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

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

БОТИРОВ ФАЙЗУЛЛАЖОН БАХТИЁРОВИЧНИНГ

КОРХОНАДАГИ АХБОРОТНИ ҲИМОЯЛАШНИНГ КЎПАГЕНТЛИ ИНТЕЛЛЕКТУАЛ УСУЛЛАРИНИ ИШЛАБ ЧИҚИШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2021

УДК: 004.056.57.

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

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

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

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

БОТИРОВ ФАЙЗУЛЛАЖОН БАХТИЁРОВИЧНИНГ

КОРХОНАДАГИ АХБОРОТНИ ҲИМОЯЛАШНИНГ КЎПАГЕНТЛИ ИНТЕЛЛЕКТУАЛ УСУЛЛАРИНИ ИШЛАБ ЧИҚИШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2021

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2020.4.PhD/T1941 рақам билан рўйхатга олинган.

Диссертация Тошкент ахборот технологиялари университетида бажарилган.

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

Илмий раҳбар:	**Бекмуратов Тулкун Файзиевич** академик, техника фанлари доктори, профессор
Расмий оппонентлар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
	Жураев Гайрат Умарович физика-математика фанлари доктори, доцент
Етакчи ташкилот:	**«UNICON.UZ» - фан – техника ва маркетинг тадқиқотлар маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.01 Илмий кенгашнинг 2021 йил «6» февраль соат 10.00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (2631 рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-ўй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2021 йил «___» _____ да тарқатилди.
(2021 йил «___» _____ даги ___ рақамли реестр баённомаси.)

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

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

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

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда кўпагентли тизимлар ёрдамида корхонанинг ахборот тизимига бўладиган ҳужумларни аниқлаш ва уларни бартараф этиш билан бир қаторда ҳужумларни аниқлаш жараёни аниқлигини ошириш ва хатоликларини камайтиришга эътибор қаратилмоқда. «Kaspersky компанияси маълумотларига кўра, 2020 йилнинг биринчи чорагида давлат ташкилотларига бўлган ҳужумлар улуши ошган бўлиб, ҳужум объектининг 89%ни – компьютерлар, серверлар ва тармоқ қурилмалари ташкил этган»[1]. Бу йўналишда хорижий мамлакатларда, жумладан, АҚШ, Россия Федерацияси, Хитой, Жанубий Корея ва бошқа давлатларда интеллектуал усуллар асосида ахборотга бўладиган таҳдидларнинг таъсир даражасини аниқлаш, ҳужумларни аниқлаш усуллари ва алгоритмларини ишлаб чиқиш ҳамда ахборотни ҳимоялаш тизимларини такомиллаштириш муҳим аҳамият касб этмоқда.

Жаҳонда тармоқ ҳужумларини аниқлашнинг модел ва алгоритмларини такомиллаштиришга ҳамда кўпагентли тизимлар ёрдамида тармоқ ҳужумларини аниқлашга қаратилган илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, жумладан сигнатурага асосланган ва пакет сарлавҳалари маълумотларини таққосланиши орқали амалга ошириладиган ҳужумларни аниқлаш усулларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланмоқда. Шу билан бирга, ахборотни ҳимоялаш жараёнида кўрилаётган объект тўғрисидаги билимлар тўлиқ бўлмаганда ёки жорий маълумотларда ноаниқликлар мавжуд бўлганда ахборотни ҳимоялаш учун кўпагентли интеллектуал тизимлардан фойдаланишни ишлаб чиқиш зарур бўлмоқда.

Республикамизда давлат ва хўжалик бошқарув органларида ахборотни ҳимоялаш жараёнида қўлланилаётган интеллектуал тизимларга асосланган ҳимоя механизмларини такомиллаштиришга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Мазкур вазифаларни амалга оширишда, ахборотга бўладиган ҳужумларни аниқлашда кўпагентли интеллектуал усулларни қўллаш ҳамда ахборотни ҳимоялашда интеллектуал тизимлардан фойдаланиш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари, 2018 йил

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

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

21 ноябрдаги ПҚ-4024-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги ва 2019 йил 14 сентябрдаги ПҚ-4452-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштиришга оид қўшимча чора-тадбирлар тўғрисида»ги Қарорлари ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга мазкур диссертация тадқиқоти маълум даражада хизмат қилади.

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

Муаммонинг ўрганилганлик даражаси. Ахборот хавфсизлигини таъминлашда нейрон тармоқлар, кўпагентли тизимлар ва шунга ўхшаш интеллектуал тизимлар оиласига мансуб йўналишларни қўллаган ҳолда ишлаб чиқилган усуллар ва алгоритмларни қўллаш бўйича А.В.Остроух, Г.А. Поллак, В.И. Васильев, Е.А. Жидко, А.В. Торопова, S. Каур, А. Алнафессаҳ, М.Сингҳ ва бошқа чет эллик олимлар томонидан илмий изланишлар олиб борилмоқда. Ахборот хавфсизлигини таъминлашда нейрон тармоқларни қўллаган ҳолда Х. Юан, Н. Шин, Ж. Лее, Й. Чои, Ж. Ким илмий изланишлар олиб боришган. Бундан ташқари, InfoWatch, RiskWatch, WatchGuard ва Trend Micro ташкилотлари томонидан интеллектуал тизимларни қўллаш орқали ахборотни ҳимоялашнинг дастурий-аппарат воситаларини ишлаб чиқиш бўйича инженерлик-тадқиқот ишлари олиб борилмоқда.

Ўзбекистонда Т.Ф.Бекмуратов, С.К.Ганиев, Н.А. Игнатьев, М.М.Каримовлар бошчилигидаги илмий жамоалар томонидан ахборотни ҳимоялашнинг интеллектуал тизимлари, ахборот хавфсизлиги рисклари, таҳдидларни аниқлашнинг усул ва алгоритмлари устида илмий изланишлар олиб борилган.

Шу билан бирга, кўпагентли тизимлар, нейрон тармоқ, машинали ўқитиш (machine learning) ва чуқур ўқитиш (deep learning) асосида ҳужумларни аниқлаш, бартараф этиш усуллари ва алгоритмлари етарлича тадқиқ этилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг илмий-тадқиқот ишлари режасининг №БВ-Ф4-023 – “Тақсимланган ахборот-коммуникация тизимларида инцидентлар ва киберхужумларга қарши харакатларни бошқариш муаммоларини тадқиқ этиш (Исследование проблем управления инцидентами и противодействия кибератакам в распределенных

информационно-коммуникационных системах)” (2017-2020) мавзусидаги лойиҳа доирасида бажарилган.

Тадқиқотнинг мақсади ахборотни ҳимоялаш тизимининг самарадорлигини оширишга имкон берувчи кўпагентли интеллектуал усулларни ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

ахборотни ҳимоялашнинг интеллектуал тизимлари ва технологияларини қиёсий таҳлил қилиш;

корхонадаги ахборотни ҳимоялашнинг кўпагентли интеллектуал тизимини қуриш концепциясини ишлаб чиқиш;

ахборотни ҳимоялашнинг интеллектуал тизими структураси ва архитектурасини ишлаб чиқиш;

корхонадаги ахборотга бўладиган таҳдидларнинг таъсир даражасини аниқлаш усулини ишлаб чиқиш;

корхона ахборот тизимига бўладиган ҳужумларни аниқлашнинг усул ва алгоритмини ишлаб чиқиш;

тармоқ аномалияларини аниқлаш алгоритмини ишлаб чиқиш.

Тадқиқотнинг объекти сифатида корхонада ахборотни ҳимоялаш жараёни олинган.

Тадқиқотнинг предметини ахборотни ҳимоялашнинг кўпагентли интеллектуал усуллари ва алгоритмлари ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот жараёнида ахборотни интеллектуал тизимлар ёрдамида ҳимоялаш усуллари, нейрон тармоқлар, норавшан тўпламлар назарияси, эҳтимоллик назарияси, графлар назарияси, дискрет математика ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

корхонадаги ахборотни химоялашнинг уч сатҳли механизмини ҳисобга олган ҳолда кўпагентли интеллектуал тизим концепцияси ишлаб чиқилган;

уч сатҳли ҳимоя механизмининг мақсадлар дарахти асосида ахборотни ҳимоялашнинг интеллектуал тизим архитектураси ишлаб чиқилган;

корхонадаги ахборотга бўладиган таҳдидларни ҳосил бўлиш частотаси асосида таъсир даражасини аниқлаш усули ишлаб чиқилган;

тармоқ ҳужумларини аниқлашнинг нейрон тармоқ усули ва алгоритми сигнатурали таҳлилга асосланган ҳолда ишлаб чиқилган;

фойдаланувчиларни олдинги ҳаракатларидан келиб чиққан ҳолда кейинги ҳаракатларини башоратловчи интерактив ва сеанс моделлар асосида тармоқ аномалияларини аниқлаш алгоритми ишлаб чиқилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

кўпагентли интеллектуал усуллар асосида корхонадаги ахборотни ҳимоялашнинг дастурий комплекси ишлаб чиқилган;

сигнатурали таҳлил асосида ҳужумларни аниқлашда Snort ва Suricata базалари умумлаштирилиб, қўшимча ҳужум сигнатураларини киритиш орқали такомиллаштирилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги корхона ахборот тизимига бўладиган таҳдидларни таъсир даражасини аниқлаш, ҳужумларни аниқлаш усулларидан турли шароитларда олинган реал ҳамда тажрибавий таҳлил натижалари билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти ишлаб чиқилган корхонадаги ахборотни ҳимоялаш жараёнида таҳдидларнинг таъсир даражасини аниқлаш усули, сигнатурага асосланган ҳужумларни аниқлашнинг нейрон тармоқ усули ва интерактив ҳамда сеанс моделлар асосида тармоқ аномалияларини аниқлаш алгоритми билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти таклиф этилган усуллар ва алгоритмлар асосида ишлаб чиқилган дастурий воситанинг корхонадаги ахборотни ҳимоялаш жараёнини интеллектуаллаштиришга кўмаклашиши билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Корхонадаги ахборотни ҳимоялашнинг кўпагентли интеллектуал усуллари ҳамда дастурий воситалари бўйича олинган илмий натижалар асосида:

корхонадаги ахборотни ҳимоялаш жараёнида сигнатурали таҳлилни қўллаган ҳолда ҳужумларни аниқлашнинг нейрон тармоқ усулининг дастурий воситаси Ўзбекистон Республикаси «Акциядорлик тижорат Халқ банки» бош амалиётлар бошқармасининг амалий фаолиятига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 24 ноябрдаги 33-8/7051-сон маълумотномаси). Илмий тадқиқот натижаси корпоратив тармоқда DoS ҳужумларни аниқлашда 94,7% аниқлик ва 5,3% хатолик, U2R ҳужумларни аниқлашда 91,4% аниқлик ва 8,6% хатолик, R2L ҳужумларни аниқлашда 93,6% аниқлик ва 6,4% хатолик, Probe ҳужумларини аниқлашда 95,8% аниқлик ва 4,2% хатолик билан тармоқ ҳужумларини аниқлаш имконини берган;

корхонадаги ахборотни ҳимоялаш жараёнида таҳдидларни таҳлиллаш усулининг дастурий воситаси «UNICON.UZ» Давлат унитар корхонаси – Фан – техника ва маркетинг тадқиқотлари марказининг амалий фаолиятига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 24 ноябрдаги 33-8/7051-сон маълумотномаси). Илмий тадқиқот натижасида ташкилотнинг локал тармоғига бўладиган ҳужумларни аниқлашда хатоликлар ҳақида тизим маъмурини огоҳлантириш имконияти яратилган;

интерактив ва сеанс моделлари асосила тармоқ аномалияларини аниқлашнинг дастурий воситаси Ўзбекистон Республикаси Мудофаа вазирлиги Ахборот – коммуникация технологиялари ва алоқа ҳарбий институтининг амалий фаолиятига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 24 ноябрдаги 33-8/7051-сон маълумотномаси). Илмий тадқиқот натижаси корпоратив тармоқдаги ҳужумларни 94,3% аниқлик ва 5,7% хатолик билан аниқлаш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 3 та халқаро ва 4 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертациянинг мавзуси бўйича жами 18 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 8 та мақола, шулардан, 4 таси хорижий ва 4 таси республика журналларида нашр этилган ҳамда 3 та ЭҲМ учун яратилган дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 112 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, мақсад ва вазифалари белгилаб олинган ҳамда тадқиқот объекти ва предмети аниқланган, олинган натижаларнинг ишончлилиги асослаб берилган, уларнинг назарий ва амалий аҳамияти, тадқиқот натижаларини амалда жорий қилиш ҳолати, нашр этилган ишлар ва диссертациянинг тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг «**Ахборотни ҳимоялашнинг кўпагентли интеллектуал тизимлари ва технологиялари»** деб номланган биринчи бобида корхонадаги ахборотни ҳимоялашнинг интеллектуал тизимлари ва технологияларининг қиёсий таҳлили ҳамда кўпагентли интеллектуал тизим асосида ахборотни ҳимоялаш механизмларини қуриш босқичлари ва корхонадаги ахборотни ҳимоялаш жараёнини автоматлаштириш бўйича тавсиялар келтирилган.

