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

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

ОЧИЛОВ НИЗОМИДДИН НАЖМИДДИН ЎҒЛИ

# ОЧИҚ КОДЛИ ОПЕРАЦИОН ТИЗИМЛАРНИНГ АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ВОСИТАЛАРИ ВА УСУЛЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

**Тошкент-2019**

УДК: 004.451.8(09)

Техника фанлар[illegible] диссертацияси



О[illegible]
докторл[illegible]

Contents of d[illegible]

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

**ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ**

**ОЧИЛОВ НИЗОМИДДИН НАЖМИДДИН ЎҒЛИ**

# ОЧИҚ КОДЛИ ОПЕРАЦИОН ТИЗИМЛАРНИНГ АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ВОСИТАЛАРИ ВА УСУЛЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

**Тошкент-2019**

**Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2019.2.PhD/T1107 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:** | **Каримов Маджит Маликович**<br>техника фанлари доктори, профессор |
| **Расмий оппонентлар:** | **Мухамедиева Дилноз Тўлкуновна**<br>физика-математика фанлари доктори, профессор |
| | **Туйчиев Ғулом Нумонович**<br>физика-математика фанлари доктори |
| **Етакчи ташкилот:** | **«UNICON.UZ» – фан-техника ва маркетинг тадқиқотлари маркази** |

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.27.06.2017.T.07.01 Илмий кенгашнинг 2019 йил «9» ноябрь соат 14:00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (2592 рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2019 йил «31» октябрь да тарқатилди.
(2019 йил «8» октябрь даги 18 рақамли реестр баённомаси.)

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

**К.Ф. Керимов**
Илмий даражалар берувчи илмий кенгаш котиби в.в.б, т.ф.н., 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 хавфсизлиги (АХ) тизимларини ишлаб чиқишга ва уларни такомиллаштиришга алоҳида эътибор қаратилмоқда. Ахборот-коммуникация тизимлари ривожининг ҳозирги даражасида самарали ахборот хавфсизлигини таъминлашнинг бирмунча муҳим механизмларидан бири бўлган операцион тизимларни ҳимоялаш масаласи айниқса долзарб бўлиб қолмоқда. «Интерфакс маълумотларига кўра Германияда 2016 йилда киберхуружлар сони 2017 йилдагига нисбатан 1,8 мартага ошган ва бу каби хуружларнинг фош этилиши 2016 йилда аввалги йилдаги 32,8% ўрнига 38,7% га ортган»[1]. Мазкур масала юзасидан АҚШ, Нидерландия, Германия, Буюк Британия, Швеция, Франция, Жанубий Корея, Хитой, Россия Федерацияси каби мамлакатларда ва бошқа давлатларда муайян соҳалар белгиланган бўлиб, уларда компьютер тизимларининг юқори даражада ҳимояланганлигини таъминловчи операцион тизимларни ҳимоялаш механизмларининг дастурий-аппарат воситаларини яратишга алоҳида эътибор қаратилмоқда.

Жаҳонда операцион тизимларни ҳимоялашнинг самарали усуллари ва воситаларини такомиллаштириш, уларнинг самарадорлиги операцион тизимларни ҳимоялашнинг юқори даражасига қадар ошириш муҳим аҳамият касб этади. Бу борада олиб борилаётган илмий-тадқиқот ишларида қуйидаги жиҳатларга алоҳида эътибор қаратилмоқда: компьютер тизимларининг ишончли ҳимоясини таъминлаш мақсадида ресурсларнинг муайян категорияларидан фойдаланишни чекловчи усулларни ишлаб чиқиш; аудит, модулларни ажратиш, оператив хотирани тозалаш, тизим файллари яхлитлигини текшириш ва ҳ.к. каби ҳимоя воситалари мажмуи (ҲВМ) асосида операцион тизимдаги маълумотлар тизимини ҳимоялаш усулларининг дастурий мажмуаларини ишлаб чиқиш; ҳуқуқлар моделлари асосида маълумотларни ҳимоялаш моделларини яратиш.

