ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

БЕКМИРЗАЕВ ОБИДЖОН НУРАЛИЕВИЧ

АХБОРОТ ТИЗИМЛАРИДА ҲУЖУМ ИЗЛАРИНИ ҚИДИРИШ ВА ТАҲЛИЛ ҚИЛИШ МОДЕЛИ, АЛГОРИТМЛАРИ ВА ДАСТУРИЙ МАЖМУАСИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари.
Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2022

УДК: 004.056

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.07.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

БЕКМИРЗАЕВ ОБИДЖОН НУРАЛИЕВИЧ

АХБОРОТ ТИЗИМЛАРИДА ҲУЖУМ ИЗЛАРИНИ ҚИДИРИШ ВА ТАҲЛИЛ ҚИЛИШ МОДЕЛИ, АЛГОРИТМЛАРИ ВА ДАСТУРИЙ МАЖМУАСИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари.
Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2022

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2022.2.PhD/T2833 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:	**Мўминов Баҳодир Болтаевич** техника фанлари доктори, профессор
Расмий оппонентлар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
	Халмуратов Омонбой Утамуратович техника фанлари бўйича фалсафа доктори
Етакчи ташкилот:	**«UNICON.UZ – фан – техника ва маркетинг тадқиқотлар маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.02 Илмий кенгашнинг 2022 йил «17» Декабр соат 10⁰⁰ даги мажлисида бўлиб ўтади. (Манзил: 100084, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: info@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (0703 рақам билан рўйхатга олинган.). (Манзил: 100084, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-70)

Диссертация автореферати 2022 йил «05» Декабр да тарқатилди.
(2022 йил «03» Декабр даги 8 рақамли реестр баённомаси.)

Б.Ш. Махкамов
Илмий даражалар берувчи илмий кенгаш раиси, и.ф.д., профессор

Э.Ш. Назирова
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 ташкилотларнинг ахборот тизимига бўладиган ҳужум изларини қидириш, аниқлаш ва уларни бартараф этиш билан бир қаторда, ҳужумларни аниқлаш жараёни аниқлигини ошириш ва хатоликларни камайтиришга эътибор қаратилмоқда. «Kaspersky» компанияси маълумотларига кўра, 2022 йилнинг учинчи чорагида давлат ташкилотларининг ахборот тизимларига бўлган ҳужумлар улуши 18% га ошган бўлиб, ҳужум объектининг 82% ни компьютерлар, серверлар ва тармоқ қурилмалари ташкил этган[1]. Дунёнинг ривожланган мамлакатлари, жумладан, АҚШ, Германия, Япония, Франция, Хитой, Жанубий Корея, Россия Федерацияси ва бошқа давлатларда интеллектуал усуллар асосида ахборот тизимларига бўладиган таҳдидларнинг таъсир даражасини аниқлаш, ахборотни ҳимоялаш тизимларини такомиллаштириш, ҳужум изларини аниқлаш усуллари ва алгоритмларини ишлаб чиқиш ҳамда қўллаш бўйича фаол илмий тадқиқотлар олиб борилмоқда.

Жаҳонда ахборот тизимларига нисбатан бузғунчи томонидан амалга оширилаётган ҳужум қилиш йўлидан қатъий назар, ҳужумни аниқлашнинг модели, усули ва алгоритмларини такомиллаштиришга ҳамда ҳужум изини қидиришга қаратилган илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, жумладан, сигнатура ва хатти-ҳаракатига ҳамда айнан бўлиб ўтган ҳужум изини қидиришда фойдаланувчиларнинг маълум чегара оралиғидаги ҳаракатларини маълумотлар базасига ёзиш орқали амалга ошириладиган бузғунчиликни аниқлаш, таҳлил қилиш модели ва алгоритмларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланмоқда. Шу билан бирга, ахборот тизимида ҳужум изларини қидириш жараёнида кўрилаётган объект тўғрисидаги билимлар тўлиқ бўлмаганда ёки жорий маълумотларда норавшанликлар (ноаниқлик) мавжуд бўлганда ҳужум изини қидириш учун интеллектуал элементлардан фойдаланиб қарорлар қабул қилишга эҳтиёж сезилмоқда.

Республикада соҳа ташкилотларининг ахборот тизимларида ҳужум изларини қисқа вақтда самарали аниқлашни такомиллаштиришга йўналтирилган кенг қамровли чора-тадбирлар ишлаб чиқилган. Хусусан, 2022-2026 йилларга мўлжалланган янги Ўзбекистоннинг тараққиёт стратегияси[2] ва Президент томонидан ЎРҚ-764-сонли «Киберхавфсизлик тўғрисида»ги Қонуни ишлаб чиқилган[3]. Ушбу қонун лойиҳасида алоҳида Республика миқёсида мавжуд ахборот тизимларини ахборот хавфсизлиги нуқтаи назаридан танқидий ўрганиб, зарур чора-тадбирларни кўриш вазифаси белгилаб берилган. Мазкур вазифаларни амалга оширишда, бўлиб ўтган ҳужум изларини қидириш, аниқлаш ва аниқланган излар рўйхатини

1 https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/#id8

[2] Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ-60-сон «2022 - 2026 йилларга мўлжалланган янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида» ги Фармони

[3] Ўзбекистон Республикасининг Қонуни, 2022 йил 15 апрельдаги йилдаги ЎРҚ-764-сонли.

шакллантириш орқали компьютер жиноятчилигини асослаб бериш каби муаммоларни аниқлаш ва керакли мутахассисга ушбу маълумотни тақдим этишда бузғунчиликнинг маълум чегара оралиғида фойдаланувчи ҳаракатларини ёзиш орқали олдини олишга қаратилган муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ–60–сонли «2022–2026 йилларга мўлжалланган янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида»ги Фармони, 2018 йил 21 ноябрдаги ПҚ–4024–сонли «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори[4] ва 2018 йил 19 февралдаги ПФ–5349–сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора–тадбирлари тўғрисида»ги Фармон 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 тизимларини ҳимоя қилиш, компьютер ҳужумларини ва зарарли дастурларни аниқлаш ҳамда рақамли криминалистика соҳасида М.В.Абрамов, В.М. Сычев, О.С. Терновой, О.В.Лукинова, А.С.Кириллов, В.М.Крундышев, А.М.Каднова, В.В. Сагитова, А.В.Остроух ва бошқа чет эллик олимлар томонидан илмий изланишлар олиб борилмоқда. Рақамли криминалистикани қўллаш орқали компьютер тизимларида зарарли дастурларни аниқлаш ва компьютер тизимларида маълумотларни ҳимоя қилиш бўйича ташкилий-ҳуқуқий чора-тадбирлари борасида О.В.Багринцева, А.В.Никишова, С.Ал-Марри, ва А.Кимар илмий изланишлар олиб боришган. Бундан ташқари, «InfoWatch», «RiskWatch», «WatchGuard» ва «Trend Micro» ташкилотлари томонидан компьютер жиноятчилигини аниқлашда компьютер криминалистикасини қўллаш орқали ахборотни ҳимоялашнинг дастурий-аппарат воситаларини ишлаб чиқиш бўйича инженерлик-тадқиқот ишлари олиб борилмоқда.

Ўзбекистонда С.К.Ганиев, М.М.Каримов, Г.У.Жураев, Б.Ф.Абдурахимов, Б.Б.Мўминов, К.Ф.Керимов, Ғ.Н.Туйчиев, Д.Я.Иргашева ва бошқалар ахборотнинг дастурий аппарат ҳимоялаш усуллари, хусусан, ахборот коммуникация тизимларида тармоқлараро экран ва мониторинглашнинг комплекс усул ва воситаларини ишлаб чиқиш, инцидентларга ва киберҳужумларга қарши ҳаракатларни бошқариш, ахборот хавфсизлиги мезонлари ва кўрсаткичларини шакллантириш усуллари, ахборотни

[4] Ўзбекистон Республикаси Президентининг 2018 лий 21 ноябрьдаги йилдаги ПҚ-4024-сонли қарори.

криптографик ҳимоялаш усулларини ишлаб чиқиш ва криптографик алгоритмларни баҳолаш билан боғлиқ тадқиқотлар олиб борилмоқда.

Ривожланаётган соҳаларни эҳтиёжлари асосида ахборот хавфсизлиги учун ахборот тизимларида ҳужум изларини қидириш, маълумотлар тўпламини тайёрлаш, таҳлиллаш модели ва алгоритмлари етарлича тадқиқ этилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университетининг илмий–тадқиқот ишлари режасининг №БВ–Ф4–023–Тақсимланган ахборот–коммуникация тизимларида инцидентлар ва киберҳужумларга қарши ҳаракатларни бошқариш муаммоларини тадқиқ этиш (2017–2020 йй.) мавзусидаги лойиҳаси ҳамда COVID–19 даврида илмий–тадқиқот ишларини ҳимоя қилиш ва онлайн тарзда ўтказиш чора–тадбирлари режаси доирасида бажарилган.

Тадқиқот мақсади ахборот тизимларида ҳужум изларини қидириш ва таҳлиллашнинг модели, алгоритмлари ва дастурий мажмуасини яратишдан иборат.

Тадқиқотнинг вазифалари:

ахборот хавфсизлигида компьютер жиноятчилиги, ўзига хос хусусиятлари, криминалистик характеристикалари, унга оид ҳуқуқий меъёрлар ва муаммоларни қиёсий таҳлиллаш;

ахборот тизимида ҳужум манбалари рўйхатини шакллантириш процедураси ва ҳужум таъсири остида тугун ҳолатининг ҳодисалар мажмуасини қуриш алгоритмини ишлаб чиқиш;

ахборот тизимида ҳужум изини қидириш моделини қуриш ва параметрларини созлаш алгоритмини ишлаб чиқиш;

ахборот тизим ҳимоясининг самарадорлигини баҳолаш услубини такомиллаштириш;

ҳужум изини қидиришга йўналтирилган дастурий мажмуанинг функционал тузилмаси ва талабларини ишлаб чиқиш.

Тадқиқотнинг объекти сифатида ахборот тизимининг ҳодисалари ва маълумотлар тўплами олинган.

Тадқиқотнинг предмети сифатида ахборот тизимида ҳужумларни аниқлаш усуллари, компьютер жиноятчилиги, ҳужум оқибатларининг эҳтимолликларини аниқлаш модели ва алгоритмлари олинган.

Тадқиқот усуллари. Тадқиқот жараёнида ахборот тизимида ҳужум изларини интеллектуал тизимлар ёрдамида аниқлаш усуллари, нейрон тармоқлар, норавшан тўпламлар назарияси, эҳтимоллик назарияси, графлар назарияси ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

ахборот тизими ва мавжуд интерфейс учун мумкин бўлган таъсир объекти асосида ахборот тизимида ҳужум манбаларининг рўйхатини шакллантириш процедураси ишлаб чиқилган;

ҳодисалар мажмуасини қуриш учун тўртта параметрни мантиқий бошқарувининг бинар муносабати асосида ҳужум таъсири остида тугун ҳолатининг ҳодисалар мажмуасини қуриш алгоритми ишлаб чиқилган;

ахборот тизимида ҳужум манбалари рўйхатини шакллантириш процедураси ва ANFIS нейро-норавшан тизими асосида ҳужум изини қидириш модели ва параметрларини созлаш алгоритми ишлаб чиқилган;

ANFIS нейро-норавшан тизими асосида ахборот тизими ҳимоясининг самарадорлигини баҳолаш услуби такомиллаштирилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

«Хавфсиз онлайн овоз бериш» тизимининг тузилмаси асосида дастурий мажмуаси ишлаб чиқилган;

ҳужум изини қидиришга йўналтирилган модели асосида дастурий мажмуанинг функционал тузилмаси ва талаблари ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги қўйилган муаммонинг математик жиҳатдан аниқ ифодаланиши, ҳужум изларини қидириш модели ва параметрларининг аниқлиги, хавфсиз онлайн овоз бериш дастурий мажмуасини ишлаб чиқилиши ва ушбу тизимда ҳужум изини қидириш дастурий мажмуасининг қўлланилганлиги, шунингдек, соҳадаги етакчи олимлар ва экспертларнинг хулосалари билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти ишлаб чиқилган ташкилотда ахборот тизимини ҳимоялаш жараёнида таҳдидлар таъсир даражасини аниқлаш усули, ҳужум изларини қидиришнинг нейро-норавшан тизими усули ва ҳужумларни таҳлиллаш модели асосида ҳужумларни аниқлаш алгоритми билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти таклиф этилган модел ва алгоритмлар асосида ишлаб чиқилган дастурий мажмуани ахборот тизими ҳимояланганлик даражасини яхшилаши билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Ахборот тизимларида ҳужум изларини қидириш ва таҳлиллаш модели ҳамда дастурий мажмуалари бўйича олинган илмий ва амалий натижалар асосида:

ахборот тизимида ҳужум манбалари рўйхатини шакллантириш процедураси ва ҳужум таъсири остида тугун ҳолатининг ҳодисалар мажмуасини қуриш орқали муассасаларнинг ахборот тизимида бўлиб ўтган ҳужум изини қидиришнинг нейро-норавшан тизим моделининг дастурий мажмуаси Муҳаммад ал-Хоразмий номидаги ТАТУга жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2022 йил 12 октябрдаги 33-8/6759-сонли маълумотномаси). Илмий тадқиқот натижасида мавжуд ахборот тизими ҳимояси талабларини қайта кўриб чиқиб, ҳимояланганлик даражаси 21% га ва тизимда бўлиб ўтган ҳужум изларини аниқлаб, аниқланган изларни маълумотлар базасини шакллантириш орқали уни келажакда такрорланишини олдини олиш даражаси 71% га ошган. Шунингдек, тизимда такрорий муваффақиятсиз уринишларни блоклаш орқали бўлиши мумкин бўлган такрорий таҳдидлар 50% га камайтирилган;

ташкилотдаги ахборот тизимида ҳужум изларини қидиришнинг дастурий мажмуаси «SSP Мароқанд» кўп функцияли ахборот маркази унитар корхонасида жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2022 йил 12 октябрдаги 33-8/6759-сонли маълумотномаси). Илмий тадқиқот натижасида муассасанинг ахборот тизимига бўлган ҳужумларни аниқлаш ва бу ҳақида тизим маъмурини огоҳлантириш имконияти яратилган;

