ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.27.06.2017.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

НАСРУЛЛАЕВ НУРБЕК БАХТИЁРОВИЧ

АХБОРОТ ХАВФСИЗЛИГИ МОНИТОРИНГИ ТИЗИМИ ИШЛАШИНИНГ САМАРАДОРЛИГИНИ ОШИРИШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2019

УДК: 004.056.5(07)

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.27.06.2017.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

НАСРУЛЛАЕВ НУРБЕК БАХТИЁРОВИЧ

АХБОРОТ ХАВФСИЗЛИГИ МОНИТОРИНГИ ТИЗИМИ ИШЛАШИНИНГ САМАРАДОРЛИГИНИ ОШИРИШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2019

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2019.1.PhD/T974 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:	**Ганиев Салим Каримович** техника фанлари доктори, профессор
Расмий оппонентлар:	**Бекмуратов Тўлқин Файзиевич** техника фанлари доктори, профессор, академик
	Туйчиев Ғулом Нумонович физика-математика фанлари доктори
Етакчи ташкилот:	**«UNICON.UZ» – фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.27.06.2017.T.07.01 Илмий кенгашнинг 2019 йил «___» _____ соат __ 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 (_____ рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-ўй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2019 йил «___» _____ да тарқатилди.
(2019 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

Р.Ж. Алоев
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, ф-м.ф.д., профессор

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда ахборот-коммуникация тизимлари ривожининг ҳозирги замон босқичида ахборот хавфсизлиги ҳолатини баҳолашнинг асосий механизмларидан бири ҳисобланган ахборот хавфсизлиги мониторинги тизимларини ишлаб чиқишга ва уларни такомиллаштиришга алоҳида эътибор қаратилмоқда. «Касперский лабораторияси маълумотига асосан 2018 йилнинг иккинчи чорагида жаҳоннинг 187 давлатларида жойлашган Интернет ресурслари орқали 962,947,023 та ҳужум амалга оширилган»[1]. Бу йўналишда ривожланган мамлакатларда, жумладан, АҚШ, Германия, Буюк Британия, Франция, Жанубий Корея, Россия Федерацияси ва бошқа давлатларда ахборот коммуникация тизимларининг ҳимояланганлигини баҳоловчи ахборот хавфсизлиги мониторинги воситаларини ишлаб чиқиш муҳим аҳамият касб этмоқда.

Жаҳонда ахборот хавфсизлиги ҳолатини тезкор ва самарали баҳолаш имкониятини берувчи ахборот хавфсизлиги мониторинги усуллари ва воситаларини яратишга йўналтирилган илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, жумладан ахборот-коммуникация тизимларини ҳимояланганлик ҳолатини реал баҳолаш, ахборотни ҳимоялаш воситаларида содир бўладиган кўп сонли ҳодисаларни нормаллаштириш, корреляцилаш ва агрегатлаш орқали ахборот хавфсизлиги инцидентларини аниқлаш, ахборотни ҳимоялаш воситаларининг ишидаги хатоликларни тезкор аниқлаш ва бартараф этиш усулларини ишлаб чиқиш муҳим аҳамият касб этади. Шу билан бирга ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш имконини берувчи жараёнларни такомиллаштиришни илмий асослаш зарур бўлмоқда.

Республикамизда давлат ва хўжалик бошқарув органларида электрон ҳукумат тизимини шакллантиришда ва электрон ҳужжат алмашинув тизимларини татбиқ этишда маълумотлар хавфсизлигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан « ... иқтисодиёт, ижтимоий соҳа, бошқарув тизимига ахборот-коммуникация технологияларини жорий этиш, ... 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 ахборотнинг дастурий-аппарат ҳимоя воситалари, хусусан тизимнинг ҳимояланганлигини реал баҳоловчи ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш усуллари ва алгоритмларини ишлаб чиқиш муҳим вазифалардан бири

[1] https://securelist.ru/it-threat-evolution-q2-2018-statistics/90919/

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

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, 2018 йил 14 мартдаги ПФ-5379-сон «Ўзбекистон Республикасининг давлат хавфсизлиги тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари ва 2018 йил 21 ноябрдаги ПҚ-4024-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти 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 коммуникация тизимларида ахборот хавфсизлиги ҳолатини мониторинглаш усуллари ва воситаларини, ҳодисаларни таҳлиллашнинг назарий-амалий концепциясини ва ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш моделлари, усуллари ва алгоритмларини ишлаб чиқиш буйича Ch.Fry, M.Nystrom, J.Smith, Ch.Sanders, I.Glover, C.Dukes, И.А.Шелудько, Т.А.Биячуев, И.В.Котенко, И.Б.Паращук, А.В.Федорченко, Д.С.Левшун, А.А.Чечулин ва бошқа чет эллик олимлар томонидан инженерлик-тадқиқот ишлари олиб борилмоқда.

Ўзбекистонда С.К.Ганиев, М.М.Каримов, Р.Н.Усмонов, А.А.Ганиев ва бошқалар томонидан ахборотнинг дастурий-аппарат ҳимоялаш усуллари хусусан, ахборот коммуникация тизимларида тармоқлараро экран ва мониторинглашнинг комплекс усул ва воситаларини ишлаб чиқиш, инцидентларга ва киберхужумларга қарши харакатларни бошқариш, ахборот хавфсизлиги мезонлари ва кўрсаткичларини шакллантириш усуллари тадқиқ қилинган.

Шунинг билан бирга ахборот хавфсизлиги мониторинги тизимини қуриш, унинг ишга лаёқатлигини таъминлаш, ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш ва уларнинг ишончлилик кўрсаткичларини баҳолаш усуллари етарли даражада ўрганилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг илмий-тадқиқот ишлари режасининг №Ф4-020 «Инфокоммуникацион

тармоқлар хавфсизлик мониторинги тизимининг ишлаши ва яратилиши муаммоларини тадқиқ этиш» (2012-2016) ва №А5-063 «Ахборот коммуникация тизимларида тармоқлараро экранлаш ва мониторинглашнинг комплекс усулини ишлаб чиқиш» (2015-2017) мавзусидаги лойиҳалар доирасида бажарилган.

Тадқиқотнинг мақсади ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш имкониятини берувчи, ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлашга асосланган усул ва алгоритмларни ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш схемасини яратиш;

маълумотларни ишлаш схемаси асосида ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал моделини ишлаб чиқиш;

«анализ орқали синтез» ёндашуви асосида ахборот хавфсизлиги мониторинги тизимини қуриш усулини ишлаб чиқиш;

дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлашнинг модификацияланган усулини ишлаб чиқиш;

ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини таъминлаш қисм-тизими структурасида уларнинг ишлаш ҳолатлари эҳтимолликларини аниқлаш алгоритмини ишлаб чиқиш.

Тадқиқотнинг объекти сифатида ахборот коммуникация тизимларида қўлланиладиган ҳимоялаш воситаларининг ишлаши жараёнлари олинган.

Тадқиқотнинг предмети сифатида ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш усуллари ва алгоритмлари олинган.

Тадқиқотнинг усуллари. Тадқиқот жараёнида ахборотни ҳимоялаш усуллари, эҳтимоллик назарияси, қиёсий таҳлиллаш усуллари, моделлаш ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

содир бўлиши мумкин бўлган инцидентлар хусусидаги маълумотларни йиғиш ва таҳлиллаш асосида ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш схемаси яратилган;

маълумотларни ишлаш схемаси асосида ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели ишлаб чиқилган;

«анализ орқали синтез» ёндашуви ёрдамида ахборот хавфсизлиги мониторинги тизимини қуриш усули ишлаб чиқилган;

ахборотни ҳимоялаш воситаларини хилларга ажратиб, уларга тегишли ҳолатларни танлаш орқали уларнинг эҳтимолликларини аниқлашнинг модификацияланган усуллари ишлаб чиқилган;

модификацияланган усуллар асосида яратилган ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини таъминлаш қисм-тизими структурасида, уларнинг ишлаш ҳолатлари эҳтимолликларини аниқлаш алгоритми ишлаб

чиқилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситалари ишлаши ҳолатлари эҳтимолликларини аниқлаш усуллари ва алгоритмлари асосида кичик ва катта кўламли тармоқлар учун ахборот хавфсизлиги мониторинги тизими дастурий воситасининг архитектураси қурилган;

ҳодисалар хусусидаги ёзувларни йиғишга асосланган ахборотни ҳимоялаш воситалари компонентларининг ишончлик кўрсаткичларини аниқлаш имконини берувчи дастурий восита ишлаб чиқилган;

дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг ишлаши ҳолати эҳтимолликларини аниқлаш усуллари ва алгоритмлари асосида ISMS дастурий воситаси ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш мақсадида ишлаб чиқилган дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш усуллари ва алгоритмларидан олинган маълумотлар ва тажрибавий-ҳисоблаш натижалари билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти яратилган ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш усуллари ва алгоритмларининг мониторинг жараёнида ҳисоблашларни соддалаштириши билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти ишлаб чиқилган усуллар ва дастурнинг ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини тиклаш вақтини қисқартириш ва нисбатан кўп инцидентларни аниқлаш ҳамда хавфсизлик маъмури йўқ ташкилотларда ҳам фойдаланиш имконияти билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш усуллари ва алгоритмлари бўйича олинган илмий натижалар асосида:

модификацияланган усуллар асосида яратилган ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини таъминлаш қисмтизими структурасида уларнинг ишлаши ҳолатлари эҳтимолликларини аниқлаш алгоритми Ўзбекистон Республикаси давлат геология ва минерал ресурслар қўмитаси тасарруфидаги «Давлат геология ахборот маркази» Давлат корхонасининг амалий фаолиятида жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 11 январдаги 33-8/161-сон маълумотномаси). Илмий тадқиқот натижасида Kaspersky антивирус дастурий таъминотининг ишга лаёқатлигини тиклаш вақтини 1,75 мартага қисқартириш ва 355 та кўп инцидентни аниқлаш имконини берган;

содир бўлиши мумкин бўлган инцидентлар хусусидаги маълумотларни йиғиш ва таҳлиллашга асосланган ахборот хавфсизлиги мониторинги

тизимларида маълумотларни ишлаш схемаси «UNICON.UZ» ДУК – Фан-техника ва маркетинг тадқиқотлари марказининг фаолиятига жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 11 январдаги 33-8/161-сон маълумотномаси). Илмий тадқиқот натижасида синовдан ўтиш жараёнида антивирус дастурий таъминотининг ишга лаёқатлигини тиклаш вақтини қисқартириш ва нисбатан кўп инцидентларни аниқлаш имконини берган;

дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситалари ишлаш ҳолати эҳтимолликларини аниқлаш усуллари ва алгоритмлари «STAND KOMPUTERS» МЧЖнинг фаолиятига жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2019 йил 11 январдаги 33-8/161-сон маълумотномаси). Илмий тадқиқот натижасида ахборот хавфсизлиги мониторинги тизимининг ишга лаёқатлигини таъминловчи қисм-тизим структурасидаги ахборотни ҳимоялаш воситалари ишончлигини таъминлаш модули ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини тиклаш вақтини 1,12 марта қисқартириш ва 40 тадан кўп инцидентни аниқлаш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 8 та халқаро ва 11 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертациянинг мавзуси бўйича жами 30 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 7 та мақола, 3 таси хорижий ва 4 таси республика журналларида нашр этилган ҳамда 3 та ЭҲМ учун яратилган дастурий воситаларни қайд қилиш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 111 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 «**Ахборот-коммуникация тизимларида ахборот хавфсизлиги мониторингининг ўзига хос хусусиятлари»** деб номланган биринчи боби ахборот-коммуникация тизимларида ахборот хавфсизлиги мониторинги муаммолари, ахборот хавфсизлиги мониторинги тизимининг

архитектураси ва унда маълумотларни ишлаш жараёнининг тадқиқига бағишланган.

Мунтазам мониторинг ўтказиш ахборотни ҳимоя қилишнинг зарур даражасини сақлаб туришнинг кафолати ҳисобланади, мониторинг тизими фаолияти доирасидаги натижалар эса ахборот хавфсизлигини таъминлаш тизимини такомиллаштиришга асос ҳисобланади. 1-жадвалда мониторинг дастурий воситаларининг, уларнинг функцияларини ўрганиб чиқиш натижасидаги, қиёсий таҳлили келтирилган.

