалаш тамойилларини шакллантириш ҳамда саноат мажмуалари тармоқ трафигини таҳлил қилишнинг аппарат-дастурий тизимлари тузилиши ва ишлаш тамойилларини синтез қилишга бағишланган.

ИЧМ ИБТ АХ даги бугунги кундаги устувор масала бўлиб конфигурацион ва бошқарувчи маълумотлар ва технологик жараён параметрлари ҳақидаги маълумотларнинг ҳаммабоплиги ва бутунлигини таъминлаш бўлиб ҳисобланади.

Шунинг учун хавфсизлик масалаларини тадқиқ қилишда ИБТ ни унинг компонентларининг турли даражалардаги ўзаро алоқаларида кўриб чиқиш зарур, бу эса мураккаб масала бўлиб ҳисобланади.

ИЧМ ИБТ ҳимоясини таъминлаш масаласи яна шу билан мураккаблашадики, автоматлаштирилган тизимларнинг (АвТ) ҳар бир синфи учун қайта ишланаётган ахборот хусусиятлари ва ундан фойдаланиш шартларига мувофиқ тарзда хавфсизликка бўлган аниқ бир талаблар ўрнатилади.

Ўз навбатида, АвТ даги ахборот ҳимояси – АвТ да қайта ишланаётган ахборот ва умуман АвТ хавфсизлигини таъминлашга йўналтирилган фаолият таҳдидларни амалга ошириш имкониятининг олдини олиш ёки уни мураккаблаштиришга ҳамда таҳдидлар амалга оширилиши натижасидаги эҳтимолий зарарлар миқдорини пасайтиришга имкон беради.

Хавфсиз ИЧМ ИБТ ни лойиҳалаш масалаларини ўрганиш хавфсиз ИЧМ ИБТ ни қуришга бўлган энг кенг тарқалган ёндашувлардан бири бўлиб эшелонлашган ҳимоя ҳисобланишини кўрсатади. Эшелонлашган ёндашув ИЧМ ИБТ ҳимояланганлигини таъминлашга бўлган мажмуавий усул ҳисобланади, чунки ушбу ёндашув концепцияси ИЧМ ИБТ нинг ишлашини компьютер тармоғи даражасида кўриб чиқишдан иборатдир ва биринчи навбатда бундай тизимнинг узлуксиз ишлашини таъминлаш асосида қурилади.

Бунда замонавий ИЧМ ИБТ хавфсизлиги технологияси киберхавфсизлик бўйича усуллар, амалий маслаҳатлар ва тавсияларни тартибга солувчи халқаро ISA/IEC- 62443 стандартлари серияси қоидаларига асосланади.

Бироқ эшелонлашган ёндашув билан мажмуавий ҳимоя тизимини қуриш – сермеҳнат ва сезиларли даражадаги инсон ресурслари ва техник воситаларни талаб қилувчи масала.

Паст ва ўртача даражадаги мураккабликка эга бўлган ИБТ қаттиқ молиявий чекланиш шароитида кам сондаги инсон ва техник ресурслар билан лойиҳаланади. Шунинг учун АХ ни таъминлаш масаласи бир четда қолиб кетади ва кўпинча хаттоки кўриб ҳам чиқилмайди.

Шу туфайли ҳозирги вақтда бир қатор тадқиқотчилар киберхавфсизликни ИБТ яратиладиган мақсадлар ёки миссиялар призмаси орқали кўриб чиқишни, яъни миссиоцентрик ёндашувни таклиф қилмоқдалар. Миссиоцентрик ёндашув ахборот тизимига бўлган таҳдидлар

ва унинг заифликларини бутунлик, ҳаммабоплик ва конфиденциаллик нуқтаи назаридан эмас, балки автоматлаштирилиши учун ИБТ дан фойдаланиладиган соҳанинг предмет терминларида таҳлил қилишга имкон беради.

Киберхавфсизлик масаласини ривожлантириш доирасида учта соҳа: саноат хавфсизлиги, функционал хавфсизлик ва ахборот хавфсизлиги методологик аппаратидан фойдаланилади.

Шу билан биргаликда ИЧМ ИБТ ҳимояси даражасига қўйиладиган асосий талаблар, ҳимояланган ИЧМ ИБТ лойиҳалаш жараёнида ишлаб чиқувчилар томонидан тўпланган кўп йиллик тажриба ҳамда бир қатор олимлар ва мутахассисларнинг фикрлари ҳимояланган ИЧМ ИБТ ни лойиҳалашнинг асосий тамойилларини аниқлашга имкон берди.

Иқтисодий самарадорлик тамойили. Бунга кўра Z ҳимоя тизимига бўлган ҳаражатлар $P(Z)$ U таҳдид томонидан етказиладиган $P(U)$ молиявий зарардан катта бўлмаслиги керак: $P(Z) \le P(U)$.

Ўз вақтидалилик ва мослик тамойили – ҳимоя тизими ахборотга бўлган таҳдидларнинг маълум турларини ўз вақтида аниқлаши ва мос тарзда жавоб қайтариши керак. Ҳимоянинг ўз вақтидалилиги, яъни маълум вақт давридаги таҳдид ва ҳимоя нисбати: $Z(t) \ge U(t)$, бу ерда $t \to \min$.

Мажмуавийлик тамойили. Мажмуавий тарзда фойдаланиш корхонада таҳдидларни амалга оширишнинг барча башорат қилинаётган каналларини ёпувчи ва унинг алоҳида компонентларининг ўзаро алоқаларида заиф жойларга эга бўлмаган бутун ҳимоя тизимини қуришда турли типдаги воситаларни мувофиқлаштиришни кўзда тутади.

$Z = \bigcup Z_\chi$, $Z = \sum_{\chi=1}^{\alpha} Z_\chi$ ва ҳар бир z_χ- мажмуа ҳимоя воситаси Z - тизим ИЧМ ИБТ ресурс D_i^λ ҳимоя қилиш учун йўналтирилган бўлиши керак: $Z \xrightarrow{Z_\chi} D_i^\lambda \to \max$.

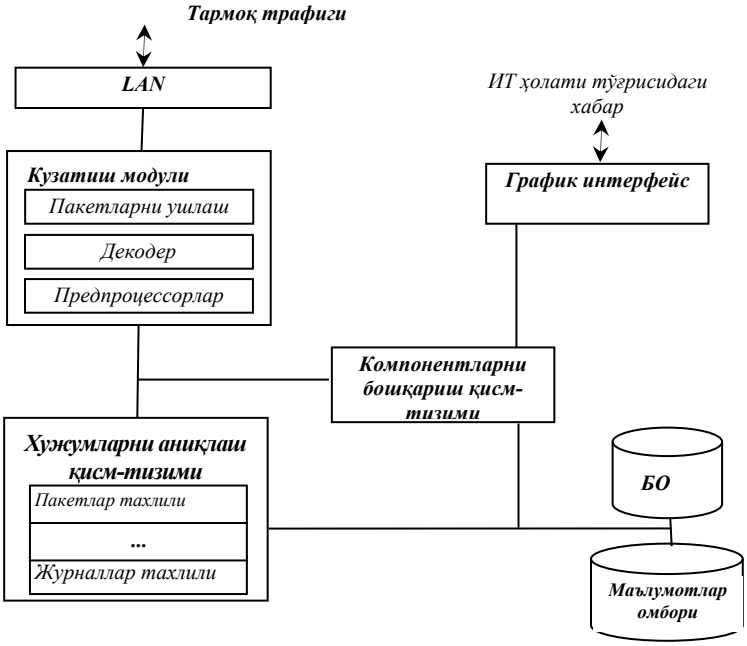
Ўз-ўзини ўқитувчанлик ва мослашувчанлик тамойили – ИБТ ресурсларининг динамик ўзгарувчи таркибига автоматик тарзда тезкор мослашиш қобилияти.

Автономлик тамойили – ташқи билимлар ва экспертлар ҳамда ҳимоянинг қонунийлиги, тизимлилиги, узлуксизлиги, ҳимоя тизимининг мослашувчанлиги, ҳимоя воситаларини қўллашнинг осонлиги тамойилларидан мустақилликдир.

ИЧМ ИБТ ни лойиҳалашда миссиоцентрик ёндашувнинг қўлланилиши ва юқорида кўрсатилган тамойилларга амал қилиниши ИЧМ ИБТ киберхавфсизлигига бўлган таҳдидларнинг учта асосий синфи: саноат хавфсизлигининг бузилиши, ишлаб чиқариш жараёни самарадорлигининг пасайиши, функционал хавфсизлик ва ишончлиликнинг бошқа бузилишларидан ҳимояланганлик билан таъминлашга имкон беради.

Баён қилинганларни ҳисобга олган ҳолда ишда қуйидаги архитектурага эга бўлган тармоқ трафигини мониторинг қилиш ва таниб олишнинг

ишончли тизимларини лойиҳалаш йўли билан ИЧМ ИБТ ҳимоясини таъминлаш усуллари таклиф қилин (1-расм).



1-расм. ИБТ таҳдидлари анализаторининг тузилмавий схемаси

Таклиф қилинган тизимдаги тармоқ трафигини таҳлил қилиш жараёни иккита усулга (сигнатурали таҳлил ва аномалияларни аниқлаш) асосланган. Сигнатурали таҳлил ва аномалияларни аниқлашнинг математик моделлари диссертациянинг учинчи бобида батафсилроқ кўриб чиқилади.

Диссертациянинг **«Дискрет оқимга эга бўлган интегралашган бошқариш тизимларида тармоқ трафигини таҳлил қилиш моделларини ишлаб чиқиш»** деб номланган учинчи бобида саноат тармоқларининг тармоқ трафигидаги аномалияларни таниб олиш усуллари ва алгоритмлари, дискрет маълумотлар оқимига эга бўлган тармоқлардаги тармоқ трафигининг сигнатурали, статистик ва фрактал таҳлиллари жараёнларининг математик моделларини ишлаб чиқиш натижалари келтирилган.

Сигнатурали солиштириш орқали телекоммуникация каналлари бўйича маълумотлар узатишнинг исталмаган пакетларини (фреймларини) қидириш масаласининг математик ифодаланишини қуйидаги кўринишда шакллантириш мумкин: айтайлик, қандайдир матн $T = \{t_1, t_2, ..., t_n\}$ мавжуд бўлсин ва унга шаблонларнинг барча киришларини топиш талаб қилинсин $P = \{p_1, p_2, ..., p_m\}$, бу ерда m ва n - мос ҳолда берилган матн T ва P шаблоннинг ўлчамлари, яъни $m \le n$.

Тадқиқот ишида сатрли қидиришнинг турли алгоритмлари ўрганиб чиқилди. Ўрганиш асосида тармоқ трафигини сигнатурали таҳлил қилиш тизимларида қўллаш мақсадида уларнинг ишлашини таҳлил қилишда амалий амалга ошириш учун кетма-кет (тўғри) қидириш (The Brute Force Algorithm) алгоритми, Бойер-Мур алгоритми, хешлаш ва қисм-сатрларни қидиришнинг иккилик алгоритми (bitap algorithm, shift-or algorithm) танлаб олинди.

Самарали башоратли баҳони олиш учун тармоқнинг юкланганлигини статистик таҳлил қилишнинг математик модели масаласининг қўйилишини қуйидагича баён қилиш мумкин. t_i лар тўпламидан ташкил топган шундай T - вақт берилган бўлсинки, $T=\sum t_i,(i=\overline{1,n})$ бўлсин. Тармоқ трафиги ҳажмини кузатиб бориш сенсори орқали i -кун t_i -вақтда ўтказилган трафик ҳажмини. $D_i(t_j)$ билан белгилаймиз. Табиийки, $K_i(t_j)$- i -кун t_i -вақтда ахборотни кўчириб олувчи ҳисоблаш воситалари (компьютерлар, серверлар, IP-телефония шлюзлари ва ҳок.) сони.

1-жадвал.

Тармоқ трафиги ҳажми, мл·с

t	D_1	K_1	D_2	K_2	....	D_m	K_m
t_1	$D_1(t_1)$	$K_1(t_1)$	$D_2(t_1)$	$K_2(t_1)$		$D_m(t_1)$	$K_m(t_1)$
t_2	$D_1(t_2)$	$K_1(t_2)$	$D_2(t_2)$	$K_2(t_2)$		$D_m(t_2)$	$K_m(t_2)$
.	.	.	.	.	.	.	.
t_n	$D_1(t_n)$	$K_1(t_n)$	$D_2(t_m)$	$K_2(t_n)$	.	$D_m(t_n)$	$K_m(t_n)$

1-жадвал асосида трафик ҳажмининг қуйидаги кетма-кетлигини шакллантирамиз:

$D_1(t_1), D_1(t_2), \ldots, D_1(t_n), D_2(t_1), D_2(t_2), \ldots, D_2(t_m), \ldots, D_m(t_1), D_m(t_2), \ldots, D_m(t_n)$.

Маълумотлар қаторини тенглаштириш ва $D^{\ln}(t)=Ln(D(t))$.экспоненциал кўринишдаги ночизиқлилик бўйича тармоқ трафиги ҳажми маълумотларини силлиқлаш учун ҳар бир олинувчи $D_j(t_i)$ қийматни логарифмлаймиз.

Маълумки, тармоқ трафиги ҳажми ҳақидаги маълумотлар $D_j^{\ln}(t_i)$ 1-жадвалда миллисонияларда (млсон) ифодаланган. Оператор томонидан тармоқ трафиги маълумотлари ифодаланишининг қулай бўлиши ҳамда ўрганилаётган масала мақсадлари учун вақт масштабини (1-жадвалдаги) олинаётган ҳар 10 та $D_j^{\ln}(t_i)$ ёзувни қўшиш ва уларнинг ўрта арифметигини қуйидагича аниқлаш йўли билан млсон. дан сонияларга айлантирамиз:

$$x_1=\frac{(D_1^{\ln}(t_{10})+D_1^{\ln}(t_9)+\ldots+D_1^{\ln}(t_1))}{10}.$$

Натижада қуйидаги қаторни оламиз:

$$x_1=\frac{(D_1^{\ln}(t_{10})+D_1^{\ln}(t_9)+\ldots+D_1^{\ln}(t_1))}{10},\ x_2=\frac{(D_1^{\ln}(t_{11})+D_1^{\ln}(t_{10})+\ldots+D_1^{\ln}(t_2))}{10},$$

$$x_3=\frac{(D_1^{\ln}(t_{12})+D_1^{\ln}(t_{11})+\ldots+D_1^{\ln}(t_3))}{10},\ldots,\ x_n=\frac{(D_1^{\ln}(t_n)+D_1^{\ln}(t_{n-1})+\ldots+D_1^{\ln}(t_{n-10}))}{10}$$

ва ҳок. Натижада трафик ҳажмининг соддалаштирилган белгиланишини олиш мумкин: $x_1, x_2, \ldots, x_n$, бу ерда $i=\overline{1,n}$ - сонияларни, $x(i)$ -тизимнинг i сониядаги юкланганлигининг ўртача арифметик қийматини билдиради. Ҳар бир янги сония билан $x(i)$ қийматлар қатори янги қиймат билан тўлдирилади. Бу

процедура трафик ҳажмини ҳисоблаш ва олдиндан айтиб беришда $D_1^{\ln}(t_i)$ га қараганда турғунроқ бўлган маълумотлар қатори $x(i)$ олишга ҳамда сонияли тартибнинг трендларини ўрганишга имкон беради. $x(i)$ ни ҳисоблаш тадқиқот объектини аниқроқ моделлаштиришга ёрдам беради.

Ўрганилаётган объектнинг математик модели аввалдан тизимнинг ўзига хос хусусиятларини ҳисобга олган ҳолда қурилганлиги учун моделни маълумотлар узатишнинг бошқа тармоқларига унификация қилиш учун қуйидаги коэффициентларни киритамиз:

– k - юқорироқ тартибдаги ўртача арифметик қийматларни ҳисоблаш учун ушланадиган сония қийматларининг сони;

– m – вақт тартиби масштаби коэффициенти. Ўрганилаётган тизимда k =15, m =2 каби белгилаб оламиз.

Тармоқ трафигининг ҳажми ҳақидаги маълумотлар қатори $x(i)$ асосида сирпанувчи ўртачалар учун қуйидаги ўртача арифметик қийматларни ҳисоблаймиз:

$M_j^1 = \frac{(x_i(k) + x_i(k-1) + ... + x_i(k-15))}{k}$ – $x(i)$ нинг сўнгги 15 та қиймати;

$M_j^2 = \frac{(x_i(k \times m) + x_i(k \times m - 1) + ... + x_i(k \times m - 15 \times m))}{k \times m}$ – $x(i)$ нинг сўнгги 30 та қиймати;

$M_j^3 = \frac{(x_i(k \times 2 \times m) + x_i(k \times 2 \times m - 1) + ... + x_i(k \times 2 \times m - 15 \times 2 \times m))}{k \times m}$ – $x(i)$ нинг сўнгги 60 та қиймати.

Шундай қилиб ҳисобланган қийматлар M_j^1, M_j^2 ва M_j^3 тармоқ трафиги ҳажмининг ўртачалаштирилган ўрта арифметик қийматлари ҳисобланади: M_j^1– 15 сонияли ўртачалаштирилган қийматлар, M_j^2 – 30 сонияли ўртачалаштирилган қийматлар, M_j^3 – 60 сонияли ўртачалаштирилган қийматлар.