Республикамизда давлат ва хўжалик бошқаруви органларида ахборот технологияларини ривожлантириш билан бир қаторда компьютер тармоқларида маълумотларни ҳимоялаш воситалари ва усулларини кенг қўллашга ва маълумотларни тармоқлардаги таҳдидлардан ҳимоялашга алоҳида эътибор қаратилмоқда. Шу муносабат билан компьютер тармоқларидаги таҳдидлар ва ҳужумларни аниқлаш ва уларни бартараф этиш борасида сезиларли натижаларга эришилди, жумладан, компьютер тармоқларининг ҳимояланганлигини таъминлаш мақсадида ахборот хавфсизлиги мониторинги тизимини, ҳужумларни аниқлаш ва уларни бартараф этиш тизимини ишлаб чиқиш йўлга қўйилди. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан, «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоя қилиш тизимини такомиллаштириш, ахборот соҳасидаги

[1] https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/343228.php

таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Шу каби вазифаларни амалга ошириш, жумладан, ташқи таҳдидлар таъсирини камайтирувчи ҳимоя воситаларининг моделлари, усуллари ва алгоритмларини яратиш ахборот технологиялари соҳаси мутахассислари олдида турган муҳим масалалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон "Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида"ги, 2017 йил 29 ноябрдаги ПФ-5264-сон "Ўзбекистон Республикаси Инновацион ривожланиш вазирлигини ташкил этиш тўғрисида"ги фармонлари, 2013 йил 27 июндаги ПҚ-1989-сон "Ўзбекистон Республикаси Миллий ахборот-коммуникация тизимини янада ривожлантириш тўғрисида" ги қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга мазкур диссертация тадқиқоти маълум даражада хизмат қилади.

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

**Муаммонинг ўрганилганлик даражаси.** Л.Торвальдс, Р.Херцог, Б.Керниган каби олимлар Linux оиласига мансуб бўлган операцион тизимларни ишлаб чиқиш борасида тадқиқотлар олиб борганлар. Р.Пайк, Б.Уорд, Д.Барретт, С.Алапати, А.Робачевский, Д.Н.Колиснеченко, М.Фленов, С.Немнюгин, О.Стесик, Т.Адельштайн, Б.Любанович, С.Л.Скловская каби хорижлик ва мамлакатимиз олимларининг Linux операцион тизимидаги маълумотларни ҳимоялаш тизимини яратиш соҳасидаги илмий-тадқиқот ишлари ўрганиб чиқилган. МДҲ мамлакатлари ҳамда Ўзбекистон Республикаси илмий ишланмаларида алгоритмларни шифрлаш, ҳимоялаш воситаларининг турли усуллари, моделлари ва алгоритмлари, ахборотни ҳимоялашнинг назарий ва амалий тамойиллари, ахборотни ҳимоялаш воситалари ва усулларини ишлаб чиқиш бўйича «Astra Linux», «Заря» операцион тизим (ОТ)лари, «Альт Linux», «РОСА» каби операцион тизимлар ўрганиб чиқилган. Турли давлат муассасаларида қўлланилувчи «Dopplx» график қобиқлари ўрганилган.

Х.А.Музаффаров ва А.Икромовлар илмий мақолаларида ГОСТ 28147-89 алгоритми билан шифрлаш ва ҳимоя тизимларини яратиш усуллари ўрганиб чиқилган. Д.Н.Колиснеченко ва В.Алленлар илмий ишларида, Linux Format журналининг 2014, 2015 ва 2016 йилларидаги барча сонларида Linux ОТ ядроси алгоритмлари ва тузилмаси, пакет маълумотларга ишлов бериш тезлиги, хавфсизлик моделлари, хавфсизликни таъминлаш воситалари тадқиқ қилинган.

Шу билан бирга, тармоқдаги таҳдидлардан ҳимоялаш воситалари ва усуллари тўла таҳлил қилинмаган, мавжуд алгоритмлардаги камчиликлар

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

аниқланган ҳамда ноқонуний таъсирлардан ҳимояловчи қурилмаларни бошқариш воситалари етарли даражада ўрганилмаган.

**Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги.** Диссертация тадқиқоти Ўзбекистон миллий университетининг илмий-тадқиқот ишлари режасига мувофиқ «Очиқ кодли операцион тизимлар асосида ихтисослашган электрон хисоблаш машиналар учун махсус белгиланган операцион тизимларни ишлаб чиқиш» (2015-2017) №5/15 мавзусидаги лойиҳалар доирасида бажарилган.

**Тадқиқотнинг мақсади** Ўзбекистон Республикасининг O'zDSt 2817:2014 асосида 2А даражадаги хавфсизлик талабларига жавоб берувчи ва махфий иш юритиш соҳасидаги стандартлар талабларини қондирувчи махсус усулларни ишлаб чиқиш ва хавфсизлик воситаларини жорий қилишдан иборат.