«Хавфсиз онлайн овоз бериш» ва «Ҳужум изини қидириш» дастурий мажмуалари «Киберхавфсизлик» маркази Давлат унитар корхонасида тест жараёнида қўлланилган. (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2022 йил 12 октябрдаги 33-8/6759-сонли маълумотномаси). Илмий тадқиқот натижасида мавжуд ахборот тизими ҳимояси талабларини қайта кўриб чиқиб, ҳимояланганлик даражаси 21% га ва тизимда бўлиб ўтган ҳужум изларини аниқлаб, аниқланган изларнинг маълумотлар базасини шакллантириш орқали келажакда олдини олиш даражаси 72% га яхшиланган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 11 та илмий-амалий анжуманларда, жумладан 4 та халқаро ва 7 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертация мавзуси бўйича жами 17 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 5 та мақола, шулардан, 1 таси хорижий ва 4 таси Республика журналларида ҳамда 1 та ЭҲМ учун яратилган дастурий мажмуаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати, қисқартмалар ва белгилар рўйхати ҳамда иловалардан иборат. Диссертация ҳажми 117 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

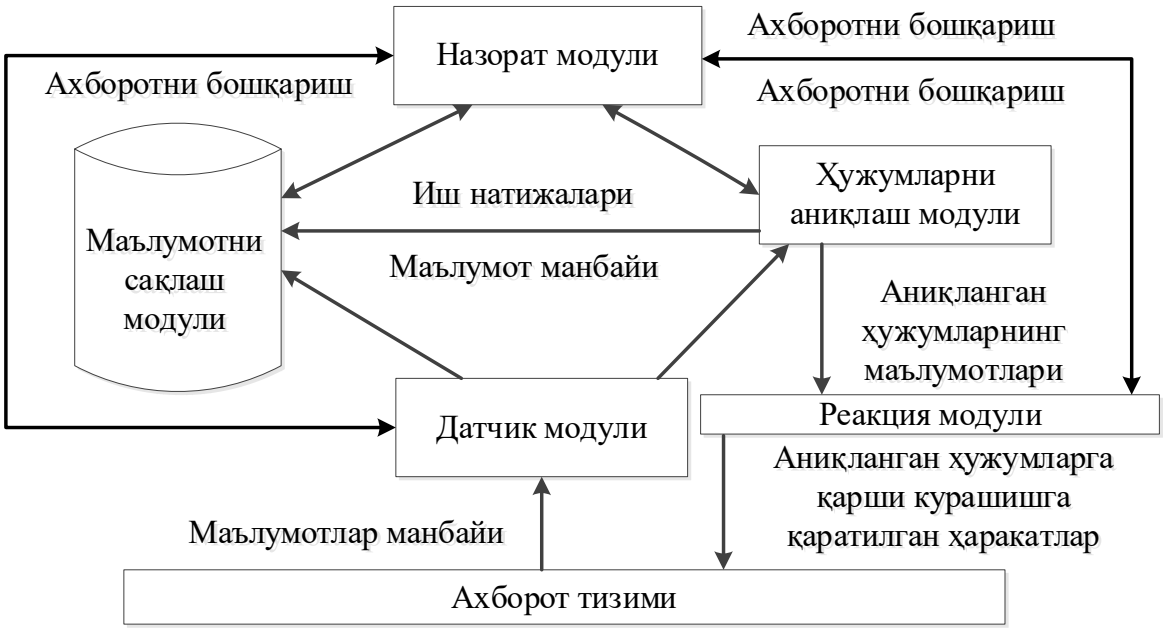
Кириш қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, мақсад ва вазифалар шакллантирилган, тадқиқот объекти ва предмети аниқланган, тадқиқотнинг илмий янгилиги ва амалий натижалари кўрсатиб ўтилган, олинган натижаларнинг ҳаққонийлиги асосланган, уларнинг назарий ва амалий аҳамияти очиб берилган, тадқиқот натижаларининг амалиётга татбиқ этилиши, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг **«Ахборот тизими хавфсизлигида компьютер жиноятчилигининг муаммолари ва назарий асослари»** деб номланган биринчи бобида ахборот хавфсизлигида компьютер жиноятчилиги ва ҳуқуқий меъёрларининг таҳлили, унинг ўзига хос хусусиятлари ва криминалистик

характеристикалари, компьютер жиноятчилиги муаммолари ва қиёсий таҳлили, компьютер жиноятчилигини аниқлаш усуллари ҳамда масаланинг қўйилиши келтирилган.

Ахборот тизимларида компьютер жиноятчилиги доирасида олиб борилган урганишлар натижасида компьютер жиноятчилиги таҳлили шуни кўрсатдики, охирги ўн йилликда уларнинг сони 22,3 марта ўсган ва йилига 3,5% да ўсишда давом этмоқда. Жиноятлардан кўриладиган моддий зарарларнинг йиллик ҳажми 8,5 миллиард долларни ташкил этган. Жиноятни маълум бир улуши муваффақиятли бўлиб, фақатгина 49% ўрганилган, жиноят ишларини умумий сонининг 25,5% аниқланган, жараёни тўхтатилган жиноий ишлар сонини ўртача кўрсаткичи 43,5% ташкил этади ва бу жиноят ишларни очиш, тергов қилиш ва огоҳлантириш бўйича фаолият юритадиган хавфсизлик ташкилотлари ходимларини малака даражасини етарли эмаслигини кўрсатади.

Ушбу келтирилган маълумотлар асосида ҳужумларни аниқлаш тизимлари ахборот тизимидаги ахборотга қаратилган ҳужумларни аниқлаш учун мўлжалланган махсус аппарат ва дастурий таъминот комплекслари жорий қилиш долзарбдир. Ҳужумни аниқлаш тизимининг одатий архитектураси қуйидаги компонентларни ўз ичига олади (1-расм).



1-расм. Ҳужумларни аниқлаш тизимларининг архитектураси

Олиб борилган тадқиқот натижаси жуда кўп тадқиқотчилар орасида фойдаланилиб келиниётган сигнатура ва ҳолатга асосланган ҳужумларни аниқлаш усулларининг таҳлилидан келиб чиқиб қўйидаги муаммоларни ечиш лозимлиги аниқланди:

1. Ахборот тизимида ахборот хавфсизлигига таҳдид манбаларини аниқлаш, шунингдек, ахборот тизими архитектураси ва ҳужум изларини таҳлил омилларига асосланган жараённинг процедурасини ишлаб чиқиш.

2. Ҳужум изларини тугун, ҳолат ва ҳодисалар сценарийларини ишлаб чиқиш.

3. Ахборот тизимида ҳужум изларини қидириш моделини қуриш ва параметрларини аниқлаш алгоритмини ишлаб чиқиш.

4. Норавшан нейрон тармоқ учун дастлабки маълумотлар тўпламини (ўқув танланмаларини) тайёрлаш услубини таклиф қилиш.

5. Ахборот тизимида ҳужум изини баҳолаш усулини ишлаб чиқиш.

6. Ахборот тизими ҳимояси самарадорлигини баҳолашга ёндашув услубини такомиллаштириш.

7. Таклиф этилаётган модел ва алгоритмлар учун дастурий мажмуанинг функционал тузилмаси талабларини ишлаб чиқиш.

Диссертациянинг **«Ҳужум моделлари ва ҳодисалар мажмуасини қуриш»** деб номланган иккинчи бобида ахборот тизимларининг архитектураси ва ҳужум моделлари тадқиқ этилган. Ахборот тизимида ҳужум манбалари рўйхатини шакллантириш процедураси ва ҳужум таъсири остида тугун ҳолатининг ҳодисалар мажмуасини қуриш алгоритми ишлаб чиқилган. Ҳужум изларини таснифлаш учун мослаштирилган нейро-норавшан тизимининг алгоритми таклиф этилган.

Тадқиқотлар натижасида ташкилотларнинг ахборот тизимига бўлиб ўтган ҳужумдан кейин келиб чиқадиган моддий ва номоддий зарар турларини ва салбий оқибатларни аниқлаш билан рўйхат шакллантирилади. Бунинг учун зарар турлари (ЗТ) ва салбий оқибатлар (СО) қуйидагича таклиф этилди:

$ЗТ_{1.1}$ – жисмоний шахсга етказилган зарар тури;

$СО_{1.1}$ – субъектга, унинг шахсий маълумотларига ноқонуний ишлов бериш орқали зарар етказиш, шу жумладан шахсий дахлсизлик, шахсий ва оилавий сирларга бўлган ҳуқуқларни бузиш;

$ЗТ_{2.1}$ – юридик шахсга етказилган зарар тури;

$СО_{2.1}$ – ахборот хавфсизлиги соҳасидаги меъёрий-услубий ҳужжатлар талабларини бузиш;

$СО_{2.2}$ – юридик шахснинг ишчанлик обрўсини бузиш;

$СО_{2.3}$ – ахборот тизимига амалга оширадиган функционал мантиқий муносабат жараёнларини ўзгартириш (қайта қуриш) зарурати;

$СО_{2.4}$ – ахборот инфратузилмалари, автоматлаштирилган жараёнларни бошқариш тизимларининг ишлаши билан боғлиқ зарар турлари;

$СО_{2.5}$ – ҳимояланган ахборотни сирқиб чиқиш ва қонунга хилоф равишда ишлов бериш орқали юридик шахсга молиявий зарар кўринишида зарар етказиш.

Ахборот тизими ва тузилмаси имкониятлар даражасига таҳмин қилиниб, қуйидагиларга эга бўлган бузғунчиларга бўлиш мумкин:

H^0 – ахборот тизимига ҳужумни амалга оширишни асосий имконияти;

H^1 – ахборот тизимига ҳужумни амалга оширишни асосий кенгайтирилган имкониятлари;

H^2 – ахборот тизимига ҳужумни амалга оширишни ўртача имконияти;

H^3 – ахборот тизимига ҳужумни амалга оширишни юқори имконияти;

H^4 – ахборот тизимига ҳужумни амалга оширишни янги имконияти.

Ушбу жисмоний ва юридик шахсларга етказилган зарар тури ва мумкин бўлган салбий оқибатлар орқали таъсир объектларига вазннинг қуйидаги

таъсир турлари мавжуд.

W_i= Конфиденциаллик, яхлитлик, фойдаланувчанлик, ҳақиқийлик, рад этмаслик, жавобгарлик, хусусиятлар бир хиллиги, ишончлилигини бузиш.

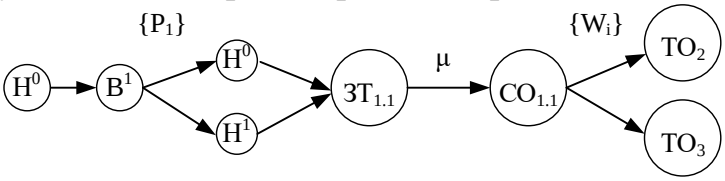
Бундан ташқари уч турдаги бузғунчи таснифига ажратилиб олинди.

B^1 – Бузғунчи таснифига ташкилотнинг ахборот тизимига ишлаш ҳолатига жавоб берадиган мутахассислар.

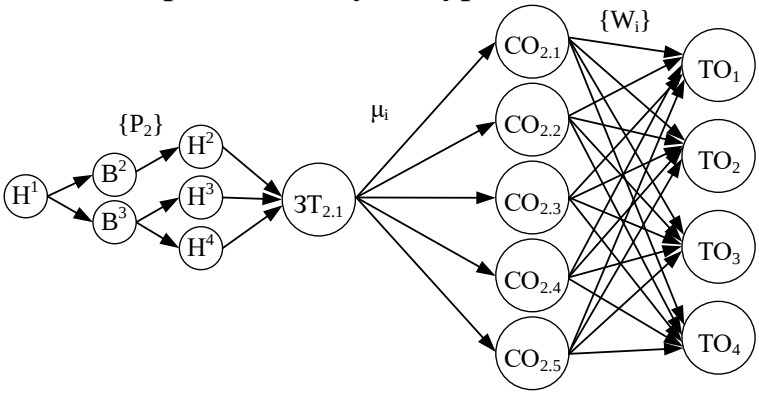
B^2 – Бузғунчи таснифига ташкилотнинг ахборот тизимига бузғунчилик қилиш мойиллиги юқори фойдаланувчи ва хизмат кўрсатувчилар.

B^3 – Бузғунчи таснифига ташкилотнинг ахборот тизимига қасддан ёки малакасиз фойдаланувчи ҳаракати киради.

Ҳужум таъсири, ажратилган тасниф даражаси, зарар таъсиридан келиб чиқиб салбий оқибатни таъсир объектига процедура ва вазнни таъсирининг визуал кўриниши қуйида 2- ва 3- расмларда келтирилган.



2-расм. Жисмоний шахснинг таъсир объектига процедура ва вазн таъсирининг визуал кўриниши



3-расм. Юридик шахснинг таъсир объектига процедура ва вазн таъсирининг визуал кўриниши

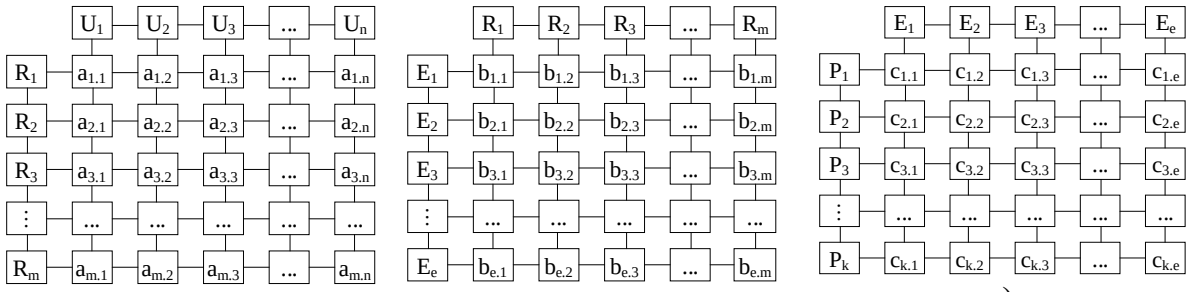
Таклиф қилинаётган процедура ахборот тизимининг ҳар бир ҳодисаси ва ҳусусиятлари, фойдаланувчи ва унинг ролига мос ҳужум таъсири остидаги тугун ҳолат ҳодисаларига боғлиқдир. Бу эса ҳужум таъсири остидаги тугун ҳолат ҳодисаларини қуришни талаб қилади.

Ахборот тизимида ҳужумларни олдини олишда ахборотнинг дастурий-аппарат ҳимоялаш усуллари хусусан, ахборот коммуникация тизимларида тармоқлараро экран ва мониторинглашнинг комплекс усул ва воситалари ҳамда тармоқ трафигини фильтрлаш каби таъсир объектлари асосида амалга оширилади. Ушбу таъсир объектлари асосида амалга оширилган чора-тадбирлар аниқлай олмайдиган ҳужумлар мавжуд. Ҳужум бўлиб ўтгандан сўнг унинг таъсир объекти ёки зарар турини кўриб аниқлашга зарурат туғилади. Бунда ахборот тизими учун ҳужум таъсири остида тугун ҳолатининг ҳодисаларини кўриш лозим.