Агар M_j^1, M_j^2 ва M_j^3 қийматлар k -қадамлар сонини ўзгартириш билан узлуксиз циклда амалга оширилса, динамик-сирпанувчи ойна учун ўртача арифметик қийматларни ҳисоблаш мумкин.

M_j^1, M_j^2 ва M_j^3 учун вақт қаторларидан фойдаланган ҳолда башорат тенгламасини полиномиал боғлиқлик кўринишида ифодалаш мумкин. Тармоқ трафигининг корреляция коэффициенти r-Пирсон алгоритми ёрдамида ҳисобланади.

Дискрет хусусиятларга эга бўлган ҳисоблаш тармоқларидаги трафик аномалияларининг фрактал таҳлилининг математик моделини (1-жадвалга қаранг) қуйидагича ифодалаймиз.

$t_i, \left(i = \overline{1,n}\right)$ – вақт;

$D_j(t_i)$ – i-кундаги t_i - вақтдаги трафик;

$K_j(t_i)$ – i-кундаги t_i - вақтдаги ишлаган компьютерлар сони;

$\lambda = \left(\lambda^1, \lambda^2, ..., \lambda^N\right)$, $\lambda^j \in \{0,1\}$, $j = \overline{1,N}$ вектор ҳосил қилади; бу ерда $\sum_{j=1}^{N} \lambda^j = \ell$

$$\vec{a}_i = \left(\frac{D_i\left(t_{p_1}\right)}{K_i\left(t_{p_1}\right)}, \frac{D_i\left(t_{p_2}\right)}{K_i\left(t_{p_2}\right)}, ..., \frac{D_i\left(t_{p_h}\right)}{K_i\left(t_{p_h}\right)} \right), \quad (\partial = \overline{1,m}).$$

$$\vec{b}_j = \left(\frac{D_j\left(t_{f_1}\right)}{K_j\left(t_{f_1}\right)}, \frac{D_j\left(t_{f_2}\right)}{K_j\left(t_{f_2}\right)}, ..., \frac{D_j\left(t_{f_h}\right)}{K_j\left(t_{f_h}\right)} \right)$$

$$N_a = \frac{(a_i, \lambda)}{(b_j, \lambda)} \tag{1}$$

(1) функция Фишер мезони ҳисобланади. a ва b векторлар компонентлари муносабатларини қуйидагича тартиблаймиз:

$$\frac{a_1}{b_1} \geq \frac{a_2}{b_2} \geq ..... \geq \frac{a_N}{b_N}. \tag{2}$$

Дастлабки ℓ та компонентда аномалия бўлиши мумкин.

У ҳолда $\lambda = \left(\underbrace{1,1,1,...,1}_{\ell}, \underbrace{0,0,0,...,0}_{N-\ell} \right)$.

(1) функционал учун қуйидаги масалани ечамиз:

$$\begin{cases} I(\lambda) = \dfrac{(a,\lambda)}{(b,\lambda)} \to \max; \\ \lambda \in \Lambda^{\ell}, \end{cases} \tag{3}$$

Қуйидаги белгилашларни киритамиз:

$$A = \sum_{i=1}^{l} a_i, \; B = \sum_{i=1}^{l} b_i, \; \begin{cases} \Delta a_{ij} = a_j - a_i \\ \Delta b_{ij} = b_j - b_i, i = \overline{1,l}, j = \overline{l+1,N} \end{cases}, \; \lambda^0 = \left(\underbrace{1,1,...1}_{l\,ma}, \underbrace{0,0,...,0}_{N-l\,ma} \right).$$

Дискрет оқимли тармоқларда сирпанчу дарча шаблонини ҳисоблаш йўли билан тармоқнинг фрактал ҳусусиятлври теоремаси исботланилган.

a, b ва $c \geq 0,\ d > 0\ (a + c \geq 0, b + d > 0)$ ҳақиқий сонлар берилган бўлсин. Тенгсизликлар хусусиятларини ҳисобга олган ҳолда тақдим этилган ифодалардан биридан фойдаланамиз. Тенгсизликларнинг қуйидаги хусусиятларидан бири ўринли:

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}, \text{ бу ерда } a > 0,\ b > 0 \text{ ва } bc > ad, \tag{4}$$

$$\frac{a}{b} > \frac{a+c}{b+d} > \frac{c}{d}, \text{ бу ерда } a > 0,\ b > 0 \text{ ва } cb < ad, \tag{5}$$

$$\frac{a}{b} > \frac{a+c}{b+d} < \frac{c}{d}, \text{ бу ерда } a < 0,\ b < 0 \text{ ва } cb < ad, \tag{6}$$

$$\frac{a}{b} < \frac{a+c}{b+d} > \frac{c}{d}, \text{ бу ерда } a < 0,\ b < 0 \text{ ва } cb > ad, \tag{7}$$

$$\frac{a+c}{b+d} \geq \frac{c}{d}, \text{ бу ерда } a \geq 0,\ b \leq 0 \text{ ва } cb \leq ad, \tag{8}$$

$$\frac{a+c}{b+d} \leq \frac{c}{d}, \text{ бу ерда } a \leq 0,\ b \geq 0 \text{ ва } cb \geq ad, \tag{9}$$

$$\frac{d}{ef} \leq \frac{d+a}{(b+e)(c+f)}, \text{ бу ерда } \frac{a}{d} \geq \frac{b}{e} + \frac{c}{f} + \frac{bc}{ef}, \tag{10}$$

$$\frac{d}{ef} > \frac{d+a}{(b+e)(c+f)}, \text{ бу ерда } \frac{a}{d} < \frac{b}{e} + \frac{c}{f} + \frac{bc}{ef}. \tag{11}$$

Тартибланган кетма-кетлик (2) ёрдамида танланган $\lambda^0 = \left(\underbrace{1,1,...1}_{l\,ma}, \underbrace{0,0,...,0}_{N-l\,ma} \right)$ вектор (3) масалага оптимал ечим бўлиши учун (4) ва (7) тенгсизликлар шартларини қаноатлантирувчи $a = \Delta a_{ij},\ b = \Delta b_{ij}$ мавжуд бўлмаслиги керак.

$\forall \lambda \in \Lambda^l$ ни танлаб оламиз. Танланган λ вектор (3) масаланинг оптимал ечими бўлиши учун (5), (7) ва (8) тенгсизликлар шартларини қаноатлантирувчи $a = \Delta a_{ij},\ b = \Delta b_{ij}\ \left(i = \overline{1,l},\ j = \overline{l+1,N}\right)$ мавжуд бўлмаслиги керак.

Ушбу усулга мос келувчи алгоритм қуйидаги қадамлардан иборат.

1-қадам. $\lambda = \{\underbrace{1,1,...,1}_{\ell}, 0,0,...0\}$ векторга бошланғич қиймат берилади.

2-қадам. А ва В қийматлари ҳисобланади, яъни $A = (a, \lambda)$, $B = (b, \lambda)$.

3-қадам. $i = 1$, $j = N$; $A_1 = A, B_1 = B$.

4-қадам. Δa_{ij} ва Δb_{ij} қийматлари ҳисобланади.

5-қадам. (4) тенгсизликни қаноатлантириш шартлари текширилади. Агар Δa_{ij} ва Δb_{ij} (4) тенгсизлик шартларини қаноатлантирса, тенгсизлик натижалари бўйича λ векторнинг *i*- ва *j*-компоненти жойларини алмаштиради, $A = A + \Delta a_{ij}$, $B = B + \Delta b_{ij}$ ҳисобланади ва 8-қадамга ўтилади, акс ҳолда – кейинги қадамга ўтилади.

6-қадам. (2) тенгсизликни қаноатлантириш шартлари текширилади. Агар Δa_{ij} ва Δb_{ij} (2) тенгсизлик шартларини қаноатлантирса, тенгсизлик натижалари бўйича λ вектор *i*- ва *j*-компонентлари қийматлари ўринларини алмаштиради, $A = A + \Delta a_{ij}$, $B = B + \Delta b_{ij}$ ҳисобланади ва 8-қадамга ўтиш амалга оширилади, акс ҳолда – кейинги қадамга ўтилади.

7-қадам. (5) тенгсизликни қаноатлантириш шартлари текширилади. Агар Δa_{ij} ва Δb_{ij} (5) тенгсизлик шартларини қаноатлантирса, тенгсизлик натижалари бўйича шакл алмаштириш амалга оширилади, λ вектор *i*- ва *j*-компонентлари қийматлари ўринларини алмаштиради, $A = A + \Delta a_{ij}$, $B = B + \Delta b_{ij}$ ҳисобланади ва 8-қадамга ўтилади, акс ҳолда – кейинги қадамга ўтилади.

8-қадам. $j > \ell$ шарт текширилади. Агар $j > \ell$ бўлса, у ҳолда $j = j - 1$ ва 5-қадамга ўтиш амалга оширилади, акс ҳолда – кейинги қадамга ўтилади.

9-қадам. $i < \ell$ шарт текширилади. Агар $i < \ell$ бўлса, у ҳолда $i = i + 1$ бўлади ва 5-қадамга ўтиш амалга оширилади, акс ҳолда – кейинги қадамга ўтилади.

10-қадам. $A_1 = A$ ва $B_1 = B$ шартлар текширилади. Агар $A_1 = A$ ва $B_1 = B$ бўлса, у ҳолда λ – оптимал ечим бўлади ва алгоритм тўхтатилади, акс ҳолда 3-қадамга ўтиш амалга оширилади.

Ҳар бир λ қисм-тизимнинг ℓ-ўлчамли вектори учун ℓ-ўлчамли белгилар фазоси аниқланади ва бунда λ қисм-фазода тегишли Евклид нормаси $\|x\|_\lambda = \sqrt{\sum_{j=1}^{N} \lambda_j \left(x^j\right)^2}$ ни киритамиз.

X_p синфни тавсифловчи ўртача объект $\bar{x}_p$ қуйидагича аниқланади:

$$x_p = \frac{1}{m_p}\sum_{i=1}^{m_p} x_{pi},\ p = \overline{1,r}.$$

Қуйидаги функцияни киритамиз:

$$S_p(\lambda) = \sqrt{\frac{1}{m_p}\sum_{i=1}^{m_p} \left\| x_{pi} - \overline{x}_p \right\|_\lambda^2}\ .$$

$S_p(\lambda)$ функция λ вектор асосида ажратиб олинган X_p синфдаги объектларнинг ўртача четланишини кўрсатади. Информативлик мезони сифатида қуйидаги кўринишдаги функционални оламиз:

$$I_1(\lambda) = \frac{\sum_{p,q=1}^{r} \left\| \overline{x}_p - \overline{x}_q \right\|_\lambda^2}{\sum_{p=1}^{r} S_p^2(\lambda)}.$$

Айтайлик, қуйидаги кўринишдаги мезон берилган бўлсин:

$$I(\lambda) = \frac{(a,\lambda)}{(b,\lambda)(c,\lambda)}.$$

Унга мос масалани кўриб чиқамиз:

$$\begin{cases} I(\lambda) = \dfrac{(a,\lambda)}{(b,\lambda)(c,\lambda)} \to \max, \\ \lambda \in \Lambda^l, \lambda_i = \{0,1\},\ i = \overline{1,N}, \\ a,b \in R^N,\ a_i \ge 0, b_i > 0,\ i = \overline{1,N}. \end{cases}$$

Қуйидаги белгилашларни киритамиз:

$$A = \sum_{i=1}^{l} a_i,\ B = \sum_{i=1}^{l} b_i,\ C = \sum_{i=1}^{l} c_i,\ \begin{cases} \Delta a_{ij} = a_j - a_i, \\ \Delta b_{ij} = b_j - b_i, i = \overline{1,l},\ j = \overline{l+1,N}. \end{cases}$$

$\forall x, y, z$ *ва* $w, e, f > 0$ $(y + e > 0, z + f > 0)$ ҳақиқий сонлар учун қуйидаги тенгсизликлар ўринли:

Агар (10) ва (11) тенгсизликларда $a = \Delta a_{ij}$, $b = \Delta b_{ij}$, $c = \Delta c_{ij}$, $d = A$, $f = C$ қабул қилинса, $e = B$ $\forall i, j$ учун $\begin{cases} A + \Delta a_{ij} \ge 0 \\ B + \Delta b_{ij} > 0 \\ C + \Delta c_{ij} > 0 \end{cases}$ (7) ёки (8) тенгсизликлардан бири ўринли бўлади.

Диссертациянинг **«Интегралашган бошқариш тизимининг ҳимояланганлигини ошириш алгоритмларини ишлаб чиқиш»** номли тўртинчи боби ишлаб чиқариш мажмуаларининг ҳимояланганлигини кучайтириш моделлари ва алгоритмларини ишлаб чиқишга бағишланган. Хусусан, ишлаб чиқариш мажмуалари тармоқларини лойиҳалашда VLAN технологияларининг математик модели, ИБТ даги ахборот ҳимоясининг криптографик усуллари ҳамда сигнатурали ва аномал таҳлил усуллари асосида дискрет оқимли саноат тармоқлари учун трафик таҳлилининг гибрид алгоритми таклиф қилинган.

ИЧМ ИБТ каби кўп босқичли тузилишга эга бўлган тизимлардаги асосий масалалардан бири бўлиб тармоқ трафигининг самарали оқимини ташкиллаштириш ҳисобланади.

Тармоқ трафиги таҳлилининг самарали динамик моделини қуриш мақсадида ҳимояланган ИЧМ ИБТ ни лойиҳалашда «Виртуал тармоқларни» (VLAN) қўллаш таклиф қилинган. Қўлланилган VLAN технологияли ИЧМ ИБТ тузилмасининг математик модели қуйидаги қисм-тармоқлар тўплами билан ифодаланди:

$$M = \left\{ \sum_{i=1}^{n} Ln_i \right\}, (i = 1,..., n_i),$$

бу ерда Ln_i - VLAN қисм-тармоғи D_i^{λ}-қандайдир Ln тегишли деб ҳисобланувчи тармоқдаги қурилмалар соники, бунда $Ln = \sum_{i=1}^{n} ln_i,\ (i = 1,...,n_i)$.

Диссертация ишида VLAN технологияси билан бир қаторда ИБТ саноат тармоқлари каналлари бўйича узатилаётган ахборотни криптоҳимоялаш алгоритми таклиф қилинган. Алгоритм қуйидаги шаклда баён қилинган: алгоритм учун кирувчи маълумотлар X, байтлар учунлиги N, қуйидаги тўртлик саноқ тизимидаги рақамлардан ташкил топган тўртлик саноқ тизимидаги $4N$ рақам узунлигига эга бўлган X_4 кўринишида ифодалаймиз: $0_4,1_4,2_4$ ва 3_4, бунда $X_4 = \overline{x_1, x_2, x_3,..., x_{4N}}$ - $4N$-хонали сон.

Кейин бу рақамлардан ҳар бирининг X_4 даги қатнашишлар сони аниқланади. Бу маълумотлар H_0, H_1, H_2 массив ва H_3 га киритилади.

Кейинги қадамда X_4 да энг кўп учровчи тўртлик c_1 рақами аниқланади. $4N$ та битдан ташкил топувчи битли майдон Y_0 ни $Y_0 = \overline{y_{0,1}, y_{0,2}, y_{0,3},..., y_{0,4N}}$ кўринишда шундай шарт билан қурамизки,

$$y_{0,k} = \begin{cases} 1, агар\ x_k = c_1 \\ 0, агар\ x_k \neq c_1 \end{cases}, \text{ бу ерда } 1 \le k \le 4N.$$

Шундан кейин X_4 дан барча «c_1« ўчирилади, $4N - H_{C_1}$ та тўртлик рақамлардан ташкил топган янги X_3, сатри ҳосил қилинади.

Кейин $X^1{}_3$ да энг кўп учровчи тўртлик рақам c_2 ни аниқлаш операцияси такрорланади, қуйидаги шарт билан $4N - H_{C_1}$ та битдан ташкил топган битлар майдони $Y_1 = \overline{y_{1,0}, y_{1,1}, y_{1,2},..., y_{1,4N-H_{C_1}}}$ қурилади:

$$y_{1,k} = \begin{cases} 1, агар\ x'_k = c_2 \\ 0, агар\ x'_k \neq c_2 \end{cases}, \text{ бу ерда } 1 \le k \le 4N - H_{C_1},$$

X_3 дан барча c_2 рақамлар ўчирилади, $4N - H_{C_1} - H_{C2}$ та тўртлик рақам узунлигидаги X_2^1 кетма-кетликни оламиз.

Кейинги босқичда $X^1{}_2$ да энг кўп учровчи тўртлик c_3 рақамни аниқлаш операцияси такрорланади ва қуйидаги шарт билан $4N - H_{C_1} - H_{C_2}$ та битдан ташкил топган битлар $Y_2 = \overline{y_{2,0}, y_{2,1}, y_{2,2},..., y_{2,4N-H_{C_1}-H_{C2}}}$ қурилади:

$$y_{2,k} = \begin{cases} 1, агар\ x''_k = c_3 \\ 0, агар\ x''_k \neq c_3 \end{cases}, \text{ бу ерда } 1 \le k \le 4N - H_{C_1} - H_{C_2}.$$

Кейин уччала битлар майдони шифрлаш натижаси бўлган битта битлар майдони $Y = Y_0 \| Y_1 \| Y_2$ га бирлаштирилади.