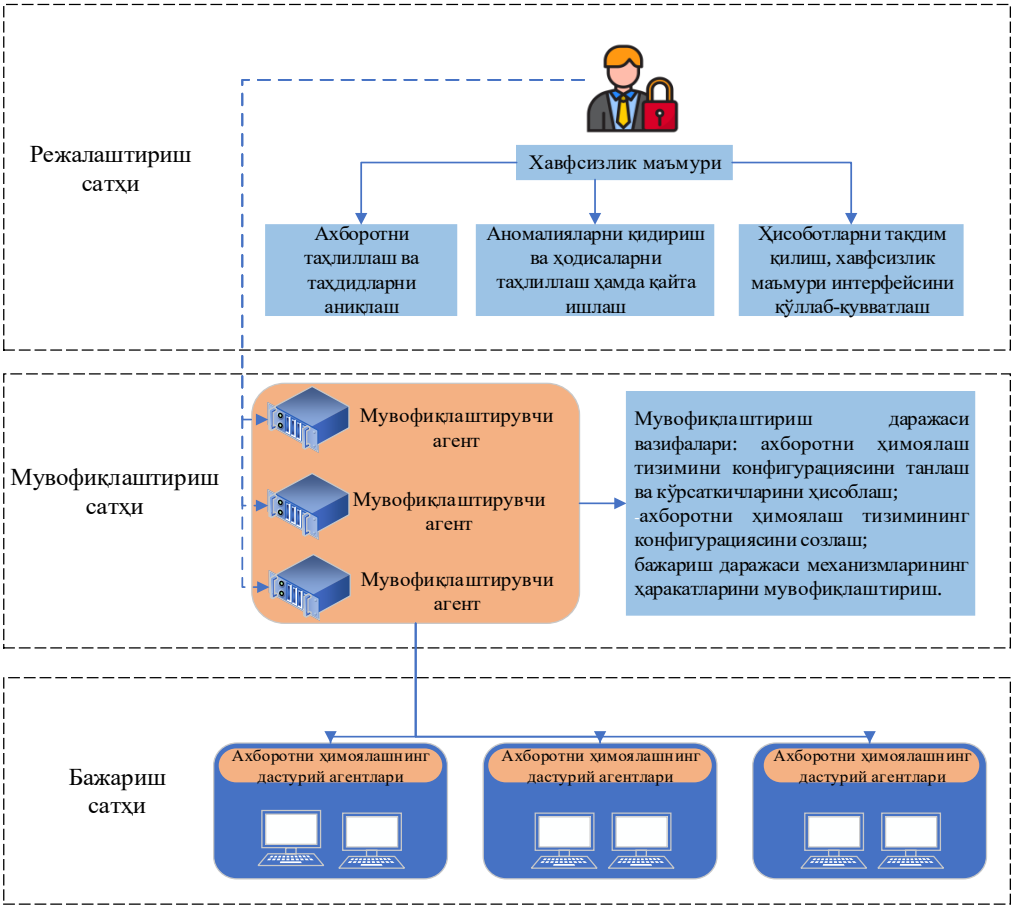
Биринчи параграфда интеллектуал тизимларни ривожланишининг замонавий босқичлари ҳамда ахборотни ҳимоялашнинг интеллектуал тизимлари ва технологияларининг қиёсий таҳлили амалга оширилган. Ахборот хавфсизлигини таъминлашда қўлланиладиган интеллектуал тизимларнинг асосий вазифалари аниқлаб олинган ва бу вазифаларни бажариш учун автономлиги, ноаниқлик шароитида мослашувчанлиги ва агентларнинг ўзаро алоқасини юқори даражада таъминлаш имконини берадиган кўпагентли интеллектуал тизимлар келтирилган.

Иккинчи параграфда агентнинг содда структураси, интеллектуал агент хусусиятлари, кўпагентли тизимларнинг фарқланувчи белгилари, ҳужумларни аниқлашда фойдаланиладиган кўпагентли тизимларнинг тақсимланган архитектураси, ахборотни ҳимоялашда кўпагентли тизимлардан фойдаланишнинг афзалликлари ва турли хусусиятларга эга бўлган агентларнинг қиёсий таҳлили келтирилган. Кўпагентли тизим

фойдаланиладиган агентларига қўйиладиган асосий талаблар шакллантирилган ва кўпагентли интеллектуал тизимлар асосида ахборотни ҳимоялаш механизмларини қуриш таклиф этилган.

1-расм. Кўпагентли интеллектуал тизим асосида ахборотни ҳимоялаш механизмларини қуриш босқичлари

Учинчи параграфда корхонада ахборотни ҳимоялаш тизимини интеллектуаллаштириш учун ахборот хавфсизлигини таъминлашнинг уч сатҳли иерархик автоматлаштирилган тизимини яратиш бўйича тавсиялар берилган. Корхонадаги ахборотни ҳимоялаш тизимини автоматлаштириш схемаси 2-расмда келтирилган.



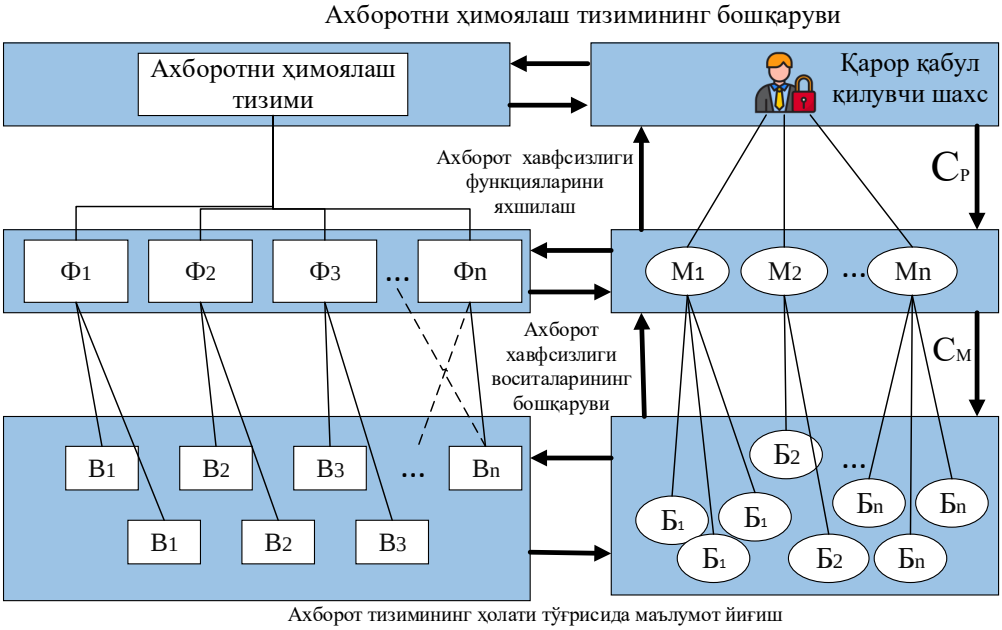
2-расм. Корхонадаги ахборотни ҳимоялаш жараёнини автоматлаштириш схемаси

Диссертациянинг **«Корхонадаги ахборотни ҳимоялашнинг кўпагентли интеллектуал тизимини қуриш концепцияси, структураси ва архитектурасини ишлаб чиқиш»** деб номланган иккинчи бобида корхонада ахборотни ҳимоялашнинг кўпагентли интеллектуал тизимини қуриш концепцияси, структураси ва архитектураси ишлаб чиқилган. Ахборотни ҳимоялашни бошқариш жараёнида бажарилиши керак бўлган вазифалар белгилаб олинган.

Мазкур бобнинг *биринчи параграфида* корхонанинг ахборот тизимида ахборотни ҳимоялашнинг автоматлаштирилган интеллектуал тизимини қуриш концепцияси ишлаб чиқилган. Концепция қуйидаги принципларни ўз ичига олади:

1. Корхонадаги ахборотни ҳимоялашнинг интеграллашган тизимини яратишни назарда тутувчи функционал интеграллаш принципи.
2. Корхонадаги ахборотни ҳимоялаш тизимини кўпсатҳли интеграллашган иерархик кўринишда ташкиллаштириш принципи.
3. Корхонадаги ахборотга бўладиган таҳдидларни таъсир даражасини аниқлаш усуллари ва алгоритмларини комплекслик принципи.
4. Ахборотни ҳимоялаш тизимини қуриш талабларини ахборотни ҳимоялаш бўйича амалдаги стандартларга мувофиқ бўлишини англатувчи стандартлаштириш принципи.
5. Корхона ахборот тизимига бўладиган ҳужумларни аниқлаш ва бартараф этишни интеллектуаллаштириш принципи.

