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

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

ХАЛМУРАТОВ ОМОНБОЙ УТАМУРАТОВИЧ

АХБОРОТ ХАВФСИЗЛИГИ КЎРСАТКИЧ ВА МЕЗОНЛАРИ ТИЗИМИНИ ШАКЛЛАНТИРИШ 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

ХАЛМУРАТОВ ОМОНБОЙ УТАМУРАТОВИЧ

АХБОРОТ ХАВФСИЗЛИГИ КЎРСАТКИЧ ВА МЕЗОНЛАРИ ТИЗИМИНИ ШАКЛЛАНТИРИШ 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 B2017.1.PhD/T55 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:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
	Курязов Давлатёр Матякубович физика-математика фанлари номзоди
Етакчи ташкилот:	**Ўзбекистон Миллий университети**

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 технологияларини оммавий тарзда ишлаб чиқиш ва эксплуатация этиш жадаллик билан ривожланиши унга бўладиган хавфлар сонининг ортишига олиб келмоқда, жумладан «McAfee компаниясининг статистик маълумотига кўра, 2017 йилда дунё бўйича кибержиноятчиликдан келтирилган зарар миқдори 2014 йилгига қараганда 35 % га ошган»[1]. Шу жиҳатдан ахборот тизимлари хавфсизлигини баҳолаш ва унинг самарадорлигини ошириш воситаларини ишлаб чиқишга катта эътибор қаратилмоқда. Бу йўналишда ривожланган мамлакатларда, жумладан АҚШ, Россия Федерацияси, Канада, Франция ва бошқа давлатларда ахборот технологияларини талаб даражасида ишлаб чиқиш ва ахборот хавфсизлигини баҳолаш имкониятини берувчи мезонларини яратиш муҳим аҳамият касб этмоқда.

Жаҳонда ахборот хавфсизлиги кўрсаткич ва мезонларини шакллантириш ҳамда улар асосида ахборот тизими хавфсизлигини баҳолаш усулларни ишлаб чиқишга йўналтирилган илмий-тадқиқот ишлари олиб борилмоқда. Жумладан, ахборот хавфсизлигини баҳолашда, ахборот тизими компонентлари, алмашиниладиган маълумотлар хусусиятларини эътиборга олган ҳолда, хавфсизлик профилини танлаш, ахборот тизими компонентлари ва хавфсизлик мезонларининг устуворлигини эътиборга олган ҳолда, ахборот хавфсизлигини назоратлаш усулларини ишлаб чиқиш муҳим вазифалардан ҳисобланади. Шу билан бирга, ахборот хавфсизлигини баҳолаш асосида ташкилот ахборот хавфсизлигини бошқариш жараёнларини такомиллаштиришни илмий асослаш зарур ҳисобланмоқда.

Республикамизда давлат ва хўжалик бошқарув органларида ахборот технологияларини ривожлантириш билан бир қаторда ахборот технологияларини таҳдидлардан ҳимоялашга ва уларни баҳолаш усул ва воситаларини татбиқ этишга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш, ... иқтисодиёт, ижтимоий соҳа, бошқарув тизимига ахборот-коммуникация технологияларини жорий этиш»[2] вазифалари белгиланган. Мазкур вазифаларни амалга ошириш, жумладан ташкилотларнинг ахборот хавфсизлигини баҳолашда кўрсаткич ва мезонлар тизимини такомиллаштириш моделлари, усуллари ва алгоритмларини яратиш муҳим масалалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги

[1] http://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности

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

ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 14 мартдаги ПФ-5379-сон «Ўзбекистон Республикасининг давлат хавфсизлиги тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги ва 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари, 2018 йил 21 ноябрдаги ПҚ-4024-сон «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишда 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 хавфсизлиги кўрсаткич ва мезонларини ишлаб чиқиш бўйича кўплаб давлатларнинг турли ташкилотлари олимлари тадқиқот олиб борганлар, жумладан А.А. Варфоломеев, В.В. Домарев, М.Л. Калужский, Ажмухамедов, О.Г. Берестнева, Ю.Я. Самохвалов, Б.М. Герасимов, А.Н. Павлов, В.Ф. Шаньгин, Д.П. Зегжда ва бошқа олимлар ишларини кўрсатиш мумкин.

Ўзбекистонда Т.Ф. Бекмуратов, М.М. Арипов, С.К. Ганиев, М.М. Каримов, Р.Х. Хамдамов, Д.Т. Мухаммадиева бошчилигидаги илмий жамоалар томонидан экспертлар хулосалари асосида билимлар базасини шакллантириш, ахборот хавфсизлигини кўрсаткич ва мезонларини шакллантириш, ҳамда ахборот тизими ҳимояланганлигини баҳолаш усуллари ўрганиб чиқилган.

Ҳозирги кунда ахборот хавфсизлигини баҳолашнинг кўрсаткич ва мезонларини марказлашган ҳолда экспертлар хулосалари ва ташкилот ахборот хавфсизлиги мезонларининг устуворлиги ҳамда ахборот тизими компонентларининг хусусиятлари асосида баҳолаш усулларини шакллантириш етарли даражада ўрганилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент ахборот технологиялари университети ва ТАТУ Урганч филиалининг илмий-тадқиқот ишлари режасининг №Ф4-019 «Ахборот хавфсизлиги кўрсаткич ва мезонлар тизимларини шакллантириш муаммоларининг тадқиқи» (2012-2016) ва №Ф636-16 «Ахборот коммуникация тизимлари ахборот хавфсизлигини баҳоловчи дастурий таъминот ишлаб чиқиш» (2016) мавзуларидаги лойиҳалари доирасида бажарилган.

Тадқиқотнинг мақсади ахборот хавфсизлиги кўрсаткич ва мезонлари

тизимини шакллантириш ва ахборот тизими хавфсизлигини баҳолаш усуллари ва воситаларини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

ахборот хавфсизлигини баҳолаш жараёнини хусусий ва қисм-тизим концептуал моделларини ишлаб чиқиш;

ахборот хавфсизлиги кўрсаткич ва мезонлари тизимининг функционал ва информацион моделларини яратиш;

ахборот хавфсизлиги кўрсаткич ва мезонлари тизимини шакллантириш алгоритмини ишлаб чиқиш;

ахборот тизими компонентларининг хавфсизлик бўйича устуворликлари асосида ахборот тизимини баҳолаш усулини ишлаб чиқиш;

ахборот хавфсизлигини баҳолаш тизимининг дастурий воситасини яратиш.

Тадқиқотнинг объекти сифатида ахборот тизими хавфсизлигини баҳолаш жараёни олинган.

Тадқиқотнинг предмети сифатида ахборот хавфсизлиги кўрсаткич ва мезонларини шакллантириш ҳамда улар асосида ахборот хавфсизлигини баҳолаш усуллари ва алгоритмлари олинган.

Тадқиқотнинг усуллари. Тадқиқот жараёнида ахборот ҳимояланганлигини тахлил қилиш усуллари, норавшан мантиқ ва норавшан тўпламлар назарияси, графлар назарияси ва объектга йўналтирилган дастурлашдан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

ташкилот ва унинг ахборот тизими компонентларининг хусусиятлари асосида ахборот тизими хавфсизлигининг хусусий ва қисм-тизим концептуал моделлари ишлаб чиқилган;

IDEF0 ва IDEF1X методологияси орқали ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизимини шакллантиришнинг функционал ва информацион моделлари ишлаб чиқилган;

баллар бериш, рутбалаш ва норавшан мантиқ назариясининг «Мамдани» усуллари ва экспертлар хулосаси ёрдамида ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонларини шакллантириш усули ишлаб чиқилган;

ахборот тизими компонентларининг хавфсизлик бўйича устуворликлари асосида ахборот тизимини баҳолаш усули ишлаб чиқилган;

ахборот тизими хавфсизлигининг хусусий ва қисм-тизим концептуал моделлари ёрдамида ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизимини шакллантириш, ахборот хавфсизлигини баҳолаш алгоритмлари ҳамда дастурий воситалари архитектураси ишлаб чиқилган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

эксперт хулосаси асосида ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонларини марказлашган ҳолда шакллантиришнинг дастурий воситаси ишлаб чиқилган;

ташкилот ахборот хавфсизлигини таъминлаш чораларини такомиллаштиришга ва ахборот хавфсизлигини ташкилот мутахассиси

томонидан баҳолашга имкон берувчи дастурий восита ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги қўйилган масаланинг математик жиҳатдан коррект ифодаланиши, ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари билимлар базасининг экспертлар томонидан шакллантирилиши, шунингдек ахборот хавфсизлигини баҳолашдаги назарий ва амалий тадқиқотлари ҳамда ишлаб чиқилган алгоритмлардан олинган реал ва тажрибавий таҳлиллар билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти таклиф этилган ахборот тизимини баҳолашнинг функционал, информацион, қисм-тизим концептуал моделлари асосида ахборот хавфсизлиги мезонларини шакллантириш ва ахборот тизими ҳимояланганлигини баҳолаш усуллари ва алгоритмларини ишлаб чиқиш билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти ахборот хавфсизлиги экспертларининг танқислиги масаласининг ечилишига имкон берувчи ахборот хавфсизлигини баҳолаш бўйича хулосаларни марказлашган ҳолда экспертлар томонидан шакллантирилиши, ахборот тизими хавфсизлигини баҳолаш эса ташкилот мутахассиси томонидан амалга оширилиши билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Ишлаб чиқилган ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонларини шакллантириш, ахборот тизимини баҳолаш усул ва алгоритмлари бўйича олинган натижалар асосида:

ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонларини шакллантириш ва ахборот тизимларини баҳолаш усуллари «Ўзбекистон почтаси» АЖ Хоразм филиалигажорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2018 йил 12 декабрдаги 33-8/9317-сон маълумотномаси). Илмий тадқиқот натижасида ахборот тизими ҳимояланганлигини баҳолаш, натижаларга ишлов бериш ва таҳлил этиш вақтини тежаган, ахборот тизими ҳимояланганлик даражасини баҳолаш ташкилотда ахборот хавфсизлигини такомиллаштириш бўйича келгуси ишларни режалаштириш ва воситаларнинг ҳимояланганлигини ошириш бўйича қарорларни қабул қилишда хизмат қилган;

ахборот тизими хавфсизлигининг хусусий ва қисм-тизим концептуал моделлари асосида ишлаб чиқилган дастурий восита «Ўзбектелеком» АК Хоразм филиалига жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2018 йил 12 декабрдаги 33-8/9317-сон маълумотномаси). Илмий тадқиқот натижасида ташкилот учун ахборот тизимини баҳолаш ва назорат қилиш, уни таҳлил этишга ҳамда назорат мезонларини шакллантириш имконини берган;

ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизимини шакллантиришнинг функционал ва информацион моделлари асосида ишлаб чиқилган дастурий восита дастурий маҳсулотларнинг ахборот хавфсизлигини

баҳолаш мақсадида «Mustafo software» МЧЖга жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2018 йил 12 декабрдаги 33-8/9317-сон маълумотномаси). Илмий тадқиқот натижаси хавфсизлик кўрсаткичларини шакллантиришда экспертлар билан мулоқот вақтини 12 марта камайтириш, ахборот хавфсизлигини баҳолашда кўрсаткичлар қийматларини ҳисоблашда экспертлар хулосасини олиш вақти ва хулосалар ҳажмини 20 мартадан кўпроқ камайтириш ҳамда ташкилот томонидан ишлаб чиқилаётган дастурий маҳсулотларнинг ахборот хавфсизлигини қисқа муддатда баҳолаш ва камчиликларни ўз вақтида бартараф этиш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 5 та халқаро ва 13 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертациянинг мавзуси бўйича жами 29 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 5 та мақола, 1 таси хорижий ва 4 таси республика журналларида нашр этилган ҳамда 2 та ЭҲМ учун яратилган дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертациянинг ҳажми 108 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 технологияларида ахборот хавфсизлигини баҳолашга ёндашувлар»** деб номланган биринчи боби ахборот коммуникация технологияларида ахборот хавфсизлигини баҳолаш муаммолари, баҳолаш соҳасидаги мавжуд меъёрий ҳужжат ва стандартлар ҳамда ахборот хавфсизлигини баҳолашнинг замонавий усуллари тадқиқига бағишланган.

Ахборотни ҳимоялаш сифатини баҳолаш масалаларини ечиш усул ва ёндашувларининг таҳлили шуни кўрсатадики, замонавий ахборот-коммуникация технологияларига мўлжалланган ахборотни ҳимоялаш тизимлари мураккаб инсон-машина тизими ҳисобланади. Умуман, бундай тизимнинг ишлаш сифатини баҳолаш фақат эксперт хулосаси ва

натижаларнинг кейинги талқини билан боғлиқ турли хил эвристик усуллар орқали амалга оширилиши мумкин. Аҳборотни ҳимоялаш тизимларининг ишлаш сифатини баҳолаш масаласини ечиш учун ахборотни ҳимоялаш тизимини синтезлашни оптималлаштиришга, тизим ишлаши самарадорлигини миқдорий баҳолашга ва бундай тизимларни қуришнинг турли вариантларини таққослашга имкон берувчи сифат кўрсаткичларидан фойдаланиш лозим.

Бундай масаланинг ўзига хослиги классик усуллар ёрдамида оптимал ечимни олишга имкон бермайди. Бундай шароитларда эксперт баҳоларини олиш зарурати билан боғлиқ норавшан тўпламлар назарияси ва эвристик ёндашувлар қўлланилади. Ушбу шароитларда нисбатан кичик вақт ва ҳисоблаш харажатларида баҳолашнинг юқори ишончлигини таъминлайдиган рутбали усулларнинг қўлланилиши эътиборга молик.

Ахборот хавфсизлигини баҳолаш борасида соҳанинг етакчи давлатлари томонидан бир қанча стандартлар ва меъёрий ҳужжатлар ишлаб чиқилган. Олиб борилган тадқиқотларда стандартларни универсаллик, мослашувчанлик, кафолатланганлик, амалга оширилувчанлик, долзарблик кўрсаткичлари бўйича таққослаш натижалари Умумий мезонлар (O‘z DSt ISO/IEC 15408 стандарти) нинг қолган стандартларга қараганда афзалликларга эга эканлиги аниқланди. Шу сабабли диссертация ишидаги кейинги барча тадқиқотлар ушбу стандартга асосланади.