Сигнатурали таҳлил алгоритмлари ёлғон сигналларсиз баён қилинган шаблонлар асосида корхона ҳисоблаш тармоғи бўйлаб ўтувчи зарарли дастур кодларини аниқ аниқлашга имкон беради. Бироқ юқорида айтиб ўтилганидек, сигнатурали усул бир қатор жиддий камчиликларга эга. Шунинг учун айрим корхоналарда тармоқ трафигидаги аномалияларни таҳлил қилиш усулига асосланувчи анализаторлар қўлланилади. Тармоқ трафигидаги аномалияларни таҳлил қилиш усулининг афзаллиги ҳужумлар ва таҳдидларнинг янги ёки аввалари маълум бўлмаган турларини аниқлашга имкон беради. Тармоқ трафигидаги аномалияларни аниқроқ аниқлаш учун ушбу ишда статистик ва фрактал таҳлил қилиш усуллари таклиф қилинади.

Корхоналарнинг тармоқ трифигидаги аномалияларни статистик таҳлил қилиш усулининг ишлаш алгоритми қуйидаги қадамлардан ташкил топади:

1. Тизимга юқорироқ тартибдаги ўртача арифметик қийматларни ҳисоблаш учун ушланувчи сонияли қийматлар миқдори бўлган k параметрлар ва вақт тартиби масштаби коэффициенти - m киритилади;

2. Тармоқ трафигини таҳлил қилиш тизими тармоқ бўйлаб t_j вақтда ўтувчи тармоқ трафиги ҳажми $D_j(t_i)$ ҳақидаги маълумотларни тўплайди ва маълумотлани МБ га ёзади;

3. Ҳажм $D_j(t_i)$ ҳақидаги маълумотлар $D^{\ln}(t) = Ln(D(t))$ тизим томонидан логарифмланади;

4. Тармоқ трафиги ҳажми ҳақидаги миллисонияли маълумотлар $D_j^{\ln}(t_i)$ жамланади ва $x_i = \frac{(D_1^{\ln}(t_n) + D_1^{\ln}(t_{n-1}) + ... + D_1^{\ln}(t_{n-10}))}{10}$ сонияли қийматлар бўйича x_i кўринишида ифодаланади;

5. M_j^1 – 15 сонияли ўртачалаштирилган қийматлар; M_j^2 – 30 сонияли ўртачалаштирилган қийматлар; M_j^3 – 60 сонияли ўртачалаштирилган қийматларга тармоқ трафигининг кутилаётган башорати графигини қуриш учун x_i қийматлари асосида 3 та сирпанувчи ўртачалар маълумотлари қатори шакллантирилади.

$$M_j^1 = \frac{(x_i(k) + x_i(k-1) + ... + x_i(k-15))}{k},$$

$$M_j^2 = \frac{(x_i(k \times m) + x_i(k \times m - 1) + ... + x_i(k \times m - 15 \times m))}{k \times m},$$

$$M_j^3 = \frac{(x_i(k \times 2 \times m) + x_i(k \times 2 \times m - 1) + ... + x_i(k \times 2 \times m - 15 \times 2 \times m))}{k \times m};$$

6. Ҳисобланган вақт қаторлари M_j^1, M_j^2 ва M_j^3 дан фойланиб полиномиал боғлиқлик кўринишидаги башорат тенгламаси қурилади;

7. k ва m коэффициентларига боғлиқ равишда x_i - тармоқ трафиги ҳажми, кутилаётган M_j^1, M_j^2 ва M_j^3 қийматлари маълумотлари графиги ҳисобланади, график қурилади ва диспетчер мониторига чиқарилади.

Таклиф қилинган тармоқ трафигини фрактал таҳлилида сурилувчи ойна шаблонларини ҳисоблаш қуйидаги йўл билан амалга оширилади:

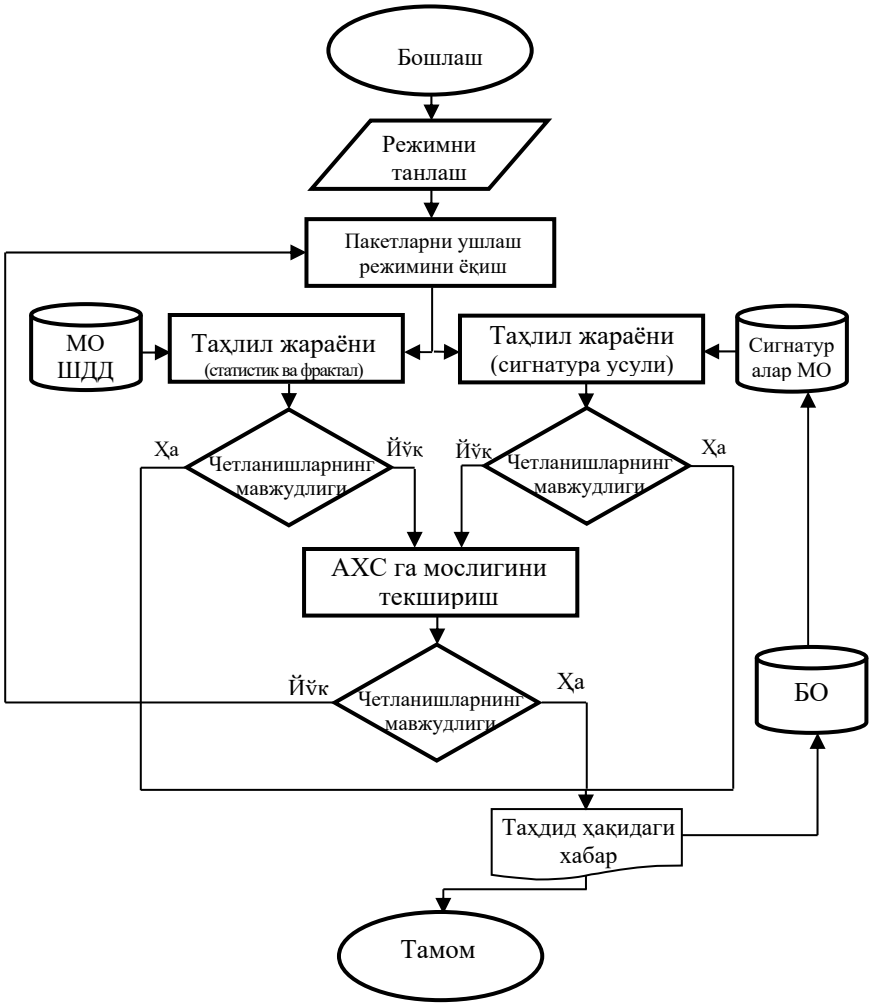
1. Тизим киришига ушланган трафик ҳажми ҳақидаги маълумотлар $D_i(t_i)$ ва $K_i\left(t_j\right)$ – j-куннинг t_j-вақтида ишлаган компьютерлар сони берилади;

2. Ушланган трафик ҳажми ҳақидаги маълумотлар $D_i(t_i)$ билан $K_i\left(t_j\right)$ – ишлаган компьютерлар сонининг нисбати шакллантирилади: $a_i = \left(\frac{D_i(t_{p_1})}{K_i(t_{p_1})}, \frac{D_i(t_{p_2})}{K_i(t_{p_2})}, \ldots, \frac{D_i(t_{p_h})}{K_i(t_{p_h})} \right)$ ва $b_j = \left(\frac{D_j(t_{f_1})}{K_j(t_{f_1})}, \frac{D_j(t_{f_2})}{K_j(t_{f_2})}, \ldots, \frac{D_j(t_{f_h})}{K_j(t_{f_h})} \right)$;

3. Кейин олинган a_i ва b_j қийматлар маълумотлар узатиш тармоғининг турли ишлаш вақти даврларидаги тегишли маълумотлар билан солиштирилади;

4. Ўрнатилган қоидалар асосида тармоқнинг ишлашидаги аномалиялар аниқланади.

Таклиф қилинган тармоқ трафигини таҳлил қилишнинг сигнатурали ва аномал усуллари алгоритмларидан фойдаланиб корхоналар тармоқ трафигини мониторинг қилишнинг гибрид усули алгоритми ишлаб чиқилди (2-расм).



2-расм. ИБТ даги ностандарт вазиятларни таниб олиш гибрид алгоритмининг блок-схемаси

Саноат тармоқларини таҳлил қилишнинг таклиф қилинган гибрид усулининг алгоритми ИЧМ ИБТ архитектурасининг барча даражаларидаги ностандарт вазиятларни аниқроқ, минимал даражадаги ёлғон огоҳлантирувчи сигналлар билан аниқлашга имкон беради. Шу билан бир қаторда таклиф қилинган алгоритм ИЧМ ИБТ ни ҳолатини таҳлил қилиш ва бошқариш тизимларини қисман ўз-ўзини ўқитишга ҳам имкон беради.

«Ҳимояланган интегралашган бошқариш тизимларининг маълумотлар базалари ва дастурий мажмуаларини лойиҳалаш ва ишлаб чиқиш» деб номланган бешинчи бобда ишлаб чиқилган ҳимояланган ИБТ ни лойиҳалаш усуллари, алгоритмлари, дастурий мажмуаларини қўллаш натижалари келтирилади.

Диссертация иши натижалари икки босқичда тажриба-синовдан ўтказилди. Биринчи босқичда бир қатор амалга оширилган моделлар ва алгоритмлар лаборатория шароитларида синовдан ўтказилди. Хусусан, тармоқ трафигининг сигнатурали таҳлили алгоритмларининг (кетма-кет (тўғри) қидириш, Бойер-Мур алгоритми, хешлаш ва қисм-сатрларни иккилик қидириш) ишлашини баҳолаш мақсадларида улар Acer компьютерида синовдан ўтказилди. Алгоритмлар олдига мавжуд $T = \{t_1, t_2, ..., t_n\}$ матндан $P = \{p_1, p_2, ..., p_m\}$ шаблонларни қидириш вазифаси қўйилди, бу ерда $m \le n$.

Қидириш учун лотин ва кириллча шрифтлардаги турли сондаги сўзларга (10 дона, 50 дона, 100 дона) шаблонлар берилди. Кетма-кет қидириш алгоритмларининг C++ дастурлаш тилида амалга оширилган дастурий кодининг ҳажми 777 байтни, Боейер – Мур алгоритминики-1862 байтни, сигнатура бўйича хешлаш алгоритминики -1290 байтни, қисм-сатрларни иккилик қидириш алгоритминики -3217 байтни ташкил қилди, бу эса ССОВ да қўллаш учун яроқли бўлиб ҳисобланади. Барча амалга оширилган дастурларни синовдан ўтказиш Intel Core i5, 2,4 Ггц процессорига эга бўлган, тезкор хотираси 4 Гб бўлган Acer шахсий компьютерида ўтказилди.

Алгоритмлар унумдорлигини баҳолашнинг асосий параметрлари сифатида компьютер томонидан дастурларни бажаришга сарфланган вақтни ва дастурнинг ишлаши учун талаб қилинадиган машина тезкор хотирасининг ҳажмини белгилаймиз. Алгоритмларни солиштириш тажрибасининг натижалари 2-жадвалда келтирилган.

2-жадвал.

Алгоритмларни солиштириш тажрибаси

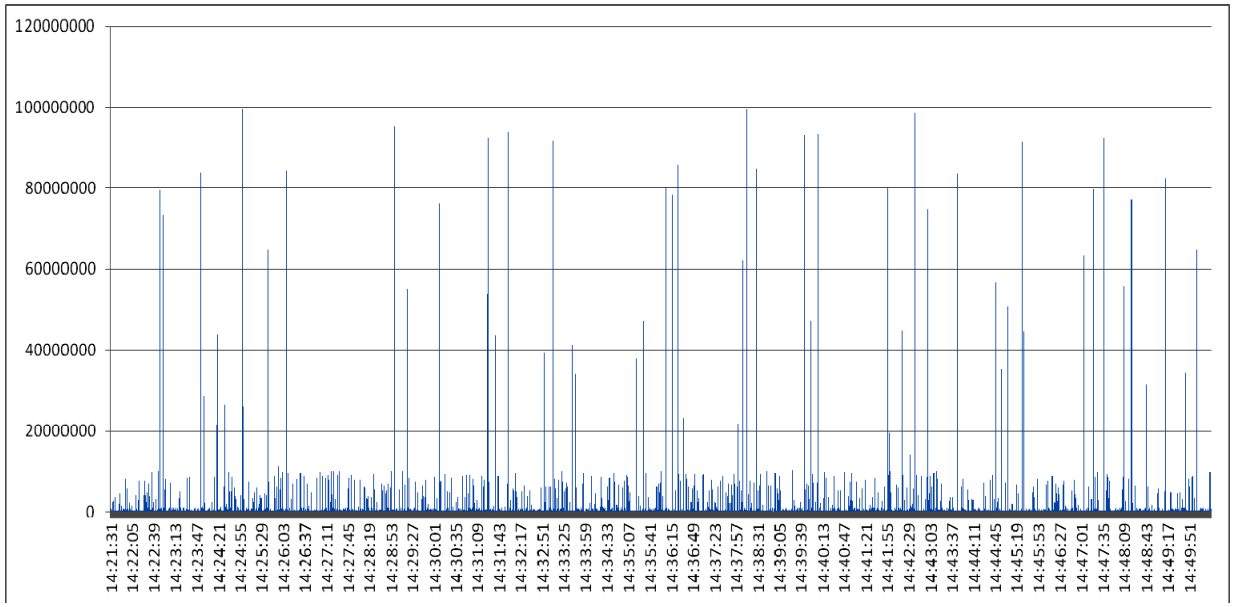
№	Алгоритм номи	Берилган матндан 10 та шаблонни қидириш		Берилган матндан 50 та шаблонни қидириш		Берилган матндан 100 та шаблонни қидириш	
		Қидириш вақти (мс)	Хотира ҳажми (мб)	Қидириш вақти (мс)	Хотира ҳажми (мб)	Қидириш вақти (мс)	Хотира ҳажми (мб)
1.	Кетма-кет (тўғри) қидириш	0,0918	5,3	0.7248	5,4	2,129	5,4
2.	Боейер – Мур	0,1202	5,4	0,6674	5,4	1,6455	5,4
3.	Сигнатура бўйича хешлаш	0,0946	5,4	0,5694	5,4	1,529	5,4
4.	Қисм-сатрни иккилик қидириш	0,1786	5,4	0,8593	5,4	2,1285	5,4

Олинган натижаларнинг таҳлили P шаблон ва T матннинг берилган ҳажми қидириш вақтига сезиларли даражада таъсир қилишини кўрсатади. Бунинг асосий сабаби бўлиб бажариладиган дастурнинг солиштириш операциялари сони ҳисобланади. Шу билан биргаликда талаб қилинадиган тезкор хотира ҳажми (5,4 мб) дастурларнинг ишлаши жараёнида алгоритмларнинг барча турлари учун деярли ўзгаришсиз қолади.

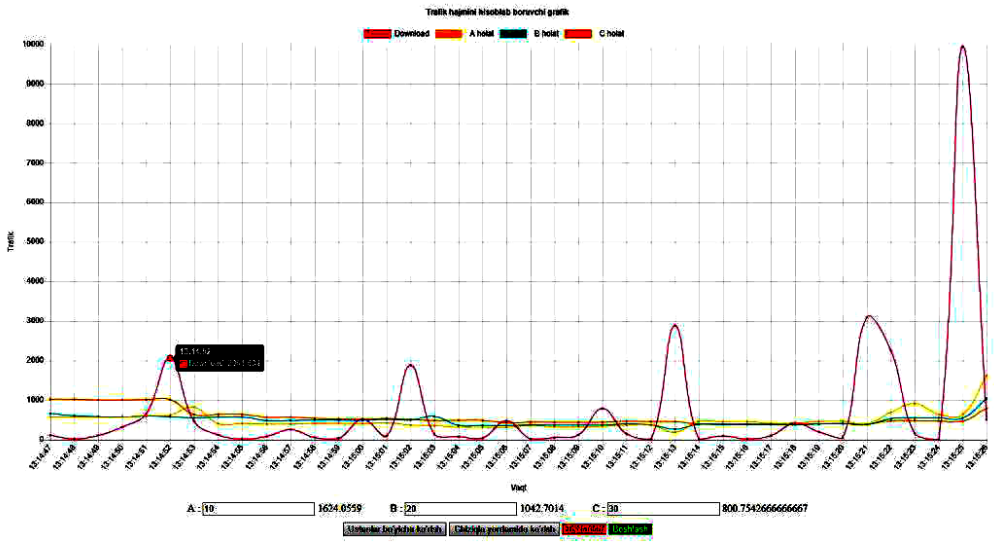
Тажриба натижаларини ҳисобга олган ҳолда юқорида кўриб чиқилган алгоритмлар орасидан таҳлил қилиш тизимларида амалга ошириш учун кэнг қўлланувчани хешлаш ва Боейер-Мул алгоритмлари эканлигини деб айтиш мумкин, чунки телекоммуникацион тизимларда оқиб ўтувчи тармоқ пакетлари оқимларининг ҳажми анчагина баландир.

Иккинчи босқичда ушбу ишда таклиф қилинган моделлар, алгоритмлар ва дастурий мажмуалар Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ахборот ва жамоатчилик хавфсизлиги Маркази, Ўзбекистон Республикаси Марказий банки ахборотлаштириш Бош марказида ҳамда «Жиззах аккумулятор заводи» АЖ да тажрибавий-саноат синовидан ўтказилди.

Моделларни олиш ва амалий фойдаланиш учун Жиззах аккумулятор заводида аккумуляторлар чиқариш технологик жараёнининг нормал ишлаш шароитларида саноат тажрибаси ўтказилди. Завод ИБТ тармоқ трафигини таҳлил қилиш бўйича дастлабки тадқиқотлар объект параметрларига нисбатан сигнатурали усул ва аномалияларни аниқлаш усулини қўллаш мумкинлигини кўрсатди (4-расм). Завод ИБТ ахборот инфратузилмасини сегментация қилиш мақсадида VLAN технологияси қўлланилди. Тажриба-синов ишларини ўтказиш вақти 1 ойни ташкил қилди.