Ахборот тизимининг тугун ҳолат ҳодисалари тизим эгаси томонидан қуйилган талаблар асосида қурилди.

Фойдаланувчи $(U_i),\ (i=1,...N)N-$ фойдаланувчилар сони, рол $(R_j),\ (j=1,...M)M-$ роллар сони, ахборот тизимида бошқариладиган ҳар бир ҳодиса ва уларни сони ахборот тизимининг функционал имкониятларига боғлиқ, ҳодиса $(E_e),\ (e=1,...L)L-$ ҳодисалар сони, ахборот тизимида ҳар бир объектни ҳусусияти олинган, хусусият сони чекланган ва хусусият $(P_k),\ (k=1,...K)K-$ хусусиятлар сонидир.

Ҳосил қилинган параметрлар асосида мантиқий бошқарувини бинар муносабатининг тугун ҳолати ҳодисалар мажмуасини қуриш 4-расмда келтирилган.



а) б) с)

4-расм. а), б) ва с) фойдаранувчи, рол, ҳодиса ва хусусиятларнинг мантиқий бошқарувини бинар муносабати

Диссертациянинг **«Ахборот тизимида ҳужум изларини қидириш ва баҳолаш»** деб номланган учинчи бобида ахборот тизимида ҳужум изини қидириш моделини қуриш ва параметрларини созлаш алгоритми таклиф этилган. Ахборот тизимида ҳужум изини баҳолаш усули ва алгоритми ишлаб чиқилган. Ахборот тизими ҳимояси самарадорлигини баҳолаш услуби такомиллаштирилган. Ҳужум изини қидиришда дастурий мажмуанинг функционал тузилмаси ва талаблари ишлаб чиқилган.

Ахборот тизимида ҳужум изини қидириш қоидаларга асосланган норавшан нейрон тармоғи моделини амалга ошириш қоидалари қуйидагича:

$$R_i: Агар\ (x_i == A_i, \cap \ldots \cap\ (x_{ij} == A_{ij}) \cap \ldots \cap\ (x_{im} == A_{im})\ \text{бўлса}$$

$$y = c_{io} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1 \ldots n\ \text{ёки}\ R_i := \bigcap_{j=1}^{m} (x_{ij} == A_{ij})\ \text{бўлса, унда} \qquad (1)$$

$y_i = c_{io} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1 \ldots r, i = 1 \ldots n$. $R = \sum_{i=1}^{m} R_i -$ умумий қоидалар тўплами.

(1) ифодада ахборот тизимида ҳужум изларини қидириш методологиясини қоидалар базаси белгилаб беради.

ANFIS норавшан нейрон тармоқ қуйидаги қоидаларга асосланади:

– киритилган ўзгарувчилар аниқлиги;

– тегишлилик функциялари Гаусс функцияси билан аниқланганлиги.

$$\mu_{ij}(y_j) = \exp\left(-\frac{1}{2}\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right)$$

Бунда y_j кириш тармоқлари, a_{ij} ва b_{ij} созланиши тегишлилик функциялари параметрларидир.

Чиқиш ўзгарувчисини олиш учун дефуззификациядан кейин функционал боғлиқлик қуйидаги кўринишда ифодаланади:

$$y^{'} = \frac{\sum_{i}^{n}((c_{io} + \sum_{j=1}^{m} c_{ij} x_j)\prod_{j=1}^{m} \mu_{A_{ij}}(x_j^{'}))}{\sum_{i=1}^{n}\prod_{j=1}^{m} \mu_{A_{ij}}(x_j^{'})} = \frac{\sum_{i}^{n}(c_{io} + \sum_{j=1}^{m} c_{ij} x_j)\prod_{j}^{m} \exp\left[-(\frac{x_j^{'} - a_{i,j}}{b_{i,j}})^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m} \exp\left[-(\frac{x_j^{'} - a_{i,j}}{b_{i,j}})^2\right]}$$

Ушбу ифода беш қадамни ўз ичига олган Takagi–Sugeno–Kang (TSK) алгоритмидан фойдаланган ҳолда ANFIS тармоғига асосланади:

Биринчи қадам киритилган аниқ ўзгарувчиларни фаззификацияси қуйидаги процедурани амалга оширади $x_j^{'}\ (j = 1, 2, ..., n)$.

Иккинчи қадам a_{ij} ва b_{ij} элементлари Гаусс функциялари томонидан берилган тегишлилик функциялари $\mu_{A_j}(x_j^{'})$, вазнлари ва қийматларининг параметрлари билан ҳисоблаб чиқилади.

Учинчи қадам иккинчи қадамнинг элементлари бўйича натижалар билан кўпайтирилади ва функция қийматларини ҳосил қилади, яъни

$$y_i = (c_{jo} + \sum_{j=1}^{m} c_{ij} x_j^{'}).$$

Тўртинчи қадам биринчи элементи 3-қадамда йиғилган қийматларга, қоидаларнинг зарурий шартларига тегишлилик даражаларига мувофиқ қоидаларнинг хулосаларини фаоллаштириш учун зарур. Тўртинчи қоиданинг иккинчи элементи ANFIS тармоғининг натижасини кейинчалик фаззификацияси учун қўшимча амаллар бажарилади.

Ушбу қадамда битта нормаллаштирувчи элементдан иборат бўлиб, ANFIS тармоғининг натижаларини дификациялайди.

Нейро-норавшан тизими Takagi–Sugeno–Kang алгоритми асосида ANFISни қўришда 2 та параметрик қоидани ўз ичига олади (1 ва 3 қадамда). ANFIS тармоғини ўқитиш жараёнида созланиши мумкин бўлган параметрлар:

– биринчи қадамда чизиқли бўлмаган параметрлар a_{ij} ва b_{ij} тегишлилик функциялари фаззификатордир;

– учунчи қадамда чизиқли функцияларнинг c_{io} ва c_{ij} параметрлари $y_i = (c_{io} + \sum_{j=1}^{m} c_{ij} x_j^{'})$ қоидалар базасининг хулосаларидан фойдаланади.

n та қоида ва m та кириш ўзгарувчилари мавжуд бўлганда, биринчи қадамнинг параметрлари сони $2nm$ га, иккинчи қадамнинг параметрлар сони эса $2 - n(m+1)$ га тенг. Созланиши мумкин бўлган параметрларнинг умумий сони $n(3m+1)$ ни ташкил қилади.

Таклиф этилаётган моделнинг кейинги босқичида чизиқли функцияларнинг c_{io} ва c_{ij} параметрлари a_{ij} ва b_{ij} параметрларининг белгиланган қийматлари шарти билан ҳисобланади.

c_{io} ва c_{ij} параметрлари чизиқли тенгламалар системасини ечиш орқали топилади. Бу сон чиқиш ўзгарувчисини қуйидаги шаклда ифодаланади:

$$y' = \sum_{i=1}^{m} w_i'(c_{io} + \sum_{j=1}^{m} c_{io} x_j) \text{ бунда } W_i' = \frac{\prod_{j=1}^{m} \mu_{A_{ij}}(x_j')}{\sum_{i=1}^{n}\prod_{j=1}^{m} \mu_{A_{ij}}(x_j')} = \frac{\prod_{j}^{m} \exp\left[-(\frac{x_j' - a_{i,j}}{b_{i,j}})^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m} \exp\left[-(\frac{x_j' - a_{i,j}}{b_{i,j}})^2\right]} = const$$

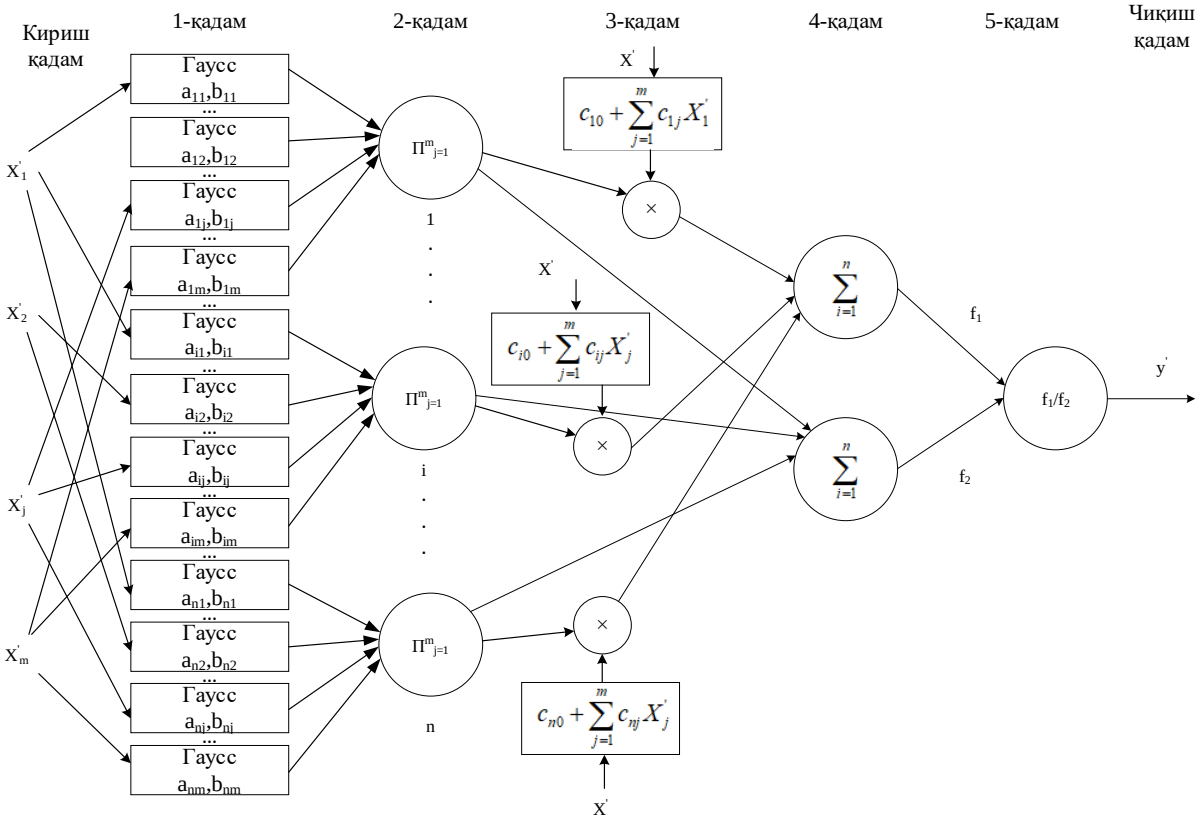
Танланган i, j – чизиқли параметрларини аниқлагандан сўнг, барча ўқув танланмалар учун тармоқнинг ҳақиқий чиқиш маълумотларини тузатиш, ҳисоблаш ва улар учун чизиқли муносабатлардан фойдаланилади:

$$y' = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} = w \cdot c$$

бунда хато векторини қуйидагича аниқланади: $e = y' - y$, бундан жорий параметрлар аниқланади:

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) + c\frac{dE^{(k)}(t)}{da_{ij}^{(k)}} \text{ ва } b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) + c\frac{dE^{(k)}(t)}{db_{ij}^{(k)}}$$

Takagi – Sugeno – Kang алгоритмидан фойдаланган ҳолда нейро-норавшан ANFIS тизимига асосланган ҳужум изини қидириш модели 5-расмда келтирилган.



5-расм. Нейро-норавшан ANFIS тизимига асосланган ҳужум изини қидириш модели

Таклиф этилаётган усулда Takagi – Sugeno – Kang норавшан хулоса чиқариш алгоритми билан ANFIS тизими тармоғининг ишлаши алгоритми туридаги қоидаларга асосланган норавшан ишлаб чиқариш моделини амалга оширишдан иборат:

$$R: \text{агар } x_i == A_i \text{ бўлса } y = c_{io} + \sum_{i=1}^{N} c_i x_i, i = 1,...N.$$

Олдин белгиланган ахборотни муҳофаза қилиш кўрсаткичлари ва талаблари асосида, шунингдек, ахборот тизимининг жорий ахборот тизимида ҳужум изи ҳамда ахборот тизими инфратузилмаси рўйхати асосида қоидалар базаси шакллантирилди, унинг бир қисми 1-жадвал асосида ишлаб чиқилди.

Ишда ахборот тизими инфратузилмаси учун ечимлар, ахборот тизимига ҳужумнинг статик моделлари каби катта ҳажмдаги маълумотлар таҳлили ўтказилди. Бу асосида ахборот тизими ҳимоясининг самарадорлигини баҳолаш услуби такомиллаштирилди.

1-жадвал.

Ахборот тизимида ҳужум изини қидириш мажмуасининг самарадорлигини баҳолаш учун қоидалар базаси

№	Агар (IF)			У ҳолда (THEN)
	Кириш параметрлар	Чиқиш параметрлар	Ҳужум изи даражаси	
1	x_1	z_1	Жуда паст (эҳтимоллиги жуда кам)	Самарадорликга эришилади
2	x_2	z_2	Паст (эҳтимоллиги кам)	Самарадорликга эришилади
3	x_3	z_3	Ўртача (мумкин бўлган)	Самарадорликга эришилади
4	x_4	z_4	Юқори (эҳтимоллиги бўлган)	Самарадорликга эришилади
5	x_5	z_5	Жуда юқори (тез-тез учраб турадиган)	Самарадорликга эришилмайди

Лингвистик ўзгарувчиларнинг миқдорий қийматлари 2-жадвалда келтирилган.

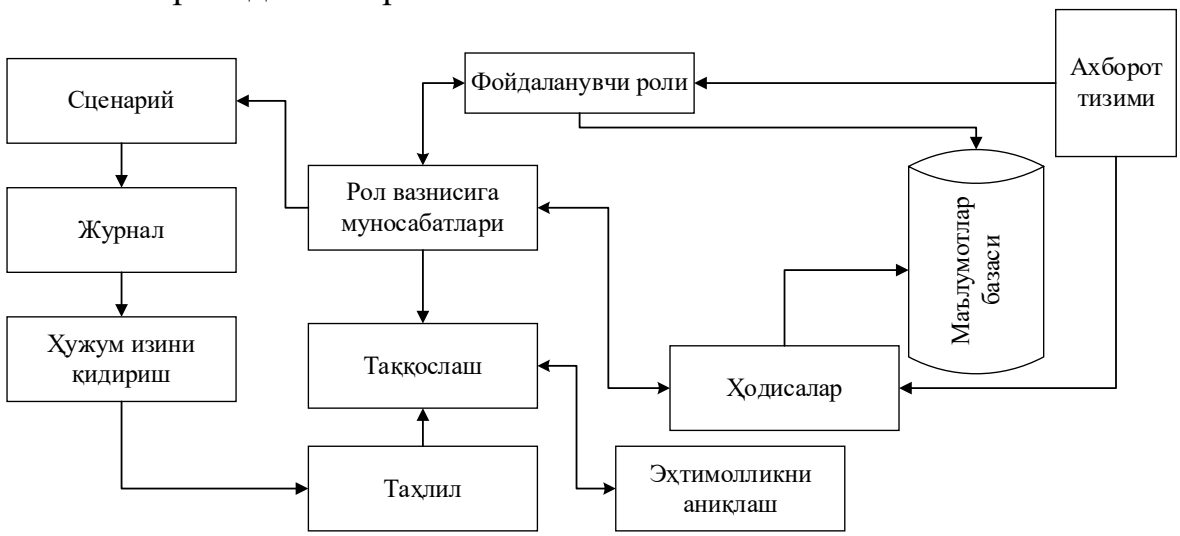
2-жадвал.