Бугунги кунда ахборот хавфсизлигини баҳолаш борасида амалга оширилаётган ишларни иккита гуруҳга ажратиш мумкин. Биринчи гуруҳ хавф-хатар даражасини ахборот хавфсизлиги талабларига мослигини баҳолаш йўли билан ўрнатишга имкон беради. Иккинчи гуруҳ ҳужумларни амалга ошириш эхтимоллигини аниқлашга ва уларнинг зарар даражасига асосланади.

Ахборот хавфсизлигини баҳолаш усулларининг таҳлили шуни кўрсатадики, уларнинг энг муҳум муаммоси минимал автоматлаштирил-ганлигидир. Деярли барча усуллар ҳар бир қадамда маълумотларнинг белгиланган шаклда ва тартибда бўлишини талаб қилади, аммо улар берилган маълумотлардан бундай ахборотни шакллантириш механизмларига эга эмас. Бу усулларнинг яна битта камчилиги баҳоланаётган объектнинг ахборот хавфсизлиги хусусиятлари устуворлигини эътиборга олинмаслигидир.

Диссертациянинг **«Ахборот коммуникация технологиялари ҳимоя-ланганлигини баҳолашнинг хусусий концептуал модели»** деб номланган иккинчи боби ахборот тизимини баҳолаш жараёнида қўллашга мўлжалланган баҳолаш мезонлари ва улар орасидаги боғлиқликларни ўз ичига олувчи ахборот хавфсизлигини баҳолашнинг хусусий ва қисм-тизим концептуал моделларини қуришга бағишланган.

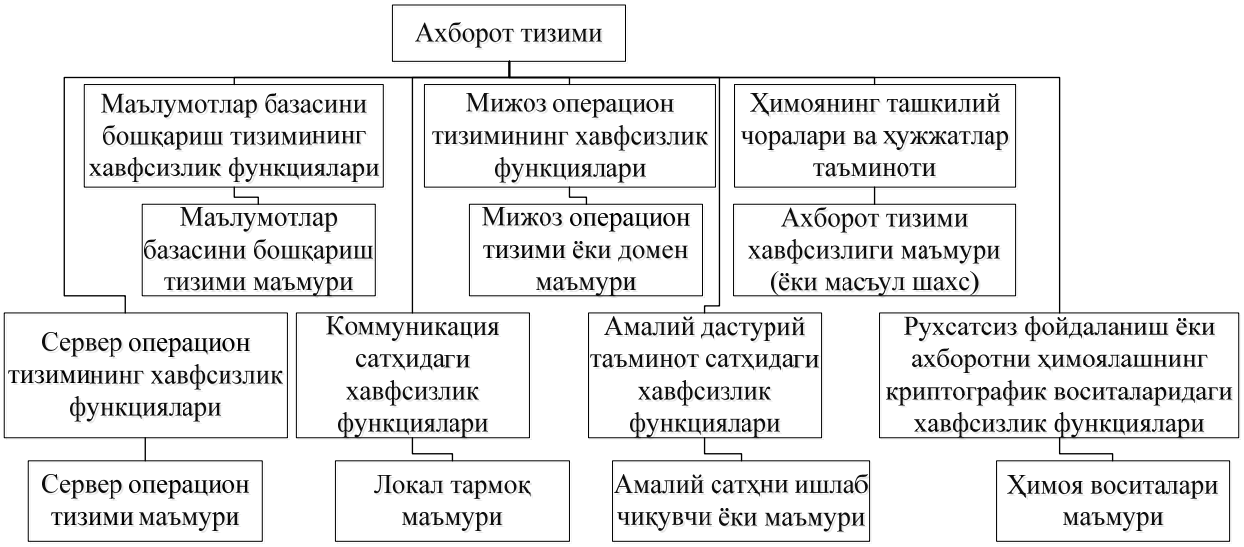
Ахборот тизимларида ҳимояланганликни назоратлаш, таҳлиллаш ва баҳолашни амалга ошириш учун ҳимояланганликни аниқловчи барча талаблар хавфсизликнинг хусусий модели кўринишида шакллантирилади.

Ахборот тизими хавфсизлиги ва унинг сатҳлари хавфсизлиги орасидаги муносабатларни қуйидагича ифодалаш мумкин:

$$H = H_{\text{СОТ}} \cup H_{\text{МББТ}} \cup H_{\text{ТС}} \cup H_{\text{МОТ}} \cup H_{\text{МИ}} \cup H_{\text{ХТ}}$$

Бу ерда Н–ахборот тизими хавфсизлиги, $H_{\text{СОТ}}$–сервер операцион тизими сатҳи хавфсизлиги, $H_{\text{МББТ}}$–маълумотлар базасини бошқариш тизими сатҳи хавфсизлиги $H_{\text{ТС}}$–тармоқ сервислари сатҳи хавфсизлиги, $H_{\text{МОТ}}$–мижоз операцион тизими сатҳи хавфсизлиги, $H_{\text{МИ}}$–махсус иловалар сатҳи хавфсизлиги, $H_{\text{ХТ}}$–ҳужжатлар таъминоти сатҳи хавфсизлиги.

Сатҳларга ажратиш жавобгарлик зоналари бўйича хавфсизликни назоратлаш имкониятини ҳам яратади. Ахборот тизими хавфсизлигининг хусусий концептуал модели 1-расмда келтирилган.



1-расм. Ахборот тизими хавфсизлигининг хусусий концептуал модели

Ахборот тизими компонентларининг хавфсизлик моделларига ҳимоя профилларидаги хавфсизликнинг барча функционал талаблари киритилган бўлиши лозим. Чунки бу талаблар хавфсизлик таҳдидлари ва мақсадлари билан мослаштирилган. Бундан ташқари, ҳар бир функционал талабнинг (кўрсаткич) ўзаро боғлиқлигини кузатиш зарур. Кўрсаткичлар боғлиқликлари хусусий хавфсизлик моделларига киритилган бўлиши ва ахборот тизими структурасининг бирор сатҳида қаноатлантирилиши лозим. Яъни боғлиқлик сервер операцион тизим, маълумотлар базасини бошқариш тизими, тармоқ сервислари, мижоз операцион тизими, махсус иловалар ва ҳужжатлар таъминоти мос сатҳида қаноатлантирилиши лозим.

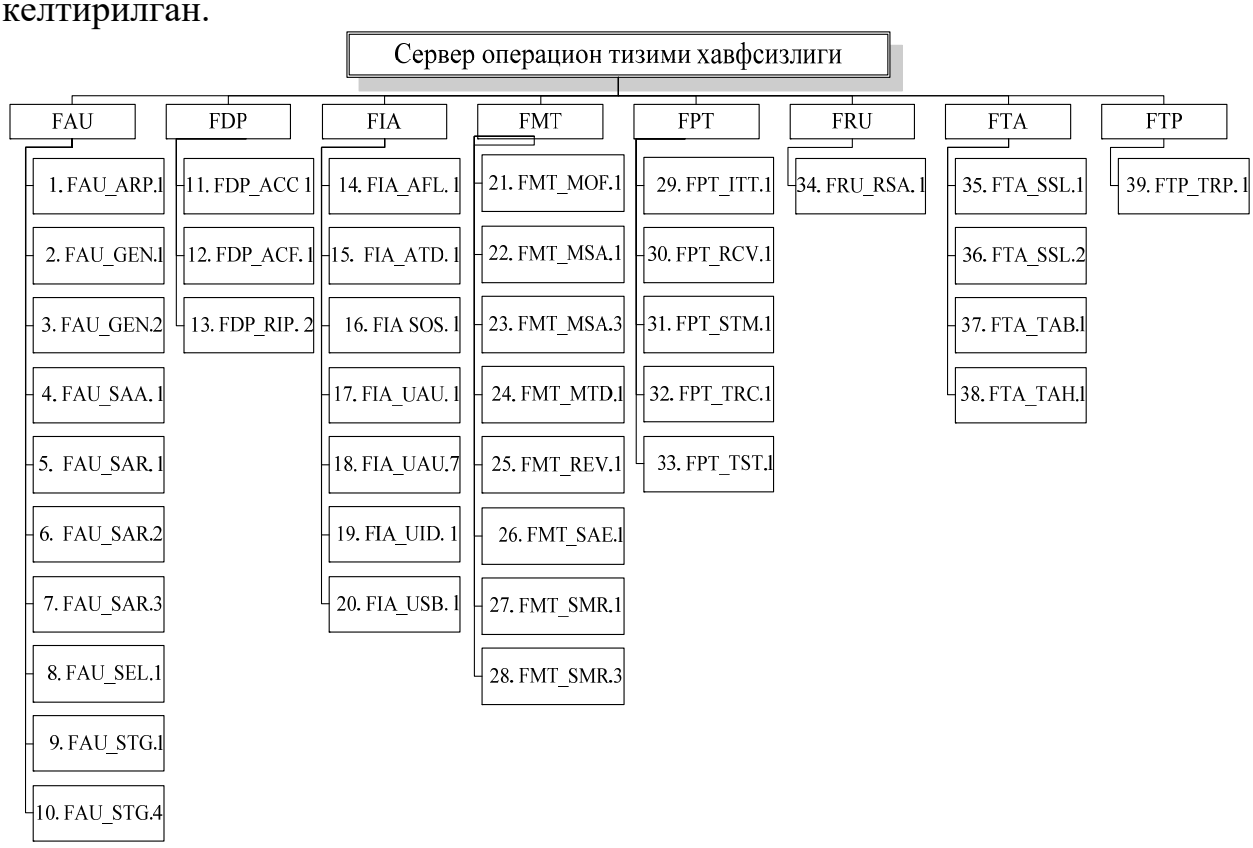
Ахборот тизими таркибий компоненти хавфсизлигини баҳолашнинг қисм-тизим моделини қуриш Умумий мезонлар атамаларидан фойдаланган ҳолда ва аниқ бир ташкилот ахборот хавфсизлиги сиёсатини, ресурсларга бўлган хавфсизлик таҳдидларини ва тахминларини инобатга олган ҳолда амалга ошириш таклиф этилади.

Сервер операцион тизими хавфсизлигини баҳолашнинг қисм-тизим концептуал моделини шакллантириш файл тизими, чоп этиш хизмати, тармоқ хизматлари, маълумотларни архивлаш хизмати ва бошқа иловаларга

(масалан, почта, маълумотлар базаси) эга умуммўлжалланган кўп фойдаланувчили операцион тизим учун танланган ҳимоя профилидан (таянч ҳимоя профилидан) иборат.

Танланган ҳимоя профили тўлиқ ва асосланган талаблар тўпламига эга бўлиб, бу талабларнинг қаноатлантирилиши активлар учун ўртача хавф-хатар даражаси мавжуд муҳитда етарлича ҳимояланганлик даражасини таъминлайди. Ушбу хавф-хатар даражасига мос ҳолда эҳтимоллик ва алмаштириш (криптографик эмас) механизмлари асосида амалга ошириладиган ишончлилик талаби ва хавфсизлик функцияларининг ўртача барқарорлиги таъминланади.

Ҳимоя профили талабларига жавоб берувчи операцион тизим махфий маълумотлар ишланадиган муҳитни мададлайди. Бундай имкониятнинг мавжудлиги операцион тизимда идентификаторлар асосида амалга ошириладиган мурожаатларнинг дискрецион бошқарувини таъминлаш талаб этилади. Операцион тизимнинг хавфсизлик функциялари фойдаланувчига бирор амалга рухсат этишдан олдин тақдим этган идентификаторнинг ҳақиқийлиги тасдиқланиши лозим. 2-расмда сервер операцион тизими хавфсизлигини баҳолашнинг қисм-тизим концептуал моделининг схемаси келтирилган.

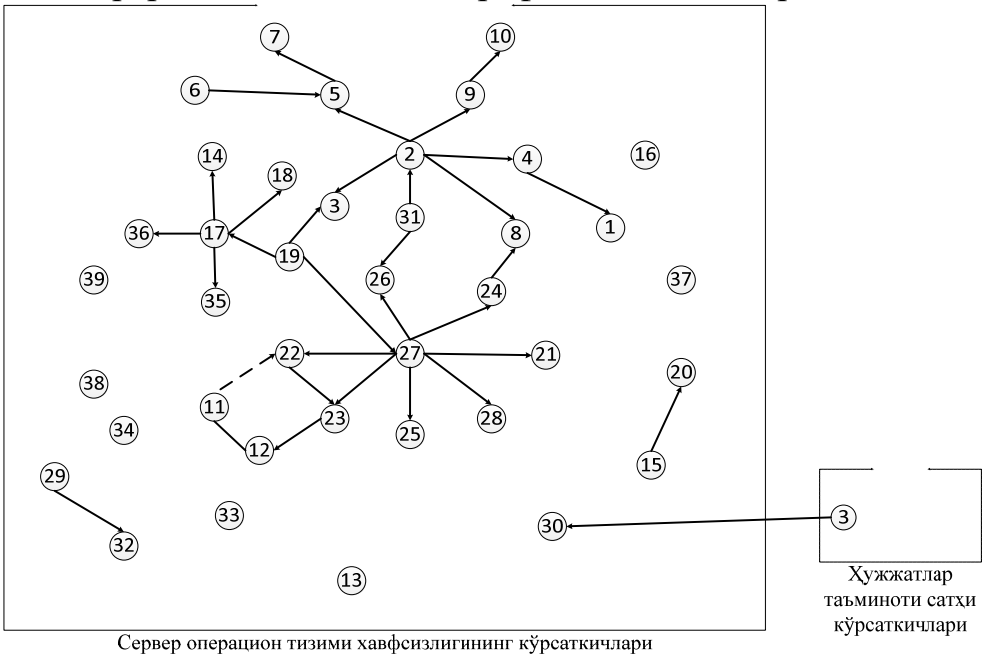


2-расм. Сервер операцион тизими хавфсизлигини баҳолашнинг қисм-тизим концептуал модели схемаси

Хавфсизликни баҳолашнинг яратилган қисм-тизим моделига сервер операцион тизим сатҳида маълумотлар ҳимоясига таъсир қилувчи 39 та кўрсаткич киради, улардан 14 таси мустақил кўрсаткичлар, 26 таси ҳисобга

олинган ички боғлиқликка эга ва 1 та кўрсаткич ҳужжатлар таъминоти сатҳи ишонч талаблари (етказиб бериш ва эксплуатациянинг тўғрилиги синфи) билан сатҳлараро боғлиқликка эга.