1-жадвал

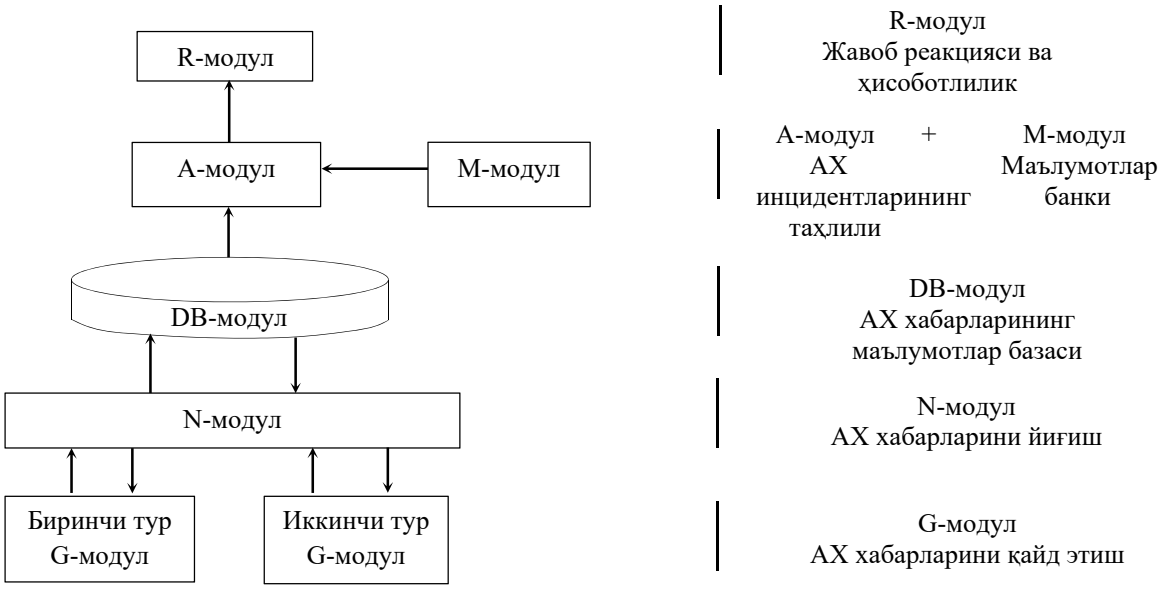
Ахборот хавфсизлиги мониторинги дастурий воситаларининг қиёсий таҳлили

Мезонлар / Ахборот хавфсизлиги мониторинги дастурий воситалари	Таҳдидларни аниқлаш	Ресурс талаби	Унумдорлик	Фойдаланувчанлик	Жорий қилиниши	Бошқарилиши	Мададланиши	Масштабланиши	Воситалар ишлаши ҳолатлари эҳтимолликларининг аниқланиши	Σ
InTrust	3	3	3	3	2	3	3	3	1	24
EventTracker	4	3	4	3	3	3	4	4	2	30
Sentinel Log Manager	4	3	4	4	3	4	4	4	2	32
NXLog	3	4	3	3	3	4	3	3	1	27
LOGStorm	3	3	3	3	3	3	4	3	1	26

Жадвалда келтирилган ахборот хавфсизлиги мониторинги дастурий воситаларининг қиёсий таҳлили воситалар ишлаши ҳолатлари эҳтимолликларининг аниқланиши мезони бўйича 40% қониқарли ва 60% қониқарсиз натижаларни қайд этган. Демак, ҳозирги кунда ташкилотларда фойдаланилаётган ахборот хавфсизлиги мониторинги дастурий воситалари ёрдамида ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш кутилган натижаларни бермайди.

Ахборот хавфсизлиги мониторинги тизимини таҳлиллаш учун унинг беш сатҳли архитектураси ва ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш жараёни энг муҳим ҳисобланади. Ахборот хавфсизлиги мониторинги тизими архитектураси доирасида амалларнинг ҳар бирининг бажарилиши учун алоҳида модуллар жавоб беради (1-расм).

Ахборот хавфсизлиги мониторинги тизими архитектураси асосида таклиф этилган ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш схемаси махсус модуллар ёрдамида ахборотни ҳимоялаш воситаларида генерацияланадиган ахборот хавфсизлиги хабарларини йиғиш, нормаллаштириш, маълумотлар базасида сақлаш, таҳлиллаш ва инцидентларга нисбатан жавоб реакциясини ишлаб чиқиш имконини беради.



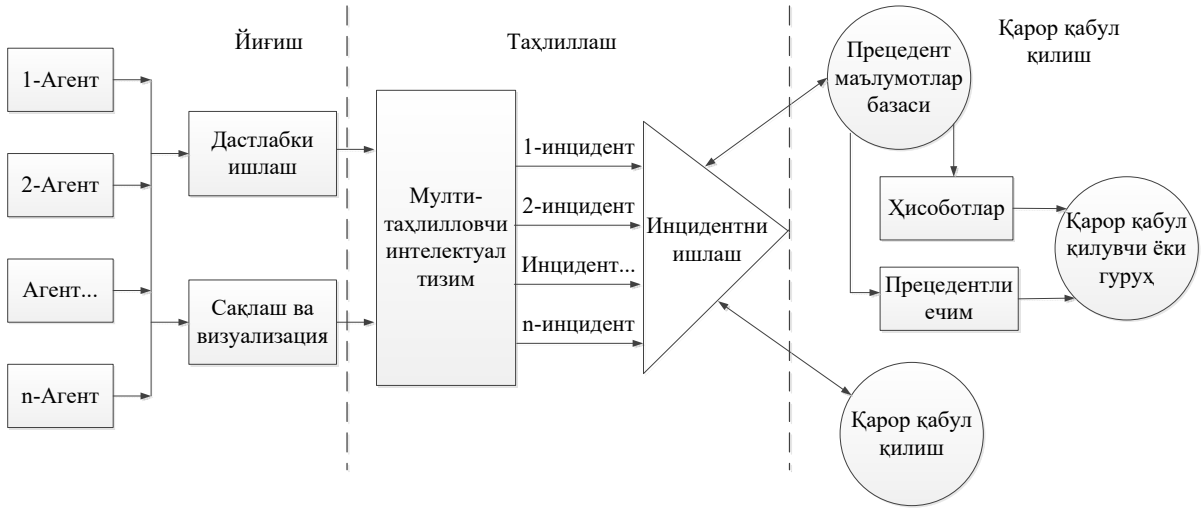
1-расм. Ахборот хавфсизлиги мониторинги тизими архитектураси

Диссертациянинг **«Ахборот хавфсизлиги мониторинги тизимининг модели ва структураси»** деб номланган иккинчи бобида ахборот хавфсизлиги мониторинги натижаларини қулай ва аниқ ифодалаш имконини берувчи ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели ишлаб чиқилган. Ахборотни ҳимоялаш воситаларини эҳтимолий ишчи ҳолатларини аниқлаш имконини берувчи ахборот хавфсизлиги мониторинги тизимини қўллаш структураси таклиф этилган. Лойиҳалаш босқичида дастлабки ва ишчи ечимларни шакллантириш инструменти сифатида ишлатилиши мумкин бўлган ахборот хавфсизлиги мониторинги тизимини қуриш усули таклиф этилган.

Ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели вазифалар, функциялар, жараёнлар ва агентлардан ташкил топган. 2-расмда кўрсатилганидек, архитектура одатда йиғиш, таҳлиллаш ва қарор қабул қилиш модулларини ўз ичига олади. Ҳар бир модул маълум функцияларни бажарадиган қисмлардан иборат.

Ишлаб чиқилган ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели ҳимояланаётган тизим ва ахборотни ҳимоялаш воситаларидаги ахборот хавфсизлигининг аномал ҳодисаларини аниқлашга ва бу ҳодисалар ҳақида ахборот хавфсизлиги маъмурига ўз вақтида, зарур қарорларни қабул қилиш учун, керакли маълумотлар билан таъминлаш имконини беради.

Қатор омилларнинг мукаммал формаллаштириш мумкин эмаслиги натижасида, муайян вазиятга мўлжалланмаган ечимни қабул қилиш хавфи сабабли, аниқ математик усуллар ёрдамида ахборот хавфсизлиги мониторинги тизимини қуриш масаласини ечиш етарлича мураккаб ҳисобланади.



2-расм. Ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели

Бундай вазиятда «итератив синтез» ёки «анализ орқали синтез» деб аталувчи ёндашишдан фойдаланиш мақсадга мувофиқ ҳисобланади. Синтез масалаларини анализ орқали анъанавий ечиш усули итератив жараённи қуришни кўзда тутади. Мезон катталигини ҳисоблашнинг ҳар бир итерациясида тизимни қуришнинг навбатдаги варианти модификацияланади, сўнгра вариант баҳоланади. 3-расмда мониторинг тизимини қуриш усулининг блок схемаси келтирилган.

3-расм. Мониторинг тизимини қуриш усулининг блок схемаси

Диссертация ишининг «**Ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш усуллари**» номли учинчи бобида дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг иш графиги даврида рўй берадиган бузилишлар, содир бўлувчи хатоликлар ва ҳолатларининг ўзгаришини аниқлаш имконини

берувчи модификацияланган усуллар ва алгоритмлар ишлаб чиқилган. Ишлаб чиқилган алгоритм асосидаги мутлақо янги ахборотни ҳимоялаш воситаларининг ишончлилигини баҳолаш модули ишлаб чиқилган.

Ахборотни ҳимоялашнинг турли воситаларининг ишлаши ҳолати эҳтимолликларини аниқлаш учун математик усулларни танлаш биринчи навбатда уларнинг тоифасига, яъни унинг ишлаш вақтининг дискретлигига ёки узлуксизлигига боғлиқ.

Дискрет иш вақтли ахборотни ҳимоялаш воситалари компонентлари ишининг бузилиши ёки уларнинг ишга лаёқатлигининг тикланиши сабабли бўлиши мумкин бўлган ҳолатлар тўплами қуйидаги кўринишга эга:

$$H_{DT} = \left\{ \begin{array}{c} h_0^{DT}, h_1^{DT}, h_2^{DT}, h_3^{DT}, h_4^{DT}, h_5^{DT}, h_6^{DT}, h_7^{DT}, h_8^{DT}, h_{21}^{DT}, h_{24}^{DT}, h_{25}^{DT}, h_{26}^{DT}, h_{27}^{DT}, \\ h_{28}^{DT}, h_{31}^{DT}, h_{35}^{DT}, h_{36}^{DT}, h_{37}^{DT}, h_{38}^{DT}, h_{47}^{DT}, h_{48}^{DT}, h_{51}^{DT}, h_{53}^{DT}, h_{54}^{DT}, h_{56}^{DT}, h_{57}^{DT}, \\ h_{58}^{DT}, h_{63}^{DT}, h_{64}^{DT}, h_{65}^{DT}, h_{67}^{DT}, h_{68}^{DT}, h_{71}^{DT}, h_{75}^{DT}, h_{76}^{DT}, h_{85}^{DT}, h_{86}^{DT} \end{array} \right\}$$

H_{DT} тўпламидан фойдаланиб дискрет иш вақтли ахборотни ҳимоялаш воситалари ҳаракатини, дискрет вақтда ишловчи объект сифатида, йўналтирилган граф кўринишида тасвирлаш мумкин. Дискрет иш вақтли ахборотни ҳимоялаш воситаларига заифликларни аниқлаш тизимининг ва контент фильтрлаш тизимининг тааллуқлиги ҳисобга олинса, қуйидаги белгилашни қабул қилиш мумкин:

$$H_i^{DT_k},$$

бу ерда i – (i=0,…8) дискрет иш вақтли ахборотни ҳимоялаш воситаларининг ҳолатлари индекси;

k – дискрет иш вақтли ахборотни ҳимоялаш воситаларининг хили.

Демак қуйидагиларни келтириш мумкин:

$k = 1$ – заифликларни аниқлаш ва $k = 2$ – контент фильтрлаш тизими.

Заифликларни аниқлаш тизими ҳолатлари:

$$H^{DT_1} = \left\{h_0^{DT_1}, h_1^{DT_1}, h_2^{DT_1}, h_3^{DT_1}, h_4^{DT_1}\right\}$$

Контент фильтрлаш тизими ҳолатлари:

$$H^{DT_2} = h_0^{DT_2}, h_5^{DT_2}, h_6^{DT_2}, h_7^{DT_2}, h_8^{DT_2}$$

4-расмда келтирилган граф учлари заифликларни аниқлаш тизимининг бўлиши мумкин бўлган ҳолатлари $P_{\mathrm{q,q}}$ни характерласа, граф ёйлари орқали тизим ишлашининг дискретлигини белгиловчи қандайдир Δt вақт оралиғидаги унинг бир ҳолатдан иккинчи ҳолатга ўтишлари эҳтимолликлари $P_{\mathrm{q,r}}$ ($\mathrm{q} \neq \mathrm{r}$)ни характерлайди.