Лингвистик ўзгарувчиларнинг миқдорий қийматлари

№	Белгиланиш	Бошланғич ифода	Қиймати
1	Жуда паст (эҳтимоллиги жуда кам)	$0,1 < \lvert x_1 - z_1 \rvert \le 0,3$	$0,1 \sim 0,3$
2	Паст (эҳтимоллиги кам)	$0,3 < \lvert x_1 - z_1 \rvert \le 0,5$	$0,3 \sim 0,5$
3	Ўртача (мумкин бўлган)	$0,5 < \lvert x_1 - z_1 \rvert \le 0,7$	$0,5 \sim 0,7$
4	Юқори (эҳтимоллиги бўлган)	$0,7 < \lvert x_1 - z_1 \rvert \le 0,9$	$0,7 \sim 0,9$
5	Жуда юқори (тез-тез учраб туралиган)	$0,9 < \lvert x_1 - z_1 \rvert \le 1$	$0,9 \sim 1$

Ҳужум изини қидиришни дастурий мажмуасининг функционал

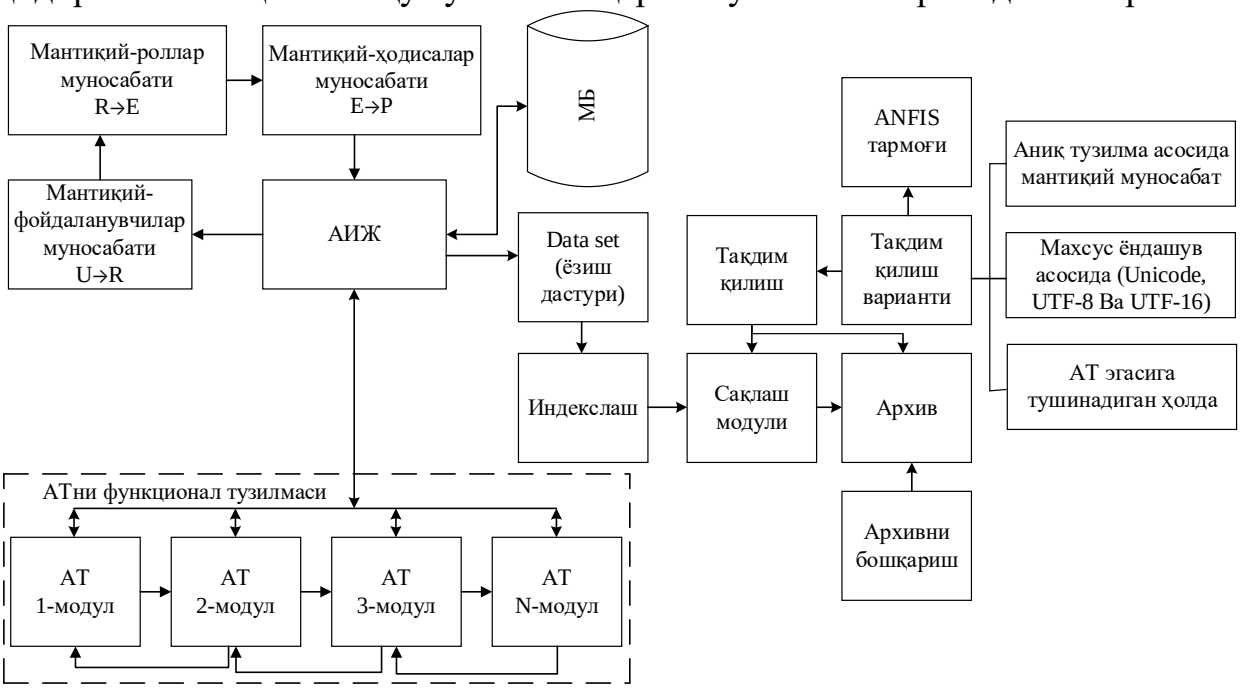
тузилмаси 6-расмда келтирилган.



6-расм. Ҳужум изини қидиришни дастурий мажмуасининг функционал тузилмаси

Диссертациянинг **«Дастурий мажмуани функционал вазифалари ва жорий қилиш натижалари»** деб номланган тўртинчи бобида жорий қилинган “Хавфсиз онлайн овоз бериш” тизимини функцианал тузилмаси, ахборот тизимида ҳужум изини қидириш моделининг самарадорлигини баҳолаш ва таҳлили ҳамда жорий қилиш талаблари ва натижалар таҳлилига бағишланган.

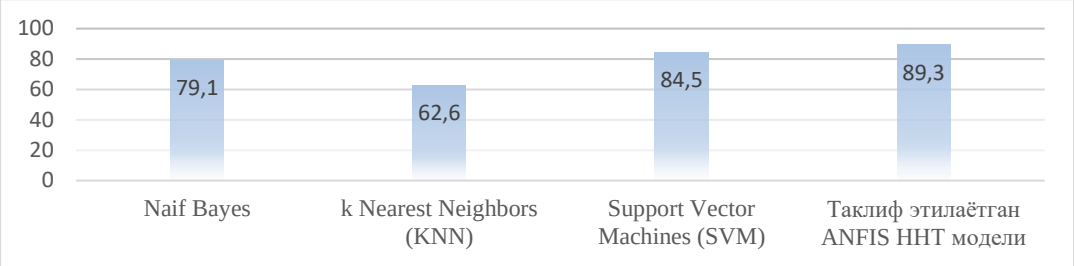
Ахборот тизимида ҳужум изини қидириш учун қоидалар асосида билимлар базаси шакллантирилади, у асосида data set қўрилади. Ҳар доим ҳар бир ахборот тизими учун алоҳида-алоҳида data set ишлаб чиқилади, сабаби ҳар бир ахборот тизими фойдаланувчилари тизимда ролидан келиб чиққан ҳолда ҳар бир тизим data set қўрилади. Шу асосида ахборот тизимида ҳужум изини қидириш ва аниқланган ҳужумни бошқариш тузилмаси 7-расмда келтирилган.



7-расм. АТда ҳужум изини қидириш ва аниқланган ҳужумни бошқариш схемаси

Тадқиқотда тавсия этилган модел, алгоритмлар бундай муаммоларни ҳал қилиш учун маълум таснифлаш моделлари ишини қиёсий таҳлил қилиш учун тажрибалар ўтказилди.

Илмий тадқиқотда data setни қуриш асосида «Python» дастурлаш тилида мавжуд моделлар ва элементларини созлаш асосида таклиф этилаётган ANFIS тизимни қиёсий таҳлилининг график кўриниши 8-расмда келтирилган.



8-расм. Муаммони ечиш моделларини қиёсий таҳлил қилиш графиги

Шундай қилиб, муаммонинг берилган шартлари учун ҳужум изини қидириш ва аниқлаш кўрсаткичи учун тавсия этилган модел энг яхшисидир.

Таклиф қилинган ҳужум изини қидиришнинг қўлайлиги ва самарадорлигини аниқлаш учун тизим жорий қилинмасдан олидинги ҳолат ва жорий қилингандан сўнги ҳолатлар таққослаш орқали амалга оширилди.

Тизимнинг натижадорлиги ва самарадорлигини аниқлаш учун қуйидаги кўрсаткичларни белгилаймиз:

- фойдаланувчи тизимга киргандан сўнг, ушбу номдан киришни чеклаш орқали ҳимояланиш (H_c, бирлиги фоизда);
- изни қидириш ва аниқланган изларни МБга ёзиш орқали олдини олиш (B_t, бирлиги фоизда);
- мутахассиснинг иш самарадорлиги (M_s, бирлиги фоизда);
- ҳужумни мутахассис томонидан назоратланиши (E_t, бирлиги фоиз);

Бу кўрсаткичлар асосида умумий кўрсаткични ҳисоблаш қуйидагича амалга оширилади.

$$k_1 = \frac{H_c - H_c^0}{H_c^0}, k_2 = \frac{B_t}{B_t^0}, k_3 = \frac{M_s}{M_s^0}, k_4 = 1 - \frac{E_t}{E_t^0}$$

Бунда N – кўрсаткичлар сони (N=4 га тенг), k_i - мос ҳолда ҳар бир ташкилотнинг мезонлари асосида кўрсаткичларнинг самарадорлги. Бунда k_i кўрсаткичнинг самарадорлиги қуйидагича ҳисобланади («4-жадвалга қаранг»).

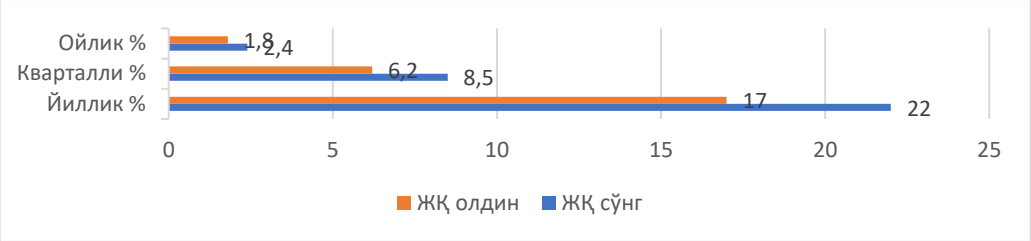
4 -жадвал.

«Киберхавсизлик» маркази ташкилотининг кўрсатқичлар бўйича натижалари

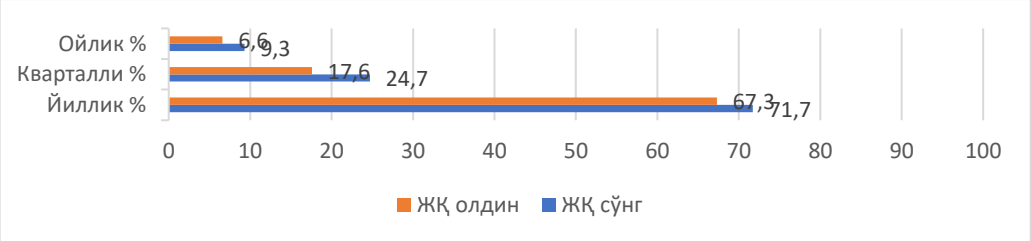
	Ойлик			Кварталли			Йиллик			Ўртача
	C^-	C^+	T_1	C^-	C^+	T_2	C^-	C^+	T_3	$T_{ў}$
H_c	18	24	21	62	85	22	179	220	20	21
B_t	66	93	71	176	247	71	713	967	74	72

4–жадвалда келтирилган C^- –тизимни жорий қилишдан олдинги ҳолат, C^+ –тизимни жорий қилингандан сўнги ҳолат ва T – жорий кўрсаткич бўйича самарадорлик.

Ҳужум изини қидиришнинг самарадорлигини аниқлашда ойлик, квартал ва йиллик нисбатлари алоҳида аниқланади (9-10-расмлар).



9-расм. Тизим ҳимоясини такомиллаштиришни натижадорлигининг график кўриниши



10-расм. Изни қидириш ва аниқланган изларни маълумотлар базасига ёзиш орқали самарадорликнинг график кўриниши

Олинган статистик маълумотлардан танлаб олинган кўрсаткичлар асосида алоҳида - алоҳида маълумотларни визуал солиштириш учун ҳар бир ташкилот миқиёсида диаграммалари шакллантирилган.

ТАТУ ташкилотида “Хавфсиз онлайн овоз бериш”га мўлжалланган тизимда, “Киберхавфсизлик” маркази ва “SSP Maroqand” кўп функцияли ахборот маркази унитар корхонаси”да тест жараёнида ҳужум изини қидиришга асосланган таклиф қилинаётган нейро-норавшан тармоқга асосланган ANFIS орқали қўйидаги самарадорликга эришилди. Тизимда инцидентлар мавжуд бўлиб, бу инциденларни урганиш жараёнида ахборот хавфсизлиги эксперти ва тизим томонидан бузғунчиликни криминалистик таҳлиллари 5-жадвалда келтирилган.

5-жадвал.

Ҳужум изини қидиришнинг самарадорлиги натижалари

Ташкилот номи	Ҳужумлар сони, x	Эксперт аниқланган ҳужум излари сони, y	ANFIS аниқланган ҳужум излари сони, Z	Самарадорлик, %
ТАТУ	45	28 (62%)	32 (71%)	9%
“Киберхавфсизлик” маркази ДУК	83	54 (65%)	60 (72%)	7%
“SSP Maroqand” МЧЖ	24	16 (67%)	19 (79%)	12%

Ушбу жадвалда келтирилган нисбат ҳисоблашлар қуйидаги ифода ёрдамида амалга оширилган.

$$A_1 = \frac{y}{x} \cdot 100\%, A_2 = \frac{z}{x} \cdot 100\% \text{ ва } B = |z - y|$$

Ахборот тизимида ҳужум изини қидириш ва криминалистик текширишларни амалга ошириш жараёнида ахборот хавфсизлиги эксперти тақдим қилган натижаларга нисбати нейро-норавшан тизимига асосланган таклиф қилинаётган ANFIS ҳужум изини қидириш вақти ҳамда криминалистик натижаларнинг сон ва сифат жиҳатдан устунлиги ҳисоблашларда ўз аксини топди.