3-расм. Тармоқ трафигининг бошланғич параметрлари



4-расм. ИБТ тармоқ трафигини таҳлил қилиш натижалари

Синов натижалари таклиф қилинган моделлар, алгоритмлар ва тармоқ трафиги аномалияларини аниқлаш ва ИЧМ ИБТ ҳимояланганлигини таъминлаш дастурий мажмуасининг техник-иқтисодий самарадорлигини кўрсатди (4-расм).

Диссертация ишида таклиф қилинган усуллар ва алгоритмларнинг амалий жиҳатдан амалга оширилиши турли корхоналарда саноат шароитларида ижобий натижалар берди.

Синов натижалари таклиф қилинган моделлар, алгоримтлар ва ИЧМ ИБТ ҳимояланганлигини таъминлаш дастурий мажмуасининг техник-иқтисодий жиҳатдан самарадорлигини кўрсатди.

Алгоритмлар ва дастурларни турли корхоналарда амалга ошириш натижасида уларнинг тармоқни таҳлил қилиш қисм-тизимларининг унумдорлиги 12-15 % га ортди, «Жиззах аккумулятор заводи» АЖ да эса кутиладиган иқтисодий самарадорлик йилига 178 118 278,00 сўмни ташкил этди.

ХУЛОСА

Диссертацияда тизимли таҳлил, тизимлар назариялари, математик таҳлил, вақт қаторларининг статистик ва фрактал таҳлили усуллари ҳамда берилган сигнатуралар шаблонларини самарали таниб олиш учун контекстли қидиришнинг математик усуллари асосида ишлаб чиқариш мажмуаларини ҳимояланган интеграллашган бошқариш тизимларини автоматик лойиҳалашнинг конструктив методологияси ишлаб чиқилди.

Натижада қуйидаги илмий натижалар олинди:

1. Ишлаб чиқариш мажмуаларини ҳимояланган интеграллашган бошқариш тизимларини автоматик лойиҳалаш концепцияси ва методологияси ишлаб чиқилди. Таклиф қилинган концепция ва методология эҳтимолий таҳдидларга қарши курашиш ва турли объектларнинг узлуксиз ишлаши ва уларни адаптив бошқаришни таъминлашга имкон беради.

2. Ўрганилаётган объектнинг хусусиятлари, мураккаб ишлаб чиқариш-технологик объектларни бошқариш тизимларига бўлган таҳдидлар ва уларнинг заиф томонларининг таҳлилини ҳисобга олган ҳолда ИЧМ ИБТ тузилмасини ситез қилиш амалга оширилди.

3. Маълумотларнинг тармоқ оқимидаги зарарли кодларни қидириш учун сигнатурали усул алгоритмларининг таҳлили ўтказилди. Таҳлил натижалари энг самарали сатрли қидириш алгоритмларини аниқлашга имкон беради.

4. Статистик таҳлил концепциялари асосида дискрет маълумотлар оқимига эга бўлган ИЧМ ИБТ даги тармоқ трафигини мониторинг қилишнинг математик моделлари ишлаб чиқилди. Олинган моделлар технологик жараённинг ҳақиқий вақтлар режимида тўғри ишлашининг таҳлилини ўтказишга имкон беради.

5. Дискрет маълумотлар оқимига эга бўлган ИЧМ ИБТ даги тармоқ трафигини фрактал таҳлил қилишнинг такомиллаштирилган алгоритмлари ва моделлари ишлаб чиқилди. Таклиф қилинган алгоритмлар ва моделлар ИЧМ ИБТ даги ахборот оқимлари ҳақидаги маълумотларни самарали жамлаш уларни таниб олишни амалга оширишга имкон беради.

6. Ишлаб чиқариш объектларини интеграллашган бошқариш тизимларидаги ахборотни мажмуавий криптографик ҳимоя қилиш алгоритмлари таклиф қилинди. Олинган алгоритмлар бошқарувчи маълумотлар билан рухсатсиз танишиб чиқиш имкониятини аниқлаш ва бунинг олдини олиш ва алоқа каналлари бўйича ахборот узатиш жараёнларини ҳимоя қилиш имкониятини беради.

7. ИЧМ ИБТ даги исталмаган оқимларни мониторинг қилиш ва таниб олишнинг гибрид алгоритмлари ишлаб чиқилди. Таклиф қилинган алгоритмлар ИЧМ ИБТ архитектурасининг турли даражаларидаги мақсадли киберҳужумларни аниқлаш имкониятини беради ва улар қисман ўз-ўзини ўқитиш қобилиятига эга.

8. VLAN-технологияларидан фойдаланиш услубияти таклиф қилинди ва ИБТ тузилмасини синтез қилиш алгоритми ишлаб чиқилди. Таклиф қилинган алгоритм ахборот оқимларини оптималлаштириш ва саноат тармоқлари алоқа каналлари бўйлаб узатилаётган маълумотларни ҳимоя қилишга имкон беради.

9. Ишлаб чиқаришни интеграллашган бошқариш тизимлари маълумотлар базаларининг носозликларга чидамлилигини ошириш усуллари ва алгоритмлари таклиф қилинди. Олинган натижалар саноат мажмуалари МО сақлаш ва заҳиравий нусхалаш тизимларининг юқори даражадаги самарадорлигини таъминлайди.

10. Дискрет маълумотлар оқимига эга бўлган ИБТ даги тармоқ трафигини мониторинг ва башорат қилиш дастурий мажмуаси ишлаб чиқилди. Таклиф қилинган дастурий мажмуа мақсадли ҳужумларни аниқлаш динамикасини акс эттирувчи ҳисоботлар, графикалар ва диаграммаларни визуаллаштиришга имкон беради.

НАУЧНЫЙ СОВЕТ DSc.27.06.2017.T.03.02 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ ГОСУДАРСТВЕННОМ ТЕХНИЧЕСКОМ УНИВЕРСИТЕТЕ

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИСМАИЛОВ ОТАБЕК МИРХАЛИЛОВИЧ

МЕТОДЫ И АЛГОРИТМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ИНТЕГРИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ КОМПЛЕКСАМИ

05.01.08 – Автоматизация и управление технологическими процессами и производствами

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА НАУК (DSc) ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент – 2019

Тема диссертации доктора наук (DSc) зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за №B2018.4.DSc/T244

Диссертация выполнена в Ташкентском государственном техническом университете.

Автореферат диссертации на трёх языках (узбекский, русский, английский (резюме)) размещен на веб-странице по адресу www.tdtu.uz и на Информационно-образовательном портале «ZiyoNet» по адресу www.ziyonet.uz.

Научный консультант:	**Юсупбеков Нодирбек Рустамбекович** доктор технических наук, профессор, академик
Официальные оппоненты:	**Камилов Мирзаян Мирзаахмедович** доктор технических наук, профессор, академик
	Игамбердиев Хусан Закирович доктор технических наук, профессор, академик
	Каримов Мажит Маликович доктор технических наук, профессор
Ведущая организация:	**Бухарский инженерно-технологический институт**

Защита диссертации состоится «___» _____ 2019 года в ___ часов на заседании Научного совета DSc.27.06.2017.T.03.02 при Ташкентском государственном техническом университете по адресу: 100095, г.Ташкент, ул. Университетская, 2. Тел: (99871) 246-46-00; факс: (99871) 227-10-32; e-mail: tstu_info@tdtu.uz.

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского государственного технического университета (зарегистрировано за №__). Адрес: 100095, г. Ташкент, ул. Университетская, 2. Тел.: 246-03-41.

Автореферат диссертации разослан «____» _____ 2019 г.
(реестр Протокола рассылки №___ от «____» _____ 2019 г.)

Ф.Т.Адилов
Заместитель председателя Научного совета
по присуждению учёных степеней,
доктор технических наук, профессор

У.Ф.Мамиров
Ученый секретарь Научного совета
по присуждению учёных степеней,
доктор философии по техническим наукам (PhD)

Х.З. Игамбердиев
Председатель Научного семинара
при Научном совете по присуждению учёных степеней,
доктор технических наук, профессор, академик

ВВЕДЕНИЕ (аннотация диссертации доктора наук (DSc))

Актуальность и востребованность темы диссертации. В последнее время в мире в области автоматизации технологических процессов и производств одной из важнейших задач является разработка методов и алгоритмов автоматизированного проектирования защищенных интегрированных систем управления производственными комплексами (ИСУ ПК). В этой области особое внимание уделяется разработке унифицированных моделей и алгоритмов мониторинга состояния функционирования промышленных сетей, а также своевременного выявления возможных угроз и адаптивного реагирования на них в режиме реального времени. В связи с этим разработка различных методов мониторинга, идентификации и обеспечения защищенности промышленных объектов является одной из основных задач.

В мире ведутся научно-исследовательские работы по созданию универсального подхода к проектированию защищенных промышленных комплексов, ориентированных на решение задач противодействия возможным угрозам, обеспечения бесперебойного функционирования и адаптивного управления объектами при различных угрозах. В этой связи совершенствование и модификация методов и алгоритмов автоматизированного проектирования защищенных ИСУ ПК на основе концепций миссиоцентрического подхода, разработка методов и алгоритмов статистического и фрактального анализов сетевого трафика в ИСУ ПК с дискретным потоком данных, создание методов и алгоритмов адаптивного реагирования на угрозы, возникающие в инфраструктуре промышленных комплексов, являются важной задачей.

В республике большое внимание уделяется направлениям автоматизации и управления, а также проектированию защищенных ИСУ ПК, обеспечивающих бесперебойное функционирование технологических процессов и производств. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017–2021 гг. отмечены задачи, в том числе по «… сокращению энергоемкости и ресурсоемкости экономики, широкому внедрению в производство энергосберегающих технологий, повышению производительности труда в отраслях экономики, … внедрению информационно-коммуникационных технологий в экономику, социальную сферу, системы управления»[1]. Решение данных проблемы, в том числе разработка современных методов и алгоритмов, позволяющих повысить уровень защиты ИСУ ПК, является одной из основных задач.

Данное диссертационное исследование в определённой степени служит выполнению задач, предусмотренных Указом Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан» и Постановлениями

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

Президента Республики Узбекистан №ПП–1730 от 21 марта 2012 г. «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий», №ПП–3151 от 27 июля 2017 г. «О мерах по дальнейшему расширению участия отраслей и сфер экономики в повышении качества подготовки специалистов с высшим образованием» и №ПП–3682 от 27 апреля 2018 г. «О мерах по дальнейшему совершенствованию системы практического внедрения инновационных идей, технологий и проектов», а также другими нормативно-правовыми документами, принятыми в данной сфере.

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

Обзор зарубежных научных исследований по теме диссертации[2]. Научные исследования, направленные на разработку и усовершенствование методов и алгоритмов автоматизированного проектирования защищенных интегрированных систем управления производственными комплексами, осуществляются в ведущих научных центрах мира и высших образовательных учреждениях, в том числе «Honeywell», Rockwell Automation*,* Inc*.,* University of California, Massachusetts Institute of Technology (США), «Check Point Software Technologies» (США, Израиль), Technical University Munich, Karlsruhe Institute of Technology, Technical University Darmstadt (Германия), Imperial College London, The University of Edinburgh (Великобритания), Linksping University (Швеция), University of Chemical Technology in Prague (Чехия), The University of Tokyo, Tokyo Institute of Technology (Япония), Seoul National University, Korea Advanced Institute of Science and Technology (Южная Корея), Институте автоматики (Китай), Научно-техническом центре «Станкоинформзащита», Московском государственном техническом университете им. Н.Э.Баумана, Санкт-Петербургском институте информатики и автоматизации, Самарском государственном университете (Россия), Туринском политехническом институте, Ташкентском государственном техническом университете, Ташкентском университете информационных технологий (Узбекистан).

В результате исследований, проведенных в мире по разработке методов и алгоритмов автоматизированного проектирования защищенных ИСУ ПК, а также по усовершенствованию систем защиты в области автоматизации производства и технологических процессов, получен ряд научных результатов, в том числе: созданы методы и алгоритмы защиты устройств

[2] Обзор научных исследований по теме диссертации: https://www.honeywell.com, https://www.rockwellautomation.com/site-selection.html, https://www.universityofcalifornia.edu, http://web.mit.edu, https://www.checkpoint.com, https://www.tum.de, https://www.kit.edu, https://www.tu-darmstadt.de, http://www.imperial.ac.uk, https://www.ed.ac.uk, https://liu.se, https://www.vscht.cz/?jazyk=en, https://www.u-tokyo.ac.jp/en/index.html, https://www.titech.ac.jp/english, http://en.snu.ac.kr, http://www.kaist.edu, http://english.ia.cas.cn, https://www.ntcsiz.ru, http://www.bmstu.ru, http://www.spiiras.nw.ru, https://polito.uz, http://tdtu.uz, https://tuit.uz и других источников.

ИСУ ПУ нижнего уровня («Honeywell», University of California, Massachusetts Institute of Technology, George Mason University, США; Институт проблем управления Российской Академии наук, Россия); разработаны алгоритмы обеспечения защиты от несанкционированного доступа к объектам управления (прямых команд управления, изменения параметров режима и противоаварийной защиты, а также подмены значений измерений) ИСУ ПК («Фонд перспективных исследований», Россия); разработаны алгоритмы и аппаратно-программные комплексы по обеспечению безопасности критических инфраструктур ИСУ ПК (серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и других ключевых систем информационной инфраструктуры) (Massachusetts Institute of Technology, США; Linksping University, Швеция; «Modcon Systems», Великобритания; Seoul National University, Южная Корея; Московский государственный технический университет им.Н.Э.Баумана, Санкт-Петербурский институт информатики и автоматизации, Россия); разработаны методы и алгоритмы мониторинга технических неисправнистей аппаратных средств автоматизированных систем управления («Honeywell», США; Seoul National University, Южная Корея; Tokyo Institute of Technology, Япония; Научно-технический центр «Станкоинформзащита», Россия); разработаны методы и алгоритмы проектирования ИСУ ПК нефтегазовой, химической, биотехнологической отраслей производства («Honeywell», США; Научно-технический центр «Станкоинформзащита», Россия); разработаны программно-технические комплексы автоматического управления системой сигнализации, блокировки и мониторинга электроэнергетической и транспортной отраслей производства («Honeywell», США; Linksping University, Швеция; Научно-технический центр «Станкоинформзащита», Россия).

В мире для решения задач по усовершенствованию разрабатываемых методов и алгоритмов автоматизации проектирования защищенных ИСУ ПК проводится ряд исследований по следующим перспективным направлениям, в том числе выявление угроз в системах, имеющих сложные динамические процессы, оценка риска и усовершенствование управления; управление несанкционированным доступом в ресурсы и объекты управляемых; системы мониторинга нестандартных ситуаций и оповещения при функционировании промышленных объектов; разработка адаптивных систем управления и противодействия угрозам; разработка моделей, обеспечивающих независимое функционирование систем управления при внешних и внутренних возмущающих воздействях.

Степень изученности проблемы. Большой вклад в разработку методов, моделей и алгоритмов автоматизированного проектирования интегрированных систем управления производственными комплексами внесли многие зарубежные ученые – такие, как J.C. Smith, D.J. Howard, R.N. Selin, R. Lippmann, R. Kwitt, A. Ghosh, E. Eskin, N. Cristianini, M. Salem, H. Amstrong, P. Barford, J. Kline, H. J. Kim, P. Casas, В.А. Артамонов, Д.Ю. Гамаюнов, Ю.В. Писецкий, С. Гордейчик, В. Дубровин, В.И. Маркоменко,

Р.В. Базаев, В.А. Конявский, В.А. Галатенко и др., а также отечественные ученые А.А. Абдукадиров, Б.М. Азимов, О.П. Ахмедова, Т.Ф. Бекмуратов, Ш.М. Гулямов, И.И. Жуманов, О.О. Зарипов, Х.З. Игамбердиев, А.А. Кадыров, Н.З. Камалов, М.М. Камилов, М.М. Каримов, А.Р. Марахимов, Т.Р. Нурмухамедов, М.А. Рахматуллаев, О.Х. Расулова, И.Х Сиддиков, Ш.Х. Фозилов, Н.Р. Юсупбеков и др.

Анализ трудов зарубежных и отечественных ученых свидетельствует о том, что методы обеспечения безопасности информации, предлагаемые ими, в основном, направлены на построение многоуровневой модели безопасности и в эшелонированном подходе к организации защиты ИСУ ПК либо ограничиваются минимальными средствами – такими, как криптографическая защита. В частности, О.П. Ахмедова, О.Х. Расулов, М.М. Каримов предлагают различные аппаратно-программные средства кодировки данных, которые обеспечивают защиту данных в информационных системах.