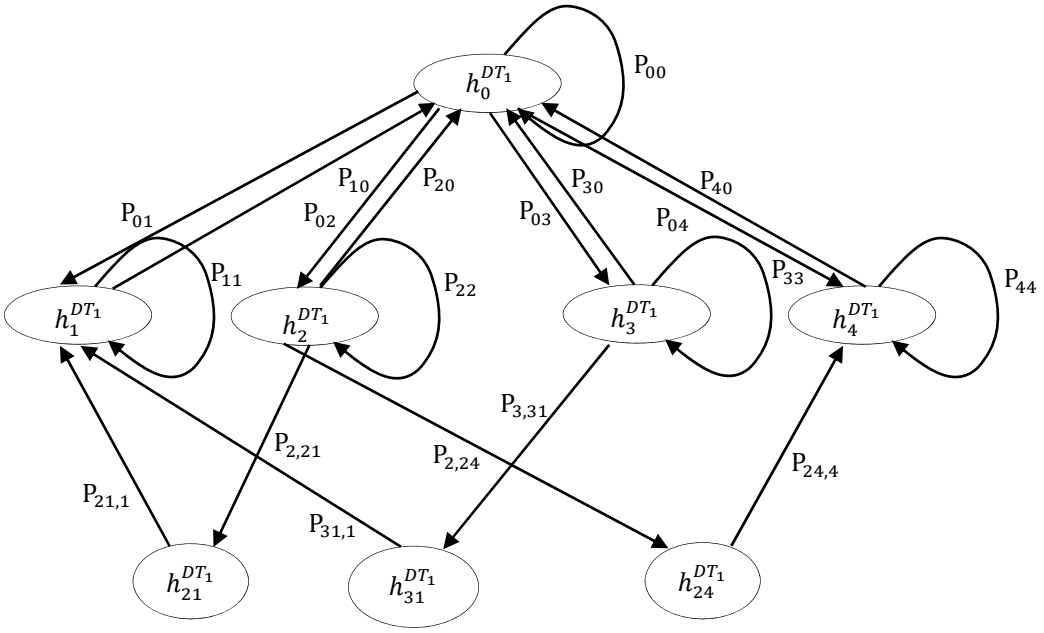
Демак, заифликларни аниқлаш тизими ишлашининг ҳолатларига ўтиш эҳтимолликларини қуйидаги тенгламалар системасини кўринишида ифодалаш мумкин:

$$\begin{cases} \overline{p}_0 = P_{00}\overline{p}_0 + P_{10}\overline{p}_1 + P_{20}\overline{p}_2 + P_{30}\overline{p}_3 + P_{40}\overline{p}_4, \\ \overline{p}_1 = P_{01}\overline{p}_0 + P_{11}\overline{p}_1, \\ \overline{p}_2 = P_{02}\overline{p}_0 + P_{2,21}\overline{p}_{21} + P_{22}\overline{p}_2 + P_{2,24}\overline{p}_{24}, \\ \overline{p}_3 = P_{03}\overline{p}_0 + P_{3,31}\overline{p}_{31} + P_{33}\overline{p}_3, \\ \overline{p}_4 = P_{04}\overline{p}_0 + P_{44}\overline{p}_4. \end{cases}$$

Бунда

$$\overline{p}_0 + \overline{p}_1 + \overline{p}_2 + \overline{p}_3 + \overline{p}_4 = 1,$$

бу ерда $\overline{p}_q,\ q = 0,1,2,3,4$- қидирилаётган чегаравий эҳтимолликлар.



4-расм. Заифликларни аниқлаш тизими ишлаш ҳолатларига ўтиш эҳтимолликлари графи

Ишлаб чиқилган усул ўлчами катта бўлмаган ҳолатлар тўпламидан фойдаланиб, ўтишлар граф-схемасини тавсифлашга, кичик разрядли квадрат матрицани тузишга ва улар асосида дискрет иш вақтли ҳимоялаш тизимлари хилига кирувчи контент фильтрлаш тизими учун ҳам тенгламалар системасини осон тавсифлашга имкон беради.

Узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг бўлиши мумкин бўлган ҳолатлари тўплами қуйидаги кўринишга эга:

$$H_{UT} = \begin{Bmatrix} h_0^{UT}, h_1^{UT}, h_2^{UT}, h_3^{UT}, h_4^{UT}, h_5^{UT}, h_6^{UT}, h_7^{UT}, h_8^{UT}, h_{13}^{UT}, h_{15}^{UT}, h_{18}^{UT}, h_{21}^{UT}, \\ h_{23}^{UT}, h_{24}^{UT}, h_{25}^{UT}, h_{26}^{UT}, h_{28}^{UT}, h_{34}^{UT}, h_{35}^{UT}, h_{36}^{UT}, h_{38}^{UT}, h_{41}^{UT}, h_{43}^{UT}, h_{45}^{UT}, h_{46}^{UT}, \\ h_{48}^{UT}, h_{51}^{UT}, h_{52}^{UT}, h_{53}^{UT}, h_{54}^{UT}, h_{56}^{UT}, h_{57}^{UT}, h_{58}^{UT}, h_{61}^{UT}, h_{62}^{UT}, h_{68}^{UT}, h_{71}^{UT}, h_{73}^{UT}, \\ h_{74}^{UT}, h_{76}^{UT}, h_{78}^{UT}, h_{81}^{UT}, h_{82}^{UT}, h_{86}^{UT}, \end{Bmatrix}$$

Узлуксиз иш вақтли ахборотни ҳимоялаш воситалари ишлаши ҳолатларини аниқлаш учун ўзгарувчан интенсивликлар усулидан фойдаланилди. Қуйида антивирус дастурий таъминоти ишлаши ҳолатларини аниқлашнинг модификацияланган усули таклиф этилди. Унга кўра қуйидаги

қиймат киритилди:

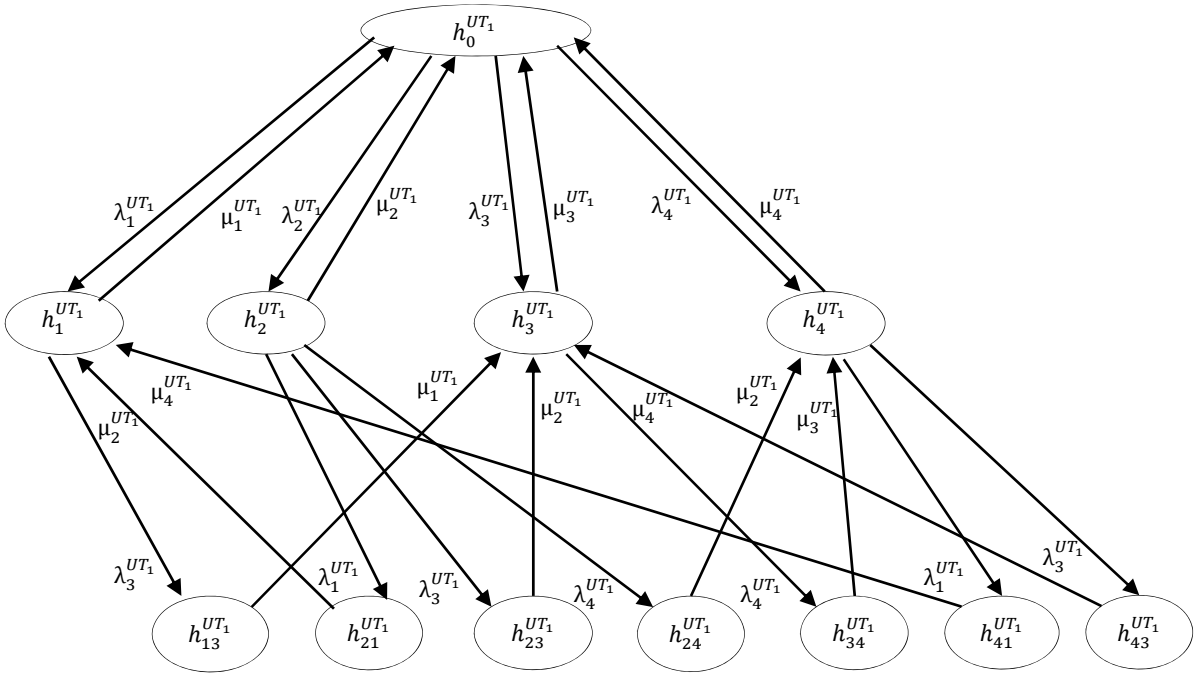
$$H_i^{UT_k},$$

бу ерда: i – узлуксиз иш вақтли ахборотни ҳимоялаш воситалари ишлаши ҳолатларининг индекси, k =1,2,3,4 узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг хиллари.

Ахборот хавфсизлиги мониторинги тизими антивирус дастурий таъминотини таҳлиллаганида ҳолатлар қуйидагича ифодаланади:

$$H_{UT_1} = \{h_0^{UT_1}, h_1^{UT_1}, h_2^{UT_1}, h_3^{UT_1}, h_4^{UT_1}, h_{13}^{UT_1}, h_{21}^{UT_1}, h_{23}^{UT_1}, h_{24}^{UT_1}, h_{34}^{UT_1}, h_{41}^{UT_1}, h_{43}^{UT_1}\}$$

Ушбу тўпламдан фойдаланиб антивирус дастурий таъминоти ишлаши ҳолатлари орасидаги ўтишларни йўналтирилган граф кўринишида тасвирлаш мумкин (5-расм).



5-расм. Антивирус дастурий таъминоти ишлаши ҳолатларини аниқлаш графи

Турли ёйлар кириши ва чиқиши мумкин бўлган мос учлар (кейинчалик тенгламада q- каби белгиланган) билан тасвирланувчи антивирус дастурий таъминоти h_q ҳолатини аниқлашнинг p_q эҳтимоллигининг ўзгариши $\frac{dp_q(t)}{dt}$ антивирус дастурий таъминотининг бу ҳолатга ўтиш ва ундан чиқиш интенсивлиги билан аниқланади:

$$\frac{dp_q(t)}{dt} = \sum_{k=1}^{K} p_k(t)\Lambda_{k,q} - p_q(t)\sum_{l=1}^{L}\Lambda_{q,l}$$

$$q = 0,1,2,3,4,13,21,23,24,34,41,43.$$

Бу ерда:

$p_k(t)$ - $\Lambda_{k,q}$ интенсивлик билан h_q ҳолатга (q-уч) ўтувчи h_k (k-уч) ҳолатдаги антивирус дастурий таъминотининг топиш эҳтимоллиги;

$\Lambda_{q,l}$ - h_q ҳолатдан h_l ҳолатга (l-уч) ўтиш интенсивлиги;

К - h_q учи билан боғлиқ кирувчи ёйларнинг учлари сони;

$L - h_q$ учи билан боғлиқ чиқувчи ёйларнинг учлари сони.

Ишлаб чиқилган узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг ишлаши ҳолатларини аниқлашнинг модификацияланган усули антивирус дастурий таъминоти учун граф схемадаги ўтишлар сонини ва, демак ишлаш ҳолатларини аниқлаш вақтини 4 марта қисқартиришга имкон беради.

Таклиф этилган ахборот хавфсизлиги мониторинги тизимининг ишга лаёқатлигини таъминловчи қисм-тизим структураси таркибида ахборотни ҳимоялаш воситалари ишончлигини баҳолаш модули тамомила янги ҳисобланади (6-расм).

6-расм. Ахборотни ҳимоялаш воситалари ишончлигини баҳолаш модулининг структура схемаси

Ушбу модул ёрдамида олдин содир бўлган бузилишлар хусусидаги мунтазам янгиланувчи (жорий эксплуатация маълумотлари бўйича) ахборотдан фойдаланиб ахборотни ҳимоялаш воситаларининг ишлаш холатлари эҳтимолликлари ҳисобланди. Модулда ахборотни ҳимоялаш воситалари ишлаши ҳолатлари эҳтимолликларини аниқловчи алгоритм асосий ҳисобланади.

Диссертациянинг «**Ахборот хавфсизлиги мониторинги тизимини дастурий воситасининг архитектураси ва тажриба-ҳисоблаш натижалари**» номли тўртинчи бобида ахборот хавфсизлиги мониторинги бўйича тажриба-ҳисоблаш натижалари келтирилган. Антивирус дастурий таъминоти компонентларининг ишончлилик кўрсаткичлари аниқланиб, улар асосида компонентларнинг ишлаши ҳолатлари эҳтимолликлари ҳисобланган ва ахборот хавфсизлиги мониторинги тизимининг самарадорлиги баҳоланган.

2-жадвалда антивирус дастурий таъминотининг ишлаши ҳолатларига

мувофиқ содир бўлиши мумкин бўлган тўрт хил хатоликлар мавжудлигини таҳлиллаш натижасида аниқланган хатоликларнинг характеристикалари келтирилган.

Ушбу характеристикалар бўйича узлуксиз иш вақтли ахборотни ҳимоялаш воситалари ишлаши ҳолатлари эҳтимолликларини аниқлашнинг модификацияланган усули асосида антивирус дастурий таъминоти учун олинган биринчи тартибли дифференциал тенгламалар системасини Mathcad дастурий таъминоти ёрдамида ечими олинган.

2-жадвал

Аниқланган хатоликларнинг характеристикалари

№	Вақтий бўлаклар	Хатолик хусусидаги ёзувлар сони	Олдинги хатолик онидан бошлаб бузилмасдан ишлаш вақти T_i^j, с	Тикланиш вақти ξ_i^j, с
1	07.08.2018 (03:11:01)-07.08.2018(03:28:05)	2	4513,18	0,28
2	11.09.2018 (04:15:08)-13.09.2018(05:16:12)	11	1008,78	48,01
3	09.11.2018 (02:18:15)-10.11.2018(03:24:16)	8	603	25,01

Mathcad дастурий таъминоти орқали олинган тажриба-ҳисоблаш натижалари асосида антивирус дастурий таъминотининг 240 соат ва 3000 соат вақт оралиқларда ишлаш ҳолатлари $p_0, p_1, p_2, p_3, p_4, p_{13}, p_{21}, p_{23}, p_{24}, p_{34}, p_{41}, p_{43}$ эҳтимолликларнинг қийматлари қуйидаги шартни қаноатлантириши исботланди:

$$\sum p_q(t) = 1, \forall t \in [0, \infty), \qquad \text{q} = 0,1,2,3,4,13,21,23,24,34,41,43$$

«Давлат геология ахборот маркази» корхонасида ахборот хавфсизлиги мониторинги тизимига ишга лаёқатликни таъминлаш қисм-тизимини жорий қилинмасдан олдинги ва жорий қилинганидан кейинги самарадорликлари баҳоланган. Самарадорликни баҳолашда 3-жадвалда келтирилган ахборот коммуникация тизимидаги ахборотни ҳимоялаш воситаларининг суткалик иш кўрсаткичларидан фойдаланилган.