ХУЛОСА

«Ахборот тизимларида ҳужум изларини қидириш ва таҳлил қилиш модели, алгоритмлари ва дастурий мажмуаси» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Ахборот тизимида ҳужум манбалари рўйхатини шакллантириш процедураси ишлаб чиқилган. Ишлаб чиқилган процедура ва шакллантирилган ҳужум манбалари рўйхати, тизимда ҳужум изларини қидириш ва аниқлашга хизмат қилади.
2. Ҳужум таъсири остида тугун ҳолатининг ҳодисалар мажмуасини қуриш алгоритми ишлаб чиқилган. Ишлаб чиқилган алгоритм асосида белгилаб олинган параметрларнинг мантиқий бошқарувини бинар муносабати ҳужум изини қидириш имконини беради.
3. Ахборот тизимида ҳужум изини қидириш модели ва параметрларини созлаш алгоритми ишлаб чиқилган. Ишлаб чиқилган модель ва параметрларни созлаш алгоритми асосида ҳужум изини қидириш қоидалари яратилади ва қоидалар асосида билимлар базаси шакллантирилиб, нейро-норавшан тармоқ орқали ўқитиш имконини беради.
4. Ахборот тизими ҳимояси самарадорлигини баҳолаш услуби танқидий ўрганилиб, баҳолаш учун қоидалар базаси ва лингвистик ўзгарувчиларни миқдорий қийматлари асосида баҳолаш услуби такомиллаштирилган.
5. Ахборот тизимида ҳужум изини қидиришга йўналтирилган дастурий мажмуанинг функционал тузилмаси ва талаблари ишлаб чиқилган. ишлаб чиқилган дастурий мажмуанинг функционал тузилмаси ва талаблари асосида ўтказилган ҳисоблаш тажриба натижалари бўйича таклиф этилган дастурий мажмуа ҳимояси талабларини қайта кўриб чиқиб, ҳимояланганлик даражаси 21% га, ҳужумларни аниқлаб, ҳужум изини ёзиш орқали келажакда олдини олиш даражаси 72% га ошган.

Таклиф этилган ҳужум изини қидириш модели асосида ахборот тизими ишлашида мамурга ва компьютер жиноятчилиги борасида криминалистик маълумотлар тўплаш имконини беради.

НАУЧНЫЙ СОВЕТ DSc. 13/30.12.2019.T.07.02 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

БЕКМИРЗАЕВ ОБИДЖОН НУРАЛИЕВИЧ

МОДЕЛЬ, АЛГОРИТМЫ И ПРОГРАММНАЯ КОМПЛЕКС ПОИСКА И АНАЛИЗА СЛЕДОВ АТАКИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

05.01.05 – Методы и системы защиты информации.
Информационная безопасность

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ

Тошкент–2022

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2022.2.PhD/T2833.

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:	**Муминов Баходир Болтаевич** доктор технических наук, профессор
Официальные оппоненты:	**Каримов Маджит Маликович** доктор технических наук, профессор
	Халмуратов Омонбой Утамуратович доктор философии по техническим наукам
Ведущая организация:	**«UNICON.UZ» - центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «17» декабря 2022 года в 10[00] часов на заседании Научного совета DSc. 13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: info@tuit.uz.

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №2403) (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-70)

Автореферат диссертации разослан «05» декабря 2022 года.
(протокол рассылки № 8 от «03» декабря 2022 года.)

Б.Ш. Махкамов
Председатель научного совета по присуждению ученых степеней, д.э.н., профессор

Э.Ш. Назирова
Ученый секретарь научного совета по присуждению ученых степеней, д.т.н., доцент

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

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В настоящее время, помимо поиска, выявления и устранения следов атак на информационную систему организаций, большое внимание уделяется повышению точности процесса обнаружения атак и уменьшению ошибок. По данным компании «Kaspersky», в третий квартале 2022 года доля атак на информационные системы государственных организаций увеличилась на 18%, причем 82% объектов атак составляли компьютеры, серверы и сетевые устройства[1]. В развитых странах мира, включая США, Германию, Японию, Францию, Китай, Южную Корею, Российскую Федерацию, проводятся активные научные исследования на основе интеллектуальных методов определения степени влияния угроз на информационные системы, совершенствованию систем защиты информации, разработке и применению методов и алгоритмов обнаружения следов атак.

Во многих странах мира проводятся научные исследования, направленные на совершенствование моделей, методов и алгоритмов обнаружения атак, а также поиска следов атак, независимо от способа осуществленния атак на информационные системы. Одной из наиболее важных задач в этом направлении является выявление и разработка моделей и алгоритмов анализа взлома, в том числе, путем записи в базе данных действий пользователей в пределах определенного диапазона, а также в поисках сигнатуры, поведениея и следов имевшей место атаки. Вместе с тем, при поиске следов атаки в информационной системе, когда знания о просматриваемом объекте неполные или имеются неясности (неопределенности) в анализируемой информации, возникает необходимость принятия решений с использованием методов, включающих интеллектуальные элементы.

В Республике Узбекистан за последнее время, во исполнение закона подписанного Президентом Республики Узбекистан «Стратегия развития нового Узбекистана на 2022 – 2026 годы»[2], а также Закона Республики Узбекистан ЗРУ – 764 «О Кибербезопасности»[3], в отраслевых организациях разработаны комплексные меры, направленные на повышение эффективности обнаружения следов атак. В частности, в этих законах поставлены задачи принятия необходимых мер путем критического изучения существующих информационных систем на уровне республики с точки зрения информационной безопасности. При реализации этих вопросов одной из важных задач является выявление таких проблем, как обоснование компьютерного преступления путем поиска, выявления следов совершенной атаки и формирования списка выявленных следов, а также предотвращение

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/#id8

[2] Указ Президента Республики Узбекистан УП-60, от 28 января 2022 года «О стратегии развития нового Узбекистана на 2022 - 2026 годы»

[3] Закон Республики Узбекистан, ЗРУ-764, от 15 апреля 2022 года.

взлома путем записи действий пользователя в пределах определенного диапазона при предоставлении этой информации необходимому специалисту.

Настоящее диссертационное исследование посвящено в определенной степени выполнению задач, определенных в Указах Президента Республики Узбекистан УП–60, от 28 января 2022 года, «О стратегии развития нового Узбекистана на 2022 - 2026 годы», в Постановлении ПП–4024, от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»[4], а также Указа УП–5349, от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», а также в других нормативно-правовых документах, посвященных этой проблематики.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствие с приоритетным направлением развития науки и технологий, определенных в документе «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. Научные исследования в области защиты информационных систем, обнаружения компьютерных атак и вредоносных программ, а также цифровой криминалистики проводятся М.В.Абрамовым, В.М. Сычевым, О.С. Терновой, О.В.Лукиновой, А.С.Кирилловым, В.М.Крундышевым, А.М.Кадновой, В.В. Сагитовой, А.В.Остроухом и другими зарубежными учеными. О. В. Багринцева, А. В. Никишова, С. Аль-Марри, А. Кимар проводили научные исследования об организационно-правовых мерах по обнаружению вредоносных программ в компьютерных системах и защите данных с помощью цифровой криминалистики. Кроме того, организациями «InfoWatch», «RiskWatch», «WatchGuard» и «Trend Micro» ведутся инженерно-исследовательские работы по разработке программно-аппаратных средств защиты информации с использованием компьютерной криминалистики при раскрытии компьютерных преступлений.

В Узбекистане под руководством С.К.Ганиева, М.М.Каримова, Г.У.Жураева, Б.Ф.Абдурахимова, Б.Б.Муминова, К.Ф.Керимова, Г.Н.Туйчиева, Д.Я.Иргашевой и другими проводятся исследования, связанные с программно-аппаратными методами защиты информации, в частности разработкой комплексных методов и средств межсетевого экрана и мониторинга в информационных системах связи, управлением инцидентами и реагированием на кибератаки, методами формирования критериев и показателей информационной безопасности, разработкой методов криптографической защиты информации с оценкой криптографических алгоритмов.

Однако, исходя из потребностей отрасли в области защиты информационных систем, поиск следов атак в информационных системах для

[4] Постановление Президента Республики Узбекистан ПП-4024, от 21 ноября 2018 года.

обеспечения информационной безопасности, подготовки набора данных, моделей анализа и алгоритмы недостаточно исследованы.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного исследовательского учреждения, где выполнена диссертация. Диссертационное исследование выполнено а рамках проекта №БВ–Ф4–023– Изучение проблем управления инцидентами и кибератаками в распределенных информационных и коммуникационных системах (2017–2020 гг.), согласно плана научно-исследовательских работ Ташкентского университета информационных технологий имени Мухаммада аль-Хоразми, а также плана мероприятий по защите научно-исследовательских работ и их проведению в онлайн-режиме в период COVID-19.

Целью исследования заключается создание модели, алгоритмов и программного комплекса для поиска и анализа следов атак в информационных системах.

Задачи исследования:

сравнительный анализ компьютерной преступности в области информационной безопасности, ее специфики, криминалистических характеристик, связанных с ней правовых норм и проблем;

разработка процедуры формирования списка источников атаки в информационной системе и алгоритма построения комплекса событий состояния узла под воздействием атаки;

построение модели поиска следов в информационной системе и разработка алгоритма настройки параметров;

совершенствование методики оценки эффективности защиты информационной системы;

разработка функциональной структуры и требований к программному комплексу, направленному на поиск следов атак.

В качестве **объекта исследования** рассмотрены события и набор данных информационной системы.

Предметом исследования являются методы обнаружения атак в информационной системе, компьютерная преступность, модели и алгоритмы определения вероятностей последствий атаки.

Методы исследования. В ходе исследования были использованы методы обнаружения следов атаки в информационной системе с использованием интеллектуальных систем, нейронных сетей, теории неопределенных множеств, теории вероятностей, теории графов и методов объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

на основе объекта возможного воздействия на информационную систему и существующего интерфейса разработана процедура формирования списка источников атаки в информационной системе;

для построения логического управления четырьмя параметрами комплекса событий разработан алгоритм построения комплекса событий, состояния узла под воздействием атаки на основе бинарной связи;

на основе процедуры формирования списка источников атаки в информационной системе и нейро-неопределенной системы ANFIS разработан алгоритм настройки поисковой модели на параметры следов атаки;

на основе нейро-неопределенной системы ANFIS усовершенствована методика оценки эффективности защиты информационной системы.

Практическая ценность работы заключается в следующем:

разработан программный комплекс на основе структуры системы «Безопасное онлайн-голосование»;

разработаны функциональная структура и требования программного комплекса на основе модели, ориентированной на поиски следа атаки.

Достоверность результатов исследования. Достоверность результатов исследования объясняется точностью математического представления задачи, точностью модели и параметров поиска следов атак, разработкой программного комплекса безопасного онлайн-голосования и использованием в этой системе программного комплекса поиска следов атак, а также выводами ведущих ученых и специалистов в данной области.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования подтверждается эффективностью метода определения степени воздействия угроз в процессе защиты информационной системы в разрабатываемой организации, алгоритмом обнаружения атак на основе нейро-неопределенного системе метода поиска следов атак, а также разработанной модели анализа атак.

Практическая значимость результатов исследования объясняется тем, что программный комплекс, разработанный на основе предложенной модели и алгоритмов, повышает степень защищенности информационной системы.

Внедрение результатов исследования. На основе разработанной модели поиска и анализа следов атаки в информационных системах, а также научно-практических результатов по разработанному программному комплексу:

«Программный комплекс нейро-неопределенной системе модели поиска следа имевшей место атаки в информационной системе учреждений с помощью процедуры формирования списка источников атаки в информационной системе и алгоритма построения комплекса событий состояния узла под воздействием атаки» внедрен в ТУИТ имени Мухаммада ал-Хоразми (справка №33-8/6759 от 12 октября 2022 года Министерства по развитию информационных технологий и коммуникаций). По результатам научных исследований, после пересмотра требований к защите существующей информационной системы, степень ее защищенности повысилась на 21%. С помощью формирования базы данных следов, выявленных от предыдуших атак на систему степень предотвращения ее повторения в будущем увеличилась на 71%. Кроме того, путем блокировки повторных неудачных попыток в системе возможные повторные угрозы были уменьшены на 50%;

«Программный комплекс для поиска следов атаки в информационной системе организации» был внедрен на Унитарном предприятии многофункционального информационного центра «SSP Марокканд» (справка №33-8/6759 от 12 октября 2022 года Министерства по развитию

информационных технологий и коммуникаций). В результате научного исследования создана возможность обнаружения атак на информационную систему учреждения и предупреждения об этом системного администратора;

Программные комплексы «Безопасное онлайн-голосование» и «Поиск следа атаки» был использован в тестовом режиме в Государственном унитарном предприятии «Центр кибербезопасности». (справка №33-8/6759 от 12 октября 2022 года Министерства по развитию информационных технологий и коммуникаций). В результате научного исследования, путем пересмотра текущих требований к защите информационных систем, уровень защиты увеличилась на 21%, а за счет формирования базы данных обнаруженных следов, уровень предотвращения в будущем увеличилась на 72%.

Апробация результатов работы. Результаты данного исследования обсуждены на 11 научно-практических конференциях, в частности 4 международных и 7 республиканских научно-практических конференциях.

Опублекованность результатов исследования. По теме диссертации опубликованы всего 17 научных работ, из них 5 статей в научных изданиях, рекомендованных для публикации основных научных результатов диссертации Высшей аттестационной комиссией Республики Узбекистан, в том числе 1 – в иностранных и 4 – в республиканских журналах, также получено 1 свидетельство регистрации программного продукта созданного для ЭВМ.

Структура и объем диссертации. Структура диссертации состоит из введения, четырех глав, заключения, списка использованной литературы, список сокращений и обозначений а также приложения. Объем диссертации составляет 117 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИСЕРТАЦИИ

Во введении обоснованы актуальность и востребованность темы диссертации, показано соответствие темы диссертации с приоритетными направлениями развития науки и технологий Республики Узбекистан. Сформулированы цель и задачи, определены объект и предмет исследования, изложена научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта их теоретическая и практическая значимость. Приведен перечень внедрения результатов исследования в практику, структура диссертации, а также сведения об опубликованных работах по теме диссертации.

В первой главе диссертации, озаглавленной **«Проблемы и теоретические основы компьютерной преступности в безопасности информационных систем»** представлен анализ компьютерной преступности и существующие правовые нормы в области информационной безопасности, ее специфические свойства и криминалистические характеристики, проблемы компьютерной преступности и сравнительный анализ методов определения

компьютерного преступления, а также сформированы задачи диссертационной работы.

Изучение и анализ компьютерных преступлений в информационных системах показал, что за последнее десятилетие их количество увеличилось в 22,3 раза и продолжает расти на 3,5% в год. Годовой объем материального ущерба от преступлений составил 8,5 миллиард долларов. Определенный процент преступлений осуществляется успешно, но из них изучено только 49%. Это составляет 25,5% от общего количества уголовных дел, средний показатель количества приостановленных уголовных дел составляет 43,5%. Это свидетельствует о недостаточном уровне квалификации сотрудников организаций по безопасности, осуществляющих деятельность по возбуждению, расследованию и предупреждению уголовных дел.

Все вышесказанное беспорно доказывает об актуальности внедрения в системы обнаружения атак специальных программно-аппаратных комплексов, предназначенных для их обнаружения. Типичная архитектура системы обнаружения атак включает в себя следующие компоненты (Рисунок 1).