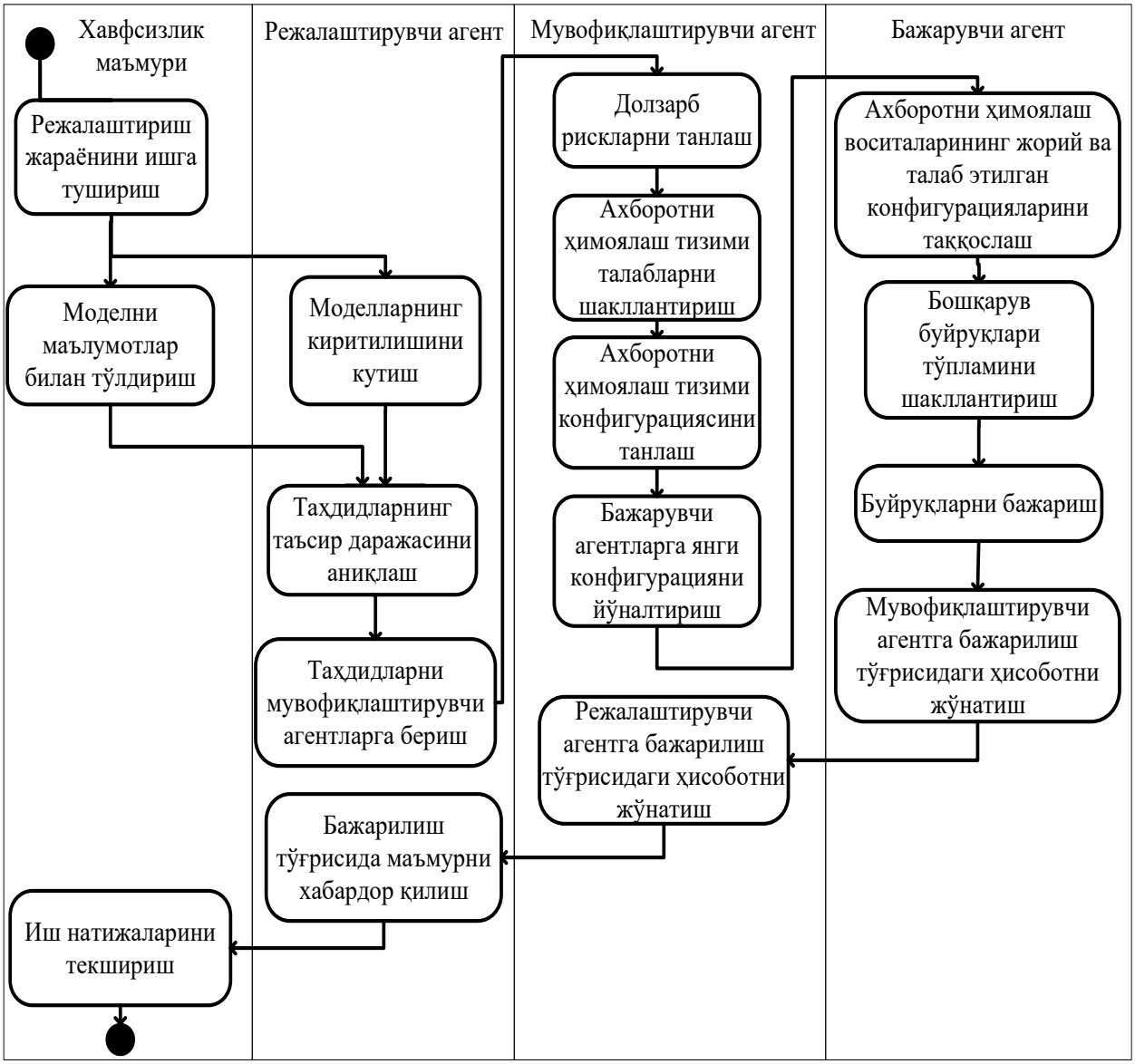
Иккинчи параграфда концепцияда кўрсатилган принциплар асосида корхона ахборотини ҳимоялашни бошқариш тизимининг мақсадлар дарахти шакллантирилган. Мақсадлар дарахтининг иерархияси асосида ахборотни ҳимоялашнинг автоматлаштирилган бошқариш схемаси ва интеллектуал тизими структураси ишлаб чиқилган. 3-расмда ахборотни ҳимоялашнинг интеллектуал тизими структураси келтирилган.



3-расм. Ахборотни ҳимоялашнинг интеллектуал тизими структураси

Хавфсизлик маъмурлари, яъни қарор қабул қилувчи шахслар ишининг натижаси $С_Р$ мувофиқлаштирувчи агентларга бажариш учун йўналтирилади, бу ерда: $С_Р -$ режалаштириш ва мувофиқлаштириш сатҳи орасидаги маълумот алмашиш агенти; $С_М -$ мувофиқлаштириш ва бажариш сатҳи орасидаги маълумот алмашиш агенти; $М_i$ – мувофиқлаштириш сатҳидаги агентлар, $i = 1,2 , \dots n.$; $Б_i$ – бажариш сатҳидаги агентлар, $i = 1,2 , \dots n.$; $Ф_i$ –корхона ахборот тизимидаги фойдаланувчи $i = 1,2 , \dots n.$; $В_i$ – корхона ахборот тизимидаги восита элементи $i = 1,2 , \dots n.$;

Учинчи параграфда ахборотни ҳимоялашнинг кўпагентли интеллектуал тизимининг архитектураси ишлаб чиқилган (4-расм). Корхона ахборот тизимининг барча тугунларига дастурий модуллар шаклидаги дастурий агентларни жойлаштириш, ахборотни ҳимоялаш қисмтизимлари ва барча воситаларини бошқариш ва ахборот активлари хавфсизлигига таъсир қилувчи барча ҳодисаларни қайд этиш имконини беради.



4-расм. Ахборотни ҳимоялашнинг интеллектуал тизимининг архитектураси

Диссертация ишининг «**Корхонанинг ахборот тизимига бўладиган таҳдидларни таъсир даражасини ва ҳужумларни аниқлаш усуллари ва алгоритмлари**» номли учинчи бобида корхонадаги ахборотга бўладиган таҳдидларни таъсир даражасини аниқлаш усули, корхона ахборот тизимига бўладиган ҳужумларни аниқлашнинг нейрон тармоқ усули ҳамда интерактив ва сеанс моделлар асосида тармоқ аномалияларини аниқлаш алгоритмлари ишлаб чиқилган.

Биринчи параграфда пайдо бўлиш частотаси асосида таҳдидларни таъсир даражасини аниқлаш усули ишлаб чиқилган. Таҳдидларнинг таъсир даражаси иккита мезон бўйича аниқланади: таҳдиднинг пайдо бўлиш частотаси ва потенциал бузғунчи томонидан таҳдидлар амалга оширилганда кўриладиган эҳтимолий зарарнинг катталиги. Таҳдидларнинг таъсир даражасини аниқлашнинг биринчи қадамида пайдо бўлиш частотаси мезони бўйича T таҳдидларни таққослаш матрицаси тузилади.

$$T = \begin{pmatrix} 1 & {t_1}/{t_2} & \dots & {t_1}/{t_x} \\ {t_2}/{t_1} & 1 & \dots & {t_2}/{t_x} \\ \vdots & \vdots & \dots & \vdots \\ {t_x}/{t_1} & {t_x}/{t_2} & \dots & 1 \end{pmatrix}, \qquad T_c = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_x \end{pmatrix}$$

бу ерда Т–таҳдидларнинг жуфт таққосланиш матрицаси. $T_C - T$ устуворликлар матрицасининг нормаллашган хусусий векторлари. $\forall\, t_a \in T, \quad a = 1, 2, \dots . x$:

Кейин ҳар бир таҳдид учун заифликларни таққослаш матрицаси Z, таҳдидларни амалга оширишнинг эҳтимолий йўлини кўрсатувчи Z_c устуворликлар вектори тузилади.

$$Z = \begin{pmatrix} 1 & {z_1}/{z_2} & \dots & {z_1}/{z_n} \\ {z_2}/{z_1} & 1 & \dots & {z_2}/{z_n} \\ \vdots & \vdots & \dots & \vdots \\ {z_n}/{z_1} & {z_n}/{z_2} & \dots & 1 \end{pmatrix}, Z_c = \begin{pmatrix} z_1^1 & z_1^2 & \dots & z_1^x \\ z_2^1 & z_2^2 & \dots & z_2^x \\ \vdots & \vdots & \dots & \vdots \\ z_n^1 & z_n^2 & \dots & z_n^x \end{pmatrix}$$

бу ерда Z_c – Z устуворликлар матрицасининг нормаллашган хусусий векторлари.$\forall\, z_b \in Z,\ b = 1, 2, \dots . n$:

$$R = \begin{pmatrix} 1 & {r_1}/{r_2} & \dots & {r_1}/{r_s} \\ {r_2}/{r_1} & 1 & & {r_2}/{r_s} \\ \vdots & \vdots & \dots & \vdots \\ {r_s}/{r_1} & {r_s}/{r_2} & \dots & 1 \end{pmatrix}, R_c = \begin{pmatrix} r_1^1 & r_1^2 & \dots & r_1^z \\ r_2^1 & r_2^2 & \dots & r_2^z \\ \vdots & \vdots & \dots & \vdots \\ r_s^1 & r_s^2 & \dots & r_s^z \end{pmatrix}$$

бу ерда R – ресурсларнинг жуфт таққосланиш матрицаси. $R_c - R$ устуворликлар матрицасининг нормаллашган хусусий векторлари матрицаси. $\forall\, r_v \in R,\ v = 1, 2, \dots . s$:

Бу қадамдан сўнг D ифода бўйича таҳдид таъсир даражасини ҳисоблаш амалга оширилади.

$$D = \begin{pmatrix} \sum_{j=1}^{n} t_1^c * z_j^c * r_1^c & \sum_{j=1}^{n} t_1^c * z_j^c * r_2^c & \dots & \sum_{j=1}^{n} t_1^c * z_j^c * r_s^c \\ \sum_{j=1}^{n} t_2^c * z_j^c * r_1^c & \sum_{j=1}^{n} t_2^c * z_j^c * r_2^c & \dots & \sum_{j=1}^{n} t_2^c * z_j^c * r_s^c \\ \vdots & \vdots & \dots & \vdots \\ \sum_{j=1}^{n} t_x^c * z_j^c * r_1^c & \sum_{j=1}^{n} t_x^c * z_j^c * r_2^c & \dots & \sum_{j=1}^{n} t_x^c * z_j^c * r_s^c \end{pmatrix}$$

Таҳдидларнинг таъсир даражасини ҳисоблаш уларни камайтириш ёки бартараф этиш бўйича қарор қабул қилиш иконини беради.

Иккинчи параграфда сигнатурали таҳлил асосида ҳужумларни аниқлашнинг нейрон тармоқ усули ва алгоритми ишлаб чиқилган. Ушбу усул учта босқичда амалга оширилади:

биринчи босқичда тармоқ трафигини ушлаб олиш амалга оширилади. Таҳлилланувчи трафикни характерловчи тармоқ пакетлари сарлавҳалари ҳақидаги маълумотларни тўплаш учун махсус сниффер пакети TCP ва UDP протоколлари бўйича ўтадиган барча пакетларни ушлаб қолади;

иккинчи босқичда тармоқ фаоллигини характерловчи устуворлиги юқори бўлган параметрлар ажратиб олинади. Классификатор ёрдамида устуворлиги юқори бўлган параметрлар гуруҳларга таснифланади ва ҳужумларни аниқлаш жараёнида ҳар бир параметрни таҳлиллаш ўрнига устуворлиги юқори бўлган параметрларни таҳлиллаш аниқликни ошириш имконини беради;

учинчи босқичда ҳужумларни аниқлаш амалга оширилади. Бу босқичда пакет сарлавҳаларини оддий таққослашга асосланган ҳужумларни аниқлаш тизимларига нисбатан жорий тармоқ фаоллиги белгиларини қанчалик ўхшашлик даражасини аниқлаш имконияти самарали бўлган нейрон тармоқдан фойдаланилади.

Шундай қилиб, кириш йўли трафигини таҳлили асосида тузилган классификаторни кириш йўли параметрлари вектори ўз ичига қуйидаги ўзгарувчиларни олади:

A_1 – битта пакет келишининг ўртача вақти;

A_2 – турли ташқи IP-манзилли пакетлар фоизи;

A_3 – турли ташқи портли пакетлар фоизи;

A_4 – нотўғри сарлавҳали пакетлар фоизи.

Классификаторнинг чиқиш йўли қиймати “ҳужумда ишончлилик даражаси” ҳолатини аниқлаб берадиган B экспертлар томонидан амалга оширилади. Юқорида кўрсатилган тармоқ трафигини A_1, A_2, A_3, A_4 параметрлари ва ҳужумда ишончлилик даражаси B қуйидаги кўринишга эга:

- АГАР пакетларнинг_келиш_вақти = «кичик» ва турли_ташқи_IP_манзиллар_фоизи «кичик» ва

турли_портлар_фоизи = «кичик» бўлса, у ҳолда
ҳужумнинг_таъсир_даражаси = **«ўртача»**;

- АГАР (пакетларни_келиш_вақти = «кичик» ёки
пакетларни_келиш_вақти «ўртача») ва
(турли_ташқи_IP_манзиллар_фоизи «катта» ёки
турли_портлар_фоизи = «катта» ёки
нотўғри_сарлавҳали пакетлар_фоизи = «катта») бўлса, у ҳолда
ҳужумнинг_таъсир_даражаси = **«юқори»**;
- АГАР пакетларни_келиш_вақти «катта» бўлса, у ҳолда
ҳужумнинг_таъсир_даражаси = **«паст»**.