Демак, 11 ойда (334 суткада) аниқланган ахборот хавфсилиги инцидентлари сони $N_1 = 334 * 58 = 19372$ тани ташкил этди. Иш журналларида қайдланган тўрт хил хатоликлар пайдо бўлганидан сўнг антивирус дастурий таъминотининг ишга лаёқатлигини тиклашга сарф қилинган умумий вақт қуйидагига тенг:

$T_{\text{тик}} = (0,78 + 72,1 + 38,18) + (72,78 + 60,55 + 50,3) + 12 + 20 = 326,69$

ёки $326,69/24 = 13,61$ сутка

Шундай қилиб, антивирус дастурий таъминоти 334 суткадан аслида 320,39 суткада ишлаган. Антивирус дастурий таъминоти компонентлари ишида бузилишлар бўлмаганида аниқланган ахборот хавфсизлиги инцидентларининг суткалик сонини 11 ой ичида аниқланган ахборот

хавфсизлиги инцидентларининг умумий сонини ушбу вақтга бўлиш орқали олиш мумкин, яъни:

$$N_{\text{сутка}} = 19372 \text{ инцидент}/320{,}39 \text{ сутка} = 60{,}46 \text{ инцидент}$$

3-жадвал

Ахборотни ҳимоялаш воситаларининг суткалик иш кўрсаткичлари

Ахборотни ҳимоялаш воситалари	Бир кун давомидаги ахборот хавфсизлиги ҳодисалари сони	Бир кун давомидаги ахборот хавфсизлиги инцидентлари сони	Нисбат
Антивирус дастурий таъминоти	58	58	1
Заифликларни аниқлаш тизимлари	70	4	17,5
Тармоқлараро экранлар	90154	832	108,35
Суқилиб киришларни аниқлаш тизимлари	102482	1124	91,1

Демак, агар антивирус дастурий таъминоти хатосиз ишлаганида қуйидаги сонли ахборот хавфсизлиги инциденти аниқланган бўлар эди:

$$N = 334 * 60{,}46 = 20193{,}64 \approx 20194 \text{ инцидент}$$

Ахборот хавфсизлиги мониторинги тизимининг ишга лаёқатлигини таъминловчи қисм-тизимдан фойдаланиш натижасида антивирус дастурий таъминотининг ишга лаёқатлигини тиклашнинг умумий вақти қуйидагига тенг:

$$T_{\text{тик1}} = (0{,}28 + 48{,}01 + 25{,}01) + (46{,}54 + 21{,}43 + 24{,}1) + 9{,}46 + 11 = 185{,}83 \text{ ёки } 7{,}743 \text{ сутка.}$$

Ахборот хавфсизлиги мониторинги тизимининг ишга лаёқатлигини таъминловчи қисм-тизимни жорий этиш натижасида антивирус дастурий таъминотининг ишга лаёқатлигини тиклаш вақти қуйидагича қисқарди:

$$S = T_{\text{тик}}/T_{\text{тик1}} = 13{,}61/7{,}743 = 1{,}75$$

Ушбу вақт мобайнида антивирус дастурий таъминоти ишлашидаги бузилишлар туфайли ўтказиб юборилган ёки айтарли даражада кечикиш билан аниқланган ахборот хавфсизлиги инцидентларининг сони қуйидагига тенг:

$$N' = 7{,}743 * 60{,}46 = 468{,}14 \approx 468 \text{ инцидент}$$

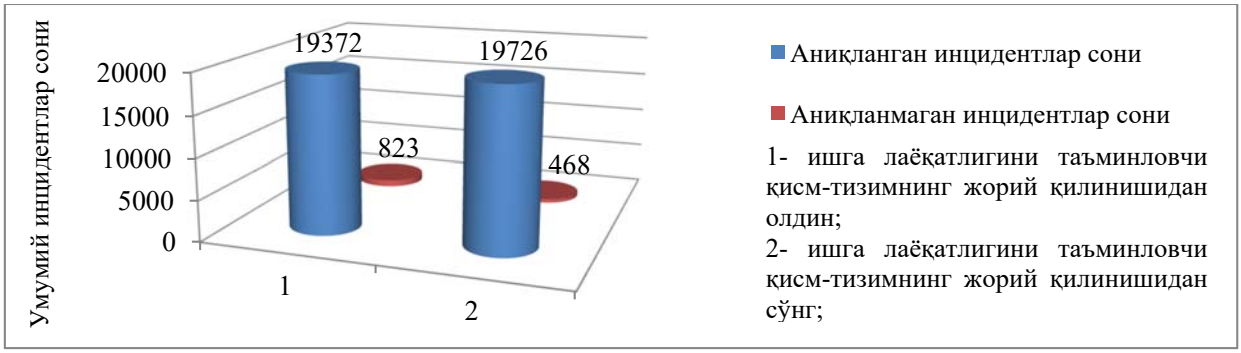
Кузатиш вақти мобайнида ахборот хавфсизлиги мониторинги тизимининг ишга лаёқатлигини таъминловчи қисм-тизимини жорий этиш натижасида аниқланган инцидентлар сони қуйидагига тенг:

$$N_2 = N - N' = 20194 - 468 = 19726 \text{ инцидент}$$

8-расмда ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини таъминловчи қисм-тизимни жорий қилишдан олдин ва сўнг, аниқланган ва аниқланмаган инцидентлар сони диаграмммаси келтирилган.

Демак, ахборот хавфсизлиги мониторинги тизимига ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини таъминловчи қисм-тизимнинг жорий қилиниши 334 суткада 19726 та инцидентни, яъни қисм-тизим жорий қилинмасдан олдинги аниқланган инцидентлар сонидан 355 та (1,82 % га) кўп инцидентни аниқлашга ва антивирус дастурий

таъминотининг ишга лаёқатлигини тиклаш вақтини 1,75 мартага қисқартиришга имкон берди.



8-расм. Ахборотни ҳимоялаш воситаларининг ишга лаёқатлигини таъминловчи қисм-тизимни жорий қилишдан олдин ва сўнг олинган натижалар диаграмммаси

ХУЛОСА

«Ахборот хавфсизлиги мониторинги тизими ишлашининг самарадорлигини ошириш усуллари ва алгоритмлари» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Содир бўлиши мумкин бўлган инцидентлар хусусидаги маълумотларни йиғиш ва таҳлиллаш асосида ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш схемаси яратилди. Ишлаб чиқилган ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш схемаси хабарларни генерациялаш, йиғиш, сақлаш, таҳлиллаш ҳамда ахборотнинг ҳимояланганлик даражасини баҳолаш имконини берди.

2. Маълумотларни ишлаш схемаси асосида ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели ишлаб чиқилди. Ишлаб чиқилган ахборот хавфсизлиги мониторинги тизимининг хусусий концептуал модели ахборотни ҳимоялаш воситаларидаги аномал ҳодисаларни аниқлашга ва бу ҳодисалар хусусида ахборот хавфсизлиги маъмурини ўз вақтида, зарур қарорларни қабул қилиши учун, керакли маълумотлар билан таъминлашга имкон берди.

3. «Анализ орқали синтез» ёндашуви асосида ахборот хавфсизлиги мониторинги тизимини қуриш усули ишлаб чиқилди. Ишлаб чиқилган усул эксплуатация босқичида тизим ишлашидаги заиф жойларни аниқлаш ва уларни бартараф этиш бўйича талабларни ва тавсияларни ишлаб чиқиш имконини берди.

4. Ахборотни ҳимоялаш воситаларини хилларга ажратиб, уларга тегишли ҳолатларни танлаш асосида уларнинг эҳтимолликларини аниқлашнинг модификацияланган усуллари ишлаб чиқилди. Ишлаб чиқилган усуллар узлуксиз иш вақтли ахборотни ҳимоялаш воситасининг (антивирус дастурий таъминоти мисолида) ишлаш ҳолатлари ўрганилганида, улардаги

ўтишлар сони ва шунга мос равишда ҳисоблаш вақтининг 4 мартагача қисқаришига имкон берди.

5. Дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситалари ишлаши ҳолатларининг эҳтимолликларини аниқлаш алгоритми асосида ахборотни ҳимоялаш воситаларининг ишончлигини баҳолаш модули ишлаб чиқилган. Ишлаб чиқилган модул хавфсизлик маъмурига ахборотни ҳимоялаш воситаларининг жорий ишончлиги хусусидаги ахборотни оператив тарзда олиш ва унинг келажагини башоратлаш имконини берди.

6. Дискрет ва узлуксиз иш вақтли ахборотни ҳимоялаш воситаларининг ишлаши ҳолатлари эҳтимолликларини аниқлаш усуллари ва алгоритмлари асосида турли хил ташкилотларнинг ахборот коммуникация тизимларида қўллаш имконини берувчи ISMS дастурий воситаси ишлаб чиқилди. Ишлаб чиқилган дастурий восита «Давлат геология ахборот маркази» давлат корхонаси ахборот коммуникация тизимида шу турдаги мавжуд воситаларга нисбатан 355 та (1,82 % га) кўп инцидентларни аниқлаш ва антивирус дастурий таъминотининг ишга лаёқатлигини тиклаш вақтини 1,75 мартага қисқартириш имконини берди.

**НАУЧНЫЙ СОВЕТ DSc.27.06.2017.T.07.01
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

НАСРУЛЛАЕВ НУРБЕК БАХТИЁРОВИЧ

МЕТОДЫ И АЛГОРИТМЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

05.01.05 – Методы и системы защиты информации. Информационная безопасность

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

Ташкент-2019

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2019.1.PhD/T974.

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:	**Ганиев Салим Каримович** доктор технических наук, профессор
Официальные оппоненты:	**Бекмуратов Тулкин Файзиевич** доктор технических наук, профессор, академик
	Туйчиев Гулом Нумонович доктор физико-математических наук
Ведущая организация:	**«UNICON.UZ» – центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «____» _____2019 года в ____ часов на заседании Научного совета DSc.27.06.2017.T.07.01 при Ташкентский университет 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 №____). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «_____» _____ 2019 года.
(протокол рассылки №_____ от «_____» _____ 2019 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

Р.Ж. Алоев
Председатель научного семинара при научном совете по присуждению ученых степеней, д.ф-м.н. профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В мире на современном этапе развития информационных и коммуникационных систем особое внимание уделяется к разработке и усовершенствованию системы мониторинга информационной безопасности являющихся одним из основных механизмов оценки состояния обеспеченности информационной безопасности. «По данным «Лаборатории Касперского» во втором квартале 2018 года осуществлено 962,947,023 атак через ресурсы Интернет, которые расположены в 187 странах мира.[1]. В развитых странах, таких как США, Германия, Великобритания, Франция, Южная Корея, Российская Федерация и других, важную роль играет разработка средств мониторинга информационной безопасности, позволяющих оценить защищенность информационных и коммуникационных систем.

В настоящее время большое количество научных исследований посвящены разработке методов и средств мониторинга информационной безопасности, позволяющих быстро и эффективно оценивать состояние информационной безопасности. В этом направлении важнейшими задачами являются разработка методов, позволяющих реально оценивать состояние защищенности информационно-коммуникационных систем, обнаруживать инциденты информационной безопасности путем нормализации, корреляции и агрегирования большого числа событий, происходящих в средствах защиты информации. Наряду с этим, остается необходимым научное обоснование усовершенствования процессов, позволяющих повышения эффективности функционирования системы мониторинга информационной безопасности.

В нашей республике предпринимаются масштабные меры по обеспечению безопасности данных при внедрении в органы государственного и экономического управления систем электронного документооборота и формировании системы электронного правительства. В «Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг.» отмечены задачи, в том числе и задача «…внедрение информационно-коммуникационных технологий в экономику, социальную сферу, системы управления, ... совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[2]. Для выполнения поставленных задач одной из наиболее важной проблемой является разработка программно-аппаратных средств защиты информации, в частности методов и алгоритмов повышения эффективности функционирования системы мониторинга информационной безопасности, позволяющих реально оценивать состояние защищенности системы.

Данное диссертационное исследование в определенной степени вносит вклад в выполнение задач, предусмотренных Указами Президента

[1] https://securelist.ru/it-threat-evolution-q2-2018-statistics/90919/

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

Республики Узбекистан № УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», № УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», № УП-5379 от 14 марта 2018 года «О Мерах по совершенствованию системы государственной безопасности Республики Узбекистан», и Постановлением Президента Республики Узбекистан № ПП-4024 от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», а также других нормативно-правовых документов, принятых в данной сфере.

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

Степень изученности проблемы. Разработке моделей, методов и средств мониторинга состояния информационной безопасности, анализа событий в информационно-коммуникационных системах, моделей, методов и алгоритмов обработки данных в системах мониторинга информационной безопасности посвящены инженерно-исследовательские работы Ch.Fry, M.Nystrom, J.Smith, Ch.Sanders, I.Glover, C.Dukes, И.А.Шелудько, Т.А.Биячуева, И.В.Котенко, И.Б.Паращук, А.В.Федорченко, Д.С.Левшуна, А.А.Чечулина и других зарубежных ученых.