3-расмда сервер операцион тизими хавфсизлиги кўрсаткичларининг ўзаро ва сатҳлараро боғлиқлигининг граф-схемаси келтирилган.



3-расм. Сервер операцион тизими хавфсизлиги кўрсаткичларининг ўзаро ва сатҳлараро боғлиқлигининг граф-схемаси

Диссертация ишида маълумотлар базасини бошқариш тизими, тармоқ сервислари, мижоз операцион тизими, махсус иловалар ва ҳужжатлар таъминоти сатҳлари хавфсизлигини баҳолашнинг ҳам қисм-тизим концептуал моделлари ишлаб чиқилган.

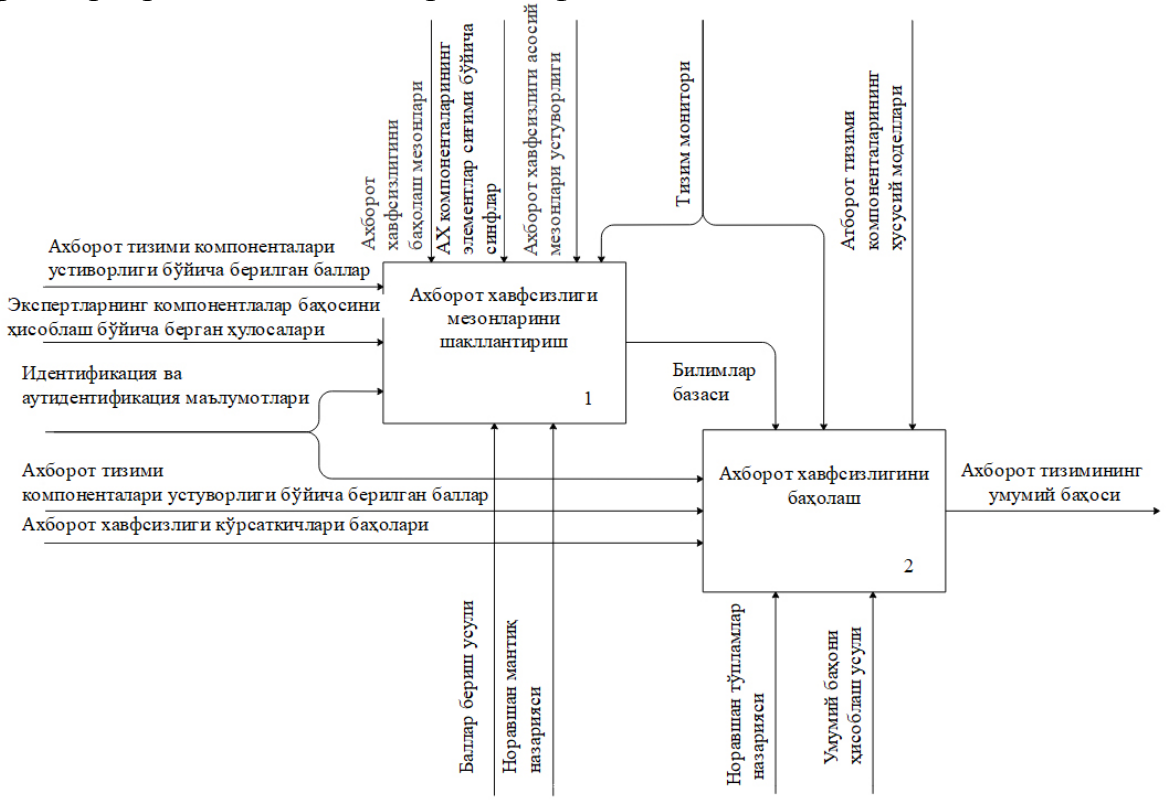
Диссертация ишининг «**Ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизимини шакллантириш**» номли учинчи бобида қисм-тизим концептуал моделларига асосланган ахборот технологиялари компонентларининг хавфсизлигини баҳолашга имкон берувчи кўрсаткич ва мезонлар тизимини шакллантириш модели ва алгоритми келтирилган.

Ахборот хавфсизлиги кўрсаткич ва мезонлари тизимини шакллантириш моделини яратишда IDEF0 методологиясидан фойдаланилди. Маълумки, IDEF0 методологияси тизимни иерархик диаграммалар кўринишида тавсифлайди. Аввал тизимни бир бутун кўриниши ва ташқи дунё билан алоқалари ёритиб берилади, сўнгра декомпозицияси амалга оширилади (4-расм). Тизим декомпозиция натижасида қуйи тизимларга ажратилади ва ҳар бир қуйи тизим алоҳида тавсифланади. Шу тариқа талаб даражасидаги деталларга эришилади.

Ҳар бир диаграмма блоклар ва ёйлардан ташкил топган бўлиб, блоклар лойиҳаланаётган тизим функцияларини тавсифлайди, ёйлар эса блокларнинг ўзаро таъсир ва алоқаларини ифодалайди.

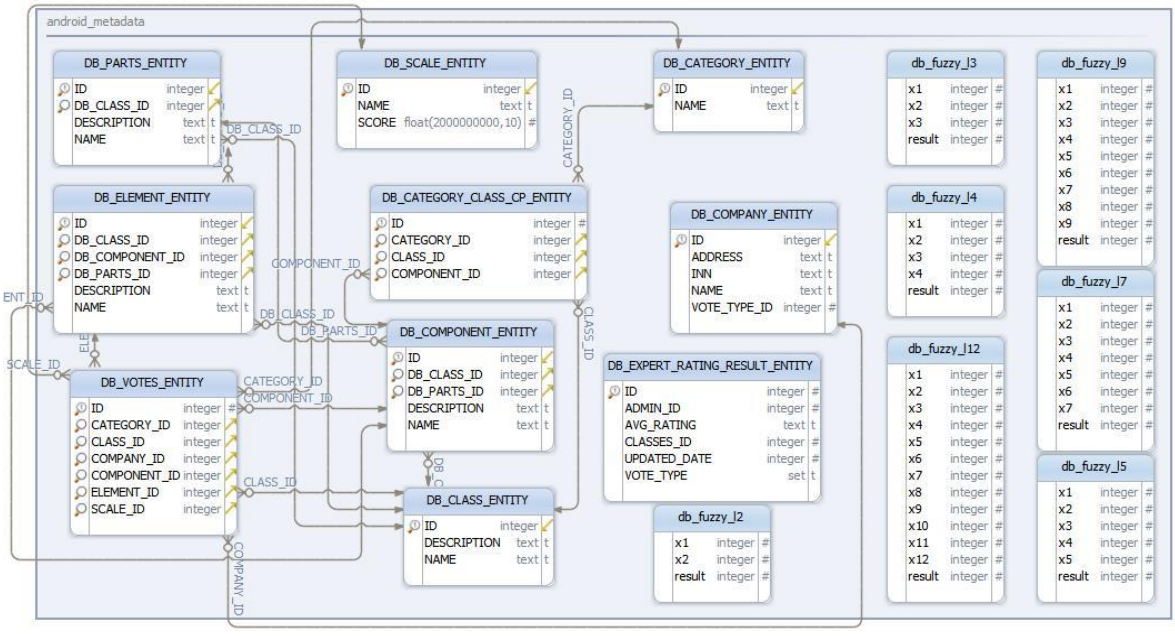
Диаграммага биноан чапдан келган параметрлар кирувчи

маълумотларни, юқоридан келган параметрлар бошқарувчи маълумотларни, пастдан келган параметрлар механизмларни, блокнинг ўнг томонида чиқувчи параметрлар натижавий ахборотни ифодалайди.



4-расм. Ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонларини шакллантириш тизимининг декомпозицияси

Ахборот тизими хавфсизлигини баҳолаш дастурий воситаси маълумотлар базасининг структураси IDEF1X методологияси асосида ишлаб чиқилган ва у қуйидаги 17 та жадвалдан ташкил топган (5-расм).



5-расм. Ахборот тизими хавфсизлигини баҳолаш дастурий воситаси маълумотлар базасининг IDEF1X модели

Ахборот хавфсизлиги кўрсаткич ва мезонлари тизимини шакллантириш экспертлар гуруҳи томонидан ахборот хавфсизлигининг асосий учта принципи махфийлик, фойдаланувчанлик ва яхлитликнинг устуворликлари асосида ахборот хавфсизлиги мезонларига баллар бериш ва берилган баллар асосида уларнинг салмоқлилик коэффицентларини аниқлаш ҳамда ахборот тизимининг хавфсизлигини баҳолаш бўйича экспертлар хулосасини олиш, норавшан мантиқ назарияси асосида қоидалар ишлаб чиқишдан иборат. Кўрсаткичларга берилган баҳолар асосида ахборот тизимининг ҳимояланганлик даражасини ҳисоблаш амалга оширилади.

Ахборот тизимининг ҳимояланганлигини баҳолашга қаратилган ҳодисаларнинг бажарилиш кетма-кетлигини белгиловчи алгоритмни қуйидагича ёзиш мумкин:

1. Экспертлар томонидан ахборот хавфсизлиги принциплари устуворлиги асосида ахборот хавфсизлиги кўрсаткич ва мезонларига баллар бериш ҳамда улар асосида маълумотлар базасини шакллантириш.

2. Билимлар базасини шакллантириш. Баҳолашда лингвистик шкалани аниқлаш. Тегишлилик функциясини қуриш.

3. Норавшан маълумотларнинг қоидалар базасини яратиш. Мазкур қоидалар негизида зиддиятлар ва пайдо бўлган мураккаб вазифаларни ҳал қилиш. Олинган баҳоларни дефаззификациялаш.

4. Ахборот тизими компонентларининг устуворлигини аниқлаш ва салмоқлилик коэффицентини ҳисоблаш.

5. Ахборот тизимининг барча компонентларини ахборот хавфсизлиги мезонларининг энг қуйи сатҳи (элементлари) асосида лингвистик атамалар орқали баҳолаш.

6. Зарурат туғилганида, ахборот хавфсизлиги мезонларининг компонентлари баҳоларини билимлар базаси асосида тегишлилик функцияси орқали ҳисоблаш.

7. Кўрсаткичлар ўртасидаги боғлиқликларни ҳисоблаш. Ўз навбатида хавфсизлик мезонларининг оила ва синфлари баҳосини ҳисоблаш.

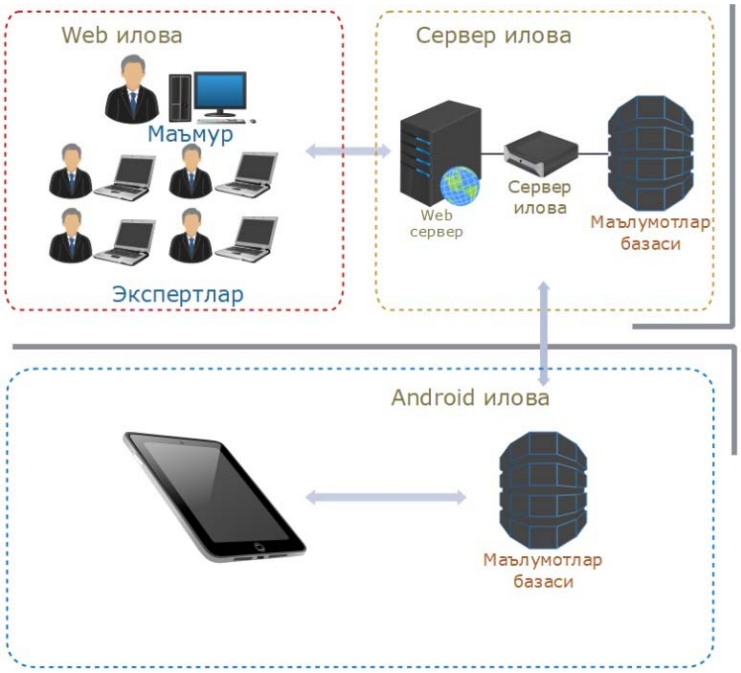
8. Ахборот тизими компонентлари ва тизимнинг умумий баҳосини ҳисоблаш.

9. Баҳолаш натижаларини таҳлиллаш. Ҳисоботни расмийлаштириш.

Диссертациянинг «**Ахборот хавфсизлигини баҳолашнинг дастурий воситаларини ишлаб чиқиш ва тажриба-ҳисоблаш натижалар**» номли тўртинчи бобида диссертациянинг иккинчи ва учинчи бобларида ишлаб чиқилган моделлар асосида ахборот хавфсизлигини баҳолаш тизими дастурий воситаларининг архитектураси ҳамда хавфсизликни баҳолаш бўйича тажриба-ҳисоблаш натижалари келтирилган.

Ташкилотда ахборот тизими хавфсизлигини баҳолаш экспертлар хулосаси бўйича шакллантирилган билимлар базасига асосланиб ташкилот ходими томонидан амалга оширилади.

Ахборот хавфсизлигини баҳолаш тизими дастурий воситалари ишлаб чиқилган–Web илова, сервер илова ва Android илова (6-расм).



6-расм. Ахборот хавфсизлигини баҳолаш дастурий воситасининг структураси

Web иловадан маъмур ва ахборот хавфсизлиги экспертлари фойдаланади. Маъмур ахборот хавфсизлиги бўйича экспертлар учун профил яратиш, уларни ўчириш ҳамда экспертларнинг фикрлари асосида хавфсизлик мезонларининг салмоқлилик коэффицентларини ҳисоблаш ишларини амалга оширади. Экспертлар эса хавфсизлик принциплари комбинациялари бўйича хавфсизлик мезонларига баллар ва ахборот хавфсизлиги компонентлари баҳоларини ҳисоблаш учун хулосалар беради.

Сервер илова Web иловадан олинган маълумотларни базага ёзади ва хавфсизлик мезонларининг салмоқлилик коэффицентларини ҳисоблайди. Бундан ташқари, Android иловадан келган сўров асосида унинг билимлар базасини янгилайди.

Android илова серверидан билимлар базасини юклаб олинганидан сўнг мутахассис Android иловага баҳоланаётган ахборот тизими моделини, яъни унинг компонентларининг устуворлиги киритилади. Бундан ташқари, ахборот тизими компонентларининг ахборот хавфсизлиги талабларининг элементларига қай даражада жавоб бериши баҳоланади ва натижавий баҳо фойдаланувчига тақдим этилади.