**Тадқиқотнинг вазифалари:**

ахборот хавфсизлиги соҳасидаги энг муҳим миллий ва халқаро стандартлар ва бошқа ҳужжатларни ҳамда махсус очиқ кодли замонавий хавфсиз ОТларни таҳлил этиш;

белгили драйвер асосида ҳимояланган операцион тизимлари ядроларида қурилмаларнинг инициализация ва ўчириш усуллари алгоритмини такомиллаштириш;

Ўзбекистон Республикаси стандартлари талаблари ва таҳдидлар, хавфсизлик бузғунчиси моделлари асосида таркибий тизимларни қайд этиш ва ҳодисаларни ҳисобга олиш, таркибий тизим яхлитлигини таъминлаш, чоп этилаётган ҳужжатларнинг маркировкаси механизмларини, тезкор хотирани тозалашни ишлаб чиқиш ҳамда дастурлар билан ишлаш учун график дастурларини очиқ кодли операцион тизимларида хавфсизлик воситаларини ишлаб чиқиш;

идентификация ва аутентификация усуллари учун кўп босқичли назорат хоссаларини сақлаган ҳолда, киришни назорат қилиш воситаларини ишлаб чиқиш;

**Тадқиқотнинг объекти** сифатида операцион тизимларни ҳимоялаш модуллари ва дастурлари олинган.

**Тадқиқотнинг предмети** сифатида Linux операцион тизими асосидаги ҳимояланган операцион тизимларни қуриш технологиялари ва усуллари олинган.

**Тадқиқот усуллари.** Тадқиқот жараёнида ахборотни ҳимоялаш усулларидан, алгоритмлар назариясидан, математик моделлаштириш усулларидан ҳамда тартибли ва объектга йўналтирилган дастурлашдан фойдаланилган.

**Тадқиқотнинг илмий янгилиги** қуйидагилардан иборат:

асос бўлувчи миллий ва халқаро (ТЭНБФХ (Техник ва экспорт назорати бўйича федерал хизмат) томонидан ишлаб чиқилган) стандартлар таҳлили ва хавфсизликни бузувчи модели асосида унинг математик модели ҳамда имкониятлари ишлаб чиқилган;

белгили драйвер асосида қурилмаларнинг инициализация ва ўчириш усуллари алгоритми такомиллаштирилган;

Ўзбекистон Республикаси стандартлари талаблари ва таҳдидлари талабида, хавфсизлик бузғунчиси моделлари асосида таркибий тизимларни қайд этиш ва ҳодисаларни ҳисобга олиш, таркибий тизим яхлитлигини таъминлаш, чоп этилаётган ҳужжатларнинг маркировкаси механизмларини, тезкор хотирани тозалаш, ҳамда дастурлар билан ишлаш учун график дастурларининг очиқ кодли операцион тизимларида хавфсизлик воситалари яратилган;

идентификация ва аутентификация усуллари учун кўп босқичли назорат хоссаларини сақлаган ҳолда киришни назорат қилиш воситалари такомиллаштирилган.

**Тадқиқотнинг амалий натижалари қуйидагилардан иборат:**

хавфсизликни бузувчининг таянч модели асосида ва автоматлаштирилган тизим (АТ)нинг математик моделини ишлаб чиқилди;

белгили драйвер асосида қурилмаларни номлаш ва олиб ташлаш услубининг алгоритми такомиллаштирилди;

Ўзбекистон Республикаси стандартлари талабларини қондирувчи ва хорижий стандартлар асосида ҳодисаларни ҳисобга олиш ва таркибий тизимларни қайд этиш, таркибий тизим яхлитлигини таъминлаш, чоп этилаётган ҳужжатларнинг маркировкаси механизмлари ишлаб чиқиш, тезкор хотирани тозалашдан иборат бўлган ҳамда дастурлар билан ишлаш учун график дастурлар хавфсизликни бузувчи ва таҳдидлар моделлари асосида очиқ кодли операцион тизимлар учун ишлаб чиқилган;

идентификация ва аутентификация модули учун кўп босқичли назорат хоссаларини сақлаган ҳолда фойдаланишни назорат қилиш воситалари ишлаб чиқилган.

**Тадқиқот натижаларининг ишончлилиги.** Натижаларни миқдор ва сифат жиҳатдан баҳолашни қўллаган ҳолда тадқиқот мақсади ва вазифалари, предметга мос бўлган усулларда; назарий ва амалий даражада тадқиқот ўтказиш орқали; тадқиқот методологиясининг асосланганлиги таъминланган.