В Узбекистане в работах С. К. Ганиева, М. М. Каримова, Р. Н. Усмонова, А. А. Ганиева и других изучены методы программно-аппаратной защиты информации, в частности, методы и средства межсетевого экранирования и мониторинга, управление противодействием инцидентам и кибератакам, методы формирования критериев и показателей информационной безопасности в информационно-коммуникационных системах.

Вместе с тем, недостаточно изучены методы построения системы мониторинга информационной безопасности, методы обеспечения их работоспособности, методы определения вероятности состояния функционирования средств защиты информации, а также методы оценки показателей их надежности.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках научного проекта согласно планам научно-исследовательских работ Ташкентского университета информационных технологий № Ф4-020 «Исследование проблем функционирования и создания системы мониторинга безопасности инфокоммуникационных систем» (2012-2016) и № А5-063 «Разработка комплексных методов межсетевого экранирования и мониторинга в информационно-коммуникационных системах» (2015-2017).

Цель исследования состоит в разработке методов и алгоритмов,

основанных на определении вероятностей состояния функционирования средств защиты информации, позволяющих повысить эффективность функционирования системы мониторинга информационной безопасности.

Задачи исследования:

создать схему обработки данных в системах мониторинга информационной безопасности;

разработать частную концептуальную модель системы мониторинга информационной безопасности на основе схемы обработки данных;

разработать метод построения системы мониторинга информационной безопасности на основе подхода «анализ через синтез»;

разработать модифицированный метод определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы;

разработать алгоритм для определения вероятностей состояния функционирования средств защиты информации в структуре подсистемы обеспечения их работоспособности.

Объектом исследования являются процессы функционирования средств защиты, применяемые в информационно-коммуникационных системах.

Предмет исследования являются методы и алгоритмы определения вероятностей состояний функционирования средств защиты информации.

Методы исследования. В процессе исследования использованы теория систем защиты информации, теория вероятности, методы сопоставительного анализа, методы моделирования и объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

создана схема обработки данных в системе мониторинга информационной безопасности на основе накопления и анализа данных о потенциальных инцидентах;

разработана частная концептуальная модель системы мониторинга информационной безопасности на основе схемы обработки данных;

разработан метод построения системы мониторинга информационной безопасности с помощью подхода «анализ через синтез»;

разработаны модифицированные методы определения вероятности на основе выбора состояний относящийся к средствам защиты информации, выделив их на виды;

на основе модифицированных методов разработан алгоритм определения вероятностей состояния функционирования средств защиты информации в структуре подсистемы обеспечения их работоспособности

Практические результаты исследования заключаются в следующем:

построена архитектура системы мониторинга информационной безопасности для сетей малого и большого размера, основанная на методах и алгоритмах определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы;

разработано программное средство, позволяющее возможность определения показателей надежности компонентов средств защиты информации на основе сбора записей о событиях;

разработано программное средство ISMS, основанное на использовании методов и алгоритмов определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы.

Достоверность результатов исследования. Достоверность результатов исследования подтверждаются данными, полученными на основе разработанных методов и алгоритмов определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы, с целью повышения эффективности функционирования системы мониторинга информационной безопасности, а также результатами экспериментальных вычислений.

Научная и практическая значимость результатов исследования. Научная значимость полученных результатов исследований заключается в том, что разработанные методы и алгоритмы определения вероятностей состояния функционирования средств защиты информации в процессе мониторинга позволяют упростить вычисления.

Практическая значимость полученных результатов исследования заключается в том, что разработанные методы и программное средство позволяют уменьшить время восстановления работоспособности средств защиты информации и обнаружить значительно большее число инцидентов. Разработанное программное средство может быть использовано в организациях, где отсутствует администратор безопасности.

Внедрение результатов исследования. На основе полученных научных результатов по методам и алгоритмам повышения эффективности функционирования системы мониторинга информационной безопасности:

на основе модифицированных методов созданных в структуре подсистемы обеспечения работоспособности средств защиты информации, алгоритм определения вероятностей состояния их функционирования внедрено в практическую деятельность Государственного предприятия «Государственный геологический информационный центр» при Государственном Комитете Республики Узбекистан по геологии и минеральным ресурсам (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 11 января 2019 года №33-8/161). В результате научного исследования стало возможным сократить время восстановления работоспособности антивирусного программного обеспечения Kaspersky в 1,75 раза и обнаружить на 355 инцидентов больше;

схема обработки данных в системе мониторинга информационной безопасности на основе накопления и анализа данных о потенциальных инцидентах, было внедрено практическую деятельность в ГУП «UNICON.UZ» – центре научно-технических и маркетинговых исследований,

с целью обнаружения ошибок, появляющийся в функционировании средств защиты информации (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 11 января 2019 года №33-8/161). В результате научного исследования процесса тестирования получена возможность сокращения времени восстановления работоспособности антивирусного программного обеспечения и обнаружения значительно большего числа инцидентов;

методы и алгоритмы определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы, было внедрено в деятельность ООО «STAND KOMPUTERS» (справка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 11 января 2019 года №33-8/161). В результате научного исследования, посредством модуля обеспечения надежности средств защиты информации в структуре подсистемы обеспечения работоспособности системы мониторинга информационной безопасности, позволило сократить время восстановления средств защиты информации в 1,12 раза и обнаружить больше 40 инцидентов.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 8 международных и 11 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По теме исследования всего опубликовано 30 научных работ, из них 7 статей – в журнальных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 3 – в иностранных, 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 111 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и востребованность темы диссертации, показано соответствие ее с приоритетными направлениями развития науки и технологий Республики Узбекистан, сформулированы цель и задачи, а также объект и предмет исследования, изложены научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта их теоретическая и практическая значимость, приведен перечень внедрений в практику результатов исследования, сведения об опубликованных работах и структура диссертации.

Первая глава диссертации, озаглавленная как **«Особенности мониторинга информационной безопасности в информационно-коммуникационных системах»,** посвящена исследованию проблем

мониторинга информационной безопасности в информационно-коммуникационных системах, архитектуры системы мониторинга информационной безопасности и процесса обработки в ней данных.

Проведение постоянного мониторинга является гарантией поддержания необходимого уровня защиты информации, а результаты, получаемые в рамках деятельности системы мониторинга, являются основой совершенствования системы обеспечения информационной безопасности. В таблице 1 приведены результаты сравнительного анализа, осуществленного на основе изучения функционирования программных средств мониторинга.

Таблица 1

Сравнительный анализ программных средств мониторинга информационной безопасности

Критерии / Программные средства мониторинга информационной безопасности	Обнаружение угроз	Потребление ресурса	Производительность	Удобство использования	Внедренность	Управляемость	Поддерживаемость	Масштабируемость	Определение вероятности состояния функционирования средств	Σ
InTrust	3	3	3	3	2	3	3	3	1	24
EventTracker	4	3	4	3	3	3	4	4	2	30
Sentinel Log Manager	4	3	4	4	3	4	4	4	2	32
NXLog	3	4	3	3	3	4	3	3	1	27
LOGStorm	3	3	3	3	3	3	4	3	1	26

Приведенные результаты сравнительного анализа программных средств мониторинга информационной безопасности показали, что средства, по критерию определения вероятности состояния функционирования, имеют показатели 40% - удовлетворительно и 60 % - не удовлетворительно. Таким образом, в настоящее время определение вероятностей состояния функционирования средств защиты информации с помощью применяемых в организациях программных средств информационной безопасности, не предоставляет ожидаемых результатов.

Для анализа систем мониторинга информационной безопасности особо важными являются ее 5 уровневая архитектура в процессе обработки данных в системах мониторинга информационной безопасности. При этом в рамках архитектуры системы мониторинга информационной безопасности за выполнение определенных операций отвечают отдельные модули (Рис.1).

Предложенная схема обработки данных в системах мониторинга информационной безопасности, основанная на архитектуре системы мониторинга информационной безопасности, с помощью специальных модулей позволяет осуществлять накопление и нормализацию сообщений информационной безопасности, генерируемых в средствах защиты

информации, хранить их в базе данных, анализировать и генерировать ответные реакции на инциденты.

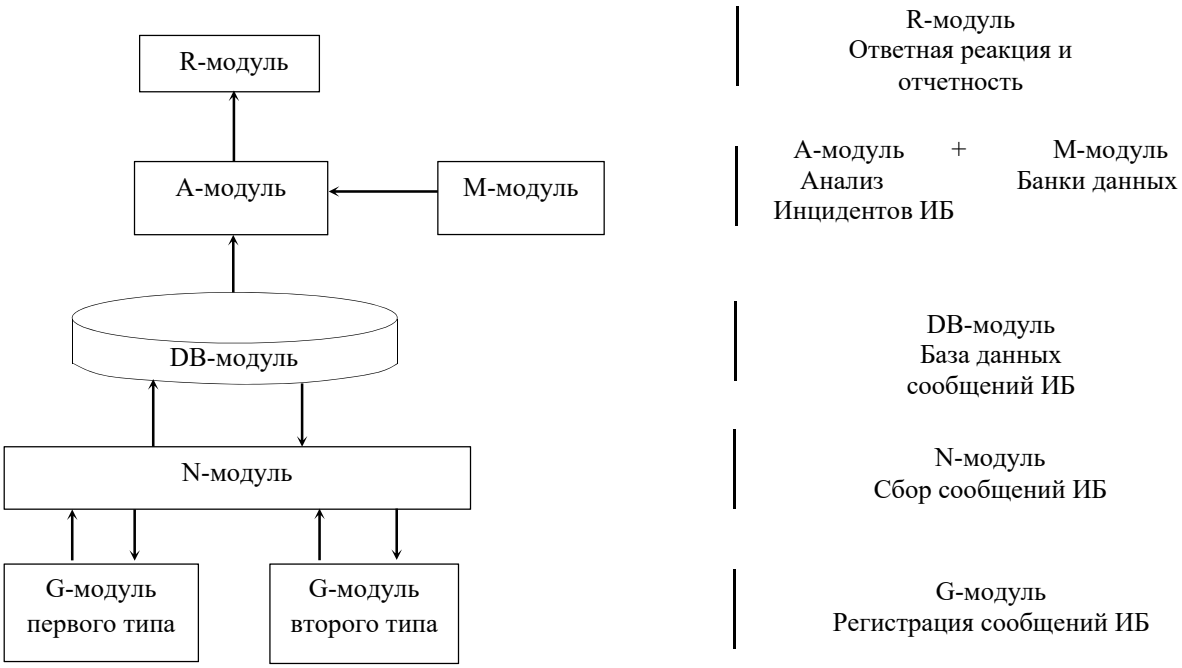


Рис.1. Архитектура системы мониторинга информационной безопасности

Вторая глава диссертации, озаглавленная как «**Модели и структура системы мониторинга информационной безопасности»,** посвящена разработке частной концептуальной модели системы мониторинга информационной безопасности, позволяющей удобно и конкретно описывать результаты мониторинга информационной безопасности. Предложена структура применения системы мониторинга информационной безопасности, позволяющей определять вероятности рабочих состояний средств защиты информации. Предложен метод построения системы мониторинга информационной безопасности, который можно использовать в качестве инструмента формирования исходного и рабочего решений на этапе проектирования.

Частная концептуальная модель системы мониторинга информационной безопасности состоит из задач и функций, процессов и агентов. Как показано на рисунке 2, типовая архитектура включает в себя модули накопления, анализа и принятия решения. Каждый модуль состоит из блоков, выполняющих определенные задачи.

Разработанная частная концептуальная модель системы мониторинга информационной безопасности позволяет обнаруживать аномальные события информационной безопасности, как в защищаемой информационной системе, так и в средствах их защиты и своевременно обеспечивать администратору необходимыми для принятия решения данными о событиях информационной безопасности.

Построение системы мониторинга информационной безопасности с помощью конкретных математических методов, из-за невозможности

полностью формализовать этот процесс, из-за ряда факторов, не соответствующих определенным ситуациям и опасности принятия неправильного решения, является достаточно сложной задачей.