Анализ исследований в данной области показывает, что на современном этапе для обеспечения бесперебойной обработки данных в защищенных интегрированных системах управления промышленными комплексами, выявления угроз промышленным системам в целях обеспечения целостности информации, разработки адаптивных систем противодействия и исследования передовых методов защиты каналов передачи данных задачи создания адаптивных систем и технологии защиты промышленных предприятиях изучены недостаточной степени.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках проектов на тему №Ф-4-56 «Разработка теоретических основ и методов структурно-параметрического синтеза на основе нечеткого множества интеллектуальных систем управления сложными технологическими объектами» (2012–2016); №А-5-42 «Программно-инструментальные средства интеллектуализации автоматизированного мониторинга и управления технологическими объектами в условиях априорной неопределенности» (2015–2017); №ОТ-Ф4-78 «Разработка теоретических основ и регулярных методов синтеза адаптивных систем управления динамическими объектами на основе идентификационного подхода» (2017–2020); №ОТ-Ф7-88 «Совершенствование теоретических основ перспективных энерго- и ресурсосберегающих тепломассообменных процессов сложных химико-технологических систем получения чистых продуктов» (2017–2020) согласно плану научно-исследовательских работ Ташкентского государственного технического университета.

Целью исследования является разработка методов и алгоритмов автоматизированного проектирования защищенных интегрированных систем управления производственными комплексами от внешних и внутренних угроз.

Задачи исследования:

разработка концепции и методологии проектирования защищенных интегрированных систем управления производственными комплексами в условиях унификации информационных и промышленных технологий;

разработка алгоритмов синтеза структуры, а также анализа угроз и уязвимостей систем управления сложными производственно-технологическими объектами;

разработка математической модели анализа аномалий сетевого трафика производственных комплексов;

разработка алгоритмов идентификации аномалий сетевого трафика интегрированных систем управления;

разработка алгоритмов повышения защищенности интегрированных систем управления производственных комплексов;

разработка гибридного алгоритма и программных комплексов выявления кибератак интегрированных систем управления;

разработка алгоритмов обеспечения бесперебойного функционирования систем хранения и резервирования баз данных промышленных комплексов.

Объектом исследования является процесс электронного воздействия на информационные ресурсы интегрированных систем управления производственными комплексами.

Предметом исследования являются разработка и совершенствование мер, моделей, алгоритмов, баз данных и программных комплексов по противодействию электронным угрозам защищенных ИСУ ПК.

Методы исследования. В процессе исследования применены системно-сравнительный и системно-функциональный подходы, анализ систем управления, структурно-параметрические методы синтеза систем управления, статистический и фрактальный анализы временных рядов, моделирование и прогнозирование.

Научная новизна исследования заключается в следующем:

разработаны концепция и методология, а также определены основные принципы проектирования защищенных интегрированных систем управления производственными комплексами в условиях унификации информационных и промышленных технологий;

разработана структура защищенной интегрированной системы управления производственными комплексами с учетом свойств исследуемого объекта, анализа угроз и уязвимостей систем управления сложными производственно-технологическими объектами;

разработаны модернизированные математические модели мониторинга сетевого трафика в защищенных интегрированных системах управления производственными комплексами с дискретным потоком данных на основе концепций статистического анализа;

разработаны усовершенствованные алгоритмы и модели фрактального анализа сетевого трафика в защищенных интегрированных системах управления производственными комплексами с дискретным потоком;

разработаны алгоритмы комплексной криптографической защиты информации в интегрированных системах управления производственными объектами;

разработаны гибридные алгоритмы мониторинга и идентификации нежелательных потоков в защищенных интегрированных системах управления производственными комплексами, обладающие способностью частичного самообучения;

разработаны методы и алгоритмы повышения отказоустойчивости баз данных интегрированных систем управления производством.

Практические результаты исследования заключаются в следующем:

разработкан алгоритм, позволяющий проведение мониторинга технологических режимов и идентификации неисправностей, выявление нежелательных сетевых трафиков технологических процессов переработки лома свинца и приготовления сплавов;

разработаны методы и алгоритмы повышения отказоустойчивости баз данных интегрированных систем управления технологическими процессами переработки лома свинца и приготовления сплавов в производстве аккумуляторов;

разработаны алгоритмы криптографической защиты информации в комплексе технологического процесса переработки лома свинца и приготовления сплавов;

разработан программный комплекс для решения задач идентификации угроз защищенных интегрированных систем управления, проведения мониторинга угроз производственных комплексов технологических процессов переработки лома свинца и приготовления сплавов.

Достоверность результатов исследования. Достоверность полученных результатов исследования обеспечивается выполнением методически обоснованных теоретических выкладок, структурно-параметрический синтез систем управления, использованием апробированных методов и алгоритмов современных теорий управления, статистического и фрактального анализов временных рядов, полученными результатами теоретических и прикладных исследований и их взаимной согласованностью.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования состоит в разработке конструктивных методов, моделей и алгоритмов автоматизированного проектирования защищенных интегрированных систем управления производственными комплексами, позволяющих повысить надежность и безопасность процессов функционирования производства.

Практическая значимость результатов работы обосновывается возможностью использования предложенных методов, моделей, алгоритмов и программ автоматизированного проектирования защищенных интегрированных систем управления для новых производственных, а также аналогичных объектов и их отдельных подсистем.

Внедрение результатов исследования. На основе полученных результатов по разработке методов и алгоритмов автоматизированного

проектирования защищенных интегрированных систем управления производственными комплексами:

разработанные гибридные алгоритмы мониторинга и идентификации нежелательных потоков в защищенных интегрированных системах управления производственными комплексами, обладающие способностью частичного самообучения, алгоритмы комплексной криптографической защиты информации в интегрированных системах управления производственными объектами и методы и алгоритмы повышения отказоустойчивости баз данных интегрированных систем управления производством внедрены в Главном центре информатизации Центрального банка Республики Узбекистан (Справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан за №33–8/1449 от 28 февраля 2019 г.). В результате повысилась производительность системы анализа сетевого трафика на 12 %;

разработанные модернизированные математические модели мониторинга сетевого трафика в защищенных ИСУ ПК с дискретным потоком данных на основе концепций статистического анализа и усовершенствованные алгоритмы и модели фрактального анализа сетевого трафика в защищенных ИСУ ПК с дискретным потоком внедрены в АО «Джизакский аккумуляторный завод» (Справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан за №33–8/1449 от 28 февраля 2019 г.). В результате реализации разработанных математических моделей и алгоритмов совершенствования системы мониторинга промышленных сетей защищенных ИСУ ПК достигнута возможность их бесперебойного функционирования;

разработанные концепции и методологии, а также определенные основные принципы проектирования защищенных интегрированных систем управления производственными комплексами в условиях унификации информационных и промышленных технологий внедрены в Центре информационной и общественной безопасности Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан, а также в ГУП «UNICON.UZ» (Справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан за №33–8/1449 от 28 февраля 2019 г.). В результате эффективность системы мониторинга трафика защищенных ИСУ ПК повысилось на 15 %.

Апробация результатов исследования. Теоретические и практические результаты диссертационного исследования докладывались и обсуждались на 3 международных и 5 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По теме диссертации опубликовано всего 26 научных работ, из них 13 научных статей, в том числе 10 – в республиканских и 3 – в зарубежных журналах, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, 8 тезисов докладов

на международных и республиканских научных конференциях, а также получены 3 свидетельства об официальной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 184 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснованы 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 апробаций результатов работы, сведения по опубликованным работам и структуре диссертации.

В первой главе – **«Современное состояние развития методов проектирования защищенных интегрированных систем управления»** – приводятся результаты исследования синтеза структуры ИСУ ПК, проанализированы проблемы существующих угроз, уязвимостей и рисков информационной безопасности (ИБ), а также перспективных средств защиты и адаптивного противодействия негативным электронным воздействиям на инфраструктуру сложных производственно-технологических объектов.

Современная ИСУ ПК представляет собой многоуровневую человеко-машинную систему управления. Взаимодействие между всеми подсистемами предприятия происходит на основе промышленной сети.

Многоуровневую промышленную сеть представим в виде ориентированного мультиграфа со взвешенными ребрами и вершинами $G=(D,S)$, где направление дуг графа G указывает направление передачи трафика.

Здесь $D=\{d_i, i=1,...,n_d\}$ – множество вершин, состоящее из различных устройств (датчиков, контроллеров, коммутаторов, компьютеров и т.д.), т.е. объектов сети, подключенных к промышленной сети ИСУ ТП;

$S=\{s_l, l=1,..., n_s\}$ – множество ребер, представленных каналами связи, соединяющими все устройства в единую сеть; $S \subset D^2$ – бинарное отношение на множестве D, характеризующее физическое соединение между устройствами такое, что

$$G=(D,S)^{def} =< D,S >,\ D \neq \varnothing\ ,\ S \subset D^2\ \&\ \forall s \in S(|s|=2)\ .$$

С внедрением новых компьютерных технологий (сетей IP/Ethernet) в интегрированные системы управления, угрозы информационных технологий (ИТ) начали негативно влиять на функционирование производственных объектов.

В ежегодном отчете Американского центра реагирования на инциденты ICS-CERT за 2018 г., в котором компания проанализировала информацию по 108 инцидентам в области ИБ, отмечено, что наибольшее число инцидентов зафиксировано в областях энергетики (27,4%), нефтяной и нефтеобрабатывающей промышленности (21,3%), химической промышленности (11,4%), управления водными ресурсами (6,3%) и на других критически важных производствах.

Для более эффективного противостояния новым угрозам ИСУ технические решения ИТ сферы успешно внедряются в ИСУ ПК.

В состав таких технических решений входят и системы обнаружения атак (СОА), антивирусы или системы предотвращения вторжений (СПВ). Однако в ИСУ ПК имеется ряд компонентов (устройств, датчиков), подключенных к сетевой инфраструктуре IP/Ethernet, но для них не всегда возможна установка средств обеспечения информационной безопасности – таких, как антивирусы, СОА или СПВ на уровне хоста.

В этой связи возникает необходимость в исследовании перспективных методов, алгоритмов и технологий, позволяющих повысить защиту ИСУ ПК. Одним из таких решений видится внедрение систем анализа сетевого трафика промышленных сетей производственных комплексов с учетом специфики объекта исследования.

С учетом изложенного представляется актуальной необходимость разработки новых систем и совершенствования информационной среды и систем защиты для государственных и коммерческих предприятий Республики Узбекистан. Основу этого должны составлять мировой опыт проектирования и технологические решения ведущих компаний проектировщиков и производителей ИСУ ПК, вычислительной техники, коммуникационных систем и оборудования, а также новые научные результаты и предложения специалистов в данной отрасли знаний.

Следовательно, для обеспечения эффективной защиты ИСУ ПК необходимо постоянно совершенствовать и модернизировать системы проектирования компьютерных систем промышленных предприятий. В связи с этим выбранная тема является актуальной и своевременной.

Вторая глава диссертации – **«Разработка концепции и методологии проектирования защищенных интегрированных систем управления»** – посвящена разработке концептуальных подходов в задачах проектирования защищенных ИСУ ПК, выработке методологии проектирования защищенных ИСУ, формулированию принципов проектирования защищенных ИСУ, а также синтезу структуры и принципов функционирования аппаратно-программных систем анализа сетевого трафика промышленных комплексов.

Сегодняшним приоритетом в ИБ ИСУ ПК является обеспечение доступности и целостности конфигурационной и управляющей информации, и информации о параметрах технологического процесса.

В этой связи при исследовании проблем безопасности необходимо рассматривать ИСУ на различных уровнях взаимодействия ее компонентов, что является сложной задачей.

Задача обеспечения защиты ИСУ ПК усложняется еще тем, что для каждого класса автоматизированных систем (АС) в соответствии со свойствами обрабатываемой информации и условиями ее эксплуатации устанавливаются конкретные требования к безопасности.

В свою очередь, защита информации в АС – деятельность, которая направлена на обеспечение безопасности обрабатываемой в АС информации и АС в целом, – позволяет предотвратить или усложнить возможность реализации угроз, а также снизить величину потенциальных убытков в результате реализации угроз.

Изучение вопросов проектирования безопасных ИСУ ПК показывает, что одним из распространенных подходов к построению защищенных ИСУ ПК служит эшелонированная защита. Эшелонированный подход является комплексным методом обеспечения защищенности ИСУ ПК, так как концепция данного подхода заключается в рассматривании функционирования ИСУ ТП на уровне работы компьютерной сети и строится на обеспечении, в первую очередь, бесперебойности работы такой системы.

При этом современная технология безопасности ИСУ ПК базируется на основных положениях серии международных стандартов ISA/IEC- 62443, которые регламентируют методы, практические советы и рекомендации по киберзащите.

Однако построение комплексной системы защиты эшелонированным подходом – задача весьма кропотливая и требующая значительных человеческих ресурсов и технических средств.

ИСУ малой и средней сложности проектируется малыми человеческими и техническими ресурсами в условиях жесткой финансовой ограниченности. Поэтому вопрос обеспечения ИБ остается в стороне и чаще всего даже не рассматривается.

В связи с этим в настоящее время ряд исследователей предлагают рассматривать кибербезопасность сквозь призму цели или миссии, для которой создается ИСУ, т.е. миссиоцентрический подход. Миссиоцентрический подход позволяет анализировать угрозы и уязвимости информационной системы не в контексте обеспечения целостности, доступности и конфиденциальности, но в терминах предметной области, для автоматизации которой используется ИСУ.

В рамках развития вопроса кибербезопасности используется методологический аппарат трех дисциплин: промышленной безопасности, функциональной безопасности и информационной безопасности.

При этом основные требования, предъявляемые к уровню защиты ИСУ ПК, многолетний опыт, накопленный разработчиками в процессе проектирования защищенных ИСУ ПК, а также высказывания ряда ученых и специалистов позволили выявить следующие основные принципы проектирования защищенных ИСУ ПК:

Принцип экономической эффективности. В соответствии с этим принципом – затраты $P(Z)$ на систему защиты Z не должны превышать финансовый ущерб $P(U)$, наносимый U -угрозой: $P(Z) \le P(U)$.

Принцип своевременности и адекватности – система защиты должна вовремя выявлять и соответственно реагировать на определенные виды угроз информации. Своевременность защиты, т.е. соотношение угрозы и защиты к определенному временному периоду: $Z(t) \geq U(t)$, где $t \to \min$.

Принцип комплексности. Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты на предприятии, перекрывающей все прогнозируемые каналы реализации угроз и не содержащей уязвимых мест во взаимодействии отдельных ее компонентов:

$Z = \bigcup Z_\chi$, $Z = \sum_{\chi=1}^{\alpha} Z_\chi$ и каждое z_χ – средство защиты комплекса Z -системы должно быть направлено на защиту D_i^λ -ресурса ИСУ ПК: $Z \xrightarrow{Z_\chi} D_i^\lambda \to \max$.

Принцип самообучаемости и адаптируемости – способность автоматически оперативно подстраиваться к динамически изменяющемуся содержимому ресурсов – ИСУ.

Принцип автономности – независимость от внешних баз знаний и экспертов, а также принципов законности, системности, непрерывности защиты, гибкости системы защиты, простоты применения средств защиты.

Применение миссиоцентрического подхода и соблюдение вышеуказанных принципов в проектировании ИСУ ПК позволит обеспечить защищенность от трех основных классов угроз кибербезопасности ИСУ ПК: нарушения промышленной безопасности, снижения эффективности производственного процесса, других нарушений функциональной безопасности и надежности.

С учетом изложенного в диссертации предлагаются методы обеспечения защиты ИСУ ПК путем проектирования надежных систем мониторинга и идентификации сетевого трафика с архитектурой, представленной на рис.1.

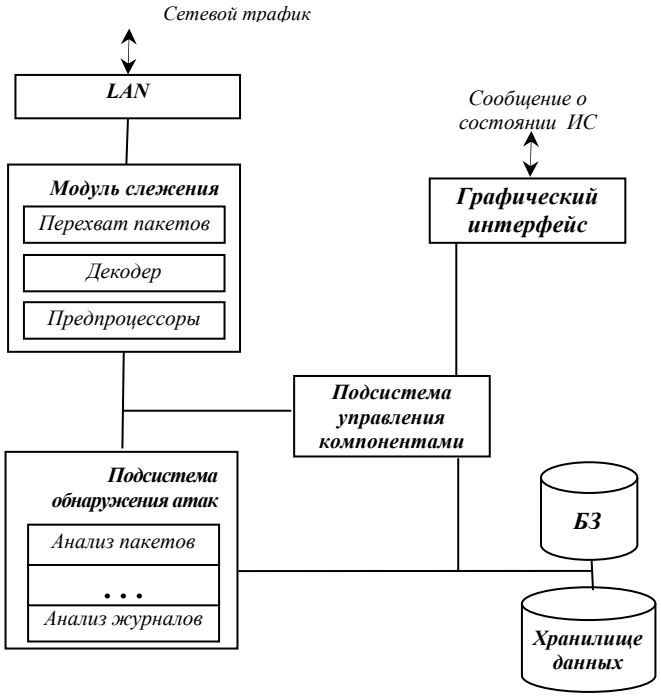


Рис.1. Структура анализатора угроз ИСУ

Процесс анализа сетевого трафика в предложенной структуре основан на двух стратегиях – анализа сигнатур и идентификации аномалий. Математические модели идентификации сигнатур (шаблонов) и выявления аномалий более подробно исследованы в третьей главе диссертации.

В третьей главе диссертации – **«Разработка моделей анализа сетевого трафика в интегрированных системах управления с дискретным потоком»** – приводятся результаты разработки методов и алгоритмов идентификации аномалий сетевого трафика промышленных сетей, математических моделей процессов сигнатурного, статистического и фрактального анализов сетевого трафика в сетях с дискретным потоком данных.