Шундай қилиб, корхона ахборот тизимига бўладиган тармоқ ҳужумлари таъсир даражасини (паст, ўрта, юқори) аниқлаш имконини беради.

Учинчи параграфда интерактив ва сеанс моделлар асосида тармоқ аномалияларини аниқлаш алгоритми ишлаб чиқилган. Аномалияларни аниқлашнинг интерактив ва сеанс моделларининг чиқиш қийматлари олинади: интерактив моделнинг чиқиш қиймати (Y_t), сеанс моделнинг чиқиш қиймати (Y'_t). Бу моделларнинг чиқиш йўли қийматлари аномалияларнинг бор ёки йўқлиги тўғрисидаги қарорларни қабул қилиш, овозларни ўлчаш йўли билан бирга аномалияларни тармоқ трафигида параллел таҳлилланади. Бирламчи ва иккиламчи хатоликни минималлаштириш, таснифлаш аниқлиги ва тўлиқлигини ошириш таклиф этилган.

№1. Алгоритмнинг бошланиши.

№2. Трафикни таҳлиллаш амалга оширилади.

№3-5. Трафикни аномалиялар борлиги бўйича таҳлиллайди ва ҳар бир модель чақируви сифатида амалга оширилади. Агар таснифлаш натижалари, (Y_t) алгоритми бўйича аномалия бўлса, унда y_t=+1. Акс ҳолда, y_t=-1. Натижада ҳар бир усул аномалиялар бор ёки йўқлигига овоз беради y_t=±1, y'_t =±1.

№6. Аномалияга яқин трафикни қидириш амалга оширилади.

№7. Ҳар бир модель чиқувчи қиймати учун таҳлилланган трафикда аномалиялар бор ёки йўқлиги тўғрисидаги умумий қарорни қабул қилишда овоз юкини ўрнатиш учун F-ўлчов асосидаги таснифлаш сифат кўрсаткичи ҳисобланади.

№8. Агар иккита моделнинг ҳам чиқиш йўли қийматлари аномалия йўқлигига овоз берса, унда овоз бериш талаб этилмайди ва таснифлаш натижалари тўғрисида ҳамкорликдаги бирламчи қарор қабул қилинади аномалия тармоқда мавжуд эмас (№9). Агар ҳеч бўлмаганда, битта моделнинг чиқиш қиймати аномалия борлигини аниқласа, ҳамкорликдаги қарор қабул қилишда овоз бериш талаб этилади ва №10 га ўтиш амалга оширилади.

№10. Аномалияларнинг бор ёки йўқлиги тўғрисидаги S овоз бериш амалиёти ишга туширилади.

№11-13. Агар S>0 бўлса, овоз бериш натижаси тармоқ аномалияси йўқ. Акс ҳолда, овоз бериш натижасида тармоқ аномалияси мавжуд бўлади.

№14-16. Агар алгоритм таҳлилидан ўтадиган пакет охирги бўлса, унда алгоритмнинг иши тугатилади. Акс ҳолда №8 га қайтарилади.

Диссертациянинг «**Кўпагентли интеллектуал усуллар асосида ахборотни ҳимоялаш тизимининг самарадорлигини баҳолаш ва амалиётга татбиқ этиш натижалари**» номли тўртинчи бобида ҳужумларни аниқлашнинг нейрон тармоқ усули ва алгоритмининг самарадорлиги баҳоланган ҳамда интерактив ва сеанс моделлардан фойдаланиб қурилган тармоқ аномалияларини аниқлаш алгоритмининг дастурий воситасини ишлаш принципи ва жорий этишдан олинган тажриба-ҳисоблаш натижалари келтирилган.

Биринчи параграфда ҳужумларни аниқлашда нейрон тармоқ усулининг самарадорлиги учта асосий кўрсаткич бўйича баҳоланган. Ҳужумларни аниқлашда нейрон тармоқ усули ҳужумларни таъсир даражаси бўйича аниқлашга ҳамда тизимнинг ёлғон ишга тушиш эҳтимолини камайтиришга ва ҳужумларни аниқлаш кўрсатгичларини оширишга имкон беради.

1-жадвал

Ҳужумларни аниқлашнинг нейрон тармоқ усулини тестлаш натижалари

Ҳужум синфи	Жами ҳужумлар сони	Аниқланган ҳужумлар %	Аниқланмаган ҳужумлар %	Тизимни ёлғон ишга тушишлари %
DoS	32678	95,1	4,1	0,8
U2R	68	94,3	5,2	0,5
R2L	1265	92,3	7,1	0,6
Probe	3233	91,1	8,2	0,7

Иккинчи параграфда тармоқ аномалияларини аниқлаш алгоритмининг самарадорлиги баҳоланган, аномалияларни аниқлашни унумдорлиги турлича бўлган процессор ва график процессорли компьютерларда ўтказилган тестлаш натижалари 2-жадвалда келтирилган.

2-жадвал

Аномалияларни аниқлашнинг унумдорлиги турлича бўлган процессор ва график процессорли компьютерларда ўтказилган тестлаш натижалари

Аномалияларни аниқлаш тизимлари (ААТ)	Intel core i3 3.3GHz, 4Gb тезкор хотира	Intel core i9 7900K, 32Gb тезкор хотира	Intel core i9 7900K, 32Gb тезкор хотира, GTX 1080 TI график процессор
MAS (ААТ)	0,4 с	30 мс	14 мс
NeuroDAT (ААТ)	2 с	57 мс	51 мс
Visor (ААТ)	1 с	55 мс	43 мс
Security Capsule (ААТ)	0,8 с	49 мс	21 мс
Suricata 5.0.3 (ААТ)	0,6 с	35 мс	15 мс

3-жадвал

Аномалияларни аниқлашда тизимнинг ёлғон ишга тушиш кўрсатгичлари

Аномалияларни аниқлаш тизимлари (ААТ)	Аномалиялар сони	Аниқлик %	Тизимнинг ёлғон ишга тушиш %
MAS (ААТ)	65	96,4	3,6
NeuroDAT (ААТ)	65	91,8	8,9
Visor (ААТ)	65	93,4	6,6
Security Capsule (ААТ)	65	94,6	5,4
Suricata 5.0.3 (ААТ)	65	95,2	4,8

Учинчи параграфда кўпагентли интеллектуал усуллар ёрдамида корхонадаги ахборотни ҳимоялаш тизимининг дастурий воситаси ва уни амалиётга татбиқ этиш натижалари келтирилган.

MAS тизими реал вақт маштабида (real-time packet analysis) тармоқ пакетларини таҳлиллаш технологияси бўйича қурилган бўлиб, тармоқнинг бутун сегментини (network-based) ҳимоялашга йўналтирилган ҳужумларни аниқлаш тизимидир.

Корхона ахборот тизимига бўладиган ҳужумларни аниқлаш дастурий воситаси Ўзбекистон Республикаси «Акциядорлик тижорат Халқ банки» бош амалиётлар бошқармасида, «UNICON.UZ» Давлат унитар корхонаси – Фан – техника ва маркетинг тадқиқотлари марказида ва Ўзбекистон Республикаси Мудофаа вазирлиги Ахборот – коммуникация технологиялари ва алоқа ҳарбий институтида жорий этилган ва натижалар қуйида келтирилган:

Ўзбекистон Республикаси «Акциядорлик тижорат Халқ банки» бош амалиётлар бошқармасида барча тармоқ ҳужумлари 4 та гуруҳга ажратиб олинди. Булар: DoS ҳужум; U2R ҳужуми; R2L ҳужум; Probe ҳужуми. Ишлаб чиқилган дастурий таъминот нейрон тармоқ усулидан фойдаланганлиги сабабли, DoS ҳужумларни аниқлашда 94,7% аниқлик ва 5,3% хатолик, U2R ҳужумларни аниқлашда 91,4% аниқлик ва 8,6% хатолик, R2L ҳужумларни аниқлашда 93,6% аниқлик ва 6,4% хатолик, Probe ҳужумларини аниқлашда 95,8% аниқлик ва 4,2% хатолик билан тармоқ ҳужумларини аниқлаш имконини берган;

«UNICON.UZ» Давлат унитар корхонаси – Фан – техника ва маркетинг тадқиқотлари марказида ташкилотнинг локал тармоғига бўладиган ҳужумларни аниқлаш жараёнида пайдо бўлган хатоликларни аниқлаш мақсадида тажриба синовлари ўтказилди. Синовдан ўтиш жараёнида хатоликлар хақида тизим маъмурини огоҳлантириш функцияси мавжуд эканлиги аниқланди;

Ўзбекистон Республикаси Мудофаа вазирлиги Ахборот – коммуникация технологиялари ва алоқа ҳарбий институтида ташкилотнинг корпоратив

тармоғига бўлган ҳужумларни аниқлаш жараёнида, ҳужумларни 94,3% аниқлик ва 5,7% хатолик билан аниқлаш имконини берган.

Дастурий маҳсулотни ташкилотларда қўллаш натижасида олинган натижалар асосида айтиш мумкинки, битта ҳужумга тегишли бўлган сигнатуралар турли кўринишда бўлиши мумкинлигини ва ҳужум сигнатуралар сонининг кўплиги ҳужумни таниб олиш даражасининг ортишига олиб келади. Аномалияларни аниқлаш асосида янги турдаги ҳужумларни аниқлаш, корхонанинг корпоратив тармоғидаги ҳар бир фойдаланувчи ҳаракатларини алоҳида агентлар томонидан назоратга олишга ва бу фойдаланувчилар тўғрисидаги ҳисоботга эга бўлишга ҳамда тармоқ маъмурларининг баъзи вазифаларини автоматлаштиришга эришилди.

ХУЛОСА

«Корхонадаги ахборотни ҳимоялашнинг кўпагентли интеллектуал усулларини ишлаб чиқиш» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Ахборот хавфсизлигини таъминлашда фойдаланиладиган гибрид тизимларни таҳлил қилиш асосида корхонадаги ахборотни ҳимоялашнинг кўпагентли интеллектуал тизимини қуриш концепцияси ишлаб чиқилди. Натижада концепцияда кўрсатилган принциплар асосида корхонадаги ахборотни ҳимоялашни бошқариш тизимининг мақсадлар дарахтини шакллантириш имконини берди.

2. Мақсадлар дарахти асосида корхонадаги ахборотни ҳимоялашни интеллектуал тизимининг архитектураси ишлаб чиқилди ва хавфсизлик маъмурига ўз кучларини режалаштиришни ташкиллаштиришга ва корхона ахборот активларини ҳимояланганлик ҳолатини назоратлаш имконини берди.

3. Ҳосил бўлиш частотаси асосида таҳдидларни таъсир даражасини аниқлаш усули ишлаб чиқилди. Натижада корхонадаги ахборотни ҳимоялаш воситаларини тезкор бошқаришда қарор қабул қилиш имконини берди.

4. Сигнатурали таҳлилга асосланган ҳужумларни аниқлашнинг нейрон тармоқ усули ва алгоритми ишлаб чиқилди. Натижада корхона ахборот тизимига бўладиган тармоқ ҳужумларининг таъсир даражаси (паст, ўрта, юқори) бўйича аниқлаш имконини берди.