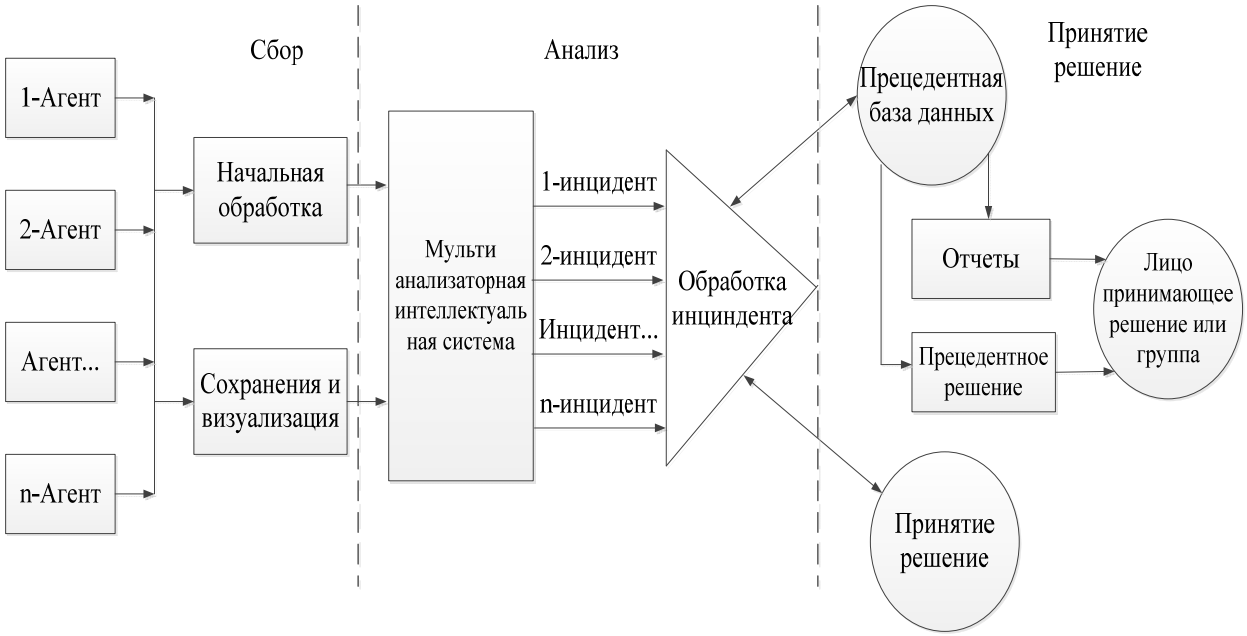


Рис.2. Частная концептуальная модель системы мониторинга информационной безопасности

В таких случаях является целесообразным использовать подход, называемый «итеративный синтез» или «анализ через синтез». Задается начальный вариант построения системы мониторинга, вычисляется величина критерия, полученный критерий сравнивается заданным требованиям и при ее несоответствии, система модифицируется. На каждом этапе итерации вычисленный вариант критерия оценивается, процесс продолжается до получения приемлемого варианта построения системы мониторинга. На рисунке 3 приведена структура метода построения системы мониторинга.

В третьей главе диссертации **«Методы определения вероятностей состояний функционирования средств защиты информации»** разработаны модифицированные методы и алгоритмы, позволяющие определять нарушения, появляющихся ошибок и изменений состояний, которые происходят в период рабочего графика средств защиты информации с дискретным и непрерывным временем работы. На основе предложенного алгоритма разработан новый модуль оценки достоверности средств защиты информации.

Выбор математических методов для определения вероятности состояния функционирования различных средств защиты информации в первую очередь зависит от ее типа, т.е. ее дискретной или непрерывной во времени работы.

Рис.3. Блок схема метода построения системы мониторинга

Набор возможных состояний, которые могут произойти по причине либо нарушения функционирования, либо восстановления работоспособности компонентов средств защиты информации с дискретным временем работы имеет следующий вид:

$$H_{DT} = \left\{ \begin{array}{c} h_0^{DT}, h_1^{DT}, h_2^{DT}, h_3^{DT}, h_4^{DT}, h_5^{DT}, h_6^{DT}, h_7^{DT}, h_8^{DT}, h_{21}^{DT}, h_{24}^{DT}, h_{25}^{DT}, h_{26}^{DT}, h_{27}^{DT}, \\ h_{28}^{DT}, h_{31}^{DT}, h_{35}^{DT}, h_{36}^{DT}, h_{37}^{DT}, h_{38}^{DT}, h_{47}^{DT}, h_{48}^{DT}, h_{51}^{DT}, h_{53}^{DT}, h_{54}^{DT}, h_{56}^{DT}, h_{57}^{DT}, \\ h_{58}^{DT}, h_{63}^{DT}, h_{64}^{DT}, h_{65}^{DT}, h_{67}^{DT}, h_{68}^{DT}, h_{71}^{DT}, h_{75}^{DT}, h_{76}^{DT}, h_{85}^{DT}, h_{86}^{DT} \end{array} \right\}$$

Используя H_{DT} набор действия средств защиты информации с дискретным временем работы можно изображать в виде ориентированного графа как объект, функционирующий в дискретное время. Если учесть, что системы обнаружения уязвимостей и системы контентной фильтрации относяться к средствам защиты информации с дискретным временем работы, можно ввести следующее значение:

$$H_i^{DT_k},$$

здесь i – (i=0,…,8) индекс состояний средств защиты информации с дискретным временем работы;

k – тип средств защиты информации с дискретным временем работы.

Таким образом, можно привести следующее:

$k = 1$ – обнаружения уязвимостей и $k = 2$ – система контентной фильтрации.

Состояния системы обнаружения уязвимостей:

$$H^{DT_1} = \left\{h_0^{DT_1}, h_1^{DT_1}, h_2^{DT_1}, h_3^{DT_1}, h_4^{DT_1}\right\}$$

Состояния системы контентной фильтрации:

$$H^{DT_2} = h_0^{DT_2}, h_5^{DT_2}, h_6^{DT_2}, h_7^{DT_2}, h_8^{DT_2}$$

Как видно из рисунка 4, вершины графа характеризуют $P_{\mathrm{q,q}}$ состояния возможных состояний системы обнаружения уязвимостей, а через дуги графа показывается $P_{\mathrm{q,r}}\ (\mathrm{q} \neq \mathrm{r})$ вероятность переходов с одного состояния на другую на определенном промежутке Δt времени, описывающая дискретность функционирования системы.

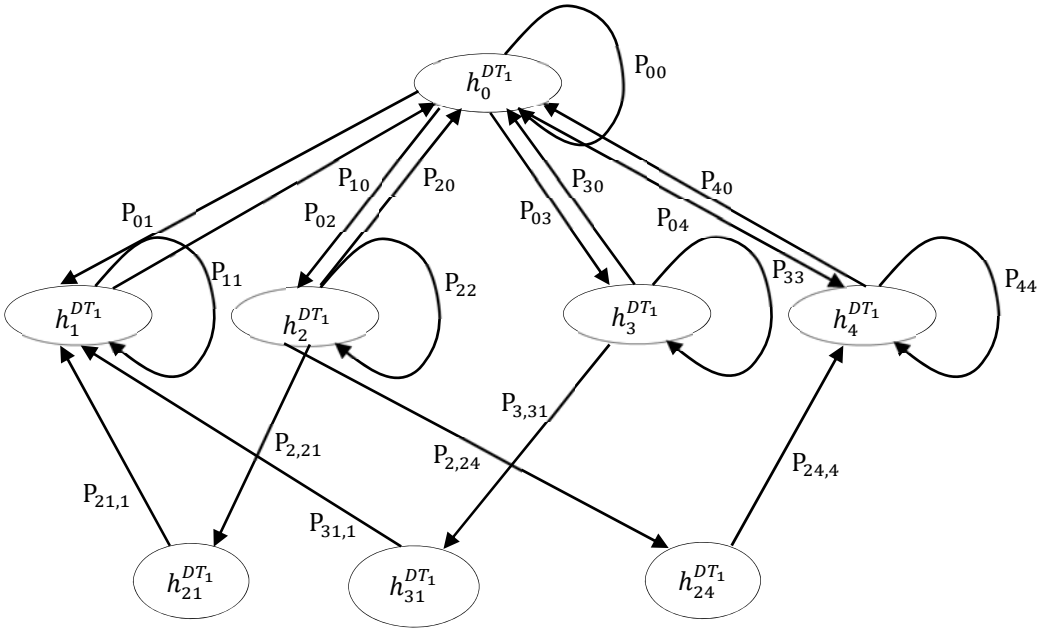


Рис.4. Граф вероятности переходов состония функционирования системы обнаружения уязвимостей

Модифицированный метод определения вероятности состояния системы обнаружения уязвимостей позволяет описывать систему уравнений следующим образом:

$$\begin{cases} \overline{p}_0 = P_{00}\overline{p}_0 + P_{10}\overline{p}_1 + P_{20}\overline{p}_2 + P_{30}\overline{p}_3 + P_{40}\overline{p}_4, \\ \overline{p}_1 = P_{01}\overline{p}_0 + P_{11}\overline{p}_1, \\ \overline{p}_2 = P_{02}\overline{p}_0 + P_{2,21}\overline{p}_{21} + P_{22}\overline{p}_2 + P_{2,24}\overline{p}_{24}, \\ \overline{p}_3 = P_{03}\overline{p}_0 + P_{3,31}\overline{p}_{31} + P_{33}\overline{p}_3, \\ \overline{p}_4 = P_{04}\overline{p}_0 + P_{44}\overline{p}_4. \end{cases}$$

При этом,

$$\overline{p}_0 + \overline{p}_1 + \overline{p}_2 + \overline{p}_3 + \overline{p}_4 = 1,$$

здесь $\overline{p}_q,\ q = 0,1,2,3,4$ - искомые граничные вероятности.

Разработанный метод, использующий небольшой набор состояний, позволяет описывать граф-схему переходов, составить квадратную матрицу с малым разрядом и на их основе легко описывать системы уравнений для систем контентной фильтрации, которые входят в ту иную разновидность

средств защиты информации с дискретным временем работы.

Набор возможных состояний средств защиты информации с непрерывным временем работы имеет следующий вид:

$$H_{UT} = \begin{Bmatrix} h_0^{UT}, h_1^{UT}, h_2^{UT}, h_3^{UT}, h_4^{UT}, h_5^{UT}, h_6^{UT}, h_7^{UT}, h_8^{UT}, h_{13}^{UT}, h_{15}^{UT}, h_{18}^{UT}, h_{21}^{UT}, \\ h_{23}^{UT}, h_{24}^{UT}, h_{25}^{UT}, h_{26}^{UT}, h_{28}^{UT}, h_{34}^{UT}, h_{35}^{UT}, h_{36}^{UT}, h_{38}^{UT}, h_{41}^{UT}, h_{43}^{UT}, h_{45}^{UT}, h_{46}^{UT}, \\ h_{48}^{UT}, h_{51}^{UT}, h_{52}^{UT}, h_{53}^{UT}, h_{54}^{UT}, h_{56}^{UT}, h_{57}^{UT}, h_{58}^{UT}, h_{61}^{UT}, h_{62}^{UT}, h_{68}^{UT}, h_{71}^{UT}, h_{73}^{UT}, \\ h_{74}^{UT}, h_{76}^{UT}, h_{78}^{UT}, h_{81}^{UT}, h_{82}^{UT}, h_{86}^{UT}, \end{Bmatrix}$$

Для определения состояния функционирования средств защиты информации с непрерывным временем работы используется метод переменных интенсивностей. На основе этого метода предложен модифицированный метод определения состояний функционирования антивирусного программного обеспечения. При этом вводится следующее значение *H*:

$$H_i^{UT_k},$$

здесь: *i* – индекс состояния средств защиты информации с непрерывным временем работы, k =1,2,3,4 - типы средств защиты информации с непрерывным временем работы.

При анализе системы мониторинга информационной безопасности антивирусного программного обеспечения состояния описываются следующим образом:

$$H_{UT_1} = \left\{h_0^{UT_1}, h_1^{UT_1}, h_2^{UT_1}, h_3^{UT_1}, h_4^{UT_1}, h_{13}^{UT_1}, h_{21}^{UT_1}, h_{23}^{UT_1}, h_{24}^{UT_1}, h_{34}^{UT_1}, h_{41}^{UT_1}, h_{43}^{UT_1}\right\}$$

Используя данный набор можно изображать ориентированный граф переходов состояний функционирования антивирусного программного обеспечения (Рис.5).

Изменение $\frac{dp_q(t)}{dt}$ вероятности p_q нахождения антивирусного программного обеспечения в состоянии h_q, характеризуемой соответствующей вершиной (обоначается далее в уравнении как *q-ая*), в которую могут входит и выходит различные дуги, определяется интенсивностью подхода антивирусного программного обеспечения к этому состоянию и выхода их него:

$$\frac{dp_q(t)}{dt} = \sum_{k=1}^{K} p_k(t)\Lambda_{k,q} - p_q(t)\sum_{l=1}^{L}\Lambda_{q,l}$$

$$q = 0,1,2,3,4,13,21,23,24,34,41,43.$$

Здесь:

$p_k(t)$ – вероятность нахождения антивирусного программного обеспечения в состоянии h_k (k-ая вершина) из которого осуществляется переход в состояние h_q (q-ая вершина) с интенсивностью $\Lambda_{k,q}$;

$\Lambda_{q,l}$ – интенсивность перехода из состояний h_q в состояния h_l (l-ая

вершина);

К - число вершин, связанных с вершиной h_q входящими дугами;

L – число вершин связанных с вершиной h_q исходящими дугами.