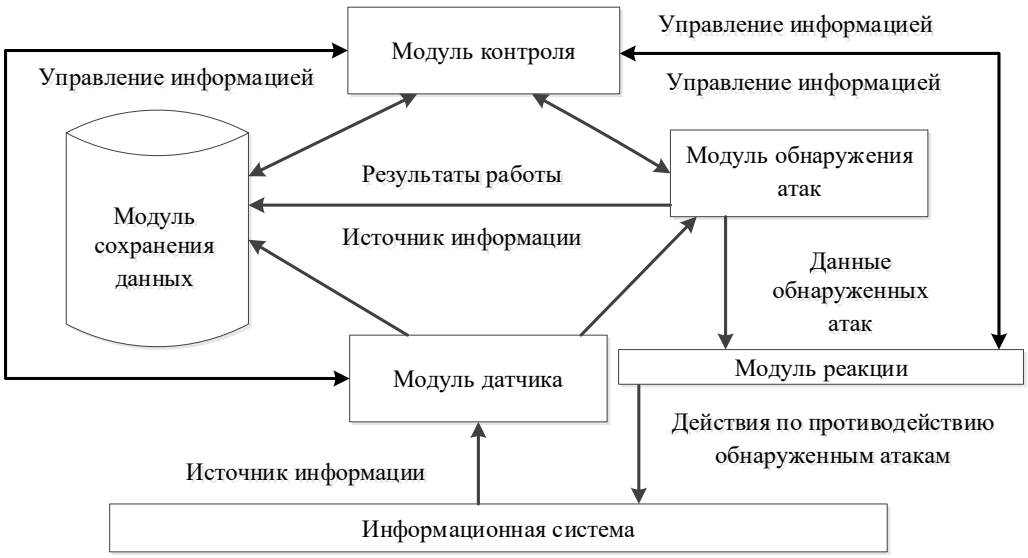


Рисунок 1. Архитектура систем обнаружения атак

В результате проведенного анализа методов обнаружения атак на основе сигнатур и состояний, используемых многими исследователями, было установлено, что для усовершенствования и повышения их эффективности необходимо решить следующие задачи:

8. Выявить источники угроз информационной безопасности в информационной системе, а также разработать процедуру процесса, основанного на архитектуре информационной системы и факторах анализа следов атаки.

9. Разработать сценарии формирования узлов, их состояния, а также изменения событий в следствие анализа следов атаки.

10. Разработать алгоритм построения модели поиска следов атак и определения ее параметров в информационной системе.

11. Предложить методику подготовки набора исходных данных (учебных выборок) для нейро-нечеткой системы.

12. Разработать метод оценки следов атаки в информационной системе.

13. Усовершенствовать методику подхода к оценке эффективности защиты информационной системы.

14. Разработать требования к функциональной структуре программного комплекса для предлагаемой модели и алгоритмов.

Во второй главе диссертации, озаглавленной **«Построение комплекса моделей и событий»** исследуется архитектура информационных систем и модели атак. Разработана процедура формирования списка источников атаки и алгоритм построения множества событий состояния узла под воздействием атаки в информационной системе. Предложен алгоритм нейро-нечеткой системы, адаптированный для классификации следов атаки.

В результате исследований сформирован перечень процедур на основе выявления видов материального и нематериального ущерба и негативных последствий, возникающих после атаки на информационную систему организации. Для этого виды ущерба (ЗТ) и негативные последствия (СО) предлагаются обознаить следующим образом:

$ЗТ_{1.1}$ – вид ущерба, нанесенного физическому лицу;

$СО_{1.1}$ – нанесение ущерба субъекту, его персональным данным путем незаконной обработки, включая нарушение прав на личную неприкосновенность, личную и семейную тайну;

$ЗТ_{2.1}$ – вид ущерба, нанесенного юридическому лицу;

$СО_{2.1}$ – нарушение требований нормативно-методических документов в области информационной безопасности;

$СО_{2.2}$ – нарушение деловой репутации юридического лица;

$СО_{2.3}$ – необходимость изменения (реконструкции) процессов функционально-логического отношения, осуществляющихся в информационной системе;

$СО_{2.4}$ – виды ущерба, связанного с функционированием информационных инфраструктур, автоматизированных систем управления процессами;

$СО_{2.5}$ – нанесение ущерба юридическому лицу в виде финансовых потерь путем утечки защищенной информации и незаконной обработки.

Прогнозирую информационную систему и степень ее возможностей структуры, злоумышленников можно разделить на группы, которые включают:

H^0 – основная возможность проведения атаки на информационную систему;

H^1 – основные расширенные возможности реализации атаки на информационную систему;

H^2 – средняя возможность реализации атаки на информационную систему;

H^3 – высокая возможность реализации атаки на информационную систему;

H^4 – новая возможность реализации атаки на информационную систему.

Существуют следующие виды влияния веса на объекты воздействия по виду причиняемого этим физическим и юридическим лицам ущерба и возможных негативных последствий:

W_i = нарушение конфиденциальности, целостности, доступности, подлинности, безотказности, подотчетности, идентичности свойств, надежности.

Кроме того, была выделена классификация по трем типам злоумышленников:

B^1 – в данную классификацию злоумышленников входят специалисты, ответственные за функционирование информационной системы организации.

B^2 – в данную классификацию злоумышленников входят пользователи и поставщики услуг с высокой склонностью к взлому информационной системы организации.

B^3 – в эту классификацию злоумышленников входят преднамеренные или некомпетентные действия пользователей в информационной системе организации.

Визуальное представление влияния процедуры и веса на объект воздействия, в следствии чего возникают негативные последствия в зависимости от степени влияния атаки, присвоенного уровная классификации, влияния ущерба представлены на рисунказ 2 и 3.

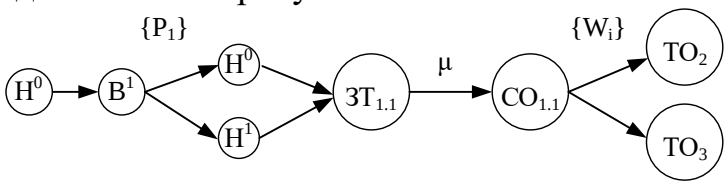


Рисунок 2. Визуальное представление влияния процедуры и веса на объект воздействия физического лица

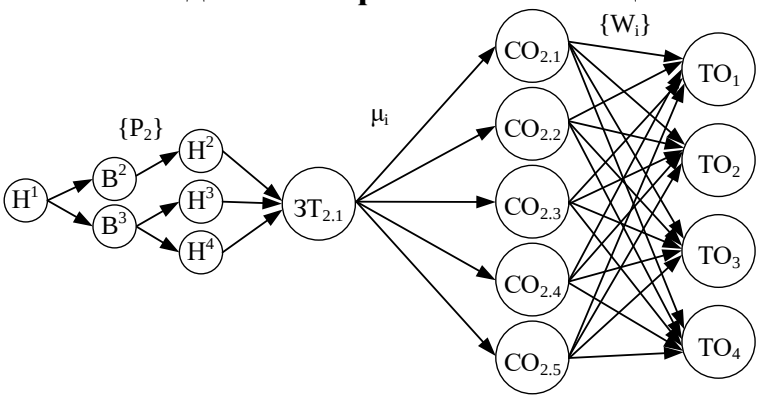


Рисунок 3. Визуальное представление влияния процедуры и веса на объект воздействия юридического лица

Предлагаемая процедура зависит от каждого события и характеристик информационной системы, а также состояния узлов при атаке, соответствующих пользователю и его роли. Это требует создания событий состояния узла, находящихся под воздействием атаки.

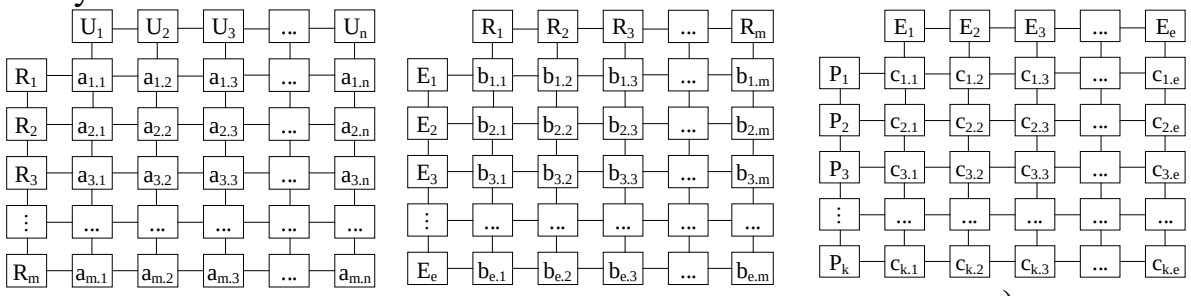
Предотвращение атак в информационной системе осуществляется на основе таких объектов воздействия как, методы программно-аппаратной защиты информации, в частности комплексные методы и средства

межсетевого экранирования и мониторинга в информационно-коммуникационных системах и фильтрации сетевого трафика. Существуют атаки, которые не могут быть обнаружены мерами, реализованными на основе этих объектов воздействия. После осуществления атаки возникает необходимость определить объект ее воздействия или вид ущерба. При этом необходимо рассмотреть события состояния узла под воздействием атаки для информационной системы.

События состояния узла информационной системы были построены на основе требований, установленных владельцем системы.

Пользователь (U_i), $(i=1,...N)$ $N-$количество пользователей, роль (R_j), $(j=1,...M)$ $M-$количество ролей. Каждое событие управляемое в информационной системе и их количество зависит от функциональных возможностей самой информационной системы, событие (E_e), $(e=1,...L)$ $L-$ количество событий, событие каждого объекта получены в информационной системе, количество характеристик ограничено и характеристика (P_k), $(k=1,...K)$ $K-$количество характеристик.

Построение комплекса событий состояния узла бинарного отношения логического управления на основе сгенерированных параметров представлен на Рисунке 4.



а) б) с)

Рисунок 4. а), б) и с) бинарное отношение логического управления пользователя, роли, события и характеристик

Во второй главе диссертации, озаглавленной **«Поиск и оценка следов атак в информационной системе»** предложен алгоритм построения и настройки параметров модели поиска следов атаки в информационной системе. Разработан метод и алгоритм оценки следа атаки в информационной системе. Усовершенствована методика оценки эффективности защиты информационных систем. Разработаны функциональная структура и требования к программному комплексу поиска следа атаки.

Правила реализации модели нечеткой нейронной сети, основанной на правилах поиска следа атаки в информационной системе имеет следующий вид:

$$R_i: Если\ (x_i == A_i, \cap \ldots \cap\ (x_{ij} == A_{ij}) \cap \ldots \cap\ (x_{im} == A_{im})\ \text{то}$$
$$y = c_{io} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1 \ldots n\ \text{или}\ R_i := \bigcap_{j=1}^{m} (x_{ij} == A_{ij}),\ \text{то}, \qquad (1)$$

$$y_i = c_{io} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1 \ldots r, i = 1 \ldots n. \quad R = \sum_{i=1}^{m} R_i - \text{набор общих правил.}$$

В выражении (1) методология поиска следов атаки в информационной системе определяется базой правил.

Нечеткая нейронная система ANFIS основана на следующих правилах:

– точность внесенных переменных;

– определенность функции принадлежности функцией Гаусса.

$$\mu_{ij}(y_j) = \exp\left(-\frac{1}{2}\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right)$$

где входные сети y_j, настройки a_{ij} и b_{ij} являются параметрамы функции принадлежности.

После дефаззификации для получения выходной переменной функциональная связь выражается в следующем виде:

$$y' = \frac{\sum_{i}^{n}((c_{io} + \sum_{j=1}^{m} c_{ij} x_j) \prod_{j=1}^{m} \mu_{A_{ij}}(x_j'))}{\sum_{i=1}^{n}\prod_{j=1}^{m} \mu_{A_{ij}}(x_j')} = \frac{\sum_{i}^{n}(c_{io} + \sum_{j=1}^{m} c_{ij} x_j) \prod_{j}^{m} \exp\left[-(\frac{x_j' - a_{i,j}}{b_{i,j}})^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m} \exp\left[-(\frac{x_j' - a_{i,j}}{b_{i,j}})^2\right]}$$

Это выражение основано на сети ANFIS с использованием алгоритма Takagi‑Sugeno‑Kang (TSK), который включает в себя пять шагов:

Первый шаг - фаззификация конкретных переменных выполняет следующую процедуру $x_j' \ (j = 1, 2, ..., n)$.

Второй шаг - элементы a_{ij} и b_{ij} вычисляются с параметрами весов и значениями функций принадлежности $\mu_{A_{ij}}(x_j')$, заданными функциями Гаусса.

Третий шаг – умножается результаты элементов второго шага и генерируется значения функции, то есть

$$y_i = (c_{jo} + \sum_{j=1}^{m} c_{ij} x_j').$$

Первый элемент четвертого шага необходим для активации выводов правил по значениям, собранным на 3-м шаге, степенями принадлежности необходимых условиям правил. Второй элемент четвертого шага выполняет дополнительные операции для дальнейшей фаззификации результата сети ANFIS.

Этот шаг состоит из одного нормализующего элемента, который дификацирует результаты сети ANFIS:

‑ в создании ANFIS на основе алгоритма Sugeno‑Kang содержится 2 параметрических правила (на шагах 1 и 3). Параметры, которые можно настроить во время обучения сети ANFIS:

– на первом шаге функции принадлежности не линейных параметров a_{ij} и b_{ij}, являются фаззификаторами;

– на третьем шаге параметры линейных функций c_{io} и c_{ij} используют выводы из базы правил $y_i = (c_{io} + \sum_{j=1}^{m} c_{ij} x_j')$.

При наличии n правил и m входных переменных количество параметров первого шага равно $2nm$, а количество параметров второго шага равно $2 - n(m+1)$. Общее количество настраиваемых параметров составляет $n(3m+1)$.