Математическую постановку задачи поиска нежелательных пакетов (кадров) транзакции записей по каналам коммуникационной связи путем сопоставления шаблонов можно сформулировать в следующем виде: пусть существует некоторый текст $T = \{t_1, t_2, ..., t_n\}$ и необходимо обнаружить любое вхождения в него сигнатур $P = \{p_1, p_2, ..., p_m\}$, где m и n – соответственно размеры исходного текста T и шаблона P, т.е. $m \le n$.

В диссертации исследованы различные методы строкового сопоставления. На основе полученных результатов выбраны алгоритм последовательного (прямого) поиска (The Brute Force Algorithm), алгоритм Бойера–Мура, хеширование и двоичный алгоритм поиска подстроки (bitap algorithm, shift-or algorithm) для практической реализации в анализе их функционирования с целью применения в системах сигнатурного анализа сетевого трафика.

Постановку задачи математической модели статистического анализа загруженности сети для получения эффективной прогностической оценки можно описать следующим образом. Пусть дано T – время, состоящее из множества t_i такое, что $T = \sum t_i, (i = \overline{1,n})$. Обозначим $D_j(t_i)$ объемом трафика, пропущенным через сенсор слежения объема сетевого трафика в t_i-время i-го дня. Естественно, $K_j(t_i)$ – количество вычислительных средств (компьютеры, сервера, шлюзы IP-телефонии и т.д.), закачиваемых информацию в t_i время i-го дня.

Таблица 1

Объем сетевого трафика, мл·с

t	D_1	K_1	D_2	K_2	....	D_m	K_m
t_1	$D_1(t_1)$	$K_1(t_1)$	$D_2(t_1)$	$K_2(t_1)$		$D_m(t_1)$	$K_m(t_1)$
t_2	$D_1(t_2)$	$K_1(t_2)$	$D_2(t_2)$	$K_2(t_2)$		$D_m(t_2)$	$K_m(t_2)$
.	.	.	.	.	.	.	.
t_n	$D_1(t_n)$	$K_1(t_n)$	$D_2(t_m)$	$K_2(t_n)$	.	$D_m(t_n)$	$K_m(t_n)$

На основании табл. 1 сформируем объем трафика в следующей последовательности:

$$D_1(t_1), D_1(t_2), \ldots, D_1(t_n), D_2(t_1), D_2(t_2), \ldots, D_2(t_m), \ldots, D_m(t_1), D_m(t_2), \ldots, D_m(t_n).$$

Каждое поступающее значение $D_j(t_i)$ логарифмируем, чтобы выровнять ряд данных и сгладить данные объема сетевого трафика по нелинейности экспотенциального вида $D^{\ln}(t) = Ln(D(t))$.

Как известно, $D_j^{\ln}(t_i)$ данные об объеме сетевого трафика в табл. 1 приведены в миллисекундах (мл·с). Для удобства представления информации операторам мониторинга сетевого трафика, а также целей исследуемой задачи масштаб времени в табл. 1 из мл·с. преобразуем в секунды путем суммирования каждых 10 новых поступающих $D_i^{\ln}(t_j)$ записей и определяем их среднеарифметическое значение такое, что

$$x_1 = \frac{(D_1^{\ln}(t_{10}) + D_1^{\ln}(t_9) + ... + D_1^{\ln}(t_1))}{10}.$$

В результате получим следующий ряд:

$$x_1 = \frac{(D_1^{\ln}(t_{10}) + D_1^{\ln}(t_9) + ... + D_1^{\ln}(t_1))}{10},\ x_2 = \frac{(D_1^{\ln}(t_{11}) + D_1^{\ln}(t_{10}) + ... + D_1^{\ln}(t_2))}{10},$$

$$x_3 = \frac{(D_1^{\ln}(t_{12}) + D_1^{\ln}(t_{11}) + ... + D_1^{\ln}(t_3))}{10}, ..., x_n = \frac{(D_1^{\ln}(t_n) + D_1^{\ln}(t_{n-1}) + ... + D_1^{\ln}(t_{n-10}))}{10}$$ и т.д.

Таким образом, можно получить упрощенное обозначение объема трафика: $x_1, x_2, ..., x_n$, где $i = \overline{1,n}$ – обозначает секунды, а $x(i)$ – логарифм среднеарифметического значения загруженности системы в секунду i. С каждой новой секундой ряд значений $x(i)$ пополняется новым значением. Эта процедура позволяет получить ряд данных $x(i)$, являющийся более устойчивым, чем $D_1^{\ln}(t_j)$ при вычислении и прогнозировании объема трафика, а также исследовать тренды секундного порядка. Вычисления $x(i)$ способствуют более точному моделированию объекта исследования.

Так как математическая модель исследуемого объекта изначально строится на основе учета специфических особенностей системы, то для унификации модели под другие сети передачи данных введем следующие коэффициенты:

- k – количество секундных значений, захватываемых для расчета среднеарифметических значений более высокого порядка;
- m – коэффициент масштаба временного порядка. Пусть в исследуемой системе определим k =15, m =2.

На основе ряда данных $x(i)$ об объеме сетевого трафика предпримем попытку вычислить следующие среднеарифметические значения для скользящих средних:

$M_j^1 = \frac{(x_i(k) + x_i(k-1) + ... + x_i(k-15))}{k}$ – последние 15 значений $x(i)$;

$M_j^2 = \frac{(x_i(k \times m) + x_i(k \times m - 1) + ... + x_i(k \times m - 15 \times m))}{k \times m}$ – последние 30 значений $x(i)$;

$M_j^3 = \frac{(x_i(k \times 2 \times m) + x_i(k \times 2 \times m - 1) + ... + x_i(k \times 2 \times m - 15 \times 2 \times m))}{k \times m}$ – последние 60 значений $x(i)$.

Таким образом, вычисленные значения M_j^1, M_j^2 и M_j^3 являются усредненными среднеарифметическими значениями объема сетевого трафика: M_j^1 – 15-секундные усредненные значения, M_j^2 – 30-секундные усредненные значения, M_j^3 – 60-секундные усредненные значения.

Если значения M_j^1, M_j^2 и M_j^3 осуществлять в непрерывном цикле с изменением количества шагов k, то можно вычислить средне-арифметические значения для динамическо-скользящего окна.

Используя временные ряды для M_j^1, M_j^2 и M_j^3, можно сформулировать уравнения прогноза в виде полиномиальной зависимости. Коэффициент корреляции сетевого трафика вычисляется алгоритмом r-Пирсона.

Математическую модель фрактального анализа аномалий трафика в вычислительных сетях с дискретными характеристиками (см. табл.1) сформулируем следующим образом:

$t_i, \left(i = \overline{1,n}\right)$ – время;

$D_j(t_i)$ – трафик в t_i-е время i-го дня;

$K_j(t_i)$ – количество работавших компьютеров в t_i-е время i-го дня;

$\lambda = (\lambda^1, \lambda^2, ..., \lambda^N)$, $\lambda^j \in \{0,1\}$, $j = \overline{1,N}$ – формирует вектор; здесь $\sum_{j=1}^{N} \lambda^j = \ell$;

$$\vec{a}_i = \left(\frac{D_i\left(t_{p_1}\right)}{K_i\left(t_{p_1}\right)}, \frac{D_i\left(t_{p_2}\right)}{K_i\left(t_{p_2}\right)}, ..., \frac{D_i\left(t_{p_h}\right)}{K_i\left(t_{p_h}\right)} \right), \quad (\partial = \overline{1,m}).$$

$$\vec{b}_j = \left(\frac{D_j\left(t_{f_1}\right)}{K_j\left(t_{f_1}\right)}, \frac{D_j\left(t_{f_2}\right)}{K_j\left(t_{f_2}\right)}, ..., \frac{D_j\left(t_{f_h}\right)}{K_j\left(t_{f_h}\right)} \right)$$

$$N_a = \frac{(a_i, \lambda)}{(b_j, \lambda)} \tag{1}$$

Функция (1) является критерием Фишера. Упорядочим отношения компонентов векторов a и b следующим образом:

$$\frac{a_1}{b_1} \geq \frac{a_2}{b_2} \geq ..... \geq \frac{a_N}{b_N}. \tag{2}$$

В первых ℓ компонентах возможна аномалия.

Тогда $\lambda = \left(\underbrace{1,1,1,...,1}_{\ell}, \underbrace{0,0,0,...,0}_{N-\ell} \right)$.

Для функционала (1) решим следующую задачу:

$$\begin{cases} I(\lambda) = \dfrac{(a,\lambda)}{(b,\lambda)} \to \max; \\ \lambda \in \Lambda^{\ell}, \end{cases} \tag{3}$$

Введем следующие обозначения:

$$A = \sum_{i=1}^{l} a_i, \; B = \sum_{i=1}^{l} b_i, \; \begin{cases} \Delta a_{ij} = a_j - a_i \\ \Delta b_{ij} = b_j - b_i, i = \overline{1,l}, j = \overline{l+1,N} \end{cases}, \; \lambda^0 = \left(\underbrace{1,1,...1}_{l\,ma}, \underbrace{0,0,...,0}_{N-l\,ma} \right).$$

Доказаны теоремы о фрактальных свойствах сетевого трафика путем вычисления шаблонов скользящего окна в сетях с дискретным потоком.

Пусть даны действительные числа a, b и $c \geq 0,\ d > 0\ (a + c \geq 0, b + d > 0)$. Учитывая свойства неравенств, используем одно из представленных выражений. Справедливо одно из следующих свойств неравенств:

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}, \text{ где } a > 0,\ b > 0 \text{ и } bc > ad, \quad (4)$$

$$\frac{a}{b} > \frac{a+c}{b+d} > \frac{c}{d}, \text{ где } a > 0,\ b > 0 \text{ и } cb < ad, \quad (5)$$

$$\frac{a}{b} > \frac{a+c}{b+d} < \frac{c}{d}, \text{ где } a < 0,\ b < 0 \text{ и } cb < ad, \quad (6)$$

$$\frac{a}{b} < \frac{a+c}{b+d} > \frac{c}{d}, \text{ где } a < 0,\ b < 0 \text{ и } cb > ad, \quad (7)$$

$$\frac{a+c}{b+d} \geq \frac{c}{d}, \text{ где } a \geq 0,\ b \leq 0 \text{ и } cb \leq ad, \quad (8)$$

$$\frac{a+c}{b+d} \leq \frac{c}{d}, \text{ где } a \leq 0,\ b \geq 0 \text{ и } cb \geq ad, \quad (9)$$

$$\frac{d}{ef} \leq \frac{d+a}{(b+e)(c+f)}, \text{ где } \frac{a}{d} \geq \frac{b}{e} + \frac{c}{f} + \frac{bc}{ef}, \quad (10)$$

$$\frac{d}{ef} > \frac{d+a}{(b+e)(c+f)}, \text{ где } \frac{a}{d} < \frac{b}{e} + \frac{c}{f} + \frac{bc}{ef}. \quad (11)$$

Для того, чтобы вектор $\lambda^0 = \left(\underbrace{1,1,\ldots 1}_{l\,ma}, \underbrace{0,0,\ldots,0}_{N-l\,ma} \right)$, выбранный с помощью упорядоченной последовательности (2), являлся оптимальным решением для задачи (3), необходимо, чтобы не существовали $a = \Delta a_{ij}$, $b = \Delta b_{ij}$, удовлетворяющие условиям неравенств (4) и (7).

Выберем $\forall \lambda \in \Lambda^l$. Для того, чтобы выбранный вектор λ являлся оптимальным решением задачи (3), необходимо, чтобы не существовали $a = \Delta a_{ij}$, $b = \Delta b_{ij}$ $\left(i = \overline{1,l},\ j = \overline{l+1,N}\right)$, удовлетворяющие условиям неравенств (5), (7) и (8).

Алгоритм, соответствующий данному методу, состоит из следующих шагов.

Шаг 1. Задается начальное значение вектора $\lambda = \{\underbrace{1,1,\ldots,1}_{\ell}, 0, 0, \ldots 0\}$.

Шаг 2. Вычисляются значения A и B, т.е. $A = (a, \lambda)$, $B = (b, \lambda)$.

Шаг 3. $i = 1$, $j = N$; $A_1 = A, B_1 = B$.

Шаг 4. Вычисляются значения Δa_{ij} и Δb_{ij}.

Шаг 5. Проверяются условия удовлетворения неравенству (4). Если Δa_{ij} и Δb_{ij} удовлетворяют условиям неравенства (4), то по результатам неравенства значения *i*-го и *j*-го компонентов вектора λ меняются местами, вычисляются $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$ и осуществляется переход к *шагу 8*, иначе – к следующему шагу.

Шаг 6. Проверяются условия удовлетворения неравенству (2). Если Δa_{ij} и Δb_{ij} удовлетворяют условиям неравенства (2), то по результатам неравенства значения *i*-го и *j*-го компонентов вектора λ меняются местами, вычисляются $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$ и осуществляется переход к *шагу 8*, иначе – к следующему шагу.

Шаг 7. Проверяются условия удовлетворения неравенству (5). Если Δa_{ij} и Δb_{ij} удовлетворяют условиям неравенства 5, то по результатам неравенства осуществляются преобразования, т.е. значения *i*-го и *j*-го компонентов вектора λ меняются местами, вычисляются $A = A + \Delta a_{ij}, B = B + \Delta b_{ij}$ и осуществляется переход к *шагу 8*, иначе – к следующему шагу.

Шаг 8. Проверяется условие $j > \ell$. Если $j > \ell$, то $j = j - 1$ и осуществляется переход к *шагу 5*, иначе – к следующему шагу.

Шаг 9. Проверяется условие $i < \ell$. Если $i < \ell$, то $i = i + 1$ и осуществляется переход к *шагу 5*, иначе – к следующему шагу.

Шаг 10. Проверяются условия $A_1 = A$ и $B_1 = B$. Если $A_1 = A$ и $B_1 = B$, то $\lambda -$ оптимальное решение, и алгоритм останавливается, иначе осуществляется переход к *шагу 3*.

Для ℓ-мерного вектора каждой подсистемы λ определено ℓ-мерное признаковое пространство и в этом λ подпространстве введем соответствующую Евклидову норму $\|x\|_\lambda = \sqrt{\sum_{j=1}^{N} \lambda_j \left(x^j\right)^2}$.

Средний объект $\bar{x}_p$, характеризующий класс X_p, определяется следующим образом:

$$x_p = \frac{1}{m_p} \sum_{i=1}^{m_p} x_{pi},\ p = \overline{1,r}.$$

Введем следующую функцию:

$$S_p(\lambda) = \sqrt{\frac{1}{m_p} \sum_{i=1}^{m_p} \left\| x_{pi} - \bar{x}_p \right\|_\lambda^2}.$$

Функция $S_p(\lambda)$ показывает среднее отклонение объектов в классе X_p, выделенных на основе вектора λ. В качестве критерия информативности возьмем функционал вида

$$I_1(\lambda) = \frac{\sum_{p,q=1}^{r} \left\| \bar{x}_p - \bar{x}_q \right\|_\lambda^2}{\sum_{p=1}^{r} S_p^2(\lambda)}.$$

Допустим, что дан критерий вида

$$I(\lambda) = \frac{(a,\lambda)}{(b,\lambda)(c,\lambda)}.$$

Рассмотрим соответствующую ему задачу:

$$\begin{cases} I(\lambda)=\dfrac{(a,\lambda)}{(b,\lambda)(c,\lambda)}\to \max, \\ \lambda\in\Lambda^l,\lambda_i=\{0,1\},\ i=\overline{1,N}, \\ a,b\in R^N,\ a_i\ge 0,b_i>0,\ i=\overline{1,N}. \end{cases}$$

Введем следующие обозначения:

$$A=\sum_{i=1}^{l}a_i,\ B=\sum_{i=1}^{l}b_i,\ C=\sum_{i=1}^{l}c_i,\ \begin{cases}\Delta a_{ij}=a_j-a_i,\\ \Delta b_{ij}=b_j-b_i, i=\overline{1,l},\ j=\overline{l+1,N}.\end{cases}$$

Для действительных чисел $\forall x,y,z$ *ва* $w,e,f>0\ (y+e>0,z+f>0)$ справедливы следующие неравенства:

Если в неравенствах (10) и (11) принять $a=\Delta a_{ij}, b=\Delta b_{ij}, c=\Delta c_{ij}$, $d=A$, $f=C$, то $e=B$ для $\forall i,j$ $\begin{cases}A+\Delta a_{ij}\ge 0,\\ B+\Delta b_{ij}>0\\ C+\Delta c_{ij}>0.\end{cases}$ будет справедливо одно из неравенств (7) или (8).

Четвертая глава диссертации – **«Разработка алгоритмов повышения защищенности интегрированных систем управления»** – посвящена разработке моделей и алгоритмов усиления защищенности производственных комплексов. В частности, предложены математическая модель VLAN – технологий в проектировании сетей производственных комплексов, методы криптографической защиты информации в ИСУ, а также на основе методов сигнатурного и аномального анализов гибридный алгоритм анализа трафика для промышленных сетей с дискретным потоком.

Одной из основных задач в системах с многоуровневой структурой как ИСУ ПК является организация эффективного потока сетевого трафика.

С целью построения эффективной динамической модели анализа сетевого трафика предложено применение технологии «Виртуальные сети» (VLAN) в проектировании защищенных ИСУ ПК. Математическая модель структуры ИСУ ТП с внедрённой технологией VLAN представляется набором следующих подсетей:

$$M=\left\{\sum_{i=1}^{n}Ln_i,\ \right\},(i=1,...,n_i),$$

где Ln_i – подсеть VLAN; D_i^{λ} – множество устройств сети, считающееся принадлежащим некоторой Ln, такое, что $Ln=\sum_{i=1}^{n}ln_i,\ (i=1,...,n_i)$.