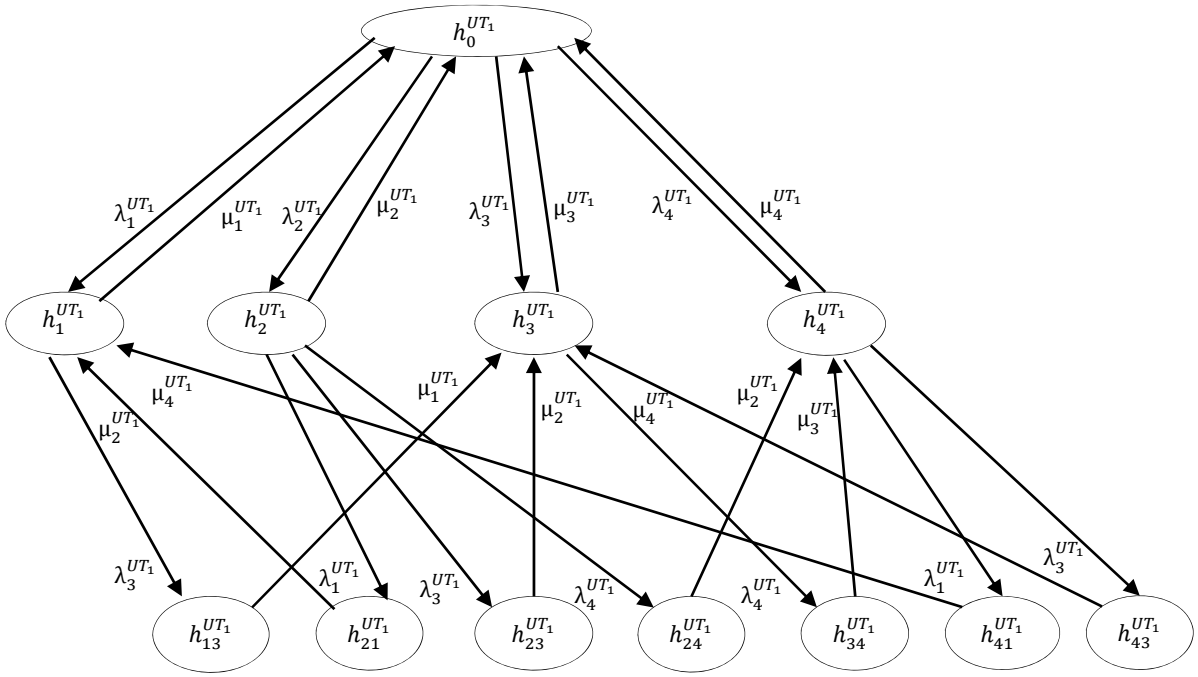


Рис.5. Граф определения состояний функционирования антивирусного программного обеспечения

Разработанный модифицированный метод определения состояний функционирования средств защиты информации с непрерывным временем работы для антивирусного программного обеспечения позволяет в 4 раза сократить количество переходов в граф-схеме и времени определения состояний функционирования.

Модуль оценки надежности средств защиты информации в предложенном составе структуры подсистемы обеспечения работоспособности системы мониторинга информационной безопасности является полностью новым (рис.6).

С помощью данного модуля вычисляется вероятность состояний функционирования средств защиты информации, использующего постоянно обновляющуюся информацию (по данным текущей эксплуатации) о предыдущих к данному моменту нарушениях. Основой функционирования модуля является алгоритм определения вероятностей состояний функционирования средств защиты информации.

В четвертой главе «**Архитектура программного средства системы мониторинга информационной безопасности и результаты экспериментальных вычислений»** приведены результаты экспериментальных данных по мониторингу информационной безопасности. Определены показатели надежности компонентов антивирусного программного обеспечения и на их основе вычислены вероятности состояний функционирования средств защиты информации. Оценена эффективность

системы мониторинга информационной безопасности.

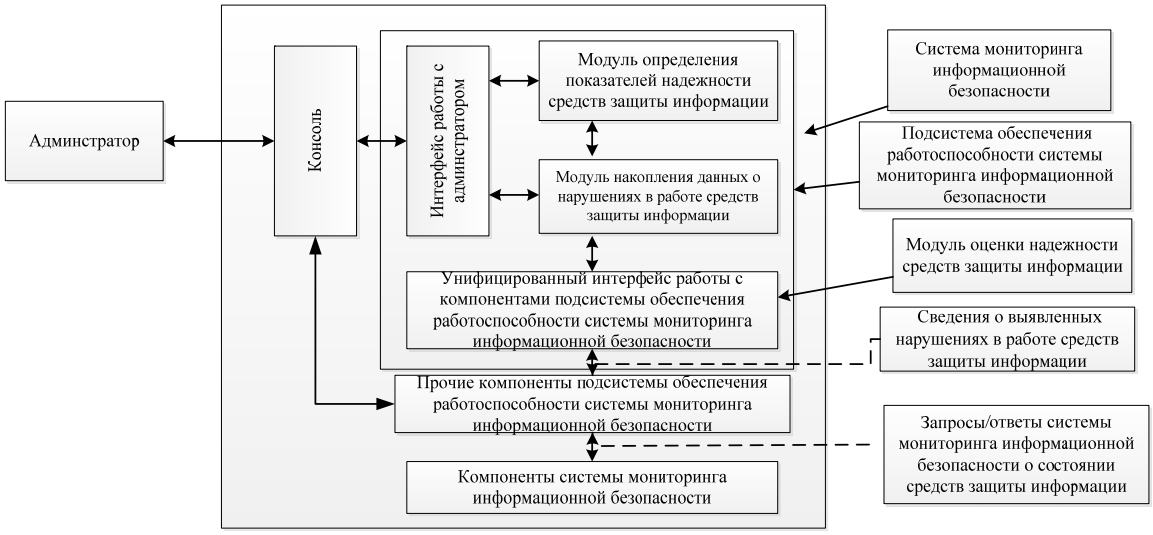


Рис.6. Схема структуры модуля оценки надежности средств защиты информации

В таблице 2 приведены характеристики обнаруженных ошибок на основе анализа существующих четырех вида ошибок, в соответствии с состояниями функционирования антивирусного программного обеспечения.

По данным характеристикам получены решения системы дифференциальных уравнений первого порядка, полученной для антивирусного программного обеспечения определения вероятностей состояний функционирования средств защиты информации с непрерывным временем работы, с помощью программного обеспечения MathCad.

Таблица 2

Характеристики обнаруженных ошибок

№	Временные разрезы	Количество записей об ошибках	Время исправного функционирования с момента предыдущей ошибки T_i^j, с	Время восстановления ξ_i^j, с
1	07.08.2018 (03:11:01)-07.08.2018(03:28:05)	2	4513,18	0,28
2	11.09.2018 (04:15:08)-13.09.2018(05:16:12)	11	1008,78	48,01
3	09.11.2018 (02:18:15)-10.11.2018(03:24:16)	8	603	25,1

На основе полученных экспериментально-вычислительных результатов с помощью программного обеспечения Mathcad доказана удовлетворительность полученных значений вероятности $p_0, p_1, p_2, p_3, p_4, p_{13}, p_{21}, p_{23}, p_{24}, p_{34}, p_{41}, p_{43}$ состояний функционирования в разрезах времени 240 и 3000 часов антивирусного программного обеспечения в соответствии нижеприведенных требований:

$$\sum p_q(t) = 1, \forall t \in [0, \infty), \qquad \text{q} = 0,1,2,3,4,13,21,23,24,34,41,43$$

Оценена эффективность до и после внедрения подсистемы обеспечения

работоспособности в системе мониторинга информационной безопасности предприятия «Государственный геологический информационный центр» при Государственном Комитете Республики Узбекистан по геологии и минеральным ресурсам. Для оценки эффективности использованы суточные показатели работы средств защиты информации в информационно-коммуникационной системе, которые приведены в таблице 3.

Таким образом, за 11 месяцев (334 суток) количество обнаруженных инцидентов информационной безопасности составляет $N_1 = 334 * 58 = 19372$. При этом после появления четыре типа ошибок, зарегистрированных на журналах функционирования, требуемое время для восстановления работоспособности антивирусного программного обеспечения равна:

$$T_{\text{тик}} = (0{,}78 + 72{,}1 + 38{,}18) + (72{,}78 + 60{,}55 + 50{,}3) + 12 + 20 = 326{,}69$$

или $326{,}69/24 = 13{,}61$ суток

Это означает, что антивирусное программное обеспечение из 334 суток работала только 320,39 суток. Если в функционировании антивирусного обеспечения не появляются ошибки, суточное количество обнаруженных инцидентов информационной безопасности можно получить с помощью деления общее количество на данные время, т.е.:

$$N_{\text{сутка}} = 19372 \text{ инцидент}/320{,}39 \text{ сутка} = 60{,}46 \text{ инцидент}$$

Таблица 3

Суточные показатели работы средств защиты информации

Средства защиты информации	Количество событий информационной безопасности за один день	Количество инцидентов информационной безопасности за один день	Соотношение
Антивирусное программное обеспечение	58	58	1
Системы обнаружения уязвимостей	70	4	17,5
Межсетевые экраны	90154	832	108,35
Системы обнаружения вторжений	102482	1124	91,1

Значить, при работе без ошибок антивирусного программного обеспечения, можно было определить количества инцидентов информационной безопасности следующим образом:

$$N = 334 * 60{,}46 = 20193{,}64 \approx 20194 \text{ инцидентов.}$$

Общее время восстановления работоспособности антивирусного программного обеспечения в результате применения подсистемы обеспечения работоспособности системы мониторинга информационной безопасности, равна следующему:

$$T_{\text{тик1}} = (0{,}28 + 48{,}01 + 25{,}01) + (46{,}54 + 21{,}43 + 24{,}1) + 6 + 8 = 179{,}37$$

или 7,743 суток.

В результате применения подсистемы, обеспечивающей

рабоспособность системы мониторинга информационной безопасности, время восстановления для работы антивирусного программного обеспечения было сокращено на

$$S = T_{\text{тик}}/T_{\text{тик1}} = 13{,}61/7{,}743 = 1{,}75$$

В течение этого времени количество пропущенных инцидентов в результате ошибок в работе антивирусного программного обеспечения или обнаруженные со значительными опозданиями, равно:

$$N' = 7{,}743 * 60{,}46 = 468{,}14 \approx 468 \text{ инцидентов.}$$

В течение времени наблюдения количество инцидентов, обнаруженных в результате внедрения подсистемы обеспечения работоспособности системы мониторинга информационной безопасности, равна:

$$N_2 = N - N' = 20194 - 468 = 19726 \text{ инцидентов}$$

На рисунке 8 приведена диаграмма количеств обнаруженных и не обнаруженных инцидентов до и после внедрения подсистемы обеспечения работоспособности средств защиты информации.

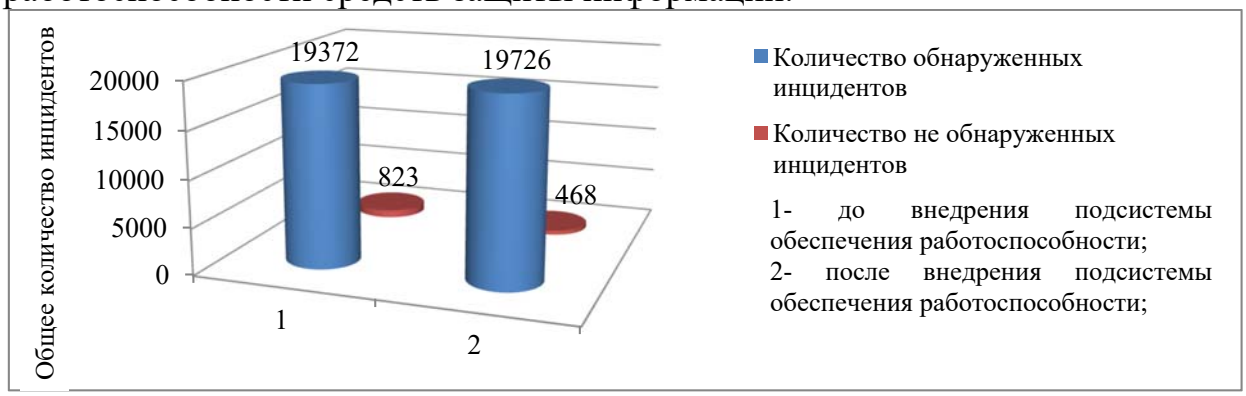


Рис.8. Диаграмма результатов, полученных до и после внедрения подсистемы обеспечения работоспособности средств защиты информации

Это означает, что внедрение подсистемы обеспечения работоспособности средств защиты информации в систему мониторинга информационной безопасности, дает возможность за 334 сутки обнаружить 19726 инцидентов, т.е. позволяет обнаружить на 355 инцидентов (1,82 %) больше и сократить время восстановления работоспособности антивирусного программного обеспечения в 1,75 раза, чем при функционировании антивируса без внедренной подсистемы.

ЗАКЛЮЧЕНИЕ

По результатам проведенных исследований по диссертационной работе на тему: «Методы и алгоритмы повышения эффективности функционирования системы мониторинга информационной безопасности», можно сделать следующие выводы:

1. Создана схема обработки данных в системе мониторинга информационной безопасности на основе накопления и анализа данных об инцидентах, которые могут произойти. Данная схема позволила генерировать, собирать, сохранять, анализировать сообщения, а также

оценивать уровень защищенности информации.

2. Разработана частная концептуальная модель системы мониторинга информационной безопасности на основе схемы обработки данных. Разработанная частная концептуальная модель позволила обнаруживать аномальные события в средствах защиты информации и своевременно обеспечивать необходимыми данными администратора информационной безопасности об этих событиях для принятия решений.

3. Разработан метод построения системы мониторинга информационной безопасности на основе подхода «анализ через синтез». Данный метод позволяет разрабатывать требования и рекомендации по обнаружению и предотвращению уязвимых мест при функционировании системы на этапе эксплуатации.

4. Разработаны модифицированные методы определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы на основе сокращений состояний. Разработанные методы позволили при изучении средств защиты информации с непрерывным временем работы (антивирусное программное обеспечение) сократить количество переходов в 4 раза и соответственно уменьшить время их вычисления.