Маълумки, ахборот тизимида қўлланилувчи ҳимоя механизмларининг сифати ташкилот хавфсизлик сиёсатини қамраб олувчи ва эксплуатация доирасида таҳдидларга қарши тура оладиган хавфсизликнинг функционал талабларининг бажарилиши даражаси билан белгиланади. Бунда, ҳимоя сифатига турли кўрсаткичларнинг таъсир даражаси ҳар хил бўлади. Шу боисдан талаб қилинаётган хавфсизлик функциясининг бажарилиш кўрсаткичининг муҳимлигини белгилаш учун ташкилотда қабул қилинган ахборот хавфсизлиги сиёсатини устуворлик билан юритиш усули таклиф қилинган (1-жадвал).

1-жадвал

Ахборот хавфсизлиги прицпларининг устуворлиги

Устуворлик	Ахборот хавфсизлигининг асосий принциплари					
1-ўрин	М	Я	Ф	Я	М	Ф
2-ўрин	Я	Ф	М	М	Ф	Я
3-ўрин	Ф	М	Я	Ф	Я	М

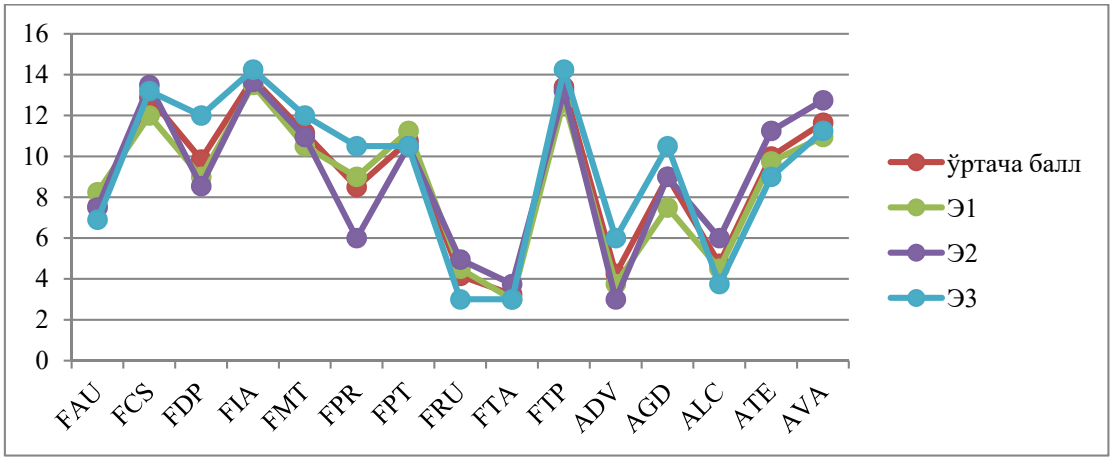
Жадвалдаги М-махфийлик, Я-яхлитлик, Ф-фойдаланувчанлик.

Ушбу усул экспертлар гуруҳи томонидан ҳар бир мезонни [0-100] оралиғида муҳимлиги бўйича баҳолашга асосланган. Бу эса бир нечта экспертларнинг мезонлар муҳимлиги бўйича берган балларини умумлаштириб сон кўринишида ёзишга имкон беради.

m та мезонларнинг муҳимлиги бўйича *k* та эксперт баҳолаган бўлсин. У ҳолда мезонларга қўйилган баҳони $H = \|h_{ij}\|$ матрица кўринишида ёзиш мумкин, бу ерда h_{ij}–*i*-экпертнинг *j*-мезонга қўйган бали.

Экспертлар фикрларининг мувофиқлигини белгиловчи мезон қанчалик юқори бўлса, уларнинг фкрлари шунчалик ишончли бўлади.

Эксперт фикрларининг мувофиқлигини ўртача балга $\overline{h_i}(i=1,...,m)$ нисбатан аниқлаш қулай, яъний: $\overline{h_i} = \frac{m}{k*100}\sum_{j=1}^{k} h_{ij}$. Бунга асосан 7 - расмда экспертларнинг ахборот хавфсизлиги мезонлари синфларига берган баллари тасвирланган.



7-расм. Экспертларнинг ахборот хавфсизлиги мезонлари синфларига берган баллари

Ўртача балл дисперсияси қуйидаги формула орқали ҳисобланади $D(\bar{h}) = \frac{1}{m}\sum_{i=1}^{m}(\overline{h_i} - \bar{\bar{h}})^2$, бу ерда $\bar{\bar{h}} = \frac{1}{m}\sum_{i}^{m}\overline{h_i}$. Максимал дисперсия қуйидагича ҳисобланади (бу экспертларнинг фикри мутлақо бир хил бўганидаги ҳолат) $D_{\text{макс}}(\bar{h}) = \frac{1}{m}\sum_{i=1}^{m}(i - \frac{m+1}{2})^2 = \frac{m^2-1}{12}$, экспертлар фикрларининг мувофиқлиги мезони қуйидаги формула орқали ҳисобланади: $W = \frac{D(\bar{h})}{D_{\text{макс}}(\bar{h})} = \frac{12}{m(m^2-1)}\sum_{i=1}^{m}(\bar{h} - \frac{m+1}{2})^2$. Кўриниб турибдики, 0≤W≤1. W = 0 да экспертлар фикрлари умуман бир-бирига мос келмайди ва W = 1 да уларнинг

фикрлари мутлақо бир хил. Шундай қилиб, W қиймати экспертлар фикрларнинг мувофиқлик даражасини белгилайди.

Юқорида келтирилган матрица элементларини $h_i = \sum_{j=1}^{k} h_{ij}$ вектор кўринишида ёзиш ва $r_{ij} = \frac{h_{ij}}{h_i}$ га асосан муҳимлилик коэффицентларини аниқлаш мумкин. Ушбу матрица $r_j = \sum_{i=1}^{m} r_{ij}$ вектор кўринишда ёзилади ва мезонларнинг салмоқлилик коэффициенти $\lambda_i = \frac{r_i}{\sum_{j=1}^{k} r_j}$ ҳисобланади, бу ерда λ-хавфсизлик синфларининг салмоқлилик коэффициенти ($\sum_{i=1}^{n} \lambda_i = 1$).

Маълумки, ташкилотнинг ахборот хавфсизлигини баҳолашда ҳар доим ҳам экспертлар иштирок эта олмайди, шу сабабли ташкилот мутахассиси хизматидан фойдаланишга тўғри келади. Шунинг учун ахборот хавфсизлигини баҳолашда қуйидаги лингвистик атамалардан фойдаланиш мақсадга мувофиқ ҳисобланади: «мос келмайди»; «қисман мос келади»; «асосан мос келади»; «мос келади».

Лингвистик ўзгарувчилар <X, T, U> учлиги орқали белгиланади. Бу ерда X–ўзгарувчи номи, T–терм (элемент) тўплами, ҳар битта терм U универсал тўпламда норавшан тўплам кўринишида намоён бўлади.

Қўйилган масалада X=«элемент баҳоси», T={«мос келмайди», «қисман мос келади», «асосан мос келади», «мос келади»}, Y={0;0,3;0,7;1},

Компонентлар сиғими бўйича экспертлардан олинган ахборот асосидаги қоидалар тўпламини қуйидагича шакллантириш мумкин:

1-қоида: Агар x_{11} ва x_{12} ва ... ва x_{1n} бўлса y_1;

...

l+1-қоида: Агар x_{l+11} ва x_{l+12} ва ... ва x_{l+1n} бўлса y_2;

...

m+1-қоида: Агар x_{m+11} ва x_{m+12} ва ... ва x_{m+1n} бўлса y_3;

...

j+1-қоида: Агар x_{j+11} ва x_{j+12} ва ... ва x_{j+1n} бўлса y_4;

Ташкилот ахборот хавфсизлиги сиёсати асосида ахборот тизимининг компонентларига хавфсизлик бўйича устуворликлар билан бирга компонентларнинг хусусиятларига асосан ахборот хавфсизлиги принципларининг устуворликлари ҳам белгиланади (2-жадвал).

2-жадвал

Баҳоланаётган ахборот тизими компонентларининг устуворликлари

Ахборот тизимининг компонентлари	СОТ	МББТ	ТС	МОТ	МИ	ХТ
Ахборот хавфсизлиги принципларининг устуворликлари	МФЯ	ФМЯ	ФМЯ	ФЯМ	ФМЯ	МЯФ
R_i-ахборот тизими компонентларининг устуворлиги	r_i	r_i	r_i	r_i	r_i	r_i

Ҳар бир *i*-компонентнинг $W_i = 1 - \frac{R_i - 1}{M}; i = \overline{1, M}$ салмоқлилик коэффициентлари аниқланади, *M*-компонентлар сони.

Салмоқлилик коэффициентларини нормаллаштириш $\lambda_k = \frac{W_k}{\sum_{i=1}^{M} W_i}$ орқали амалга оширилади, бу ерда λ_k-синфлар муҳимлигига мувофиқ нормаллаштирилган салмоқлилик коэффициентлари ($\sum_{i=1}^{m} \lambda_i = 1$).

Кейинги босқичда диссертациянинг иккинчи бобида ишлаб чиқилган қисм-тизим концептуал моделларига асосан ахборот тизими компонентларининг ахборот хавфсизлиги мезонларига қай даражада жавоб бериши ташкилот мутахассиси томонидан баҳоланади.

Айтайлик, сервер операцион тизими ахборот хавфсизлигининг мезонларининг FDP_ACF.1 «Хавфсизлик атрибутларига асосланган фойдаланишни бошқариш» компоненти талабларига жавоб бериши баҳолансин. FDP_ACF.1 компонент 4 та FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3 ва FDP_ACF.1.4 элементлардан иборат. Сервер операцион тизимнинг талабларга жавоб бериши ахборот хавфсизлиги мутахассиси томонидан қуйидагича баҳоланган бўлсин:

– FDP_ACF.1.1-қисман мос келади;
– FDP_ACF.1.2-қисман мос келади;
– FDP_ACF.1.3-асосан мос келади;
– FDP_ACF.1.4-асосан мос келади.

N та элементдан иборат компонентлар баҳосини ҳисоблаш учун экспертлар томонидан қурилган қоидалар тўплами $X = \|x_{ij}\|$ матрица кўринишида ифодаланади, бу ерда $i = \overline{1, n}$, $j = \overline{1, k}$, *n*–ахборот хавфсизлиги мезонларининг компонентидаги элементлар сони, *k*–қоидалар сони.

Агар элементлар баҳолари $A=\{a_1, a_2, \ldots, a_n\}$ бўлса, компонент баҳосини аниқлаш Гаусс тегишлилик функцияси $\mu_{ij} = e^{\frac{(a_j - x_{ij})^2}{2*\sigma}}$ ёрдамида амалга оширилади ва $M = \|\mu_{ij}\|$ матрица қурилади ҳамда ҳар бир сатр учун минимум ҳисобланади, яъни $min_i = min(\mu_{i1}, \mu_{i2}, \ldots, \mu_{in})$.

Ҳар бир терм ҳосил бўладиган қоидалар тўпламига алоҳида максимум аниқланади: $max_1 = max(min_1, min_2, \ldots, min_l)$; $max_2 = max(min_{l+1}, min_{l+2}, \ldots, min_r)$; $max_3 = max(min_{r+1}, min_{r+2}, \ldots, min_j)$; $max_4 = max(min_{j+1}, min_{j+2}, \ldots, min_k)$.

Компонентнинг баҳоси қуйидагича ҳисобланади:

$$X_{\text{компонент}} = \frac{y_1 * max_1 + y_2 * max_2 + y_3 * max_3 + y_4 * max_4}{max_1 + max_2 + max_3 + max_4}$$

Кейинги босқичда диссертациянинг иккинчи бобида ишлаб чиқилган қисм-тизим концептуал моделлар асосида ахборот хавфсизлиги компонентларининг боғлиқликлари ҳисобланади.

Агар ахборот хавфсизлиги компонентлари бевосита боғлиқликка эга бўлса (масалан, FAU_GEN.2 кўрсаткичи FAU_GEN.l ва FIA_UID.1 кўрсаткичларига бевосита боғлиқликка эга), уларнинг қиймати қуйидаги формула орқали ҳисобланади. $x_{1,3} = \lambda_3 \cdot x_{1,3} \cdot \left| \frac{\lambda_2 \cdot x_{1,2} + \lambda_{19} \cdot x_{1,19}}{\lambda_2 - \lambda_{19}} \right|$, бу ерда λ_2, λ_3,

λ_{19} - мос компонентларнинг салмоқлилик коэффициенти, $x_{1,2}$, $x_{1,3}$, $x_{1,19}$- компонентларнинг қийматлари.

Агарда компонентлар танланма боғлиқликга эга бўлса (масалан, FDP_ETC.2 компоненти FDP_ACC.l ёки FDP_IFC.1 компонентлари билан танланма боғлиқликка эга) уларнинг қиймати қуйидаги формула орқали ҳисобланади $x_{3,12} = \lambda_{12} \cdot x_{3,12} \cdot \max[\lambda_{10} \cdot x_{3,10}; \lambda_{13} \cdot x_{3,13}]$.

Кейинги босқичда ахборот хавфсизлиги оилаларини баҳолаш, аддитив кўрсаткич усулидан фойдаланган ҳолда, амалга оширилиши мумкин. $X_j = \sum_{k=1}^{n} \lambda_k X_{kj}$; $\overline{X_j} \leq 1$, бу ерда X_j-j-оила баҳоси.

ХУЛОСА

«Ахборот хавфсизлиги кўрсаткич ва мезонлари тизимини шакллантириш усуллари ва алгоритмлари» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Ахборот тизими компонентлари конфигурациясини акслантирувчи хусусий ва қисм-тизим концептуал моделлари ишлаб чиқилди. Ишлаб чиқилган моделлар ташкилот ахборот хавфсизлиги сиёсатида белгиланган ёндашувларни шакллантириш имконини берди.

2. IDEF0 методология асосида ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизимини шакллантиришнинг функционал модели ҳамда IDEF1X методология асосида ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизими маълумотлар базасининг информацион модели ишлаб чиқилди. Ишлаб чиқилган моделлар дастурий воситаларни лойиҳалашга ва уларга тегишли бўлган барча маълумотларни сақлаш ва ундан фойдаланишга имкон берди.