5. Интерактив ва сеанс моделлар асосида тармоқ аномалияларини аниқлаш алгоритми ишлаб чиқилди. Натижада тармоқ аномалияларини аниқлашда тизимнинг ёлғон ишга тушиш қўрсаткичи 1,2 % пасайишига ҳамда тизим тезлигини 1 мс ортишига имкон берди.

6. Кўпагентли интеллектуал усуллар асосида ишлаб чиқилган ҳужумларни аниқлашнинг MAS дастури 95,8% аниқликни кўрсатди. Ҳужумларни аниқлашда бунданда яхшироқ самарадорлик кўрсатгичига эришиш учун ҳужум сигнатуралар базасини доимий равишда янгилаб бориш бўйича тавсиялар келтирилди.

Таклиф этилган кўпагентли интеллектуал усуллар асосида ишлаб чиқилган корхонадаги ахборотни ҳимоялаш тизими ахборотнинг бутун ҳаётий цикли давомида ишончли ҳимоясини таъминлаш имконини беради.

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

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

БОТИРОВ ФАЙЗУЛЛАЖОН БАХТИЁРОВИЧ

РАЗРАБОТКА МНОГОАГЕНТНЫХ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

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

Ташкент-2021

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2020.4.PhD/T1941.

Диссертация выполнена в Ташкентском университете информационных технологий.

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

Научный руководитель:	**Бекмуратов Тулкун Файзиевич** академик, доктор технических наук, профессор
Официальные оппоненты:	**Каримов Маджит Маликович** доктор технических наук, профессор
	Жураев Гайрат Умарович доктор физико-математических наук, доцент
Ведущая организация:	**«UNICON.UZ» - центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «6» февраля 2021 года в 10:00 часов на заседании Научного совета DSc. 13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №263). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «___» _____ 2021 года.
(протокол рассылки №__ от «___» _____ 2021 года.)

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

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

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

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. При решении задач обнаружения и предотвращения атак на информационную систему предприятия с помощью многоагентных систем, основное внимание уделяется повышению точности процесса обнаружения атак и уменьшению количества ошибок. «По данным компании Kaspersky, в первом квартале 2020 года доля атак на государственные организации увеличилась, а атаки на такие объекты, как компьютеры, серверы и сетевые устройства составили 89% от общего числа всех атак»[1]. В зарубежных странах, в том числе в США, Российской Федерации, КНР, Южной Корее и др., проводятся работы, посвященные определению уровня воздействия информационных угроз на основе интеллектуальных методов, направленные на совершенствование моделей и алгоритмов обнаружения сетевых атак, а также на обнаружение сетевых атак с использованием многоагентных систем. В связи с этим, одной из важных задач является разработка методов обнаружения атак, в том числе на основе сигнатур и сравнения данных заголовков пакетов. Вместе с тем, необходимо развивать и направление использования многоагентных интеллектуальных систем для защиты информации в случае неполного знания рассматриваемого объекта в процессе защиты информации или неточностей в текущих данных.

В Узбекистане принимаются комплексные меры по совершенствованию механизмов защиты на основе интеллектуальных систем, используемых в процессе защиты информации в органах государственного и хозяйственного управления. В Стратегии действий по дальнейшему развитию Республики Узбекистан на 2017-2021 годы определены задачи, в том числе «...обеспечение информационной безопасности и совершенствование системы защиты информации, своевременное и адекватное реагирование на угрозы в сфере информации»[2]. Одной из важных решений при реализации этих задач является использование многоагентных интеллектуальных методов при обнаружении атак на информацию, а также использование интеллектуальных систем в защите информации.

Данное диссертационное исследование в определенной степени послужит для реализации задач, обозначенных в Указах Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-5349 от 19 февраля 2018 г. «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», в Постановлениях №ПП-4024 от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» и №ПП-4452 от 14 сентября 2019 года «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их

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

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

защиты», а также в других нормативно-правовых документах, связанных с этой деятельностью.

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

Степень изученности проблемы. По разработке методов и алгоритмов, разработанных с использованием направлений, относящихся к семейству нейронных сетей, многоагентных систем и аналогичных интеллектуальных систем по обеспечению информационной безопасности ведутся научные исследования со стороны А.В.Остроух, Г.А. Поллак, В.И. Васильев, Е.А. Жидко, А.В. Торопова, S. Kaur, A. Алнафессах, М.Сингх и многих других зарубежных ученых. Научные исследования по обеспечению информационной безопасности с применением нейронных сетей проводились Х. Юан, Н. Шин, Ж. Лее, Й. Чои, Ж. Ким. Кроме того, со стороны организаций InfoWatch, RiskWatch, WatchGuard и Trend Micro проводятся инженерные исследования по разработке программных и аппаратных средств для защити информации с использованием интеллектуальных систем.

В Узбекистане со стороны научных сообществ во главе с Т. Ф. Бекмуратовым, С. К. Ганиевым, Н .А. Игнатьевым, М. М. Каримовым проводятся научные исследования по интеллектуальным системам защиты информации, рисками информационной безопасности, методами и алгоритмам обнаружения угроз.

Вместе с тем, методы и алгоритмы обнаружения и устранения атак на основе многоагентных систем, нейронных сетей, машинного обучения (machine learning) и глубокого обучения (deep learning) недостаточно изучены.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках проекта Ташкентского университета информационных технологий №БВ-Ф4-023 – «Исследование проблем управления инцидентами и противодействия кибератакам в распределенных информационно-коммуникационных системах» (2017-2020) согласно плану научно-исследовательской работ.

Целью исследования является разработка многоагентных интеллектуальных методов, которые позволят повысить эффективность системы защиты информации.

Задачи исследования:

сравнительный анализ интеллектуальных систем и технологий защиты информации;

разработка концепции построения многоагентной интеллектуальной системы защиты информации на предприятии;

разработка структуры и архитектуры интеллектуальной системы защиты

информации;

разработка метода определения степени воздействия потенциальных угроз на информацию предприятия;

разработка методов и алгоритмов обнаружения потенциальных атак на информационные системы предприятия;

разработка алгоритмов обнаружения сетевых аномалий.

Объектом исследования является процесс защиты информации на предприятии.

Предмет исследования являются многоагентные интеллектуальные методы и алгоритмы защиты информации.

Методы исследования. В процессе исследования были использованы методы защиты информации с использованием интеллектуальных систем, нейронных сетей, теории нечётких множеств, теории вероятностей, теории графов, дискретной математики и объектно-ориентированного программирования.

Научная новизна исследования заключается в разработке:

разработана концепция многоагентной интеллектуальной системы с учетом трехуровневого механизма защиты информации на предприятии;

разработана архитектура интеллектуальной системы защиты информации на основе целевого дерева трехуровневого механизма защиты;

разработан метод определения уровня воздействия на основе частоты угроз информации на предприятии;

разработаны нейросетевой метод и алгоритм обнаружения сетевых атак основанных на сигнатурного анализа;

разработан алгоритм обнаружения сетевых аномалий на основе интерактивных и сеансовых моделей, которые предсказывают последующие действия пользователей на основе их предыдущих действий.

Практические результаты исследования заключаются в следующем:

разработан программный комплекс защиты информации на предприятии на основе многоагентных интеллектуальных методов;

в процедуре обнаружения атак на основе анализа сигнатур базы Snort и Suricata были обобщены и улучшены показатели обнаружения атак за счет добавления дополнительных сигнатур.

Достоверность результатов исследования. Достоверность результатов исследования подтверждаются результатами реального и экспериментального анализа, полученные при различных условиях - от методов обнаружения атак, до определения степени воздействия угроз на информационную систему предприятия.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования объясняется методом определения уровня воздействия угрозы в процессе защиты информации на разрабатываемом предприятии, нейросетевым методом обнаружения атак на основе сигнатуры и алгоритмом обнаружения сетевых аномалий на основе интерактивных и сеансовых моделей.

Практическая значимость результатов исследования объясняется тем, что программное средство, разработанное на основе предложенных методов и алгоритмов, помогает интеллектуализировать процесс защиты информации на предприятии.

Внедрение результатов исследования. На основе научных результатов, полученных в области многоагентных методов защиты информации и программных средств на предприятии:

- программный инструмент нейросетевого метода обнаружения атак с использованием сигнатурного анализа в процессе защиты информации на предприятии внедрен в практическую деятельность главного операционного управления Республики Узбекистан "Акционерный коммерческий Народный банк" (справка Министерства по развитию информационных технологий и коммуникаций № 33-8/7051 от 24 ноября 2020 года). Результаты научного исследования позволили обнаружить DoS-атаки в корпоративной сети с точностью в 94,7% и погрешностью в 5,3%, атаки U2R с точностью в 91,4% и погрешностью в 8,6%, атаки R2L с точностью в 93,6% и погрешностью в 6,4%, атаки Probe с точностью в 95,8% и погрешностью в 4,2%;

- программное средство метода анализа угроз в процессе защиты информации на предприятии внедрено в практическую деятельность Государственного унитарного предприятия «UNICON.UZ» - Центра научно-технических и маркетинговых исследований (справка Министерства по развитию информационных технологий и коммуникаций № 33-8/7051 от 24 ноября 2020 года). В результате научного исследования создана возможность предупреждения системного администратора об ошибках при обнаружении атак на локальную сеть организации;

- программное средство обнаружения сетевых аномалий на основе интерактивных и сеансовых моделей внедрено в практическую деятельность Военного института информационно-коммуникационных технологий и связи Министерства обороны Республики Узбекистан (справка Министерства по развитию информационных технологий и коммуникаций № 33-8/7051 от 24 ноября 2020 года). Результаты научного исследования позволили обнаруживать атаки в корпоративной сети с точностью в 94,3% и погрешностью в 5,7%.

Апробация результатов исследования. Результаты исследования были обсуждены на 3 международных и 4 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме диссертации опубликовано всего: 18 научных работ, в том числе 8 статей в научных изданиях, рекомендованных Высшей аттестационной комиссии Республики Узбекистан к публикации основных научных результатов диссертаций, из них 4 - в зарубежных и 4 - в республиканских журналах, а также получены 3 свидетельства о регистрации программных продуктов для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 112 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и востребованность темы диссертации, обосновано соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, сформулированы цель и задачи, а также определены объект и предмет исследования, обоснована достоверность полученных результатов, приведена их теоретическая и практическая значимость, состояние внедрения результатов исследования на практике, опубликованные работы и структура диссертации.

В первой главе диссертации, озаглавленной как **«Многоагентные интеллектуальные системы и технологии защиты информации»** приведены сравнительный анализ интеллектуальных систем и технологий защиты информации на предприятии и этапы построения механизмов защиты информации на основе многоагентных интеллектуальных систем, а также даны рекомендации по автоматизации защиты информации.

В *первом параграфе* проведен сравнительный анализ современных этапов развития интеллектуальных систем, а также интеллектуальных систем и технологий защиты информации. Определены основные задачи интеллектуальных систем, обеспеченных информационной безопасностью, и приведены примеры многоагентных интеллектуальных систем, обеспечивающих высокую степень автономности, гибкости в условиях неопределенности и ивзаимодействия агентов для выполнения этих задач.

Во втором параграфе представлены простая структура агента, интеллектуальные свойства агента, отличительные признаки многоагентных систем, распределенная архитектура многоагентных систем, используемых при обнаружении атак, преимущества использования многоагентных систем при защите информации, а также сравнительный анализ агентов с различными характеристиками. Сформулированы основные требования к агентам, использующим многоагентную систему, и предложено построение механизмов защиты информации на основе многоагентных интеллектуальных систем.

Рис. 1. Этапы построения механизмов защиты информации на основе многоагентной интеллектуальной системы

В третьем параграфе представлены рекомендации по созданию трехуровневой иерархической автоматизированной системы обеспечения информационной безопасности для интеллектуализации системы защиты информации на предприятии. Схема автоматизации системы защиты информации на предприятии представлена на рис..