5. Разработан модуль оценки надежности средств защиты информации на основе алгоритма определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы. Разработанный модуль позволил оперативно обеспечивать администратора информационной безопасности о текущей надежности средств защиты информации и прогнозировать их дальнейшее функционирование.

6. Разработано программное средство ISMS, позволяющее применять его в разных по размеру информационно-коммуникационных системах организаций. ISMS разработано на основе методов и алгоритма определения вероятностей состояния функционирования средств защиты информации с дискретным и непрерывным временем работы. Разработанное программное средство позволило в информационно-коммуникационной системе Государственной предприятии «Государственный геологический информационный центр» сократить в 1,75 раза время восстановления работоспособности антивирусного программного обеспечения и обнаружить на 355 инцидентов (1,82 %) больше чем существующие средства.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.27.06.2017.T.07.01 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

NASRULLAYEV NURBEK BAKHTIYOROVICH

METHODS AND ALGORITHMS FOR ADVANCING THE EFFICIENCY OF THE INFORMATION SECURITY MONITORING SYSTEM

05.01.05 – Methods and Systems of Information Protection. Information Security

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

Tashkent-2019

The theme of dissertation 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 B2019.1.PhD/T974.

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:	**Ganiev Salim Karimovich** Doctor of Technical Sciences, Professor
Official opponents	**Bekmuratov Tulkin Fayzievich** Doctor of Technical Sciences, Professor, Academician
	Tuychiev Gulom Numonovich Doctor of Physical-Mathematical Sciences
Leading organization:	**Scientific-Engineering and Marketing Researches Center «UNICON.UZ»**

The defense will take place on «____» _____ 2019 at ___ at the meeting of the Scientific Council No. DSc.27.06.2017.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 could be reviewed in the Information Resourse Centre of Tashkent University of Information Technologies (registration number No.___). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

The abstract of dissertation is distributed on «____» _____ 2019 y.
(Protocol at the register No. ___ on «____» _____ 2019 y.).

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

F.M. Nuraliev
Scientific Secretary of Scientific Council
awarding scientific degrees,
Doctor of Technical Sciences, Docent

R.J. Aloev
Chairman of the Scientific Seminar at the
Scientific Council awarding scientific degrees,
Doctor of Physical-Mathematical Sciences, Professor

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to develop methods and algorithms based on determining the probabilities of the state of functioning of information of protection tools, allowing to upward the efficiency of the information security monitoring system.

The object of the research work are the process of functioning of protection tools used on information and communication systems.

The scientific novelty of the research work:

a data processing scheme on the information security monitoring system based on the accumulation and analysis of data on potential incidents was created;

a private conceptual model of the information security monitoring system based on the data processing scheme was worked out;

a construction method of information security monitoring system based on the "analysis through synthesis" approach was worked out;

modified methods for determining the probabilities of the state of functioning of information security tools with discrete and continuous operation time were worked out;

an algorithm for determining the probabilities of the state of functioning of information protection tools in the structure of the subsystem to provide their performance based on modified methods were worked out.

Implementation of the research results. On the basis of scientific results according to methods and algorithms for beef the efficiency up of the information security monitoring system:

an algorithm for determining the probabilities of the state of functioning of information protection tools in the structure of the subsystem to provide their performance based on modified methods, was implemented in practical activities of the State Enterprise «State Geological Information Center» under the State Committee of the Republic of Uzbekistan on Geology and Mineral Resources (Certificate No. 33-8/161 as of January 11, 2019 the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan). As a result of researching, it became possible to reduce the recovery time of Kaspersky anti-virus software by 1,75 times and detect 355 more incidents;

a data processing scheme on the information security monitoring system based on the accumulation and analysis of data on potential incidents was implemented in practical activities of the SUE «UNICON.UZ» - technical and marketing research center, in order to detect errors, appearing in the function of information of protection tools (Certificate No. 33-8/161 as of January 11, 2019 the Ministry for D evelopment of Information Technologies and Communications of the Republic of Uzbekistan). As a result of researching the testing process, the possibility of reducing the recovery time of antivirus software and detecting significantly larger number of incidents was obtained;

methods and algorithms for determining the probabilities of the state of functioning of information security tools with discrete and continuous operation time, was introduced into the activities of «STAND KOMPUTERS» LLC

(Certificate No. 33-8/161 as of January 11, 2019 the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan). As a result of researching, through the module for providing the reliability of information protection tools in the structure of subsystem of the information security monitoring system, allowed to reduce time for recovering information of protection tools by 1,12 times and to detect on 40 more incidents.

The outline of the dissertation. The dissertation consists of an Introduction, four Chapters, Conclusion, a list of Bibliography and Appendices. The volume of the thesis is 111 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

1. Abduraxmanov A.A., Nasrullayev N.B., Abduraxmanova N.N. Security problems of info-communication systems and constructing a model of selection program-technical complex of information security system // TUIT BULLETIN. –Tashkent, 2015, №1 (33). -P. 101-109, (05.00.00; №10).
2. Ganiev S.K., Gulomov Sh.R., Nasrullaev N.B., Abdurakhmonov A.A. Methods monitoring of network traffics for intrusion detection and special filtering traffic on «e-government» // Кимёвий технология назорат ва бошқарув. –Tashkent, 2017. №5 (77). –P. 76-84, (05.00.00; №12).
3. Ташев К.А., Насруллаев Н.Б., Исломов Ш.З. Ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш // Муҳаммад ал-Хоразмий авлодлари. –Тошкент, 2018. №1 (3). –P. 38-44, (05.00.00; №10).
4. Насруллаев Н.Б., Исломов Ш.З., Файзиева Д.С. Ахборот хавфсизлиги мониторинги тизими архитектураси // Муҳаммад ал-Хоразмий авлодлари. –Тошкент, 2018. №2 (4). –P. 13-19, (05.00.00; №10).
5. Gulomov Sh., Nasrullayev N.B., Abdurakhmanov A. Design Method and Monitoring Special Traffic Filtering under Developing «Electronic Government» // International Journal of Emerging Technology and Advanced Engineering. –India, 2015, №5 (1). -P. 66-73, (05.00.00; №14).
6. Abdurakhmanov A.A., Nasrullayev N.B., Varisov A.A. E-Government, Open Data, and Security: Overcoming Information Security Issues with Open Data // Computer Science and Information Technology. –USA, 2015, №3 (4). -P.133-137, (05.00.00; №6).
7. Nasrullayev N.B., Bekmurodov U.B., Khaydarov S. F. Modeling the Processes of Violation Security on Monitoring System // International Journal of Advanced Research in Science, Engineering and Technology. –India, 2017, №4 (10). -P. 4693-4700, (05.00.00; №8).
8. Gulomov Sh.R., Nasrullayev N.B., Imamaliyev A.T. Approach to implementation of software and hardware control system activity protection // TUIT BULLETIN. –Tashkent, 2014, №3 (31). –P. 125-129.
9. Ганиев С.К., Насруллаев Н.Б. К вопросу применения средств мониторинга информационной безопасности инфокоммуникационных системах // Ахборот ва телекоммуникация технологиялари муаммолари илмий-техник конференцияси, -Ташкент, 2015, -P. 479-481.
10. Ганиев С.К., Насруллаев Н.Б. К вопросу оценки эффективности мониторинга инцидентов информационной безопасности предприятия // Республиканской научно-технической конференции «Проблемы информационных и телекоммуникационных технологий», -Ташкент, 2016, -С. 6-7.
11. Ганиев С.К., Насруллаев Н.Б. К вопросу выявления информационного риска в системах мониторинга безопасности // Сборник

докладов, Республиканской научно-технической конференции «Проблемы информационных и телекоммуникационных технологий», -Ташкент, 2016, -С. 102-104.

12. Ташев К.А., Насруллаев Н.Б. Метод получения комплексной оценки результатов мониторинга информационной безопасности и специальной фильтрации сетевого трафика // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения», -Ташкент, 2016, -С. 15-17.

13. Ганиев С.К., Насруллаев Н.Б. Интерполяция значений оценок математического ожидания и дисперсии количества сообщений в таблице моментов // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения», -Ташкент, 2016, -С. 17-20.

14. Ташев К.А., Насруллаев Н.Б. Анализ методов мониторинга информационной безопасности в инфокоммуникационных систем // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения», -Ташкент, 2016, -С. 65-67.

15. Хашимов Х.М., Гулямов Ш.Р., Насруллаев Н.Б. Комплексный метод мониторинга и оценки показателей качества информационной безопасности инфокоммуникационной системы // Актуальные проблемы прикладной математики и информационных технологий-Аль-Хорезми 2016, -Бухара, 2016. №1, -С. 172-175.

16. Гуломов Ш.Р., Насруллаев Н.Б. Факторы влияющие на эффективность мониторинга информационной безопасности // «Электрон ҳукумат тизимида ахборот хавфсизлиги муаммолари ва уларнинг ечимлари» мавзуси бўйича Республика семинари, -Тошкент, 2017. -Б. 22-24.

17. Гуломов Ш.Р., Насруллаев Н.Б. Недостатки существующих SIEM систем с точки зрения анализа безопасности // «Электрон ҳукумат тизимида ахборот хавфсизлиги муаммолари ва уларнинг ечимлари» мавзуси бўйича Республика семинари, -Тошкент, 2017. –Б. 60-62.

18. Ганиев С.К., Насруллаев Н.Б. Ахборот-коммуникация тизимларида ахборот хавфсизлиги мониторинги тизимини қўллаш // «Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари» Республика миқёсидаги илмий-техник конференция, -Тошкент, 2018, -Б. 19-23.

19. Ташев К.А., Насруллаев Н.Б. Ахборот хавфсизлиги мониторинги тизимида ахборотни ҳимоялаш воситаларининг ишончлилигини баҳолаш // «Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари» Республика миқёсидаги илмий-техник конференция, -Тошкент, 2018, -Б. 46-50.

20. Абдуллаев Д.Г., Насруллаев Н.Б., Қурбонов Э.И. Monitoring software of info-communication network and its role in network security // Международная научная конференция «INNOVATION - 2012», -Ташкент, 2012, -Р. 261-262.

21. Ганиев А.А., Юсупов С.Ю., Насруллаев Н.Б. Алгоритм оценки рисков при аудите информационной безопасности // Международная научно конференция «INNOVATION - 2013», -Ташкент, 2013, –P. 284-285.

22. Karimov M. M., Abdurakhmanov A.A., Nasrullayev N.B. About One of the Authentication methods. // 3rd International Conference on Application of Information and Communication Technology and Statisticsin Economy and Education ICAICTSEE – 2013. - Sofia, Bulgaria, 2013 – P. 739-745.

23. Ganiev S.K., Gulomov Sh.R., Nasrullayev N.B. Processing of data in monitoring security events // Perspectives for the development of information technologies ITPA-2015, -Tashkent, 2015, -P. 74-78.

24. Tashev K.A., Nasrullayev N.B., Islomov Sh.Z. Information security monitoring in face recognition system // Perspectives for the development of information technologies ITPA-2015, -Tashkent, 2015, -P. 113-117.

25. Tashev K., Nasrullayev N.B. Development method of code detection system on based racewalk algorithm on platform FPGA // 5th International Conference on Application of Information and Communication Technology and Statisticsin Economy and Education, ICAICTSEE – 2015. - Sofia, Bulgaria, 2015, -P. 278-285.

26. Gulomov Sh.R., Nasrullayev N.B. Method for Security Monitoring and Special Filtering Traffic Mode in Info communication Systems // International Conference on Information Science and Communications Technologies, ICISCT, --Tashkent, 2016. –P. 1-3.

27. Насруллаев Н.Б., Файзиева Д.С. Ахборот хавфсизлиги мониторинги тизимини қуриш усули // International conference on importance of information communication technologies in innovative development of sectors of economy. Dedicated to the 1235th anniversary of the birth of Muhammad al-Khwarizmi, -Tashkent, 2018. -P. 384-386.

28. Ганиев С.К., Каримов М.М., Ганиев А.А., Насруллаев Н.Б., Абдурахманов А.А., Холмуратов О.У., Юсупов Б.К., Имомалиев О.Т. «Ахборот хавфсизлиги аудитини ўтказувчи дастурий мажмуа» // Дастурга гувоҳнома № DGU 03191, 11.06.2015.

29. Ганиев С.К., Ганиев А.А., Ташев К.А., Насруллаев Н.Б., Абдурахмонов А.А., Гуломов Ш.Р., Курбонов Э.И. «Security monitoring» // Дастурга гувоҳнома № DGU 04076, 24.11.2016.

30. Ганиев С.К., Ганиев А.А., Ташев К.А., Гуломов Ш.Р., Насруллаев Н.Б., Юсупов Б.К., Нормуминов Ф.К., Абдуллаев М.Х. «Information security monitoring system» // Дастурга гувоҳнома № DGU 05820, 05.12.2018.

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

Бичими 60x84$^{1}/_{16}$. Рақамли босма усули. Times гарнитураси.
Шартли босма табоғи: 2,8. Адади 100. Буюртма № 47.

«Тошкент кимё-технология институти» босмахонасида чоп этилган.
Босмахона манзили: 100011, Тошкент ш., Навоий кўчаси, 32-уй.