**Тадқиқот натижаларининг илмий аҳамияти.** Маълумотларни жисмоний ва мантиқий ҳимоялашда ҳамкорликда фойдаланиш ва ажратиш тамойилини жорий қилиш асосида ахборот хавфсизлиги тизимларининг вазифавий имкониятларини кенгайтиришга имкон берувчи алгоритмлар ва дастурий воситалар ишида тавсия этилган амалий апробациялардан иборат. Ахборотни ҳимоялаш ва унга ишлов бериш учун универсал инфратузилмаларнинг ҳаракатланиш механизмлари тавсия этилди ва ва моделлар ишлаб чиқилди. Тавсия этилган алгоритмлар асосида Ўзбекистон Республикаси конунчилига мувофиқ, очиқ кодли операцион тизимлар учун хавфсизлик талабларига жавоб берувчи хавфсизлик тизимлари ишлаб чиқилган.

Тадқиқот натижасининг амалий аҳамияти O'zDSt 2817:2014 2A синфига мувофиқ хавфсизлик талабларига жавоб берувчи ва махфий иш юритиш соҳасидаги ахборотни ҳимоялашни таъминлаш учун давлат ва

ҳуқуқий органлар томонидан унинг хулосаларидан фойдаланиш билан боғлиқ бўлган давлат ёки тижорат муассасаларида қўллаш мумкин бўлган ахборот хавфсизлигини таъминлаш тизимини ишлаб чиқишдан иборат. Тадқиқот натижаларининг амалда жорий қилиниши Ўзбекистон Республикаси вазирликлари ва идораларида фойдаланувчи ахборот тизимлари ва технологияларини қўллаш билан боғлиқ бўлган ахборот хавфсизлигининг бирмунча асосланган ва мақсадга йўналтирилган сиёсатига ўтказишни таъминлашга имкон беради.

**Тадқиқот натижаларининг жорий қилиниши.** Ишлаб чиқилган ахборот хавфсизлигини таъминлаш воситалари ва усуллари, яратилган алгоритмлари бўйича олинган натижалар асосида:

идентификация ва аутентификация усуллари учун кўп босқичли назорат хоссаларини сақлаган ҳолда киришни назорат қилиш воситалари Ўзбекистон Республика Вазирлар Маҳкамаси ҳузуридаги Давлат тест маркази Сурхондарё вилояти бўлимида жорий қилинган (Ўзбекистон Республика Вазирлар Маҳкамаси ҳузуридаги Давлат тест марказининг 2019 йил 25 сентябрдаги 104-маълумотномаси). Илмий тадқиқот натижасида кўп босқичли назорат хоссаларини сақлаган ҳолда киришни назорат қилиш воситалари такомиллаштириш имконини берган;

белгили драйвер асосида ҳимояланган операцион тизимлари ядроларида қурилмаларнинг инициализация ва ўчириш усуллари учун алгоритми «Infoteka» МЧЖ фаолиятига жорий этилган (Ўзбекистон Республика Вазирлар Маҳкамаси ҳузуридаги Давлат тест марказининг 2019 йил 25 сентябрдаги 104-маълумотномаси). Натижада ишлаб чиқилган метод хавфсиз операцион тизими ядросидаги қурилмаларни ўчириш ва инициализациялаш усуллари иш вақтини 8,3 маротабага камайтиришга имкон берган;

«HUMO» ОТда ишлаб чиқилган маълумотларни ҳимоялаш алгоритмлари ва дастурлари махсус ҳимоя воситалари Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигидан ижобий экспертизадан ўтказилган ва жорий этиш учун қабул қилинган (Ўзбекистон Республика Вазирлар Маҳкамаси ҳузуридаги Давлат тест марказининг 2019 йил 25 сентябрдаги 104-маълумотномаси). Илмий тадқиқот натижасида очиқ кодли ОТда дастурий мажмуалар ва маълумотларнинг хавфсизлигини таъминлаш методларини қўллаш объектларга қайд қилинмаган мурожатлардан ҳимоя қилиш ва уларнинг ҳимояланган операцион тизимларини қуришдаги самарадорлигини аниқлаш имконини беради.

**Тадқиқот натижаларининг апробацияси.** Мазкур тадқиқот натижалари, жумладан, 2 та халқаро ва 2 та республика илмий-амалий анжуманида муҳокамадан ўтказилган.