На следующем этапе предлагаемой модели рассчитываются параметры c_{io} и c_{ij} линейных функций с учетом заданных значений параметров a_{ij} и b_{ij}.

c_{io} и c_{ij} араметры находятся путем решения системы линейных уравнений. Это число выражается в виде выходной переменной:

$$y^{'} = \sum_{i=1}^{m} w_i^{'}(c_{io} + \sum_{j=1}^{m} c_{io} x_j) \quad \text{где} \quad W_i^{'} = \frac{\prod_{j=1}^{m} \mu_{A_{ij}}(x_j^{'})}{\sum_{i=1}^{n}\prod_{j=1}^{m} \mu_{A_{ij}}(x_j^{'})} = \frac{\prod_{j}^{m} \exp\left[-(\frac{x_j^{'} - a_{i,j}}{b_{i,j}})^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m} \exp\left[-(\frac{x_j^{'} - a_{i,j}}{b_{i,j}})^2\right]} = const$$

После определения линейных параметров выбранного $ij-$ для всех обучающих выборок используется коррекция, вычисление фактических выходных данных сети и линейной зависимости для них:

$$y^{'} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} = w \cdot c$$

где вектор ошибки определяется следующим образом: $e = y^{'} - y$, отсюда определяются текущие параметры:

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) + c\frac{dE^{(k)}(t)}{da_{ij}^{(k)}} \quad \text{и} \quad b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) + c\frac{dE^{(k)}(t)}{db_{ij}^{(k)}}$$

Модель поиска следа атаки на основе нейро-нечеткого ANFIS с использованием алгоритма Takagi–Sugeno–Kang приведен на рисунке 5.

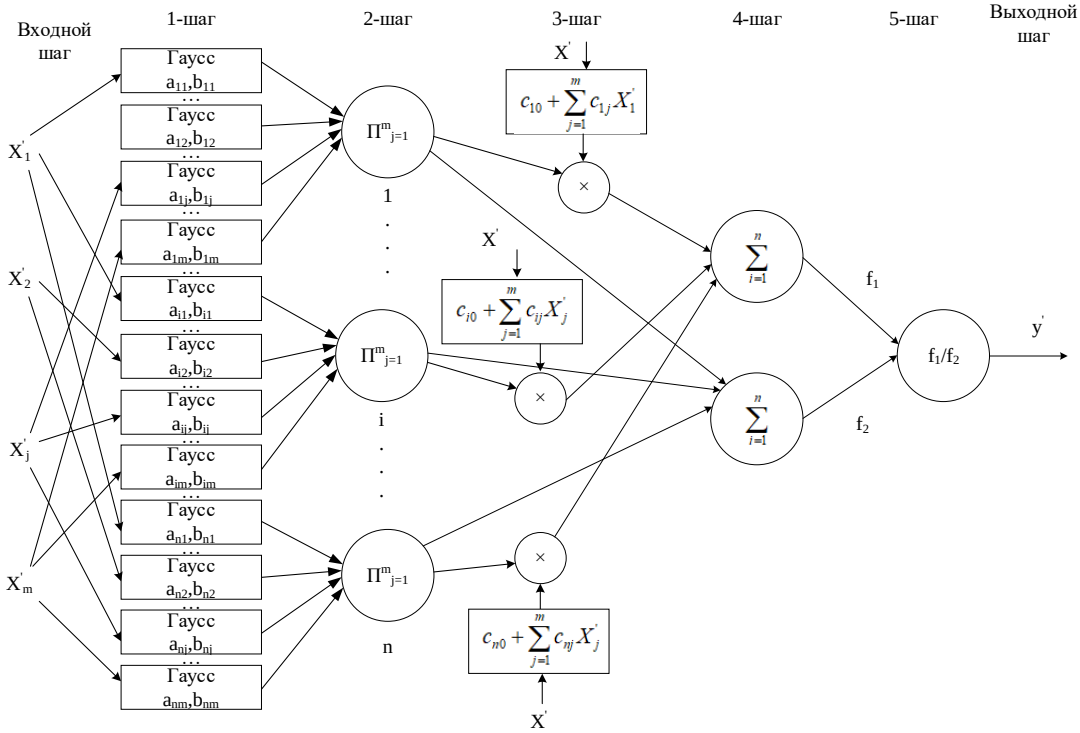


Рисунок 5. Модель поиска следа атаки на основе нейро-нечетной системы ANFIS

Предлагаемый способ заключается в реализации нечеткой производственной модели, основанной на правилах алгоритма производительности сети системы ANFIS с алгоритмом нечеткого вывода Takagi–Sugeno–Kang:

$$R: \text{если } x_i == A_i \text{ то } y = c_{io} + \sum_{i=1}^{N} c_i x_i, i = 1,...N.$$

На основе ранее установленных показателей и требований по защите информации, а также обнаруженных следов атаки в текущей информационной системе и на основе перечня ее инфраструктуры сформирована база правил, часть из них была разработана на основе Таблицы 1.

Таблица 1.

База правил для оценки эффективности комплекса поиска следа атаки в информационной системе

№	Если (IF)			Тогда (THEN)
	Входные параметры	Выходные параметры	Уровень следа атаки	
1	x_1	z_1	Очень низкий (очень маловероятный)	Эффективность достигается
2	x_2	z_2	Низкий (маловероятный)	Эффективность достигается
3	x_3	z_3	Средний (возможный)	Эффективность достигается
4	x_4	z_4	Высокий (вероятный)	Эффективность достигается
5	x_5	z_5	Очень высокий (часто встречающийся)	Эффективность не достигается

Количественные значения лингвистических переменных представлены в Таблице 2.

Таблица 2.

Количественные значения лингвистических переменных

№	Обозначение	Исходное выражение	Значение
1	Очень низкий (очень маловероятный)	$0,1 < \lvert x_1 - z_1 \rvert \le 0,3$	$0,1 \sim 0,3$
2	Низкий (маловероятный)	$0,3 < \lvert x_1 - z_1 \rvert \le 0,5$	$0,3 \sim 0,5$
3	Средний (возможный)	$0,5 < \lvert x_1 - z_1 \rvert \le 0,7$	$0,5 \sim 0,7$
4	Высокий (вероятный)	$0,7 < \lvert x_1 - z_1 \rvert \le 0,9$	$0,7 \sim 0,9$
5	Очень высокий (часто встречающийся)	$0,9 < \lvert x_1 - z_1 \rvert \le 1$	$0,9 \sim 1$

В ходе работы был проведен масштабный анализ данных, таких как решения для инфраструктуры информационной системы, статические модели атаки на информационную систему. На основании этого усовершенствована методика оценки эффективности защиты информационной системы.

Функциональная структура программного комплекса поиска следа атаки представлена на Рисунке 6.

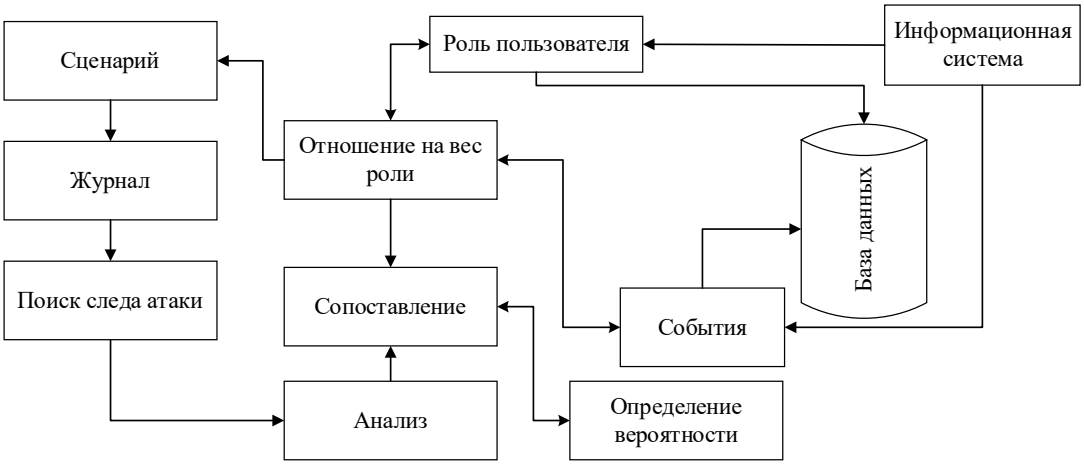


Рисунок 6. Функциональная структура программного комплекса поиска следа атаки

Четвертая глава диссертации, озаглавленная **«Функциональные задачи и результаты внедрения программного комплекса»** посвящена функциональной структуре внедренной системы «Безопасное онлайн-голосование», оценке и анализу эффективности модели поиска следа атаки в информационной системе, а также анализу требований и результатов внедрения.

Исходя из этого, поиск следа атаки в информационной системе и структура управления обнаруженной атаки представлены на рисунке 7.

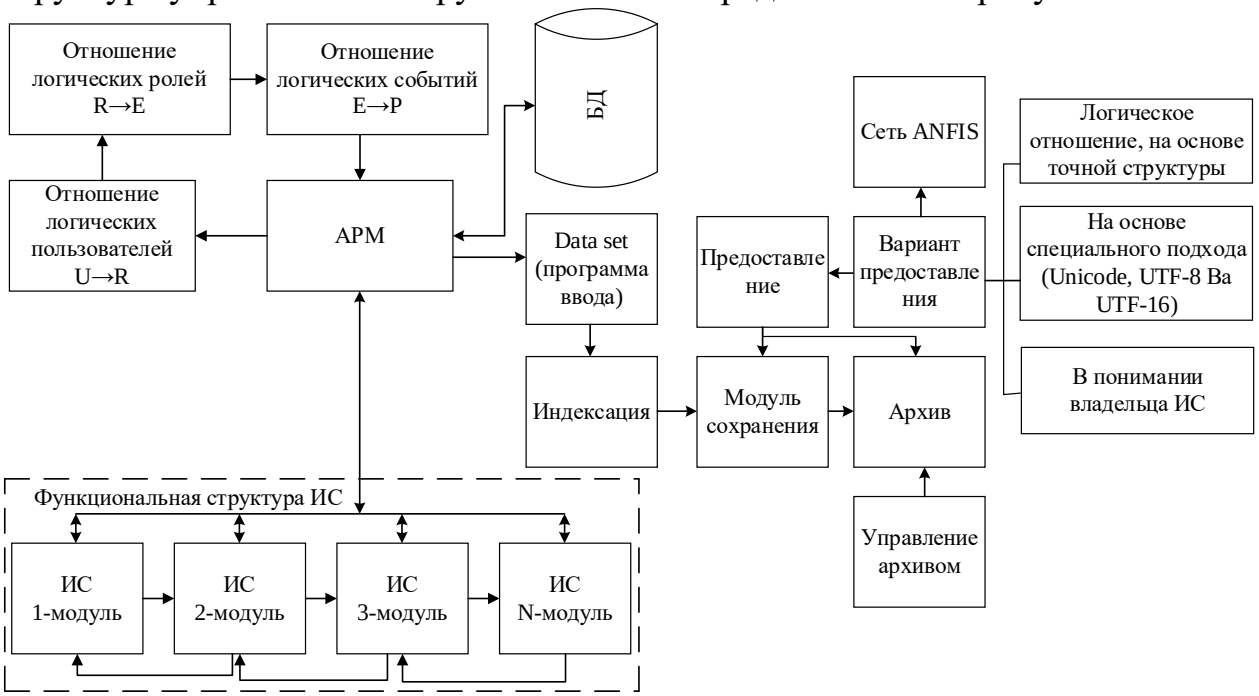


Рисунок 7. Схема поиска следа атаки в ИС и управления обнаруженной атаки

В информационной системе формируется база знаний на основе правил поиска следов атаки и на ее основе строится data set. Для каждой информационной системы всегда разрабатывается отдельный data set, поскольку каждый системный data set создается на основе роли каждого пользователя в информационной системе.

С помощи модели, предложенной в исследовании и алгоритмами для решения таких задач были проведены эксперименты по сравнению производительности некоторых моделей классификаций.

В научном исследовании графическое представление сравнительного анализа предлагаемой системы ANFIS на основе построения набора данных и корректировки существующих моделей и элементов на языке программирования «Python» представлено на Рисунке 8.

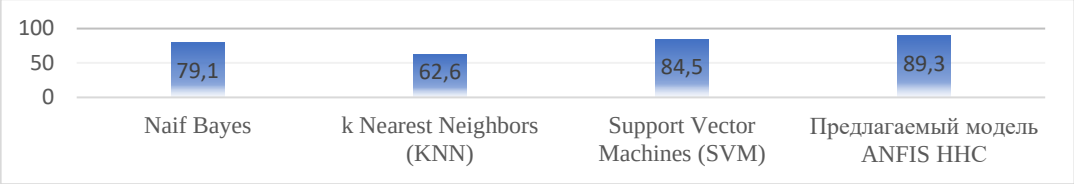


Рисунок 8. График сравнительного анализа моделей решения проблемы

Таким образом, для данных условий задачи рекомендуемый модель является наилучшим по показателям поиска и обнаружения следа атаки.

Чтобы определить удобство использования и эффективность предлагаемого поиска следа атаки, было проведено сравнение состояния системы до и после внедрения.

Для определения эффективности и результативности системы необходимо выбрать следующие показатели:

- защита путем ограничения доступа с этого имени после авторизации пользователя (H_c, единица измерения в процентах);
- предотвращение путем поиска следа и записи обнаруженных следов в БД (B_t, единица измерения в процентах);
- эффективность работы специалиста (M_s, единица измерения в процентах);
- контроль атаки специалистом (E_t, единица измерения в процентах);

Расчет суммарного показателя на основе этих показателей осуществляется следующим образом.

$$k_1 = \frac{H_c - H_c^0}{H_c^0}, k_2 = \frac{B_t}{B_t^0}, k_3 = \frac{M_s}{M_s^0}, k_4 = 1 - \frac{E_t}{E_t^0}$$

где N – количество показателей (равно N=4), k_i - эффективность показателей, основанных соответственно на критериях каждой организации. Где эффективность показателя k_i расчитывается следующим образом («см. Таблицу 4»).

Таблица 4.

Результаты по показателям организации «Центр кибербезопасности»

	Ежемесячный			Ежеквартальный			Ежегодный			Средный
	C^-	C^+	T_1	C^-	C^+	T_2	C^-	C^+	T_3	$T_{\tilde{y}}$
H_c	18	24	21	62	85	22	179	220	20	21
B_t	66	93	71	176	247	71	713	967	74	72

Исходя из таблицы 4- C^- - состояние перед внедрением системы, C^+ - состояние после внедрения системы и T – эффективность по текущему показателю.

При определении эффективности поиска следа атаки ежемесячное, ежеквартальное и годовое соотношение определяется отдельно (Рисунки 9-10).