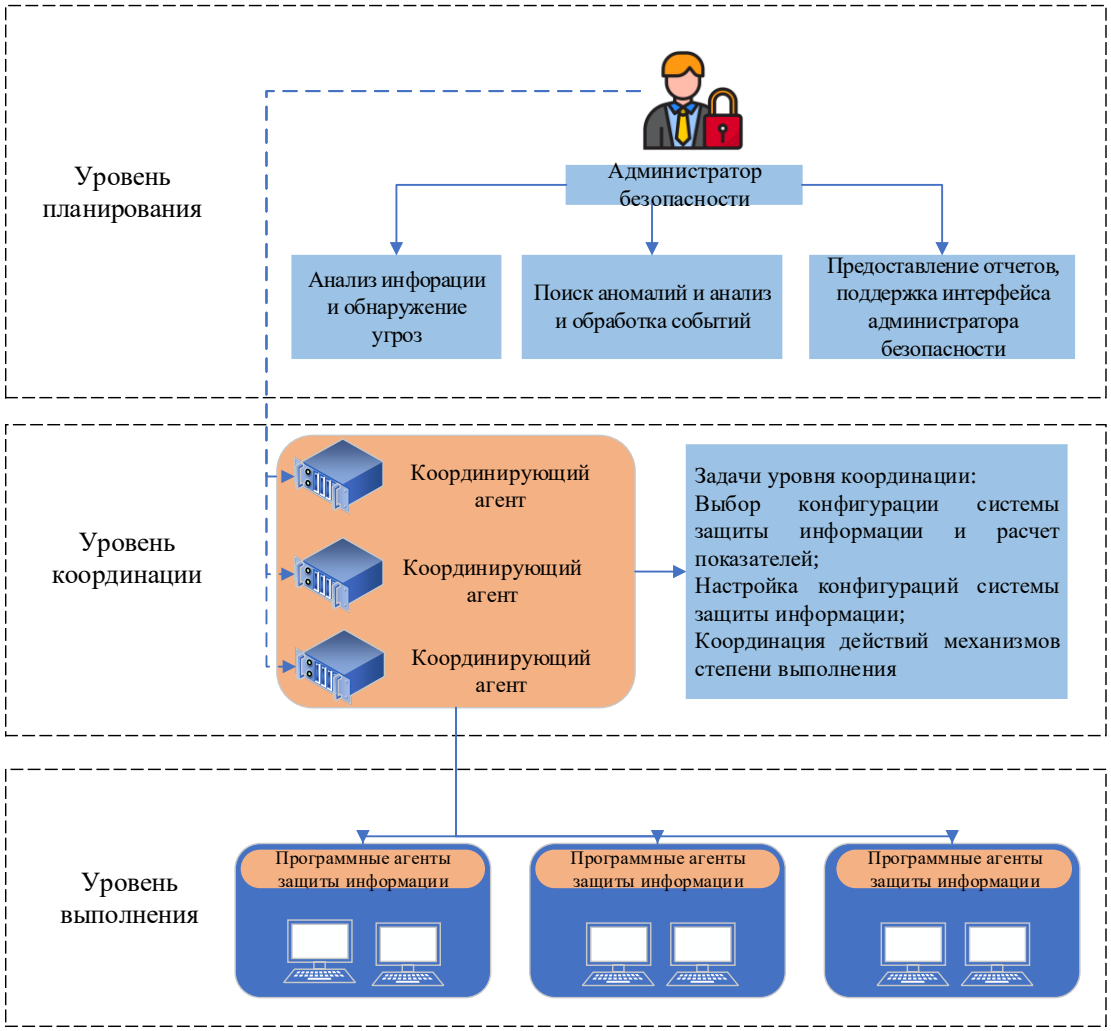


Рис. 2. Схема автоматизации процесса защиты информации на предприятии

Во второй главе диссертации под названием **«Разработка концепции, структуры и архитектуры построения многоагентной интеллектуальной системы защиты информации на предприятии»** разработаны концепция, структура и архитектура построения многоагентной интеллектуальной системы защиты информации на предприятии. Определены задачи, которые должны быть выполнены в процессе управления защитой информации.

В первом параграфе данной главы разработана концепция построения автоматизированной интеллектуальной системы защиты информации в информационной системе предприятия. Концепция включает в себя следующие принципы:

1. Принцип функционального интегрирования, который предусматривает создание интегрированной системы защиты информации на предприятии.

2. Принцип организации системы защиты информации на предприятии в многоуровневом интегрированном иерархическом виде.

3. Принцип укомплектованности методов и алгоритмов определения степени воздействия потенциальных угроз на информацию на предприятии.

4. Принцип стандартизации, означающий, что требования к построению систем защиты информации должны соответствовать действующим стандартам защиты информации.

5. Принцип интеллектуализации обнаружения и устранения потенциальных атак на информационную систему предприятия.

Во втором параграфе сформировано целевое дерево системы управления информационной безопасностью предприятия на основе принципов, изложенных в концепции. На основе иерархии целевого дерева разработана структура автоматизированной схемы управления и интеллектуальной системы защиты информации. На рис. 3 представлена структура интеллектуальной системы защиты информации.

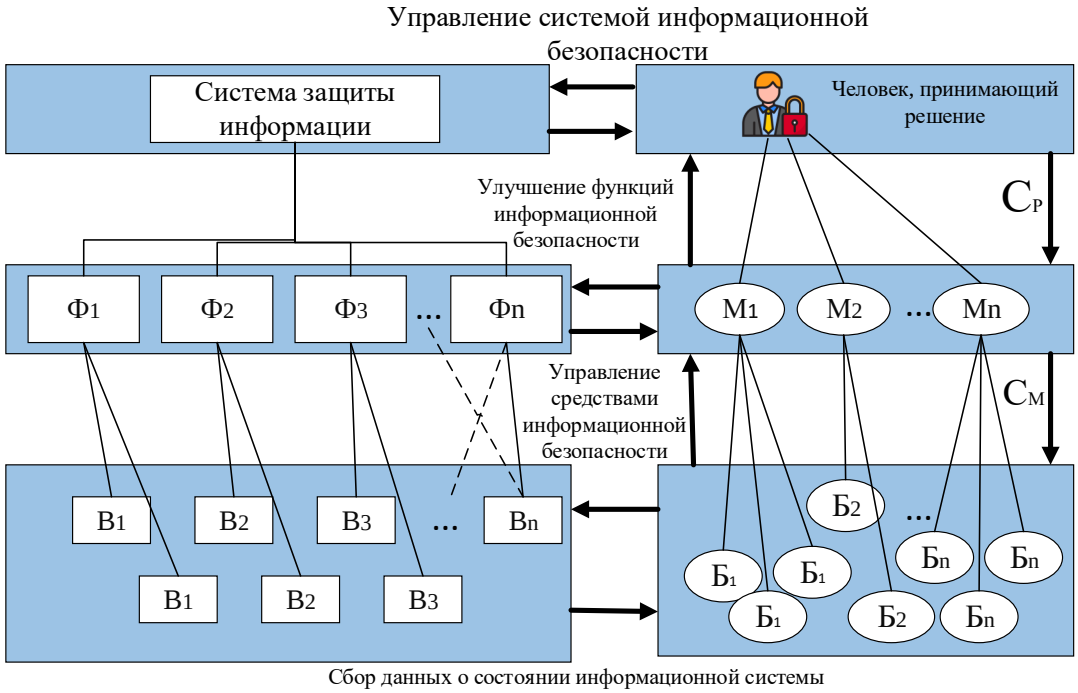


Рис. 3. Структура интеллектуальной системы защиты информации

Результат работы администраторов безопасности, то есть лиц, принимающих решения, передается для исполнения координирующим агентам $С_Р$. где: $С_Р$ – агент обмена информацией между уровнями планирования и координации; $С_М$ – агент обмена информацией между уровнями координации и реализации; $М_i$ – агенты уровня координации, $i = 1,2,\dots n.$; $Б_i$ – агенты уровня исполнения, $i = 1,2,\dots n.$; $Ф_i$ – пользователь в информационной системе предприятия $i = 1,2,\dots n.$; $В_i$ – элемент средства в информационной системе предприятия $i = 1,2,\dots n.$;

В третьем параграфе разработана архитектура многоагентной интеллектуальной системы защиты информации (рис. 4). Она позволяет размещать программные агенты в виде программных модулей на всех узлах информационной системы предприятия, управлять подсистемами защиты

информации и всеми средствами, а также записывать все события, влияющие на безопасность информационных активов.

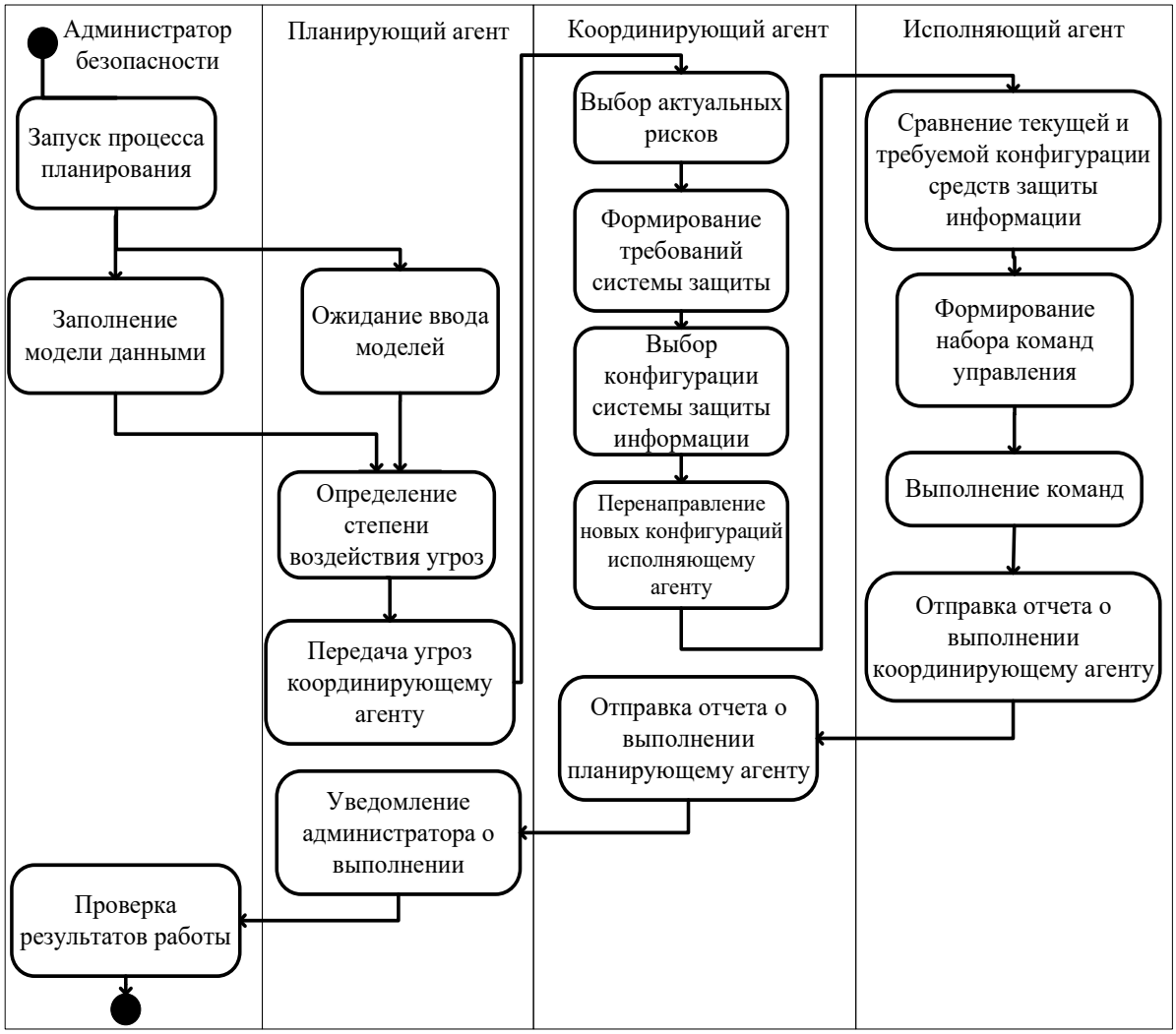


Рис. 4. Архитектура интеллектуальной системы защиты информации

Во третьей главе диссертации под названием «**Методы и алгоритмы обнаружения степени воздействия потенциальных угроз информационной системе предприятия и обнаружения атак**» разработаны метод определения степени воздействия потенциальных угроз на информацию предприятия, нейросетевой метод обнаружения атак на информационную систему предприятия, а также алгоритмы обнаружения сетевых аномалий на основе интерактивных и сеансовых моделей.