3. Экспертлар хулосаси асосида ахборот хавфсизлигини баҳолаш мезон ва кўрсатқичларини шакллантириш ҳамда ахборот тизими хавфсизлигини баҳолаш усуллари ишлаб чиқилди. Ишлаб чиқилган усуллар ташкилот мутахассисига ахборот тизими хавфсизлигини баҳолаш имконини беради.

4. Қисм-тизим концептуал моделлари асосида ахборот тизимини баҳолаш усули ишлаб чиқилди. Ишлаб чиқилган усул ахборот тизими хавфсизлигининг ҳолатини аниқлашда ва ахборотни ҳимоялаш чораларини такомиллаштиришда асосли қарор қабул қилиш имконини берди.

5. Яратилган моделлар ва усуллар асосида ахборот хавфсизлигини баҳолаш кўрсаткич ва мезонлари тизимини шакллантириш ва ахборот хавфсизлигини баҳолаш дастурий воситаларининг архитектураси таклиф этилди. Архитектура асосида ишлаб чиқилган дастурий воситалар ахборот хавфсизлиги кўрсаткич ва мезонларини марказлашган ҳолда шакллантирилиши экспертлар танқислиги масаласини ечишда самарали натижалар беради.

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

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ХАЛМУРАТОВ ОМОНБОЙ УТАМУРАТОВИЧ

МЕТОДЫ И АЛГОРИТМЫ ФОРМИРОВАНИЯ СИСТЕМЫ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ 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 B2017.1.PhD/T55.

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:	**Каримов Маджит Маликович** доктор технических наук, профессор
	Курязов Давлатёр Матякубович кандидат физико-математических наук
Ведущая организация:	**Национальный университет Узбекистана**

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 стремительное развитие массового производства и эксплуатации информационных технологий привело к увеличению числа угроз безопасности, в частности, «согласно статистическим данным компании McAfee, в 2017 году количества общего ущерба по всему миру от киберпреступности увеличился на 35 % чем в 2014 году»[1]. В связи с этим большое внимание уделяется разработке инструментов для оценки безопасности информационных систем и повышения их эффективности. В этом направлении в развитых странах, таких как США, Российская Федерация, Канада, Франция и других странах разработка информационных технологий требуемого уровня и создания критериев, позволяющих оценить информационную безопасность, имеет важную роль.

В мире проводятся научно-исследовательские работы, направленные на разработки методов оценки безопасности информационной системы на основе формирования показателей и критериев информационной безопасности. В частности, при оценке информационной безопасности важными задачами являются выбор профиля безопасности, учитывая компонентов информационной системы, свойств обменных данных, разработка методов контроля информационной безопасности, учитывая приоритетности компонентов информационной системы и критериев безопасности. Вместе с этими необходимо научно обосновать усовершенствование процессов управления информационной безопасности организации на основе оценки информационной безопасности.

В республике наряду с развитием информационных технологий в органах государственного и хозяйственного управления реализуются комплексные меры напраленные на защиту от угроз и внедрению методов и средств их оценки. В стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 годы поставлены задачи, в частности, «…совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере, …внедрение информационно-коммуникационных технологий в экономику, социальную сферу, системы управления»[2]. Реализация поставленных задач, в том числе оценка информационной безопасности организаций и разработка моделей, методов и алгоритмов совершенствование системы ее показателей и критериев является одним из важных задачей.

Диссертационное исследование в определенной мере послужит выполнению задач, поставленных в следующих документах: Указ Президента Республики Узбекистан №УП-4947 «О стратегии действий по

[1] http://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности

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

дальнейшему развитию Республики Узбекистан» от 7 февраля 2017 года, Указ Президента Республики Узбекистан №УП-5379 «О мерах по совершенствованию системы государственной безопасности Республики Узбекистан» от 14 марта 2018 года, Указ Президента Республики Узбекистан №УП-5349 «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций» от 19 февраля 2018 года, Постановления Президента Республики Узбекистан № ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» от 21 ноября 2018 года и другие нормативно-правовые документы, относяшиеся к ссответствующей сфере деятельности.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Исследование выпольнено в рамках приоритетного направления IV. «Информатизация и развитие информационно - коммуникационных технологий» развиятия республиканской науки и технологии.

Степень изученности проблемы. Ученые различных организаций многих стран провели исследования по разработке показателей и критериев информационной безопасности, среди которых Варфоломеев А.А., Домарев В.В., Калужский М.Л., Ажмухамедов И.М., Берестнева О.Г., Самохвалов Ю.Я., Герасимов Б.М., Павлов А.Н., В.Ф. Шаньгин, Д.П. Зегжда проводящие в нынешнее время научно-исследовательскую работу.

В Узбекистане под руководством Бекмуратова Т.Ф., Арипова М.М., Ғаниева С.К., Каримова М.М., Хамдамова Р.Х., Мухаммадиевой Д.Т. научными коллективами изучены процессы формирования базы знаний на основе экспертных заключений, формирования показателей и критериев информационной безопасности, методы оценки защищенности информационной системы.

В настоящее время задача формирования показателей и критериев оценки информационной безопасности на основе централизованных экспертных заключений и формирование методов оценки на основе приоритетности критериев информационной безопасности, а также специфики компонентов иформационной системы организации недостаточно изучены.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках научного проекта согласно плану научно-исследовательских работ Ташкентского университета информационных технологий и Ургенчского филиала ТУИТ по темам №Ф4-019 «Исследование проблем формирования систем показателей и критериев информационной безопасности» (2012-2016) и № Ф636-16 «Разработка программного обеспечения оценки информационной безопасности информационно-коммуникационных систем» (2016).

Цель исследования – формирование системы показателей и критериев информационной безопасности и разработка методов и средств оценки информационной безопасности информационных систем.

Задачи исследованеия:

разработка частных и подсистемных концептуальных моделей процесса оценки информационной безопасности;

создание функциональных и информационных моделей системы показателей и критериев информационной безопасности;

разработка алгоритма формирования системы показателей и критериев информационной безопасности;

разработка метода оценки информационной системы на основе приоритетности безопасности компонентов информационной системы;

создание программного средства системы оценки информационной безопасности.

Объектом исследования является процесс оценки защищенности информационной системы.

Предметом исследования является формирование показателей и критериев информационной безопасности, а также методы и алгоритмы оценки информационной безопасности.

Методы исследования. В процессе исследования использовались методы анализа защищенности информации, неформальная логика и теория неформальных множеств, теория графов и объектно-ориентированное программирование.

Научная новизна исследования состоит из следущего:

на основе особенностей организации и компонентов информационной системы разработаны частные и подсистемные концептуальные модели безопасности информационной системы;

разработаны функциональные и информационные модели формирования системы показателей и критериев оценки информационной безопасности на основе методологии IDEF0 и IDEF1X;

при помощи методов приписывания баллов, ранжирования, теории неформальной логики «Мамдани» и экспертных заключений разработан метод формирования показателей и критериев оценки информационной безопасности;

на основе приоритетности безопасности компонентов информационной системы разработана методика оценки информационной системы;

при помощи частной и подсистемной концептуальных моделей безопасности информационных систем сформирована система показателей и критериев оценки информационной безопасности, разработаны алгоритмы оценки информационной безопасности и архитектура их программного обеспечения.

Практические результаты исследования состоят из следующего:

на основе экспертных заключений разработано программное средство для централизованного формирования показателей и критериев оценки

информационной безопасности;

разработано программное средство, позволяющее усовершенствовать меры информационной безопасности организации и проводить оценку информационной безопасности специалистами организации.

Достоверность результатов исследования. Достоверность результатов исследования объясняется корректностью математических выражений интерпретирующих проблему, формированием показателей и критериев оценки информационной безопасности экспертами базы знаний, а также теоретическими и практическими исследованиями в области оценки информационной безопасности, а также реальным и экспериментальным анализом разработанных алгоритмов.

Научная и практическая значимость результатов исследования. Научная значимость полученных результатов исследований заключается в разработке методов и алгоритмов формирования критериев информационной безопасность и оценки защищенности информационной системы на основе предложенных функциональных, информационных, подсистемно концептуальных моделей оценки информационной системы.

Практическая значимость результатов исследования объясняется возможностью решать задачу при недостатке экспертов по информационной безопасности, формированием заключений по оценке информационной безопасности экспертами централизованно и реализацией оценки безопасности информационной системы специалистами организаций.

Внедрение результатов исследования. На основе результатов по применению методов и алгоритмов формирования показателей и критериев информационной безопасности и оценке информационной системы внедрены:

методы формирования показателей и критериев оценки информационной безопасности и оценки информационной системы, внедренное в Хорезмском филиале АО «Ўзбекистон почтаси» (Справка №33-8/9317 Министерство развития информационных технологий и коммуникаций от 12 декабря 2018 года). На основе результатов научного исследования экономится время, затрачиваемое на оценку защищенности информационной системы, а также при обработке и анализе результатов. Оценка защищенности информационной системы способствовала перспективному планированию мер по совершенствованию информационной безопасности и использованию в принятия решений по повышению защищенности средств;

программное средство, разработанное на основе частной и подсистемной концептуальных моделей безопасности внедрено в Хорезмском филиале АК «Узбектелеком» (Справка №33-8/9317 Министерство развития информационных технологий и коммуникаций от 12 декабря 2018 года). Результаты исследования для организации способствовало оценить и контролировать информационной системы, анализировать и формировать контрольных критериев;

программное средство разработанное на основе функциональных и информационных моделей формирования системы показателей и критериев оценки информационной безопасности внедрено в ООО «Mustafo software» в целях оценки информационной безопасности разработанных программных продуктов (Справка №33-8/9317 Министерство по развитию информационных технологий и коммуникаций от 12 декабря 2018 года). Результаты исследования по формированию показателей безопасности способствовало сокращению времени общения с экспертами в 12 раз, при расчете значений информационной безопасности - сокращению времени и количества выводов более чем в 20 раз. Оценка информационной безопасности программного обеспечения, разработанного для организации, способствовало своевременному устранению имеющихся недостатков.

Апробация результатов исследований. Результаты данного исследования обсуждались на 5 международных и 13 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По теме диссертации опубликовано 29 научных работ, в том числе 5 статей в научных изданиях, рекомендованных для публикации основных научных результатов диссертаций Высшей аттестационной комиссии Республики Узбекистан, 1 статья опубликована в зарубежных и 4 статей в республиканских журналах, а также получены 2 свидетельства о регистрации программных продуктов для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 108 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении диссертационной работы обосновывается актуальность и значимость темы, соответствие исследования приоритетам развития науки и техники Республики Узбекистан, определяются цели и задачи исследования, а также объект и предмет исследования, обосновано достоверность полученных результатов, их теоретическая и практическая значимость, состояния внедрения результатов исследования, приведены сведения об опубликованных работах и структура диссертации.

Первая глава диссертации под названием «**Подходы к оценке информационной безопасности в информационно-коммуникационных технологиях»**, посвящается проблемам оценки информационной безопасности в информационных и коммуникационных технологиях, существующим нормативам и стандартам в области оценки, а также современным методам оценки информационной безопасности.

Анализ методов и подходов решения проблем оценки качества защиты информации, показывает, что системы защиты информации в современных информационно-коммуникационных технологиях представляют собой

сложную человеко-машинную систему. В целом, оценка качества функционирования такой системы может осуществляться только экспертным заключением и различными эвристическими методами, связанными с дальнейшей интерпретацией полученных результатов. Для решения задач оценки качества функционирования систем защиты информации, необходимо использовать показатели качества, позволяющие оптимизировать синтез систем защиты информации, количественно оценить эффективность функционирования систем и сопоставить различные варианты построения таких систем.

Особенность таких задач не позволяет получить оптимальное решение классическими методами. В таких условиях используются теория неформальных множеств и эвристические подходы, связанные с потребностью получения экспертных оценок. В этих условиях, имеет особую значимость использование ранговых методов, которые относительно небольших временных и вычислительных затрат обеспечивают высокий уровень достоверности в оценке.

Для оценки информационной безопасности ведущими странами отрасли разработан ряд стандартов и нормативных документов. В проведенных исследованиях на основе результатов сравнения стандартов по показателям универсальности, гибкости, гарантии, реализуемость, релевантности определено что, «Общие критерии...» (O’z DST ISO/IEC 15408) имеет ряд достоинств относительно к остальным стандартам. Поэтому проведенные в диссертационной работе исследования опираются на этот стандарт.

В настоящее время проводится много работ по оценке информационной безопасности. Их можно разделить на две группы. Первая группа позволяет установить степень риска путем оценки соответствия требованиям информационной безопасности. Вторая группа основывается на определении вероятности совершения атаки и степени наносимого ущерба.

Анализ методов оценки информационной безопасности показывает, что важнейшей проблемой является их минимальная автоматизация. Почти все методы на каждом шаге обработки требуют, чтобы информация была в установленной форме и порядке, но они не имеют механизмов формирования такой информации из первичной. Еще одним недостатком этих методов является то, что они не учитывают приоритетность особенностей информационной безопасности оцениваемого объекта.

Вторая глава диссертации под названием «**Частная концептуальная модель оценки защищённости информационно-коммуникационных технологий»** посвящена построению частных и подсистемных концептуальных моделей оценки информационной безопасности, которые охватывает критериев оценки и их взаимосвязанность, рассчитанные для использования в процессе оценки информационной системы.

В информационных системах все требования по осуществлению контроля, анализа и оценки защищённости формулируется в виде частной модели безопасности.

Отношению между безопасностью информационной системы и безопасностью ее уровней можно определить следующим образом:

$$H = H_{\text{СОТ}} \cup H_{\text{МББТ}} \cup H_{\text{ТС}} \cup H_{\text{МОТ}} \cup H_{\text{МИ}} \cup H_{\text{ХТ}},$$

здесь Н – безопасность информационной системы, $H_{\text{СОТ}}$ - безопасность уровня операционной системы сервера, $H_{\text{МББТ}}$ - безопасность уровня системы управления базами данных, $H_{\text{ТС}}$ - безопасность уровня сетевых сервисов, $H_{\text{МОТ}}$ - безопасность уровня клиентской операционной системы, $H_{\text{МИ}}$ - безопасность уровня специальных приложений, $H_{\text{ХТ}}$ - безопасность уровня документального обеспечения.

Разделение на уровни позволяет также контролировать безопасность по зонам ответственности. Частная концептуальная модель защиты информационных систем представлена на рис. 1.