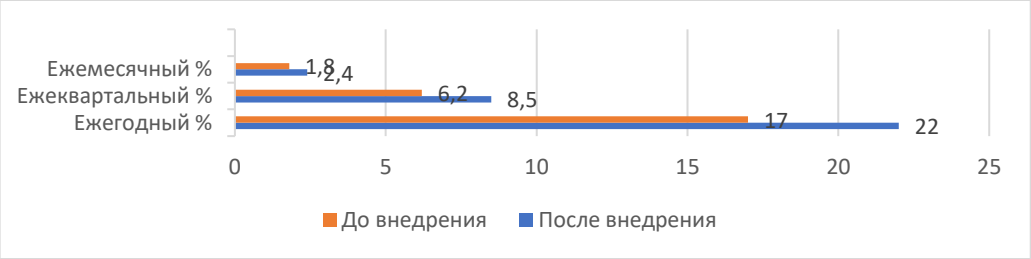


Рисунок 9. Графическое представление результативности улучшения защиты системы

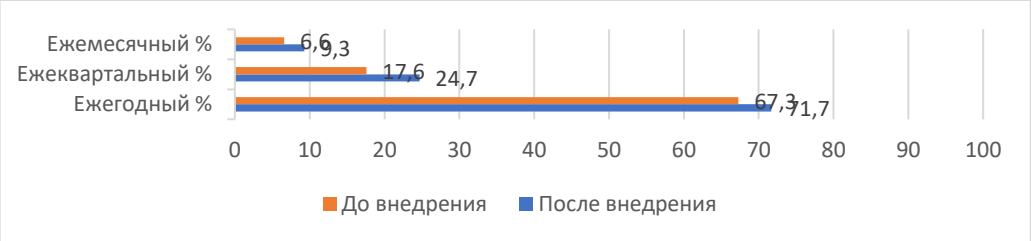


Рисунок 10. Графическое представление эффективности путем поиска следа и записи обнаруженных следов в базу данных

Из полученных статистических данных на основе выбранных показателей для наглядного сравнения отдельных данных сформированы диаграммы в масштабе каждой организации.

В рассматриваемых системах обнаруженые инциденты изучались экспертами по информационной безопасности, результаты которых сравнивались с количеством обнаруженных следов атак на основе системы ANFIS. Результаты представлены в Таблице 5.

Таблица 5.

Результаты эффективности поиска следа атаки

Наименование организации	Количество атак, x	Количество следов атак, обнаруженных экспертом, y	Количество следов атак, обнаруженных системой ANFIS, z	Эффективность, %
ТУИТ	45	28 (62%)	32 (71%)	9%
ГУП «Центр Кибербезопасности»	83	54 (65%)	60 (72%)	7%
ООО «SSP Maroqand»	24	16 (67%)	19 (79%)	12%

В организации «ТУИТ», в системе, предназначенной для «Безопасного онлайн-голосования», в «Центре кибербезопасности» и

многофункциональном информационном центре унитарного предприятия «SSP Maroqand» в тестовом режиме была достигнута значительная производительность с помощью предложенной нейро-нечеткой системы на базе ANFIS.

Расчеты отношения, представленные в этой таблице, были сделаны с использованием следующего выражения.

$$A_1 = \frac{y}{x} \cdot 100\%,\ A_2 = \frac{z}{x} \cdot 100\% \text{ и } B = |z - y|$$

Поиск следов атаки в информационной системе в ходе реализации криминалистических проверок, соотношение результатов, предоставленных экспертом по информационной безопасности и поиск следов атаки на основе нейро-нечеткой системы ANFIS, а также сравнение криминалистических результатов по количеству и качеству по этим методам отражены в расчетах.

ЗАКЛЮЧЕНИЕ

По результатам диссертационной работы на тему «Модель, алгоритмы и программная комплекс поиска и анализа следов атаки в информационных системах» были представлены следующие выводы:

1. Разработана процедура формирования списка источников атак. Разработанная процедура и сформированный список источников атак служат для поиска и выявления следов атаки в информационной системе.

2. Разработан алгоритм построения комплекса событий состояния узла под воздействием атаки. Логическое управление бинарного отношения параметров, определяемых на основе разработанного алгоритма позволяет осуществлять поиск следов атаки.

3. Разработана модель поиска следа атаки и алгоритм настройки параметров. На основе разработанной модели поиска и алгоритма настройки параметров создаются правила поиска следа атаки и на основе правил формируется база знаний, позволяющая проводить обучение через нейро-нечеткую сеть.

4. Критически изучен метод оценки эффективности защиты информационной системы, а также усовершенствована методика оценки на основе базы правил и количественных значений лингвистических переменных.

5. Разработаны функциональная структура и требования к программному комплексу, ориентированному на поиск следа атаки в информационной системе. Исходя из функциональной структуры и требований разрабтанного программного комплекса, пересматривая требования к защите предлагаемого программного комплекса по результатам вычислительного эксперимента, степень защищенности повысилась на 21%, обнаружение атак и запись следов атак позволили предотвратить будущие атаки на 72 %.

На основе предложенной модели поиска следа атаки, в процессе работы информационной системы позволяет администратору собирать криминалистическую информацию о компьютерных преступлениях.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

BEKMIRZAEV OBIDJON NURALIEVICH

MODEL, ALGORITHMS AND SOFTWARE COMPLEX OF SEARCH AND ANALYSIS OF ATTACK TRACES IN INFORMATION SYSTEMS

05.01.05 – Methods and systems of information protection.
Information security

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

Tashkent–2022

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 B2022.2.PhD/T2833.

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:	**Muminov Bahodir Boltaevich** Doctor of Technical Sciences, Professor
Official opponents:	**Karimov Madjit Malikovich** Doctor of Technical Sciences, Professor
	Xalmuratov Omonboy Utamuratovich Doctor of Philosophy in Technical Sciences
Leading organization:	**Scientific-Engineering and Marketing researches Center «UNICON.UZ»**

The defense will take place «17» December 2022 at 10^{00} at the meeting of the Scientific Council No. DSc.13/30.12.2019.T.07.02 at Tashkent University of Information Technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: info@tuit.uz).

The dissertation could be reviewed at the Information Resourse Centre of Tashkent University of Information Technologies (registration number No 2703). (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-70.

The abstract of dissertation is distributed on «05» December 2022 y.
(protocol at the register No. 8 on «03» December 2022 y.).

B.Sh. Makhkamov
Chairman of the Scientific Council awarding scientific degrees, Doctor of economic sciences, Professor

E.Sh. Nazirova
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 create a model, algorithms and software complex for searching and analyzing traces of attacks in information systems.

The object of the research work considered events and information system data set.

The scientific novelty of the research work is as follows:

based on the object of possible impact on the information system and the existing interface, a procedure has been developed for generating a list of attack sources in the information system;

to build a logical control of four parameters of a complex of events, an algorithm for constructing a complex of events, the state of a node under the influence of an attack based on a binary connection has been developed;

based on the procedure for generating a list of attack sources in the information system and the neuro-fuzzy system ANFIS, an algorithm for setting up the search model for the parameters of attack traces was developed;

on the basis of the neuro-fuzzy system ANFIS, the method for evaluating the effectiveness of information system protection has been improved.

Implementation of the research results. A software package has been developed based on our model aimed at searching and analyzing traces of attacks in information systems:

«The software complex of a neuro-fuzzy system model for searching for a trace of an attack that has taken place in the information system of institutions using the procedure for generating a list of attack sources in the information system and the algorithm for constructing a complex of events for the state of a node under the influence of an attack» was introduced at TUIT named after Muhammad al-Khwarizmi (Reference No. 33 -8/6759 of October 12, 2022 of the Ministry for the Development of Information Technologies and Communications). According to the results of scientific research, after the revision of the requirements for the protection of the existing information system, the degree of its security increased by 21%. By creating a database of traces identified from previous attacks on the system, the degree of prevention of its recurrence in the future increased by 71%. In addition, by blocking repeated failed attempts in the system, possible repeated threats have been reduced by 50%;

Our developed software package was implemented in the multi-functional information center unitary enterprise «SSP Maroqand» (certificate No. 33-8/6759 dated October 12, 2022 of the Ministry for the Development of Information Technologies and Communications). The software package developed as a result of scientific research has the ability to detect possible attacks on the organization's information system and warn the system administrator about it;

The software packages «Secure online voting» and «Search for the trace of an attack» were used in test mode at the State Unitary Enterprise «Cybersecurity Center». (Reference No. 33-8/6759 dated October 12, 2022 of the Ministry for the Development of Information Technologies and Communications). As a result of scientific research, by revising the current requirements for the protection of

information systems, the level of protection increased by 21%, and through the formation of a database of detected traces, the level of prevention in the future increased by 72%.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, four chapters, a conclusion, a list of references, list of abbreviations and symbols as well as appendix. The volume of the dissertation is 117 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (I часть; I part)

1. Б.Б. Мўминов, О.Н. Бекмирзаев Ахборот тизимларида ҳужум изларини аниқлаш усуллари // “Муҳаммад ал-Хоразмий авлодлари” илмий-амалий ва ахборот-таҳлилий журнали. Тошкент 2020. №4(14). -Б. 16-20. (05.00.00; №10).

2. B.B. Mo‘minov, O.N. Bekmirzayev Axborot tizimiga qaratilgan buzg‘unchi hujumlarining oldini olish usullari // “TATU xabarlari”, Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университетининг илмий-техника ва ахборот-таҳлилий журнали. Тошкент 2021. №1(57)/2021. – Б. 128-140. (05.00.00; №31).

3. Х.К. Самаров, О.Н. Бекмирзаев Ахборот тизимида ҳужум изларини идентификациялаш асосида олдини олиш моделини қўриш // “Муҳаммад ал-Хоразмий авлодлари” илмий-амалий ва ахборот-таҳлилий журнали. Тошкент 2021. №2(16). -Б. 42-45. (05.00.00; №10).

4. B.B. Muminov, O.N. Bekmirzaev Method of Detection and Elimination of Tracks of Attacks in the Information System // International Conference on «Information Science and Communications Technologies (ICISCT)». – Tashkent, 2021. – 2p. (ОАК раёсатининг қарори 30.10.2021, №69/8).

5. О.Н. Бекмирзаев Ахборот тизимида ҳужум изини қидириш моделини қуриш ва параметрларини созлаш алгоритми // “Муҳаммад ал-Хоразмий авлодлари” илмий-амалий ва ахборот-таҳлилий журнали. Тошкент 2022. №3(21). –Б. 249-253. (05.00.00; №10).

II бўлим (II часть; II part)

6. B.B. Muminov, O.N. Bekmirzaev Classification and analysis of network attacks in the category of “denial of service” information system // Central asian journal of education and computer sciences (CAJECS). Toshkent –2022. –№. 1. –P. 7-15.

7. Б.Б. Мўминов, О.Н. Бекмирзаев Компьютер жиноятларининг криминалистик характеристикаси ва хужумларни аниклаш воситалари // “Иқтисодиётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация тех-нологияларининг аҳамияти” Республика илмий-техник анжуманининг маърузалар тўплами. Тошкент-2020. -Б. 404-407.

8. B.B. Mo‘minov, O.N. Bekmirzayev Axborot tizimlarida hujum izlarini aniqlash usullari tahlili // “Янгиланаётган Ўзбекистон ёшлари ва инновацион фаолият” мавзусидаги иккинчи республика тармоқли илмий масофавий онлайн конференцияси материаллари. III-қисм. Тошкент-2020. –B. 543-545.

9. B.B. Mo‘minov, O.N. Bekmirzayev Axborot tizimiga qaratilgan hujumlarni oldini olish texnologiyalar // “Иқтисодиёт тармоқларининг инновацион ривожланишида ахборот-коммуникация технологияларининг

аҳамияти” Республика илмий-техник анжуманининг. Маърузалар тўплами. 2-қисм. Тошкент-2021. –B. 362-364.

10. О.Н. Бекмирзаев Ахборот хавфсизлигида компьютер жиноятчилиги ва ҳуқуқий меъёрлари таҳлили // «Ахборот коммуникация технологиялари ва дастурий таъминот яратишда инновацион ғоялар» Республика илмий-техник конференцияси МАЪРУЗАЛАР ТЎПЛАМИ. Самарқанд-2021 –Б. 391-394.

11. Б.Б. Мўминов, О.Н. Бекмирзаев Зараркунанда дастурий таъминотни самарали таҳлил қилиш ва аниқлаш // “Кибермаконда содир этилаётган жиноятларга қарши кураш: муаммолар ва ечимлар” мавзусидаги Республика илмий-амалий конференция материаллари тўплами. 24-февраль Тошкент-2022. -Б. 273-278.

12. Б.Б. Мўминов, О.Н. Бекмирзаев Тизимларни қуриш моделлари ва усуллари // “Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati” Respublika ilmiy-texnik anjumani maruzalar to‘plami. 1-qism. Toshkent-2022. –B. 402-405.

13. Б.Б. Мўминов, О.Н. Бекмирзаев Ахборот хавфсизлигига таҳдид моделлари ва ахборот тизимларига ҳужумлар таҳлили // “Zamonoviy axborot, kommunikatsiya texnologiyalari va AT-ta’lim tatbiqi muammolari” mavzusidagi Respublika ilmiy-amaliy anjumani MA’RUZALAR TO‘PLAMI I-TOM. Samarqand-2022. –B. 318-320.

14. B.B. Mo‘minov, O.N. Bekmirzayev Axborot tizimlarida raqamli kriminalistikani o‘rni va ahamiyati // “Axborot texnologiyalari, tarmoqlar va telekommunikatsiyalar” xalqaro ilmiy-amaliy anjumani, maqolalar to‘plami. Urganch-2022. -B. 495-497.

15. B.B. Muminov, O.N. Bekmirzayev Structure and algorithms of online discussion information system // Scientific Collection Interconf. № 114. Proceedings of the 10th International Scientific and Practical Conference INTERNATIONAL FORUM: PROBLEMS AND SCIENTIFIC COLUTIONS. Melbourne, Australia 2022. -P. 373-384.

16. Б.Б. Мўминов, О.Н. Бекмирзаев Построение узлов о событиях под влиянием атаки в информа-ционной системе // Scientific Collection Interconf. № 114. Proceedings of the 10th International Scientific and Practical Conference INTERNATIONAL FORUM: PROBLEMS AND SCIENTIFIC COLUTIONS. Melbourne, Australia 2022. -P. 388-396.

17. B.B. Mo‘minov, O.N. Bekmirzayev, N.X.Begmatova Real vaqtda xavfsiz ovoz berish dasturi // O‘zbekiston Respublikasi Adliya vazirligi huzuridagi Intellektual mulk agentligining EHM uchun yaratilgan dasturning rasmiy ro’yxatdan o’rkazilganligi to’g’risidagi guvohnomasi. № DGU 09729. Toshkent, 21.12.2020.

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

Босмахона лицензияси:

9338

Бичими: 84x60 $^{1}/_{16}$. «Times New Roman» гарнитураси.
Рақамли босма усулда босилди.
Шартли босма табоғи: 2,75. Адади 100 дона. Буюртма № 68/22.

Гувоҳнома № 851684.
«Tipograff» МЧЖ босмахонасида чоп этилган.
Босмахона манзили: 100011, Тошкент ш., Беруний кўчаси, 83-уй.