В первом параграфе разработан метод определения степени воздействия угроз на основе частоты их возникновения. Степень воздействия угроз определяется двумя критериями: частотой возникновения угрозы и величиной вероятного ущерба, наблюдаемого при осуществлении угрозы со стороны потенциального нарушителя. На первом шаге определения уровня воздействия угроз строится матрица сравнения угроз по критерию частоты возникновения T.

$$T = \begin{pmatrix} 1 & t_1/t_2 & \dots & t_1/t_x \\ t_2/t_1 & 1 & \dots & t_2/t_x \\ \vdots & \vdots & \dots & \vdots \\ t_x/t_1 & t_x/t_2 & \dots & 1 \end{pmatrix}, \qquad T_c = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_x \end{pmatrix}$$

где, Т-матрица двойного сравнения угроз. $T_C - T$ нормализованные собственные векторы матрицы приоритетов. $\forall\, t_a \in T,\ a = 1, 2, \dots . x$:

Затем строится матрица сравнения уязвимостей Z, для каждой угрозы с вектором приоритетов Z_c, указывающим вероятный путь реализации угроз.

$$Z = \begin{pmatrix} 1 & z_1/z_2 & \dots & z_1/z_n \\ z_2/z_1 & 1 & \dots & z_2/z_n \\ \vdots & \vdots & \dots & \vdots \\ z_n/z_1 & z_n/z_2 & \dots & 1 \end{pmatrix}, Z_c = \begin{pmatrix} z_1^1 & z_1^2 & \dots & z_1^x \\ z_2^1 & z_2^2 & \dots & z_2^x \\ \vdots & \vdots & \dots & \vdots \\ z_n^1 & z_n^2 & \dots & z_n^x \end{pmatrix}$$

где Z_c – нормированные собственные векторы матрицы приоритетов Z.
$\forall\, z_b \in Z, \qquad b = 1, 2, \dots . n$:

$$R = \begin{pmatrix} 1 & r_1/r_2 & \dots & r_1/r_s \\ r_2/r_1 & 1 & & r_2/r_s \\ \vdots & \vdots & \dots & \vdots \\ r_s/r_1 & r_s/r_2 & \dots & 1 \end{pmatrix}, R_c = \begin{pmatrix} r_1^1 & r_1^2 & \dots & r_1^z \\ r_2^1 & r_2^2 & \dots & r_2^z \\ \vdots & \vdots & \dots & \vdots \\ r_s^1 & r_s^2 & \dots & r_s^z \end{pmatrix}$$

где R – матрица двойного сравнения ресурсов. $R_c -$ матрица нормированных собственных векторов матрицы приоритетов R. $\forall\, r_v \in R,\ v = 1, 2, \dots . s$:

После этого шага рассчитывается степень воздействия угрозы по формуле D.

$$\mathrm{D} = \begin{pmatrix} \sum_{j=1}^{n} t_1^c * z_j^c * r_1^c & \sum_{j=1}^{n} t_1^c * z_j^c * r_2^c & \dots & \sum_{j=1}^{n} t_1^c * z_j^c * r_s^c \\ \sum_{j=1}^{n} t_2^c * z_j^c * r_1^c & \sum_{j=1}^{n} t_2^c * z_j^c * r_2^c & \dots & \sum_{j=1}^{n} t_2^c * z_j^c * r_s^c \\ \vdots & \vdots & \dots & \vdots \\ \sum_{j=1}^{n} t_x^c * z_j^c * r_1^c & \sum_{j=1}^{n} t_x^c * z_j^c * r_2^c & \dots & \sum_{j=1}^{n} t_x^c * z_j^c * r_s^c \end{pmatrix}$$

Вычисление степени воздействия угроз дает возможность принятия решений по их уменьшению или устранению.

Во втором параграфе разработан нейросетевой метод и алгоритм обнаружения атак на основе сигнатурного анализа. Этот метод осуществляется в три этапа:

- в первом этапе осуществляется захват сетевого трафика. Для сбора информации о заголовках сетевых пакетов, которые характеризуют

анализируемый трафик, специальный пакет-сниффер захватывает все пакеты, которые проходят через протоколы TCP и UDP;

- на втором этапе выделяются параметры с наивысшим приоритетом, характеризующие сетевую активность. С помощью классификатора высокоприоритетные параметры классифицируются по группам, и анализ высокоприоритетных параметров вместо анализа каждого параметра в процессе обнаружения атак позволяет повысить точность;

- на третьем этапе осуществляется обнаружение атак. На этом этапе используется нейронная сеть, которая эффективно определяет степень схожести текущих характеристик сетевой активности с системами обнаружения атак на основе простого сравнения заголовков пакетов.

Таким образом, классификатор, составленный на основе анализа входного трафика, включает следующие переменные, в том числе вектор параметров входа:

A_1 – среднее время прибытия одного пакета;

A_2 – процент пакетов с разными внешними IP- адресами;

A_3 – процент различных пакетов внешних портов;

A_4 – процент пакетов с неверным заголовком.

Выходное значение классификатора осуществляется экспертами *B,* которые определяют состояние «степень надежности при атаке». Параметры A_1, A_2, A_3, A_4 вышеуказанного сетевого трафика и степень надежности при атаке *B* имеют следующий вид:

- ЕСЛИ время_прибытия_пакетов = «меньше» и
  проценты_разных_внешних_IP_адресов_«меньше» и
  процент_разных_портов = «меньше», ТО
  степень_воздействия_в атаки = **«средний»**;
- ЕСЛИ (время_прибытия_пакетов = «меньше» или
  время_прибытия_пакетов = «среднее») и
  (проценты_разных_внешних_IP_адресов_«больше» или
  процент_разных_портов = «больше» или
  процент_пакетов_с неправильным_заголовком = «больше»), ТО
  степень_воздействия_в атаки = **«высокий»**;
- ЕСЛИ время_прибытия_пакетов = «больше», ТО
  степень_воздействия_в атаки = **«низкий»**.

Таким образом, она дает возможность определить степень воздействия (низкий, средний, высокий) сетевых атак на информационную систему предприятия.

В третьем параграфе разработан алгоритм обнаружения сетевых аномалий на основе интерактивных и сеансовых моделей. Получены выходные значения интерактивных и сеансовых моделей для обнаружения аномалий: выходное значение интерактивной модели (Y_t), выходное значение сеансовой модели (Y'_t). Выходные значения этих моделей анализируются параллельно в сетевом трафике для принятия решений о наличии или отсутствии аномалий, наряду с измерениями голоса. Было предложено

минимизировать первичную и вторичную погрешности, повысить точность и полноту классификации.

№1. Начало алгоритма.

№2. Выполняется анализ трафика.

№3-5. Анализирует трафик на наличие аномалий и выполняется как вызов каждой модели. Если результаты классификации являются аномалией согласно алгоритму (Y_t), то y_t=+1. В противном случае, y_t=-1. В результате каждый метод голосует, есть ли аномалии или нет y_t=±1, y'_t =±1.

№6. Производится поиск трафика, близкого к аномалии.

№7. Для каждого выходного значения модели при установке голосовой нагрузки в принятии общего решения о наличии или отсутствии аномалий в анализируемом трафике вычисляется индикатор качества классификации на основе F-измерения.

№8. Если значения выходного пути обеих моделей голосуют за отсутствие аномалии, то голосование не требуется, и принимается совместное первичное решение о результатах классификации, и аномалии не существуют в сети (№9). Если выходное значение хотя бы одной модели обнаруживает аномалию, требуется голосование в совместном решении и выполняется переход к №10.

№10. Запускается практика голосования *S* на наличие или отсутствие аномалий.

№11-13. Если S> 0, то результат голосования не является сетевой аномалией. В противном случае, в результате голосования возникнет сетевая аномалия.

№14-16. Если пакет, подвергающийся анализу алгоритма, является последним, то алгоритм завершается. В противном случае, возвращается к №8.

В четвертой главе диссертации под названием «**Результаты оценки эффективности и внедрения на практике системы защиты информации на основе многоагентных интеллектуальных методов**» оценивалась эффективность нейросетевого метода и алгоритма обнаружения атак, а также приведены принцип работы программного средства алгоритма обнаружения сетевых аномалий, построенного с использованием интерактивных и сеансовых моделей и экспериментально-расчетные результаты, полученные при внедрении.

В первом параграфе эффективность нейросетевого метода в обнаружении атак оценивалась по трем основным показателям. При обнаружении атак нейросетевой метод позволяет обнаруживать атаки по степени их воздействия, а также снижает вероятность системы на ложный запуск системы и повышает показатели обнаружения атак.

Таблица 1

Результаты тестирования нейросетевого метода обнаружения атак

Класс атаки	Общее количество атак	Обнаруженные атаки %	Не обнаруженные атаки %	Ложные запуски системы %
DoS	32678	95,1	4.1	0,8
U2R	68	94,3	5.2	0,5
R2L	1265	92,3	7.1	0,6
Probe	3233	91,1	8,2	0,7

Во втором параграфе оценивалась эффективность алгоритма обнаружения сетевых аномалий, а результаты тестирования, выполненных на компьютерах с различной производительностью обнаружения аномалий и графических процессорах, представлены в таблице 2.

Таблица 2

Результаты тестирования, выполненных на компьютерах с различной производительностью обнаружения аномалий и графических процессорах

Системы обнаружения аномалий (AAT)	Intel core i3 3,3 ГГц, 4 Гб оперативной памяти	Intel core i9 7900K, 32 ГБ оперативной памяти	Intel core i9 7900K, 32 ГБ оперативной памяти, Графический процессор GTX 1080 TI
MAS (AAT)	0,4 с	30 мс	14 мс
NeuroDAT (AAT)	2 с	57 мс	51 мс
Visor (AAT)	1 с	55 мс	43 мс
Security Capsule (AAT)	0,8 с	49 мс	21 мс
Suricata 5.0.3 (AAT)	0,6 с	35 мс	15 мс

Таблица 3

Показатели ложного запуска системы при обнаружении аномалий

Системы обнаружения аномалий (AAT)	Количество аномалий	Точность %	Ложный запуск системы %
MAS (AAT)	65	96,4	3,6
NeuroDAT (AAT)	65	91,8	8.9
Visor (AAT)	65	93,4	6,6
Security Capsule (AAT)	65	94,6	5,4
Suricata 5.0.3 (AAT)	65	95,2	4.8

В третьем параграфе представлено программное средство системы защиты информации на предприятии с использованием многоагентных интеллектуальных методов и результаты его внедрения на практике.

Система MAS построена на технологии анализа сетевых пакетов в масштабе реального времени (real-time packet analysis) и представляет собой систему обнаружения атак, ориентированную на защиту всего сегмента сети (network-based).