Рис. 1. Частная концептуальная модель безопасности информационной системы

В моделях безопасности компонентов профиля защиты информационной системы должны быть включены все функциональные требования по безопасности, потому что эти требования адаптированы с угрозами и целями безопасности. Кроме того, необходимо следить за взаимосвязанностью каждого функционального требования (показателя). Взаимосвязи показателей должны быть включены в частные модели безопасности и удовлетворяться на определенном уровне структуры информационной системы. То есть связанность должна быть удовлетворена на соответствующем уровне сервера операционной системы, системы управления базами данных, сетевого сервиса, клиентской операционной системы, специальных приложений и документного обеспечения.

Предложено построить подсистемную модель оценки безопасности структурного компонента информационной системы с использованием терминов «Общих критериев…» и с учетом политики информационной безопасности конкретной организации, возможные и предполагаемые угрозы безопасности ресурсам.

Формирование подсистемной концептуальной модели оценки безопасности серверной операционной системы состоит из выбранного профиля защиты (базовой профиль защиты) универсальной многопользовательской операционной системы с файловой системой, службой печати, сетевыми службами, службой архивации данных и другими приложениями (например, почта, база данных).

Выбранный профиль защиты имеет полный и обоснованный набор требований, и удовлетворение этих требований обеспечивает достаточную степень защищённости в среде с средней степенью угроз для активов. В соответствии с этим уровнем угрозы обеспечиваются требования надежности и средней устойчивости функций безопасности, которые реализуется на основе механизмов вероятности и обмена (не криптографических).

Операционная система, соответствующая требованиям профиля защиты поддерживает среду обработки конфиденциальных данных. Наличие такой возможности требует применения дискреционного управления доступа обращения, которое осуществляется на основе идентификаторов в операционной системе. Функционал безопасности операционной системы перед разрешением выполнения операции должен подтверждать подлинность предъявленного идентификатора. На рис. 2 показана схема подсистемной концептуальный модели оценки безопасности серверной операционной системы.

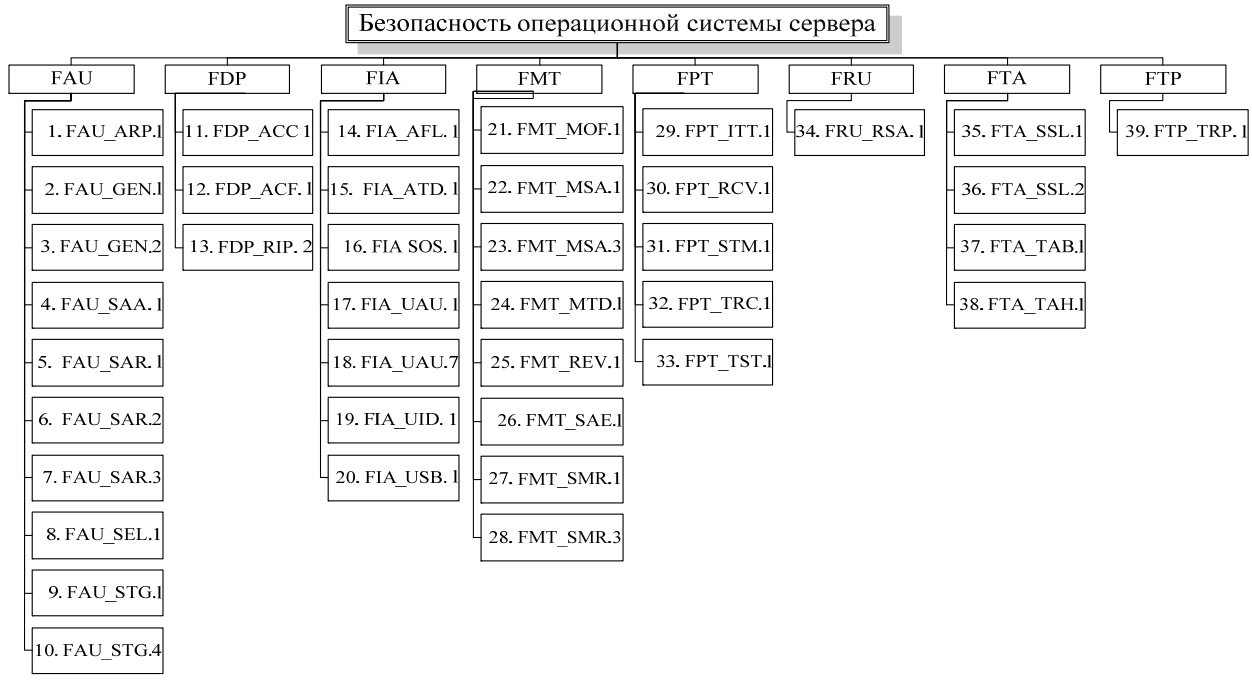


Рис. 2. Схема подсистемной концептуальной модели оценки безопасности серверной операционной системы

Созданная подсистемная модель оценки безопасности включает 39 индикаторов, влияющих на защиту данных на уровне серверной операционной системы, из которых 26 имеют внутренние зависимости, 14 являются независимыми индикаторами, а 1 показатель имеет

межуровневую связь с требованиями достоверности (класс доставки и правильность эксплуатации) уровня документного обеспечения.

На рис. 3 приведена граф-схема взаимной и межуровневой связанности показателей безопасности серверной операционной системы.

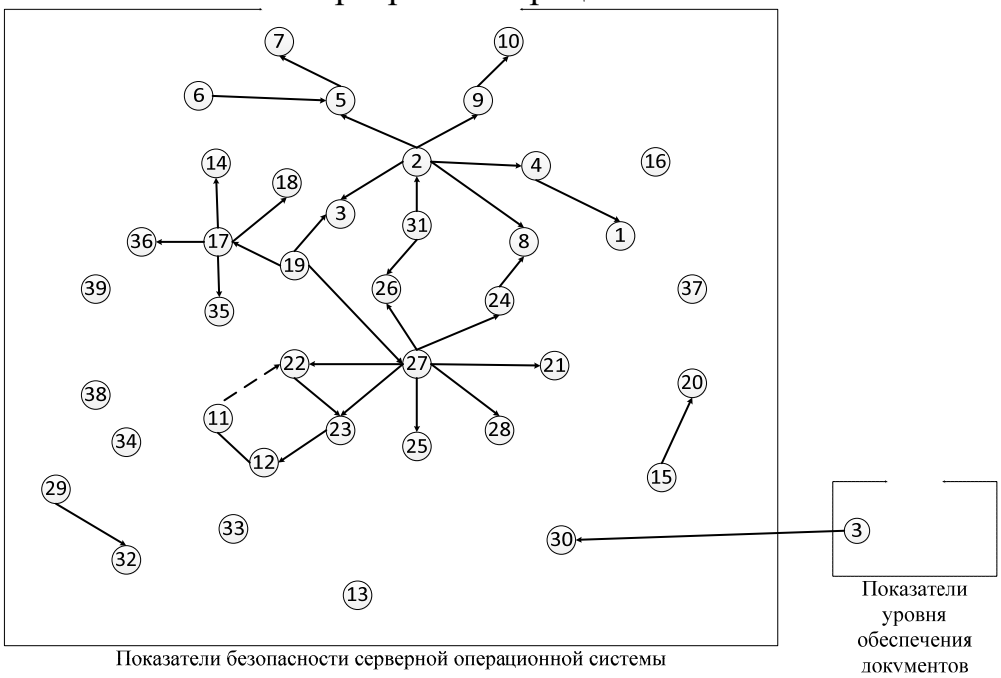


Рис. 3. Граф-схема взаимной и межуровневой связанности показателей безопасности серверной операционной системы

В диссертационной работе также разработаны подсистемные концептуальные модели, оценивающие безопасность уровней системы управления базами данных, сетевых сервисов, клиентской операционной системы, специальных приложений и документного обеспечения.

В третьей главе диссертации под названием «**Формирование системы показателей и критериев оценки информационной безопасности**» приведены модель и алгоритм формирования системы показателей и критериев, позволяющие оценить безопасность компонентов информационных технологий основанные на подсистемных концептуальных моделях.

При создании модели формирования системы показателей и критериев информационной безопасности использована методология IDEF0. Как известно, методология IDEF0 характеризует систему в виде иерархических диаграмм. Сначала освещается система как целая и отношения с внешним миром, затем осуществляется декомпозиция (Рис. 4). В результате декомпозиции система разбивается на подсистемы, и каждая подсистема характеризуется отдельно. Таким образом, достигается требуемый уровень детализации.

Каждая диаграмма состоит из блоков и дуг, блоки описывают функции проектируемой системы, а дуги представляют взаимодействия и связи блоков.

Согласно диаграмму, параметры входящие слева представляют собой

входящие данные, параметры сверху представляют управляющие данные, параметры снизу представляют механизмы, исходящие параметры с правой стороны блока представляют результаты.

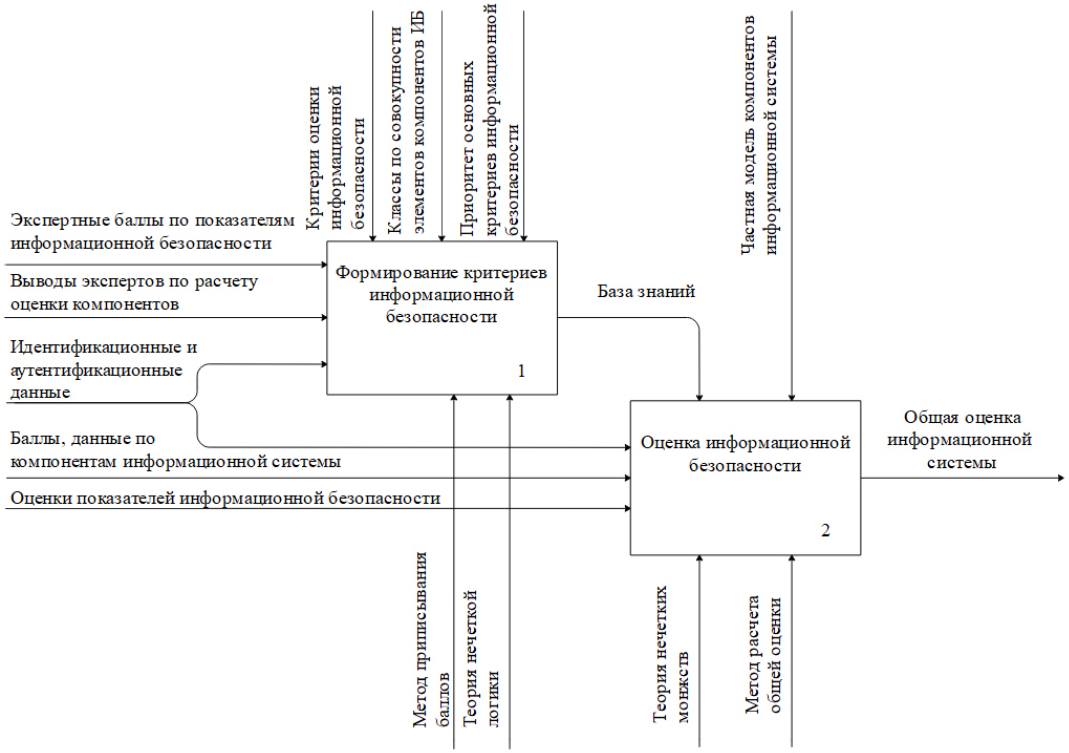


Рис. 4. Декомпозиция системы формирование показателей и критериев оценки информационной безопасности

Структура базы данных программного средства для оценки безопасности информационных систем разработана на основе методологии IDEF1X, которая состоит из следующих 17 таблиц (Рис. 5).

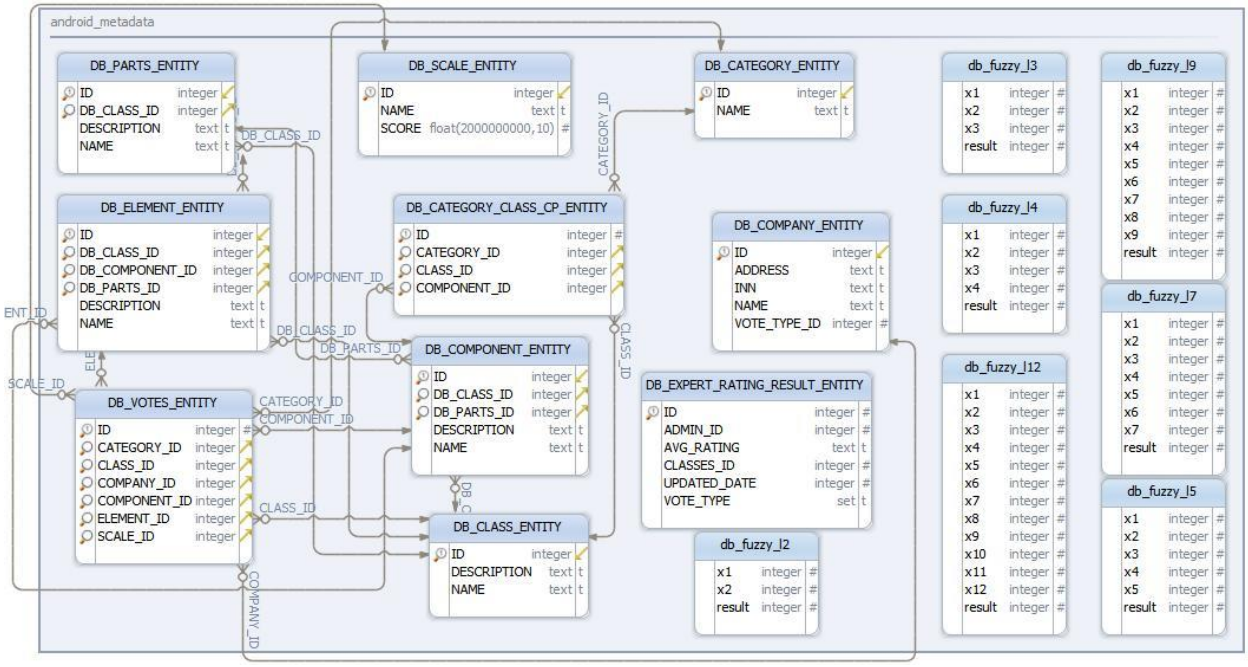


Рис. 5. IDEF1X модель базы данных программного средства оценки безопасности информационных систем

Формирования системы показателей и критериев безопасности заключается в следующем. Эксперты - на основе приоритетности трех принципов информационной безопасности: конфиденциальности, целостности и доступности - присваивают баллы согласно критериям информационной безопасности и на основе этих баллов определяют их весомый коэффициент. Эксперты также формируют экспертное заключение по оценке безопасности информационной системы и на основе теории неформальной логики разрабатывают правила, на основании которых, а также присвоенных оценок к показателям осуществляются расчет степени защищённости информационной системы.