Наряду с VLAN-технологией в диссертационной работе предложен алгоритм криптозащиты информации, передаваемой по каналам промышленных сетей ИСУ. Алгоритм описан в следующей форме: входные данные X для алгоритма длиной N байтов представим в виде четверичной системы счисления X_4 длиной $4N$ цифр, состоящей из четверичных цифр: $0_4,1_4,2_4$ и 3_4, чтобы $X_4=\overline{x_1,x_2,x_3,...,x_{4N}}$, где $4N$ – значное число.

Далее определяется количество участия каждой из этих цифр в X_4. Эти данные вносятся в массив H_0, H_1, H_2 и H_3.

На следующем шаге определяется четверичная цифра c_1, наиболее часто встречающаяся в X_4. Построим битовое поле Y_0, состоящее из $4N$ бит, $Y_0 = \overline{y_{0,1}, y_{0,2}, y_{0,3}, ..., y_{0,4N}}$ с таким условием, чтобы

$$y_{0,k} = \begin{cases} 1, если\ x_k = c_1, \\ 0, если\ x_k \neq c_1, \end{cases} \text{здесь } 1 \le k \le 4N .$$

После этого из X_4 удаляются все «c_1«, образуется новая строка X_3, состоящая из $4N - H_{C_1}$ четверичных цифр.

Далее повторяется операция определения наиболее часто встречающейся в X^1_3 четверичной цифры c_2. Строится битовое поле $Y_1 = \overline{y_{1,0}, y_{1,1}, y_{1,2}, ..., y_{1,4N-H_{C_1}}}$, состоящее из $4N - H_{C_1}$ бит с условием

$$y_{1,k} = \begin{cases} 1, если x'_k = c_2, \\ 0, где x'_k \neq c_2, \end{cases} \text{где } 1 \le k \le 4N - H_{C_1} .$$

В X_3 удаляются все цифры c_2 и получается последовательность X^1_2 длиной $(4N - H_{C_1} - H_{C2})$ четверичных цифр.

На следующем этапе повторяется операция определения наиболее часто встречающейся в X^1_2 четверичной цифры c_3 и строится битовое поле $Y_2 = \overline{y_{2,0}, y_{2,1}, y_{2,2}, ..., y_{2,4N-H_{C_1}-H_{C2}}}$ длиной $(4N - H_{C_1} - H_{C_2})$ бит с условием

$$y_{2,k} = \begin{cases} 1, если\ x''_k = c_3, \\ 0, если\ x''_k \neq c_3, \end{cases} \text{где } 1 \le k \le (4N - H_{C_1} - H_{C_2}) .$$

Далее все три битовые поля объединяются в единое битовое поле $Y = Y_0 \| Y_1 \| Y_2$, которое является результатом шифрования.

Алгоритмы сигнатурного анализа позволяют на основе описанного шаблона без ложных сигналов точно выявлять вредоносные программные коды, проходящие по вычислительной сети предприятия. Однако, как было отмечено ранее, сигнатурный метод имеет ряд существенных недостатков. В этой связи на некоторых предприятиях применяются анализаторы, базирующиеся на методе анализа аномалий в сетевом трафике. Преимущество метода анализа аномалий сетевого трафика заключается в возможности выявлять новые или ранее неизвестные типы атак и угроз. Для более точного определения аномалий сетевого трафика в данной диссертации предлагаются статистический и фрактальный методы анализа.

Алгоритм функционирования статистического метода анализа аномалий сетевого трафика предприятий состоит из следующих шагов:

1. В систему вводятся параметры: k – количество секундных значений, захватываемых для расчета среднеарифметических значений более высокого порядка, и m – коэффициент масштаба временного порядка.

2. Система анализа сетевого трафика собирает информацию об объеме $D_i(t_j)$ сетевого трафика, проходящего t_j-период времени по сети, и записывает данные в БД.

3. Данные об объеме $D_i(t_i)$ логарифмируются системой $D^{\ln}(t) = Ln(D(t))$.

4. Миллисекундные данные $D_i^{\ln}(t_j)$ об объеме сетевого трафика суммируются и представляются в виде x_i посекундных значений $x_i = \frac{(D_1^{\ln}(t_n) + D_1^{\ln}(t_{n-1}) + ... + D_1^{\ln}(t_{n-10}))}{10}$.

5. С учетом значений x_i формируется 3 ряда данных скользящих средних для построения графика ожидаемого прогноза сетевого трафика на M_j^1 – 15-секундные усредненные значения; M_j^2 – 30-секундные усредненные значения; M_j^3 – 60-секундные усредненные значения.

$$M_j^1 = \frac{(x_i(k) + x_i(k-1) + ... + x_i(k-15))}{k},$$

$$M_j^2 = \frac{(x_i(k \times m) + x_i(k \times m - 1) + ... + x_i(k \times m - 15 \times m))}{k \times m},$$

$$M_j^3 = \frac{(x_i(k \times 2 \times m) + x_i(k \times 2 \times m - 1) + ... + x_i(k \times 2 \times m - 15 \times 2 \times m))}{k \times m}.$$

6. На основе использования вычисленных временных рядов M_j^1, M_j^2 и M_j^3 строится уравнение прогноза в виде полиномиальной зависимости.

7. Строится график данных значения x_i – объема сетевого трафика, ожидаемого на M_j^1, M_j^2 и M_j^3, в зависимости от коэффициента k и m и выдается на монитор диспетчера.

Предложенный фрактальный анализ сетевого трафика путем вычисления шаблонов скользящего окна осуществляется следующим образом:

1. На вход системы подаются данные $D_i(t_i)$ об объеме захваченного трафика и $K_i(t_j)$ о количестве работавших компьютеров в t_j-е время j-го дня.

2. Формируется соотношение между данными $D_i(t_i)$ об объеме захваченного трафика и $K_i(t_j)$ о количестве работавших компьютеров:

$$a_i = \left(\frac{D_i(t_{p_1})}{K_i(t_{p_1})}, \frac{D_i(t_{p_2})}{K_i(t_{p_2})}, ..., \frac{D_i(t_{p_h})}{K_i(t_{p_h})} \right) \text{ и } b_j = \left(\frac{D_j(t_{f_1})}{K_j(t_{f_1})}, \frac{D_j(t_{f_2})}{K_j(t_{f_2})}, ..., \frac{D_j(t_{f_h})}{K_j(t_{f_h})} \right).$$

3. Далее полученные значения a_i и b_j сопоставляются с соответствующими данными в различные периоды времени работы сети передачи данных.

4. На основе установленных правил определяются аномалии в функционировании сети.

С использованием предложенных алгоритмов сигнатурного и аномального методов анализа сетевого трафика был выработан алгоритм гибридного метода мониторинга сетевого трафика предприятий (рис.2).

Предложенный алгоритм гибридного метода анализа промышленных сетей позволит более точно, с минимальной степенью ложных тревог, идентифицировать нестандартные ситуации на всех уровнях архитектуры ИСУ ПК. Наряду с этим он предоставляет возможность для частичного самообучения систем анализа и управления состояния ИСУ ПК.

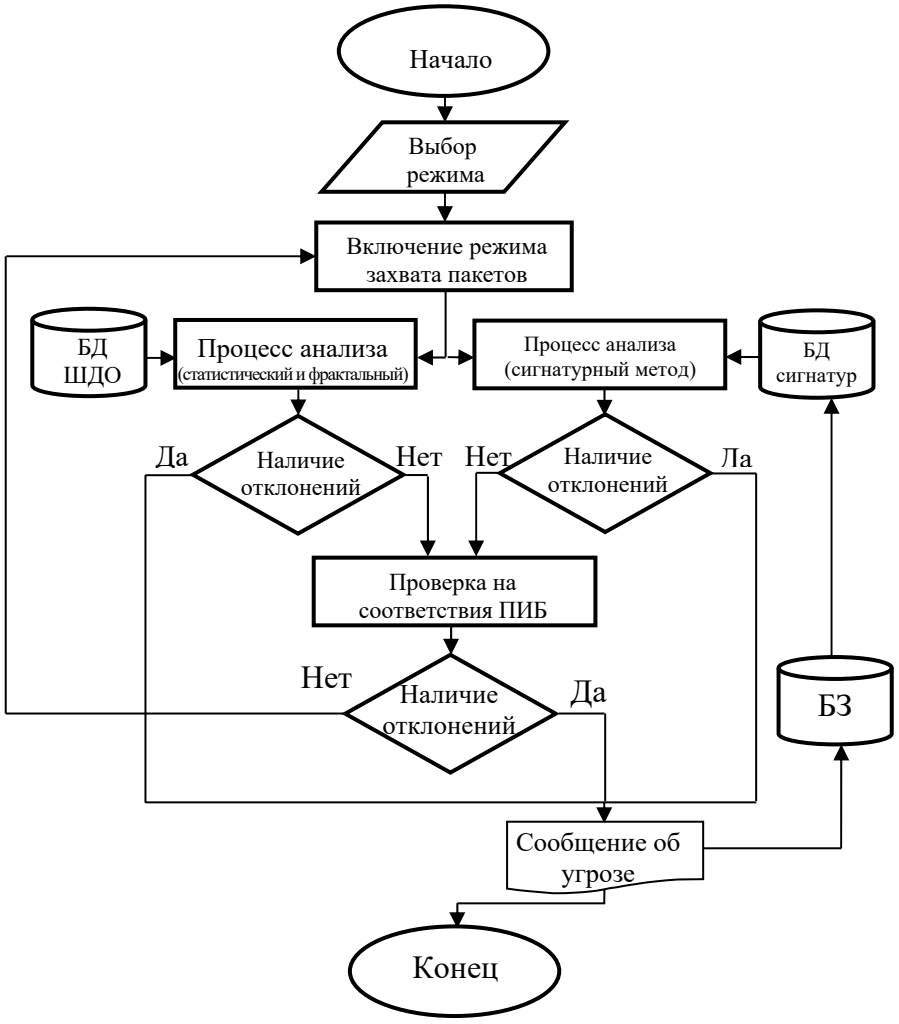


Рис. 2. Структура гибридного алгоритма идентификации нестандартных ситуаций в ИСУ

В пятой главе – **«Проектирование и разработка баз данных и программных комплексов защищенных интегрированных систем управления»** – приводятся результаты применения разработанных методов, алгоритмов, программных комплексов проектирования защищенных ИСУ.

Результаты диссертационной работы прошли опытно-испытательную апробация в два этапа.

На первом этапе ряд реализованных моделей и алгоритмов был апробирован в лабораторных условиях. В частности, в целях объективной оценки функционирования алгоритмы сигнатурного анализа сетевого

трафика (последовательного (прямого) поиска, Бойера–Мура, хеширования и двоичного поиска подстроки) были апробированы на персональном компьютере Acer. Перед алгоритмами была поставлена задача поиска $P = \{ p_1, p_2, ..., p_m \}$ шаблонов из существующего текста $T = \{ t_1, t_2, ..., t_n \}$, где $m \le n$.

Для поиска были заданы шаблоны с различным количеством слов (10 шт., 50 шт., 100 шт.), со шрифтами на латыни и кириллице. Объем программного кода реализованных на языке C++ алгоритмов последовательного поиска составил 777 байт, Боейера – Мура – 1862 байта, хеширования по сигнатуре – 1290 байт, двоичного поиска подстроки – 3217 байтов, что является допустимым для внедрения в ССОВ. Тестирование всех реализованных программ было проведено на персональном компьютере Acer с процессором Intel Core i5, 2,4 Ггц, ОЗУ-4 Gб.

В качестве основных параметров оценки производительности алгоритмов определим время, затраченное компьютером при выполнении программы, и объем ОЗУ машины, требуемый для функционирования программы. Результаты эксперимента сравнения алгоритмов сопоставления приведены в табл. 2.

Таблица 2

Эксперимент сравнения алгоритмов сопоставления

№	Наименование алгоритмов	Поиск 10 шаблонов из заданного текста		Поиск 50 шаблонов из заданного текста		Поиск 100 шаблонов из заданного текста	
		время поиска, мс	объём памяти, мб	время поиска, мс	объём памяти, мб	время поиска, мс	объём памяти, мб
1	Последовательного (прямого) поиска	0,0918	5,3	0.7248	5,4	2,129	5,4
2	Бойера – Мура	0,1202	5,4	0,6674	5,4	1,6455	5,4
3	Хеширование по сигнатуре	0,0946	5,4	0,5694	5,4	1,529	5,4
4	Двоичный поиск подстроки	0,1786	5,4	0,8593	5,4	2,1285	5,4

Анализ полученных результатов показывает, что заданный объем P шаблона и текста T существенно влияют на время поиска. Основной причиной этого является количество операций сопоставления выполняемой программой. При этом объем требуемого ОЗУ (5,4 мб) в процессе функционирования программ остается почти неизменным для всех типов алгоритмов.

Учитывая результаты эксперимента, можно утверждать, что для реализации в системах анализа из вышерассмотренных алгоритмов наиболее применимы алгоритмы хеширования и Бойера – Мура, так как в телекоммуникационных системах весьма высок объем потоков протекающих сетевых пакетов.

На втором этапе предложенные в данной диссертации модели, алгоритмы и программные комплексы прошли опытно-промышленную

апробацию в Центре информационной и общественной безопасности Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан, в Главном центре информатизации Центрального банка Республики Узбекистан, а также в АО «Джизакский аккумуляторный завод».

Для получения и практического использования моделей был проведен промышленный эксперимент в условиях нормального функционирования технологического процесса выпуска аккумуляторов на Джизакском аккумуляторном заводе. Предварительные исследования анализа сетевого трафика ИСУ завода показали, что в отношении параметров объекта можно принять сигнатурный и аномальный метод идентификации (рис.3). В целях сегментации информационной инфраструктуры ИСУ завода была применена технология VLAN. Время проведения опытно-испытательных работ составило более 1 месяца.

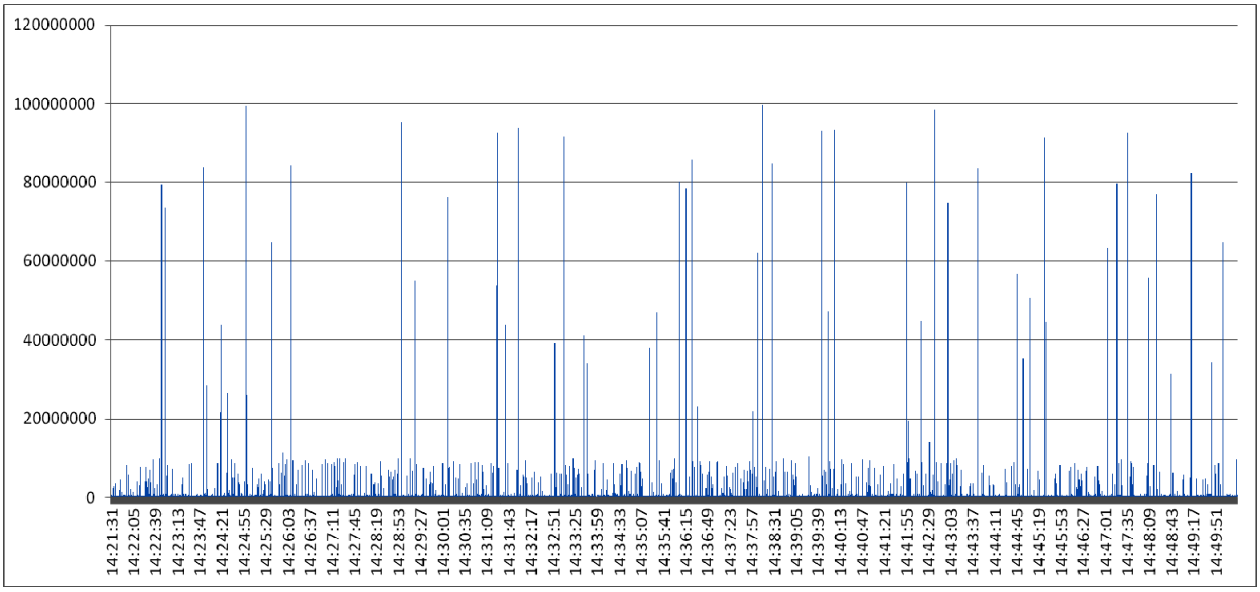


Рис. 3. Исходные параметры сетевого трафика предприятия

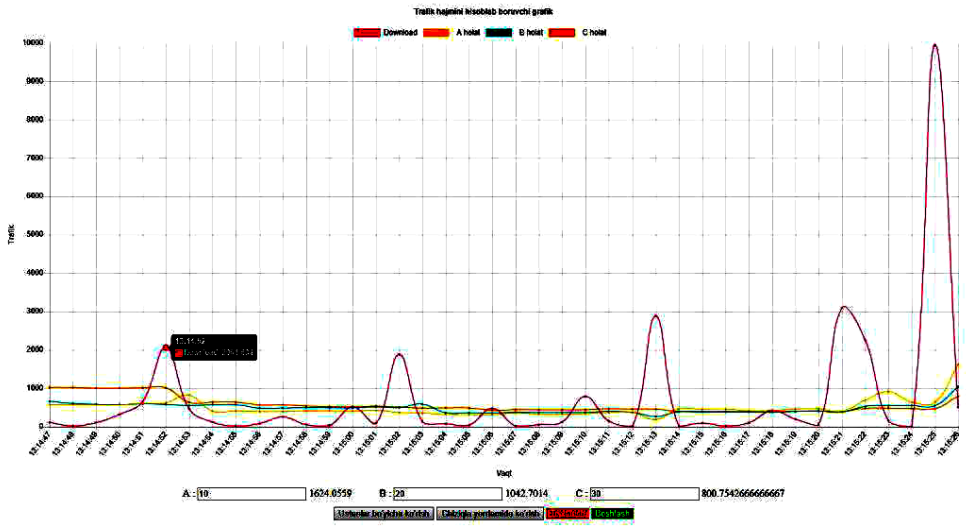


Рис. 4. График результатов анализа сетевого трафика в ИСУ

Результаты испытания показали технико-экономическую эффективность предложенной модели, алгоритмов и программного комплекса идентификации аномалий сетевого трафика и обеспечения защищенности ИСУ ПК (рис.4).