Программное средство обнаружения атак на информационную систему предприятия внедрено в главном операционном управлении «Акционерного коммерческого народного банка» Республики Узбекистан, ГУП UNICON.UZ-Центре научно-технических и маркетинговых исследований и Военном институте информационно-коммуникационных технологий и связи Министерства обороны Республики Узбекистан, результаты которого приведены ниже:

в Главном операционном управлении Акционерного коммерческого народного банка Республики Узбекистан все сетевые атаки были разделены на 4 группы. Это: DoS-атака; U2R атака; R2L атака; Probe атака. Поскольку разработанное программное обеспечение использует метод нейронной сети, результаты исследования позволили обнаруживать DoS-атаки с точностью в 94,7% и погрешностью в 5,3%, атаки U2R с точностью в 91,4% и погрешностью в 8,6%, атаки R2L с точностью в 93,6% и погрешностью в 6,4%, Probe атаки с точностью в 95,8% и погрешностью в 4,2%;

в ГУП «UNICON.UZ» - Центре научно-технических и маркетинговых исследований были проведены экспериментальные испытания с целью выявления ошибок в процессе обнаружения атак на локальную сеть организации. В процессе тестирования было обнаружено, что существует функция оповещения системного администратора об ошибках.

В процессе обнаружения атак на корпоративную сеть организации в Военном институте информационно-коммуникационных технологий и связи Министерства обороны Республики Узбекистан удалось обнаружить атаки с точностью в 94,3% и погрешностью в 5,7%.

Исходя из результатов, полученных при применении программного продукта в организациях, можно сказать, что сигнатуры, принадлежащие одной атаке, можно рассматривать по-разному, а кратность числа сигнатур атак приводит к повышению уровня распознавания атак. Были достигнуты обнаружение новых типов атак на основе обнаружения аномалий, контроль действий каждого пользователя в корпоративной сети предприятия отдельными агентами и доступ к отчету об этих пользователях, а также автоматизация некоторых функций сетевых администраторов.

ВЫВОД

В результате исследования по диссертационной работе на тему «Разработка многоагентных интеллектуальных методов защиты информации на предприятии» были сделаны следующие выводы:

1. На основе анализа гибридных систем, используемых для обеспечения информационной безопасности, разработана концепция построения многоагентной интеллектуальной системы защиты информации на предприятии. В результате, на основе принципов, изложенных в концепции, удалось сформировать дерево целей системы управления информационной безопасностью на предприятии.

2. На основе дерева целей была разработана архитектура интеллектуальной системы защиты информации на предприятии, позволяющая администратору безопасности организовать планирование своих сил и контролировать состояние защиты информационных активов предприятия.

3. Разработан метод определения степени воздействия угроз по частоте их возникновения. В результате, появилась возможность оперативно принимать решения по управлению средствами защиты информации на предприятии.

4. Разработаны нейросетевой метод и алгоритм обнаружения атак на основе анализа сигнатур. В результате, предприятие смогло идентифицировать сетевые атаки на информационную систему по степени воздействия (низкий, средний, высокий).

5. Разработан алгоритм обнаружения сетевых аномалий на основе интерактивных и сеансовых моделей. В результате, при обнаружении сетевых аномалий частота ложных запусков системы снизилась на 1,2%, а скорость системы увеличилась на 1 мс.

6. Программа MAS для обнаружения атак, разработанная на основе многоагентных интеллектуальных методов, показала точность в 95,8%. Были представлены рекомендации по регулярному обновлению базы данных сигнатур атак, чтобы повысить эффективность обнаружения атак.

Система защиты информации на предприятии, разработанная на основе предложенных многоагентных интеллектуальных методов, обеспечивает надежную защиту информации на протяжении всего жизненного цикла

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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

BOTIROV FAYZULLAJON BAXTIYOROVICH

DEVELOPMENT OF MULTI-AGENT INTELLIGENT METHODS FOR PROTECTING INFORMATION IN THE ENTERPRISE

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

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

Tashkent-2021

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2020.4.PhD/T1941

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

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

Scientific adviser:	**Bekmuratov Tulkun Fayzievich** academician, Doctor of Technical Sciences, professor,
Official opponents	**Karimov Madjit Malikovich** doctor of technical sciences, professor
	Jurayev Gayrat Umarovich doctor of Physical and Mathematical sciences, assistant professor
Leading organization:	**Scientific-Engineering and Marketing researches Center «UNICON.UZ»**

The defense will take place «6» february 2021 at 10.00 the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No2631). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on «____» _____ 2021 y.
(mailing report No. ___ on «____» _____ 2021 y.).

R.Kh. Khamdamov
Chairman of the scientific council awarding scientific degrees, doctor of technical sciences, professor

F.M. Nuraliev
Scientific secretary of scientific council awarding scientific degrees, doctor of technical sciences, associate professor

S.K. Ganiev
Chairman of the academic seminar under the scientific council awarding scientific degrees, doctor of technical sciences, professor

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is to develop the multi-agent intelligent methods that allow to increase the efficiency of the information protection system.

The object of the research work is the process of information protection in the enterprise.

The scientific novelty of the research work is as follows:

the concept of a multi-agent intelligent system, taking into account a three-level mechanism of protecting information at an enterprise is worked out;

on the basis target tree of the three-level mechanism of protection the architecture of the intellectual system of information protection is developed;

on the basis frequency of information threats at the enterprise a method for determining the level of impact is developed;

a neural network method and an algorithm for detecting network attacks based on signature analysis are worked out;

on the basis of interactive and session models the algorithm for detecting network anomalies, allowing users to predict the next actions on the basis of their previous actions is worked out.

Implementation of the research results. On the basis of scientific results obtained on multi-agent intellectual methods and software for information protection in the enterprise:

in the process of information protection in the enterprise with the use of signature analysis a software tool of the neural network method of detecting attacks was implemented into the practical activities of the main operations department of the “Joint-Stock Commercial People's Bank” of the Republic of Uzbekistan (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated November 24, 2020 No. 33-8/7051). The result of scientific research on corporative network allowed 94.7% accuracy and 5.3% error in detecting DoS attacks, 91.4% accuracy and 8.6% error in detecting U2R attacks, 93.6% accuracy and 6.4% error in detecting R2L attacks, detection of network attacks with 95.8% accuracy and 4.2% error in detecting probe attacks;

in the process of information protection in the enterprise the software tool for threat analysis was implemented into the practical activities of the State Unitary Enterprise (SUE) "UNICON.UZ" - Center for science, technology and marketing research (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated November 24, 2020 No. 33-8/7051). The result of scientific research in detecting possible attacks on the local network of organization was allowed to warn the system administrator about errors;

based on interactive and session models the software tool for detecting network anomalies was implemented into the practical activities of the Military Institute of information and communication technologies and communications of the ministry of Defense of the Republic of Uzbekistan (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated November 24, 2020 No. 33-8/7051). The results of the scientific

research allowed to detect attacks on the corporate network with 94.3% accuracy and 5.7% error.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, four chapters, conclusion, references and appendix. The volume of the thesis is 112 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

1. Бекмуратов Т.Ф., Ботиров Ф.Б., Мультиагентли тизимларни ахборот хавфсизлиги тизимларида қўлланилиши // Проблемы информатики и энергетики. 2018. № 5. - С. 78-83
2. Ганиев А.А., Ботиров Ф.Б., Турли хил вазифаларни ечиш жараёнларида интеллектуал тизимлар ва технологиялар // “Муҳаммад ал-Хоразмий авлодлари” илмий - амалий ва ахборот - таҳлилий журнали, 1(3)/2018. - С. 60-63.
3. Гулямов Ш. Р., Ботиров Ф.Б., Ахборот хавфсизлигида мультиагентли интеллектуал тизимларнинг қўлланилиши // “Muhammad al – Xorazmiy avlodlari” илмий - амалий ва ахборот - таҳлилий журнали. № 3(5) /2018. - Б. 44 – 47.
4. Bekmuratov Tulkun, Ganiev Abdukhalil, Botirov Fayzullajon, Concept Of Establishing Multi-Agent Intellectual Automatically Systems in the Enterprise, International journal of Scientific & Technology Research. Volume 9, issue 04, April 2020. -P. 347-352.
5. T.F.Bekmuratov, F.B.Botirov, Development of Structures of Intellectual Inforomation Protection System. // Chemical technology. Control and Management. 2019, №6(90). -P. 63-71.
6. Botirov Fayzullajon Baxtiyorovich, Reliable risk assessment method for effective organization of information security at enterprise // Chemical technology. Control and Management. 2020, №4(94), -P. 64-70.
7. Bekmuratov Tulkun Fayzievich, Botirov Fayzullajon Bakhtiyorovich, Haydarov Elshod Dilshod ugli. Electronic spam filtering based on neural networks, Chemical technology. Control and Management. 2020, №3(93), -P. 59-65.
8. Бекмуратов Т.Ф., Ботиров Ф.Б., Набиев М.М., Машинали ўқитиш ва чуқур ўқитишнинг вазифалари ва киберхавфсизлик // “Муҳаммад ал-Хоразмий авлодлари” илмий - амалий ва ахборот таҳлилий журнали, 3(9)/2019, -Б. 3-7.
9. Bekmuratov T.F., Botirov F.B., Axborotni himoyalash tizimini boshqarish masalasi // Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi muammolari: Respublika miqyosidagi ilmiy-texnik konferentsiya. Toshkent - 2019. -Б. 151-155.
10. Bekmuratov T.F., Botirov F.B., Multi-agent system of protecting information from unauthorized access // 2019 International Conference on international scientific and practical conference "Innovative ideas of modern youth in science and education". USA. -P.4-7.

11. Ганиев А.А., Ботиров Ф.Б., “Тармоқ ҳимояси учун машинали ўқитиш // Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари Республика илмий-техник конференцияси, Тошкент - 2019. b. 71-74.

12. Ботиров Ф.Б., Ахборотни ҳимоялашнинг кўпагентли интеллектуал автоматлаштирилган тизими // Иқтисодиётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти республика илмий-техник анжуманининг маърузалар тўплами. Тошкент – 2020. - Б.371-374.

13. Ботиров Ф. Б., Набиев М. М., (научный руководитель: Ганиев А.А.). Глубокое обучение: предыдущие и настоящие применения // “XXI Молодежная международная научно-техническая конференция учащихся, студентов, аспирантов и молодых ученых, МОСКВА МГТУ им. Н. Э. Баумана 2019. С. 50-53.

14. Bekmuratov Tulkun and Botirov Fayzullajon, "Analysis of Integrated Neural Network Attack Detection System and User Behavior Models // "2019 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent, Uzbekistan, 2019. 4 p.

15. Bekmuratov T.F., Botirov F.B. Kiberhimoya boshqaruvining intellektual mexanizmlari. // Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари:, Республика миқёсидаги илмий-техник конференция. Тошкент - 2018. -Б. 108-112.

16. Т.Ф.Бекмуратов, А.А.Ганиев, Ф.Б.Ботиров, А.Иброхимов, А.М.Ортикбоев."MAS дастури" // Дастурга гувоҳнома № DGU 09136. Тошкент, 07.09.2020 й.

17. Т.Ф.Бекмуратов, А.А.Ганиев, Ф.Б.Ботиров, А.Иброхимов, А.М.Ортикбоев."Корхоналарда ахборотларга бўладиган ҳужумларни аниқлаш ва бартараф эиш"// Дастурга гувоҳнома № DGU 09137. Тошкент, 07.09.2020 й.

18. Т.Ф.Бекмуратов, А.А.Ганиев, Ф.Б.Ботиров, А.Иброхимов, А.М.Ортикбоев."Тармоқни мониторинг қилиш ва рискларни баҳолаш дастури" // Дастурга гувоҳнома № DGU 09138. Тошкент, 07.09.2020 й.