Алгоритм, определяющий последовательность выполнения операций для оценки защищенности информационной системы можно записать следующим образом:

1. На основе приоритета принципов информационной безопасности экспертами присваиваются баллы критериям и показателям информационной безопасности, на основе которых формируется база данных.

2. Формирование базы знаний. Определение лингвистической шкалы в оценке. Построить функцию принадлежности.

3. Создание базы правил неформальных данных. На основе этих правил решаются возникающие противоречивость и сложность задачи. Дефаззификация полученных оценок.

4. Определение приоритета компонентов информационной системы и расчет весомых коэффициентов.

5. Оценка всех компонентов информационной системы с помощью лингвистических терминов на основе самых низких уровней (элементов) критериев информационной безопасности.

6. При необходимости проводится расчет оценки компонентов критериев информационной безопасности через функцию принадлежности на основе базы знаний.

7. Расчет зависимостей между показателями. В свою очередь расчет цены семьи и классов критериев безопасности.

8. Расчет общей цены информационной системы и его компонентов.

9. Анализ результатов оценки. Оформление отчета.

В четвертом разделе диссертации с названием «**Разработка программных средств оценки информационной безопасности и экспериментально-расчётные результаты»** представлены архитектуры программных средств оценки информационной безопасности на основе разработанных моделей, описанных во второй и третьей главах диссертации и экспериментально – расчётные результаты по оценке безопасности.

В организации оценка защищенности информационной системы осуществляется сотрудником организации на основе базы знаний, сформированной экспертным заключением.

Разработаны программные средства системы оценки информационной безопасности - Web-приложение, серверное приложение и Android-приложение (рис. 6).

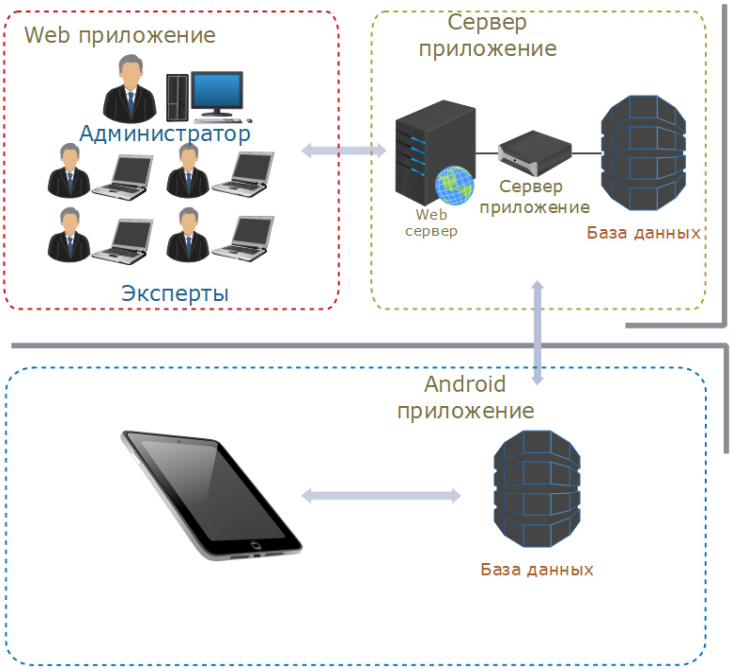


Рис. 6. Структура программного средства оценки информационной безопасности

Web–приложение используют администраторы и эксперты информационной безопасности. Администратор проводит работу по созданию профиля для экспертов по информационной безопасности, их удаления, а также на основе заключений экспертов проводит работы по расчету весовых коэффициентов критериев безопасности. А эксперты дадут баллы критериям безопасности по комбинациям принципов безопасности и заключения для расчёта оценки компонентов информационной безопасности.

Серверное приложение записывает в базу данных полученную информацию из Web-приложения и вычисляет весомые коэффициенты критериев безопасности. Кроме того, на основе запроса из Android-приложения обновляет его базу знаний.

После загрузки Android-приложением базу знаний с сервера, специалист в Android-приложении вводит модель оцениваемой информационной системы, то есть вводит приоритетность ее компонентов. Кроме того, оценивается степень соответствия компонентов информационной системы элементам требований информационной безопасности, и итоговая оценка предоставляется пользователю.

Как известно, качество механизмов защиты, используемых в информационной системе, определяется уровнем реализации функциональных требований безопасности, которые охватывают политику безопасности организации и требований противостоящие угрозам в рамках эксплуатации. При этом уровень воздействия к качеству защиты разных показателей различается. Поэтому для определения значимости требуемой функции безопасности был предложен метод определения приоритетов политики информационной безопасности (Таблица 1).

Таблица 1.

Приоритетность принципов информационной безопасности

Приоритетность	Основные принципы информационной безопасности					
1 место	М	Я	Ф	Я	М	Ф
2 место	Я	Ф	М	М	Ф	Я
3 место	Ф	М	Я	Ф	Я	М

здесь М - конфиденциальность, Я - целостность, Ф - доступность.

Этот метод основан на оценке группой экспертов каждого критерия по важности в диапазоне [0-100]. Это дает возможность фиксировать оценку чисел, суммировать баллы, которые дают несколько экспертов.

Пуст k экспертов оценили m критериев по важности. Тогда оценки поставленные по критериям можно изобразить в виде $H = \|h_{ij}\|$ матрицы, здесь h_{ij} - оценка i-эксперта поставленное j-критерию.

Чем выше критерий, определяющий соответствие мнения экспертов, тем надёжнее их мнения.

Удобно определить соответствие экспертных мнений по отношению к среднему баллу $\overline{h_i}(i=1,...,m)$ т. е.: $\overline{h_i} = \frac{m}{k*100}\sum_{j=1}^{k} h_{ij}$. На основе этого на рис.7 изображены баллы, которые эксперты давали классам критериев информационной безопасности.

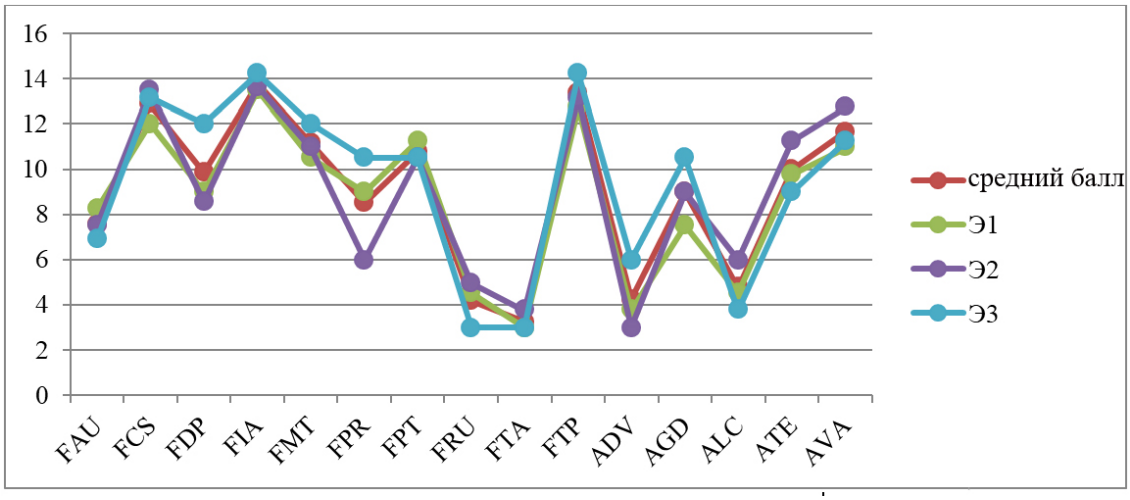


Рис. 7. Отданные баллы экспертов классам критериев информационной безопасности

Дисперсия среднего балла вычисляется формулой: $D(\overline{h}) = \frac{1}{m}\sum_{i=1}^{m}(\overline{h_i} - \overline{\overline{h}})^2$, здесь $\overline{\overline{h}} = \frac{1}{m}\sum_{i}^{m}\overline{h_i}$. Максимальная дисперсия вычисляется следующей формулой (случай когда мнение экспертов абсолютно одинаковый) $D_{\text{макс}}(\overline{h}) = \frac{1}{m}\sum_{i=1}^{m}(i - \frac{m+1}{2})^2 = \frac{m^2-1}{12}$, критерий соответствие мнений экспертов вычисляется следующей формулой: $W = \frac{D(\overline{h})}{D_{\text{макс}}(\overline{h})} = \frac{12}{m(m^2-1)}\sum_{i=1}^{m}(\overline{h} - \frac{m+1}{2})^2$. Как видно, 0≤W≤1. При W = 0 мнение экспертов абсолютно не соответствует и при W = 1 их мнение абсолютно одинаково. Таким образом, значение W определяет уровень

соответствие экспертных мнений.

Элементы выше приведенной матрицы можно записать в виде $h_i = \sum_{j=1}^{k} h_{ij}$ вектора и на основе $r_{ij} = \frac{h_{ij}}{h_i}$ можно определить коэффициенты важности. Этот матрица $r_j = \sum_{i=1}^{m} r_{ij}$ изображается в виде вектора, а весомый коэффициент критериев вычисляется через $\lambda_i = \frac{r_i}{\sum_{j=1}^{k} r_j}$, здесь λ - весомый коэффициент классов безопасности ($\sum_{i=1}^{n} \lambda_i = 1$).

Известно, что эксперты не всегда могут участвовать в оценке информационной безопасности организации, поэтому приходиться пользоваться услугами специалиста организации. При оценке информационной безопасности целесообразно использовать следующие лингвистические термины: «не соответствует»; «Частично соответствует»; «в основном соответствует»; «соответствует».

Лингвистические переменные обозначаются тройками <X, T, U>. Здесь X - имя переменной, пакет T-терм (элемент) множество, каждый терм в U универсальном множестве появляется в виде неформального множества.

В поставленной задаче X = «оценка элемента», T={«не соответствует»; «частично соответствует»; «основном соответствует»; «соответствует»}, Y= {0; 0,3; 0,7; 1}

Набор правил на основе данных, полученных от экспертов по вместимости компонентов можно сформулировать следующим образом:

Правило 1: Если x_{11}и x_{12} и ... и $x_{1n,}$ то равно y_1;

...

Правило l+1: Если x_{l+11}и x_{l+12} и ... и $x_{l+}1n$, то равно y_2;

...

Правило m+1: Если x_{m+11}и x_{m+12} ва ...и $x_{m+1n,}$то равно y_3;

...

Правило j+1: Если x_{j+11}и x_{j+12} и ... и $x_{j+}1n$, то равно y_4;

На основе политики информационной безопасности организации для компонентов информационной системы, наряду с приоритетами безопасности компонентов информационной системы, также устанавливается приоритетность по принципам информационной безопасности на основе характеристиках компонентов. (Таблица 2).

Таблица-2

Приоритеты оцениваемых компонентов информационной системы

Компоненты информационной системы	СОТ	МББТ	ТС	МОТ	МИ	ХТ
Приоритетность принципов информационной безопасности	МФЯ	ФМЯ	ФМЯ	ФЯМ	ФМЯ	МЯФ
R_i- приоритетность компонентов информационной системы	r_i	r_i	r_i	r_i	r_i	r_i

Определяется весовые коэффициенты $W_i = 1 - \frac{R_i - 1}{M}; i = \overline{1, M}$ каждого i-компонента, *M*-количество компонентов.

Нормализация весовых коэффициентов осуществляется с помощью $\lambda_k = \frac{W_k}{\sum_{i=1}^{M} W_i}$, здесь λ_k -нормализованные весовые коэффициенты в соответствии степени важности классов ($\sum_{i=1}^{m} \lambda_i = 1$).

На следующем этапе, со стороны специалиста организации, на основе подсистемных концептуальных моделей оценивается степень соответствия компонентов информационной системы критериям информационной безопасности.

Пусть проверяется соответствие FDP_ACF.1 критериев информационной безопасности серверной операционной системы к требованиям компонента «Управления доступа основанных атрибутам безопасности». Компонент FDP_ACF.1 состоит из 4-х элементов: FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3 и FDP_ACF.1.4. Допустим, специалист по информационной безопасности оценил соответствия требованиям серверной операционной системы таким образом:

- FDP_ACF.1.1 - частично соответствует;
- FDP_ACF.1.2 - частично соответствует;
- FDP_ACF.1.3 - основном соответствует;
- FDP_ACF.1.4 - основном соответствует.

Множество правил, построенных экспертами для расчета оценки компонентов, состоящих из n элементов, выражается в виде $X = \|x_{ij}\|$ матрицы, где $i = \overline{1, n}$, $j = \overline{1, k}$, n–количество элементов компонента критериев информационной безопасности, *k*–количество правил.

Если $A=\{a_1, a_2, \ldots, a_n\}$ есть оценка элементов, то определение оценки компонента определяется при помощи функции принадлежности Гаусса $\mu_{ij} = e^{\frac{(a_j - x_{ij})^2}{2*\sigma}}$ и строится матрица $M = \|\mu_{ij}\|$, также вычисляется минимум для каждой строки, то есть $min_i = min(\mu_{i1}, \mu_{i2}, \ldots, \mu_{in})$.

Для каждого сормированного набора правил определяется отдельный максимум: $max_1 = max(min_1, min_2, \ldots, min_l)$; $max_2 = max(min_{l+1}, min_{l+2}, \ldots, min_r)$; $max_3 = max(min_{r+1}, min_{r+2}, \ldots, min_j)$; $max_4 = max(min_{j+1}, min_{j+2}, \ldots, min_k)$.

Оценка компонента вычисляется следующим образом:

$$X_{\text{компонент}} = \frac{y_1 * max_1 + y_2 * max_2 + y_3 * max_3 + y_4 * max_4}{max_1 + max_2 + max_3 + max_4}$$

На следующем этапе на основе подсистемных концептуальных моделей, описываемых во второй главе диссертации, рассчитывается связанность компонентов информационной безопасности.