Практическая реализация методов и алгоритмов, предложенных в диссертационной работе, на различных предприятиях в промышленных условиях дала положительные результаты.

Результаты испытания показали технико-экономическую эффективность предложенной модели, алгоритмов и программного комплекса идентификации аномалий сетевого трафика и обеспечения защищенности ИСУ ПК.

В результате реализации алгоритмов и программ на различных предприятиях производительность подсистем анализа сети повысилась на 12-15%, а в АО «Джизакский аккумуляторный завод» ожидаемый экономический эффект составил 178 118 278,00 сум. в год.

ЗАКЛЮЧЕНИЕ

В диссертации на основе методов системного анализа, теории систем, математического анализа, статистического и фрактального анализов временных рядов, а также математических методов контекстного поиска для эффективного распознавания заданных шаблонов сигнатур разработана конструктивная методология автоматизированного проектирования защищенных интегрированных систем управления производственными комплексами.

В итоге получены следующие научные результаты:

1. Разработаны концепция и методология автоматизированного проектирования защищенных интегрированных систем управления производственными комплексами. Предложенные концепция и методология позволяют обеспечить противодействие возможным угрозам, а также бесперебойное функционирование и адаптивное управление различными объектами.
2. Осуществлен синтез структуры ИСУ ПК с учетом свойств исследуемого объекта, анализа угроз и уязвимостей систем управления сложными производственно-технологическими объектами. Проведенный синтез структуры ИСУ ПК позволяет разработать адаптивные модели и алгоритмы проектирования защищенных ИСУ.
3. Проведен анализ алгоритмов сигнатурного метода для поиска вредоносных кодов в сетевом потоке данных. Результаты анализа позволяют выявить наиболее эффективные алгоритмы строкового поиска.
4. Созданы модернизированные математические модели мониторинга сетевого трафика в ИСУ ПК с дискретным потоком данных на основе концепций статистического анализа. Полученные модели позволяют проводить анализ корректности функционирования технологического процесса в режиме реального времени.

5. Разработаны усовершенствованные алгоритмы и модели фрактального анализа сетевого трафика в ИСУ ПК с дискретным потоком информации. Предложенные алгоритмы и модели позволяют осуществлять эффективный сбор данных о потоках информации в ИСУ ПК и их идентификацию.

6. Предложены алгоритмы комплексной криптографической защиты информации в интегрированных системах управления производственными объектами. Полученные алгоритмы позволяют обнаруживать и предотвращать возможность несанкционированного ознакомления с управляющей информацией и защиту процессов передачи информации по каналам связи.

7. Разработаны алгоритмы гибридного мониторинга и идентификации нежелательных потоков в ИСУ ПК. Предложенные алгоритмы позволяют выявлять целенаправленные кибератаки на различные уровни архитектуры ИСУ ПК и обладают способностью частичного самообучения.

8. Предложена методика использования VLAN-технологии и разработан алгоритм синтеза структуры ИСУ. Предложенный алгоритм позволяет оптимизировать потоки информации и защиту передаваемых данных по каналам связи промышленных сетей.

9. Предложены методы и алгоритмы повышения отказоустойчивости баз данных интегрированных систем управления производством. Полученные алгоритмы обеспечивают высокую эффективность систем хранения и резервирования БД промышленных комплексов.

10. Разработан программный комплекс мониторинга и прогнозирования сетевого трафика в ИСУ с дискретным потоком данных. Предложенный программный комплекс позволяет визуализировать отчеты, графики и диаграммы, отражающие динамику выявления целенаправленных атак.

SCIENTIFIC COUNCIL DSc.27.06.2017.T.03.02
ON THE ADMISSION OF SCIENTIFIC DEGREES AT THE
TASHKENT STATE TECHNICAL UNIVERSITY

TASHKENT STATE TECHNICAL UNIVERSITY

ISMAILOV OTABEK MIRKHALILOVICH

METHODS AND ALGORITHMS FOR COMPUTER-AIDED SOLUTIONS FOR SECURE INTEGRATED CONTROL SYSTEMS OF INDUSTRIAL COMPLEXES

05.01.08 - Automation and control of technological processes and manufactures

ABSTRACT OF THE DISSERTATION OF
DOCTOR OF SCIENCE (DSc) ON TECHNICAL SCIENCES

Tashkent – 2019

The theme of doctor of science (DSc) dissertation is registered at the Supreme Attestation Commission under the Cabinet of Ministers of the Republic of Uzbekistan under number B2018.4.DSc/T244.

The dissertation has been prepared at Tashkent State Technical University.

The Abstract of dissertation is posted in Three languages (Uzbek, Russian, English (resume)) is placed on the web-page of Scientific Council (www.tdtu.uz) and Information and Educational Portal «Ziyonet» (www.ziyonet.uz).

Scientific consultant:	**Yusupbekov Nodirbek Rustambekovich** Doctor of Technical Sciences, Professor, Academician
Official opponents:	**Kamilov Mirzayan Mirzaakhmedovich** Doctor of Technical Sciences, Professor, Academician
	Igamberdiev Khusan Zakirovich Doctor of Technical Sciences, Professor, Academician
	Karimov Majit Malikovich Doctor of Technical Sciences, Professor
Leading organization:	**Bukhara engineering-technological institute**

Defense of dissertation will take place in «___» _____ 2019 at ____ o'clock at a meeting of the scientific council DSc.27.06.2017.T.03.02 at the Tashkent state technical university (Address: 100095, Tashkent, str. University-2, tel.: (99871) 246-46-00; fax: (99871) 227-10-32; e-mail: tstu_info@tdtu.uz).

The doctoral dissertation could be reviewed at the Information-resource center of Tashkent state technical university (registration number ___). Address: 100095, Tashkent, str. University-2, tel.: (99871) 246-03-41.

Abstract of the dissertation distributed «____» _____ 2019 year.

(mailing report № ___, on «___» _____ 2019 year).

F.T.Adilov
Deputy Chairman of scientific council
on awarding scientific degrees,
Doctor of technical sciences, Professor

U.F.Mamirov
Scientific Secretary of scientific council,
on awarding scientific degrees,
PhD in technical science

Kh.Z.Igamberdiev
Chairman of the scientific council
for awarding of the scientific degrees,
Doctor of Technical Sciences, Professor, Academician

INTRODUCTION (abstract of DSc thesis)

The goal of the thesis is to develop methods and algorithms for computer-aided design of secure integrated systems for managing derivatives from external and internal threats.

The objects of the research work is the process of electronic impact on information resources of integrated systems for managing production complexes.

Scientific novelty of the research work is as follows:

a concept and methodology have been developed, and the basic principles for designing secure integrated systems for managing production complexes in the context of unification of information and industrial technologies have been defined;

The structure of a protected integrated system for managing production complexes has been developed taking into account the properties of the object under study, analyzing threats and vulnerabilities of management systems for complex production and technological facilities;

developed modernized mathematical models for monitoring network traffic in secure integrated systems for managing industrial complexes with a discrete data flow based on the concepts of statistical analysis;

developed advanced algorithms and models of fractal analysis of network traffic in secure integrated systems for controlling production complexes with discrete flow;

Algorithms for complex cryptographic information protection in integrated systems for managing production objects have been developed;

developed hybrid algorithms for monitoring and identifying unwanted flows in secure integrated systems for managing production complexes with the ability of partial self-learning;

methods and algorithms for improving the fault tolerance of databases of integrated production management systems have been developed.

Implementation of the research results. On the basis of the obtained results on the development of methods and algorithms for computer-aided design of secure integrated systems for managing production complexes:

hybrid algorithms for monitoring and identifying unwanted flows in secure integrated systems for managing production complexes, with the ability of partial self-learning, algorithms for complex cryptographic information protection in integrated systems for managing production objects, and methods and algorithms for increasing the resiliency of databases for integrated production management systems are introduced into the Central Information Center of Central Bank of the Republic of Uzbekistan (Certificate of the Ministry of Development of Information Technologies and Communications of the Republic of Uzbekistan for the number 33–8 / 1449 of February 28, 2019). As a result, the performance of the network traffic analysis system increased by 12%;

developed modernized mathematical models for monitoring network traffic in PCs protected by ICS with discrete data flow based on statistical analysis concepts and improved algorithms and models for network traffic fractal analysis in computers

protected by ICS with discrete flow implemented in Jizzakh Accumulatory Plant JSC (Ministry of Information Development Technologies and Communications of the Republic of Uzbekistan for the number 33–8 / 1449 dated February 28, 2019). As a result of the implementation of the developed mathematical models and algorithms for improving the monitoring system of industrial networks protected by PC MIS, the possibility of their uninterrupted functioning was achieved;

developed concepts and methodologies, as well as defining the basic principles of designing secure integrated systems for managing production complexes in the context of unification of information and industrial technologies were introduced in the Information and Public Security Center of the Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan, as well as in the State Unitary Enterprise UNICON.UZ (Certificate of the Ministry of Development of Information Technologies and Communications of the Republic of Uzbekistan for the number 33–8 / 1449 of February 28, 2019). As a result, the effectiveness of the system for monitoring the traffic of PC-protected MIS increased by 15%.

The structure and volume of the dissertation. The thesis consists of an introduction, five chapters, conclusion, list of references and applications. The volume of the thesis is 184 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS
I бўлим (Часть I; Part I)

1. Исмаилов О.М. Математическое моделирование угроз вредоносных программ на распределенные вычислительные системы//ДАН РУз. – Ташкент, 2009. –№2. –С.20–24 (05.00.00; №9).
2. Исмаилов О.М. Разработка и исследование матаматической модели виртуальных частных сетей с многоканальной коммутацией// ДАН РУз. – Ташкент, 2010. – №2. – С.24 – 27. (05.00.00; №9).
3. Исмаилов О.М. Исследование методов построения сети IP-телефонии//Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2012. №4 – 5. – С.72 – 75 (05.00.00; №5).
4. Исмаилов О.М. Методы комплексной криптографической защиты информации//ДАН РУз. –Ташкент, 2012. – №4. –С.25 – 28 (05.00.00; №9).
5. Исмаилов О.М. Интеллектуальные методы защиты систем управления сложными промышленными объектами//ДАН РУз. –Ташкент, 2016. – №5. – С.40 – 43 (05.00.00; №9).
6. Ismailov O.M. Modeling of processes for designing misuse detection Intrusion detection systems with intelligent control technology // International scientific and technical journal «Chemical Technology. Control and Management» and Journal of Korea Multimedia Society, Special Issue, South Korea, Seoul – Uzbekistan, Tashkent, 2016. – №5. –P. 71 – 74 (05.00.00; №12).
7. Исмаилов О.М. Средства интеллектуальной обработки данных в системах управления//Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2017. – №3. – С.82 – 88 (05.00.00; №5).
8. Юсупбеков Н.Р., Исмаилов О.М. Методы и алгоритмы анализа и обработки сетевого трафика в системах управления производственными объектами//Международный научно-технический журнал «Химическая технология. Контроль и управление». – Ташкент, 2017. – №5(77). – С.47 – 54 (05.00.00; №12).
9. Исмаилов О.М. Построение математической модели производственных систем управления с применением технологии VLAN//Научный журнал «Проблемы вычислительной и прикладной математики». –Ташкент, 2017. – №4(10). –С.67 – 71 (05.00.00; №23).
10. Исмаилов О.М. О исследовании функционирования некоторых алгоритмов быстрого строкового сопоставления для сетевых систем обнаружения вторжений//Научный журнал «Проблемы вычислительной и прикладной математики». –Ташкент, 2017. – №6(12). – С.73 – 77 (05.00.00; №23).
11. Исмаилов О.М. Способы повышения отказоустойчивости баз данных автоматизированных систем управления производством//Журнал «Электротехника». –Москва, 2017. – №12. –С.79 – 83 (05.00.00; №96).

12. Ismailov O.M., Fozilova M.M. Fuzzy task of rational distribution resources of dynamic programming//International scientific and technical journal «Chemical Technology. Control and Management». Special Issue. –Tashkent, 2018. – №4 – 5. –P. 137 – 140 (05.00.00; №12).

13. Ismailov O.M. A Mathematical Model for Determining Traffic Anomalies in Computer Data Networks with Discrete Characteristics//International Journal of Advanced Research in Science, Engineering and Technology (website: www.ijarset.com, India). Vol. 5, Issue 11. 2018 November. – P. 7318 – 7329 (05.00.00; №8).

II бўлим (Часть II; Part II)

14. Исмаилов О.М., Исмаилова Г.А. Методология тестирования и отладки программных комплексов систем безопасности // Информационные системы контроля и управления на транспорте. Автоматизация технологических процессов в промышленности и на транспорте. Вып.11. – Иркутск: ИрГУПС, 2004. –С.41 – 45.

15. Исмаилов О.М. Математическая модель информационной безопасности вычислительных систем//Узбекский журнал «Проблемы информатики и энергетики». – Ташкент, 2007. – №3. –С.70–74.

16. Исмаилов О.М., Фозилова М.М. Метод повышения эффективности обработки сетевого трафика с применением мобильной мультиагентной системы обнаружения вторжений // IV Международная научно-практическая конференция «Перспективы, организационные формы и эффективность развития сотрудничества российских и зарубежных вузов». Сборник. – Королев МО: Изд-во ООО «ТРП», Технологический университет, 2016. – С.158 – 162.

17. Исмаилов О.М., Зияханова Г.Н. Исследование математической модели структуры АСУТП // Сборник докладов Республиканской научно-технической конференции «Значение информационно-коммуникационных технологий в инновационном развитии реальных отраслей экономики». Часть 1. 2017. 6-7 апреля. –Ташкент, 2017. –С.222 – 224.

18. Исмаилов О.М., Нурмуродов Г.Ш. Применение интеллектуальных методов в разработке компьютерных систем // Сборник докладов Республиканской научно-технической конференции «Значение информационно-коммуникационных технологий в инновационном развитии реальных отраслей экономики». Часть 1. 2017. 6-7 апреля. –Ташкент, 2017. – С.300 – 301.

19. Исмаилов О.М., Намазов А.О. Современные технологии работы с данными, вырабатываемые Интернетом вещей // Сборник докладов Республиканской научно-технической конференции «Значение информационно-коммуникационных технологий в инновационном развитии реальных отраслей экономики». Часть 1. 2017. 6-7 апреля. – Ташкент, 2017. – С.304 – 305.

20. Yusupbekov N.R., Ismailov O.M. Mathematical structure formalization of the integrated control systems over the Technical processes // Proceedings of the International conference on Integrated innovative development of Zarafshan region: achievements, Challenges and prospects. Vol. II. 2017. 26-27 October. – Navoi, 2017. – P. 62 – 66.

21. Исмаилов О.М. Математическая формализация систем отказоустойчивого доступа к данным // Материалы XXII Международной научно-технической конференции «Современные средства связи». 2017. 19 – 20 октября. –Минск, 2017. – С.305 – 306.

22. Исмаилов О.М. Эшелонированный подход к проектированию защищенных АСУ ТП // Доклады Республиканской научно-технической конференции «Современное состояние и перспективы применения информационных технологий в управлении». – Ташкент, 2017. 5-6 сентября. Научно-инновационный центр информационно-коммуникационных технологий. –Ташкент, 2017. – С. 500 – 505.

23. Исмаилов О.М., Исаков А.Ф., Маллаев Р.К., Алгоритм быстрого строкового сопоставления сетевых систем обнаружения вторжений // Труды Международной научно-технической конференции «Актуальные проблемы оптимизации и автоматизации технологических процессов и производств», 17-18 ноября 2018 г. – Карши, 2018. – С.57 – 63.

24. Исмаилов О.М, Фозилова М.И. Программное обеспечение для подборки информационных новостей из веб-сайтов. Свидетельство об официальной регистрации программы для ЭВМ. DGU 04151, 06.12.2016.

25. Исмаилов О.М. Прикладная программа для выявления вредоносных программных кодов в автоматизированной системе управления производством. Свидетельство об официальной регистрации программы для ЭВМ. DGU 05250, 24.04.2018.

26. Исмаилов О.М., Фозилова М.М. Программное обеспечение систем автоматизированного мониторинга давления и температуры технологических процессов. Свидетельство об официальной регистрации программы для ЭВМ. DGU 05251, 24.04.2018.

Автореферат «Информатика ва энергетика муаммолари» Ўзбекистон илмий журнали таҳририятида таҳрирдан ўтказилди ҳамда ўзбек, рус ва инглиз тилларидаги матнларини мослиги текширилди.

Бичими: 84x60 $^{1}/_{16}$. «Times New Roman» гарнитура рақамли босма усулда босилди.
Шартли босма табоғи: 4. Адади 100. Буюртма № 55.

«Тошкент кимё-технология институти» босмахонасида чоп этилди.
100011, Тошкент, Навоий кўчаси, 32-уй.