Если компоненты информационной безопасности имеют непосредственную связанность (например, показатель FAU_GEN.2 имеет непосредственную связанность с показателями FAU_GEN.l и FIA UID.1), их значения вычисляется следующей формулой $x_{1,3} = \lambda_3 \cdot x_{1,3} \cdot \left| \frac{\lambda_2 \cdot x_{1,2} + \lambda_{19} \cdot x_{1,19}}{\lambda_2 - \lambda_{19}} \right|$,

здесь $\lambda_2, \lambda_3, \lambda_{19}$ – весомый коэффициент соответствующих компонентов, $x_{2,1}, x_{3,1}, x_{32,1}$ - значения компонентов.

Если компонент имеет выборочную связанность (например, FDP_ETC.2 компонент имеет выборочный связанность с компонентами FDP_ACC.l или FDP_IFC.1), их значения вычисляются по формуле $x_{3,12} = x_{12} \cdot \lambda_{3,12} \cdot \max[\lambda_{10} \cdot x_{3,10}; \lambda_{13} \cdot x_{3,13}]$.

На следующем этапе оценка семейств информационной безопасности может осуществляется с применением метода аддитивных показателей. $X_j = \sum_{k=1}^{n} \lambda_k X_{kj};\ \overline{X_j} \leq 1,$ здесь X_j-j-оценка семейства.

ЗАКЛЮЧЕНИЕ

По результатам исследования диссертационной работы на тему «Методы и алгоритмы формирования системы показателей и критериев информационной безопасности» были представлены следующие выводы:

1. Разработаны частные и подсистемные концептуальные модели, отражающие конфигурацию компонентов информационной системы. Разработанные модели позволили сформировать подходы, определенные в политике информационной безопасности организации.

2. На основе методологии IDEF0 разработана функциональная модель формирования системы показателей и критериев оценки информационной безопасности, а на основе методологии IDEF1X разработана информационная модель базы данных системы показателей и критериев оценки информационной безопасности. Разработанные модели позволили проектировать программное обеспечение, а также хранить и использовать все данные, относящиеся к ним.

3. Разработаны методы формирования показателей и критериев оценки информационной безопасности на основе экспертных заключений, а также методы оценки безопасности информационной системы. Разработанные методы позволили обеспечить возможность оценить безопасность информационной системы со стороны специалиста организации.

4. Разработан метод оценки информационной системы на основе подсистемных концептуальных моделей. Разработанная методика позволили принять обоснованное решение при определении состояния безопасности информационной системы и совершенствования мер защиты информации.

5. На основе разработанных методов и моделей предложено формировать систему показателей и критериев оценки информационной безопасности, а также предложена архитектура программных средств оценки информационной безопасности. Централизованное формирование показателей и критериев информационной безопасности при помощи программных средств, разработанные на основе предложенной архитектуры, позволяет получить эффективные результаты при решении задачу недостатки экспертов.

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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

KHALMURATOV OMONBOY UTAMURATOVICH

METHODS AND ALGORITHMS OF FORMING SYSTEM OF INDICATORS AND CRITERIA OF INFORMATION SECURITY

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 B2017.1.PhD/T55.

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	**Karimov Madjit Malikovich** Doctor of Technical Sciences, Professor
	Kuryazov Davlatyor Matyakubovich Doctor of Physical-Mathematical Sciences
Leading organization:	**National University of Uzbekistan**

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 thesis)

The aim of the research work is formation of a system of criteria and indicators of information security and the development of methods and tools for evaluating the information security of information systems.

The object of the research work is the process of assessing the security of an information system.

The scientific novelty of the research work:

on the basis the characteristics of the organization and components of the information system, private and subsystem conceptual models of information system security were developed;

the functional and information models for forming a system of criteria and indicators for evaluating information security based on the IDEF0 and IDEF1X methodology were worked out;

on the basis methods of issuing points, ranking, the theory of informal logic «Mamdani» and expert outcomes, a method for forming criteria and indicators for evaluating information security was developed;

on the basis of the priority of security of the components of the information system, a methodology for evaluating the information system was worked out;

on the basis of private and subsystem conceptual models of information system security, the system of criteria and indicators for evaluating information security was formed, information security evaluation algorithms and their software architecture were developed.

Implementation of the research results. On the basis the results on the application of methods and algorithms of forming of criteria and indicators of information security and the evaluation the information system have been implemented in:

methods of forming criteria and indicators for assessing information security and evaluating an information system, implemented in Khorezm branch of «Uzbekiston pochtasi» JSC (certificate No. 33-8/9317 the Ministry for development of information technologies and communications of the Republic of Uzbekistan dated December 12, 2018). Based on the results of scientific research, the time spent on assessing the security of the information system, as well as processing and analyzing the results, is saved. The evaluation of the security of the information system contributed to the long-term planning of measures to beef up information security and use it as a basis for making decisions on improving the security of tools;

software, which was developed on the basis of private and subsystem security conceptual models implemented in Khorezm branch of «Uzbektelecom» (certificate No. 33-8/9317 the Ministry for development of information technologies and communications of the Republic of Uzbekistan dated December 12, 2018). The results of the research for the organization contributed to evaluate and control the information system, and analyze and form control criteria;

software developed on the basis of functional and information models of the formation of a system of criteria and indicators for evaluating information security

was implemented in «Mustafo software» Ltd. in order to evaluate information security of the developed software products (certificate No. 33-8/9317 the Ministry for development of information technologies and communications of the Republic of Uzbekistan dated December 12, 2018).

The results of the research on the formation of security indicators contributed to reduce the time of communication with experts by 12 times, while calculating information security values - reducing the time and number of outcomes by more than 20 times. The evaluation of information security of the software, being developed for the organization, was contributed to the timely elimination of existing disadvantages.

The outline of the dissertation. The dissertation consists of an introduction, four chapters, conclusion, list of references and applications. The volume of the thesis is 108 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

1. Халмуратов О.У., Ахборот хавфсизлиги кўрсаткичлари синфларининг муҳимлигини баҳолаш //«TATU xabarlari». –Toshkent, 2015, №1(33). – B. 110-113, (05.00.00; №10).
2. Халмуратов О.У., Насруллаев Н.Б., Турапов Ш.Н., Тармоқ ҳужумларини аниқлаш тизимларининг классификацияси //«TATU xabarlari». –Toshkent, 2015, №2(34). – Б. 137-141, (05.00.00; №10).
3. Khalmuratov O.U., Improvement of information security cases and classification systems //«European science review». – Austria, Vienna, 2018, № 5-6. –P. 86-90, (05.00.00; №3).
4. Халмуратов О.У., Ахборот технологиялари ҳимояланганлигини баҳолашнинг концептуал модели //«Muhammad al-Xorazmiy avlodlari». – Toshkent, 2018, №3(5).-B.47-51, (05.00.00; №10).
5. Халмуратов О.У., Ахборот хавфсизлиги кўрсаткич ва мезонлари тизимининг функционал модели //«Muhammad al-Xorazmiy avlodlari». – Toshkent, 2018, №4(6) . -B 45-49, (05.00.00; №10).
6. Ganiyev S.K., Khalmuratov O.U., Khudoykulov Z.T., Detection weighty coefficient of functional requirements classes of standard «Information technology. Security techniques evaluation criteria for it security» //«Chemical technologies. Monitoring and control» –Тошкент, 2014, №2. - P. 68-72.
7. Халмуратов О.У., Тажиев Д., Султанов Й. У., Ташкилотларда ахборот хавфсизлигига бўладиган хавф-хатар баҳолаш усули ҳақида //«Молодой учёный». – Россия, 2016, № 9.5 (113.5). –Б. 35-38.
8. Халмуратов О.У., Тожиев Д. Қ., Хужамов Д. Ж., Ахборот коммуникация технологияларида ахборот хавфсизлигини баҳолашга ёндашувлар таҳлили //«Технологии техника инженерия». Международный научный журнал». – Россия, 2017, № 2.1 (4.1). – Б. 35-38.
9. Халмуратов О.У., Тожиев Д. Қ., Хужамов Д. Ж., Ахборот хавфсизликнинг умумий моделларини тавсифи //«Технологии техника инженерия ». – Россия, 2017, № 2.1 (4.1). – Б. 38-40.
10. Ганиев С.К., Халмуратов О.У., Абрамов А.С., Критерии оценки защищенности информационных систем //«Актуальные проблемы развития инфокоммуникаций и информационного общества» Международная конференция, Ташкент, 2012. –С. 676-681.
11. Иргашева Д.Я., Халмуратов О.У., К вопросу оценки эффективности ролевой модели разграничения доступа с зональной политикой //«Ахборот технологиялари ва телекоммуникация муаммолари», ёш олимлар, тадқиқотчилар, магистрант ва талабаларнинг Республика илмий-техник анжумани маърузалар тўплами, Тошкент, 2012. I ТОМ. -Б. 217.
12. Ганиев С.К., Халмуратов О.У., Абрамов А.С, К вопросу оценки защищенности информационных систем //«Innovation-2012» халқаро илмий

анжуман, илмий мақолалар тўплами, Тошкент, 2012. –С. 252-253.

13. Халмуратов О.У., Абрамов А.С., Абдуллаев Д.Г., Основные нормативные документы по оценка защищенности информационных систем //«Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения» Сборник тезисов и докладов: Республиканский семинар, Ташкент, 2012. –С. 25-26.

14. Ғаниев С. К., Халмуратов О.У., Абрамов А.С,. Норавшан мантиқ назарияси асосида хавф-хатарни баҳолаш алгоритми //«Информационная безопасность в сфере связи, информатизации и телекоммуникационных технологий. Проблемы и пути их решения». Сборник тезисов и докладов Республиканский семинар, Ташкент, 2013, –Б. 34.

15. Ганиев С. К., Халмуратов О.У., Абрамов А.С., К вопросу оценка безопасности продуктов информационных технологий //«Ахборот технологиялари ва телекоммуникация муаммолари», ёш олимлар, тадқиқотчилар, магистрант ва талабаларнинг Республика илмий-техник анжумани маърузалар тўплами, Тошкент, 2013, I қисм, -С. 242.

16. Иргашева Д.Я., Халмуратов О.У., К вопросу анализа скрытых каналов утечки информации //Труды Северо-кавказского филиала Московского технического университета связи и информатики. Подготовлены по результатам международной молодежной научно-практической конференции СКФ МТУСИ «ИНФОКОМ-2013», Ростов-на-Дону, 2013, –С. 308-311.

17. Халмуратов О.У., Babamukhamedov B.A., Khudoykulov Z.T., Features of information security in information and communication system //International scientific conference «Perspectives for development of information technologies ITPA-2014», Tashkent, 2014, -P. 82-84.

18. Халмуратов О.У., Ахборот тизимларини ҳимояланганлигини баҳолаш хусусида //«Ахборот технологиялари ва телекоммуникация тизимларини самарали ривожлантириш истиқболлари» Республика илмий-техник конфиренцияси маърузалар тўплами, 2 қисм, Тошкент, 2014, –Б. 177-178.

19. Иргашева Д.Я., Халмуратов О.У., Концептуальный анализ понятия комплексной безопасности //«Ахборот технологиялари ва телекоммуникация тизимларини самарали ривожлантириш истиқболлари» Республика илмий-техник конфиренцияси маърузалар тўплами, 2 қисм, Тошкент, 2014, –Б. 170-172.

20. Халмуратов О.У., Маматов А.Ш., Многоуровневая система показателей информационной безопасности //«Radiotexnika, telekommuni-katsiya va axborot texnologiyalari: muammolari va kelajak rivoji» Xalqaro ilmiy-texnik konferensiya maqolalar to’plami, II-tom, Toshkent, 2015, -C. 137-140.

21. Халмуратов О.У., Ахборот хавфсизлиги тизимларига бўладиган ҳавфларни баҳолашга ёндашувлар //«Ахборот ва телекоммуникация технологиялари муаммолари». Республика илмий-техник конференцияснинг маърузалар тўплами, Тошкент, 2015, 1-қисм, -Б. 416-417.

22. Ганиев С. К., Халмуратов О.У., Ахборот тизими ҳимояланганлигини структурали баҳолаш //«Ахборот ва телекоммуникация технологиялари муаммолари». Республика илмий-техник конференциясининг маърузалар тўплами, Тошкент, 2015, 1-қисм, -Б. 413-415.

23. Халмуратов О.У., Норқулова С.Б., Тармоқ хужумларини аниқлаш тизимларини баҳолаш мезонлари ҳақида //«Ахборот ва телекоммуникация технологиялари муаммолари». Республика илмий-техник конференциясининг маърузалар тўплами, Тошкент, 2016, 4-қисм, -Б. 187-190.

24. Халмуратов О.У.,Тоджиев Д.К., Инфокоммуникацион тизимларнинг ҳимояланганлигини баҳолаш усули ҳақида //«Ахборот ва телекоммуникация технологиялари муаммолари». Республика илмий-техник конференциясининг маърузалар тўплами, Тошкент, 2016, 4-қисм, -Б. 159-160.

25. Халмуратов О.У., Ахборот коммуникация технологияларида ахборот хавфсизлигини баҳолаш усуллари //«Информационная безопасность в сфере связи, информатизации. Проблемы и пути их решения». Сборник тезисов и докладов Республиканский семинар, Ташкент, 2016, –Б, 51-53.

26. Халмуратов О.У., Ахборот технологиялари хавфсизлигининг умумлашган моделини қуриш //«Информационная безопасность в сфере связи, информатизации. Проблемы и пути их решения». Сборник тезисов и докладов Республиканский семинар, Ташкент, 2016, –Б. 53-55.

27. Халмуратов О.У., Ахборот хавфсизлиги кўрсаткич ва мезонлари тизимининг функционал модели //«Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари». Республика миқёсидаги илмий-техник конференция, Тошкент, 2018, –Б 283-286.

28. Ганиев С.К., Иргашева Д.Я., Халмуратов О.У., Насруллаев Н.Б., Маматов А.Ш., Бабамухамедов Б.А., Гулямов Ш.Р., Абрамов А.С. «Estimation on the bases of Common Criteria» ахборот тизими //Дастурга гувоҳнома №DGU04077, 24.11.2016.

29. Халмуратов О.У. «Info Security»-Axborot xavfsizligi mezon va ko’rsatkichlarini shakllantirish dasturi //Дастурга гувоҳнома №DGU05754, 06.11.2018.

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 № 46.

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