**Тадқиқот натижаларининг эълон қилинганлиги.** Тадқиқот мавзуси бўйича жами 14 та илмий мақола чоп этилган бўлиб, шулардан 4 та мақола Ўзбекистон Республикаси Олий аттестация коммисиясининг докторлик диссертациялари асосий натижаларини чоп этиш тавсия этилган, 2 таси

**Тадқиқот натижаларининг апробацияси.** Мазкур тадқиқот натижалари 4 та халқаро ва 4 та республика илмий-амалий анжуманларида апробациядан ўтган.

**Тадқиқот натижаларининг эълон қилиниши.** Диссертация мавзуси бўйича жами 10 та илмий иш, шулардан 3 таси халқаро журналада, нашр этилган ҳамда Ўзбекистон Республикаси Интелектуал мулк агентлигининг 1 та ихтирога ва 1 та фойдали моделга патенти олинган.

## ТАДҚИҚОТНИНГ АСОСИЙ МАЗМУНИ

**Ўзбекистон Республикасининг «Объект юзасининг суръати бўйича уни қиёсий анализ учун қурилма» (№ 04195-2010 й.) ихтирога патенти**

**Фойдаланиш соҳаси:** емирмайдиган назорат

**Вазифаси:** Объект эталонисиз тахлил қилиш имкониятини таъминлаш.

**Ихтиро моҳияти:** қурилма таркибига мос предметли столчалари бор иккита солиштириш тармоқларидан ташкил топган солиштириш микроскопи, тасвирлар майдончаларини қўшиш блоки ва ўз ичига объективни ўтказувчи ойнани визуал ва телевизион каналларни олган кузатиш блоки кирган. Тасвирлар майдонларини қўшиш блоки солиштириш тармоқлари ва телевизион каналлар орасида жойлашган. Қурилма унинг оптик ўқининг устида кетма-кет жойлашган нурланиш манбайидан, линзадан, улардан биттаси (36) ўтказиш имконияти билан ўрнатилган иккита ярим шаффоф ойналардан (33, 36) ва акс эттирувчи пластинанинг устида жойлаштирилган ясси қаварик линзадан ташкил топган ва Ньютон ҳалқаларини шакиллантиргич билан таъминланган. Қурилма шунингдек предмет столчасида бурчак остида солиштириш тармоқларидан бирининг ва ярим шаффоф кўзгунинг (33) ўзаро перпендикуляр оптик ўқларида кесишиш нуқтасида жойлашган оғиш ойнаси, иккинчи солиштириш тармоғи ва ўтказувчи ойна (36) оптик ўқларининг кесишиш нуқтасида худди шундай бурчак остида предмет столчасининг устида Ньютон ҳалқаларини шакиллантирувчи ўтказувчи кўзгуси (36) ва назорат объекти орасида ўрнатилган ярим шаффоф кўзгу (29) билан таъминланган.

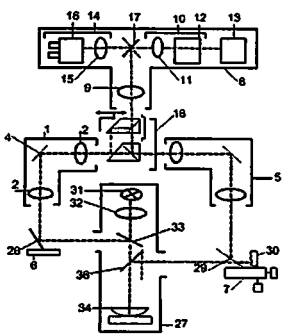
Илк бора Ньютон ҳалқаларини ҳосил қилувчи қурилмага, ёруғлик манбаи, линзалар, 2 та ярим шаффоф кўзгу, улардан бири силжиш имкониятига эга ва қайтарувчи пластинадаги ясси қаварик линзалар оптик ўқда кетма-кет жойлашган ҳалқаларни ҳосил қилувчи ўзаро перпендикуляр тармоқлардаги таққословчи ўқлардан бирида жойлашган нуқтада кесишувчи предмет столчасидаги қайтарувчи кўзгу ва биринчи ярим шаффоф кўзгу, иккинчи ярим шаффоф кўзгу, Ньютон ҳалқаларини ҳосил қилувчи силжувчи кўзгулар орасида маълум бурчакда жойлаштирилган ва иккинчи таққослаш ўқларининг оптик кесишиш нуқтасидаги предмет столчасидаги таққосланувчи объект ва алмаштирувчи кўзгулардан иборат.

Солиштириш тармоқлари (1) ва (5)нинг кириши Ньютон ҳалқаларини шакиллантирувчи (27), (6) предмет столчасига ўрнатилган қайтарувчи кўзгу (28) ва (30) объектдан олдин (7) предмет столчасида жойлаштирилган ярим

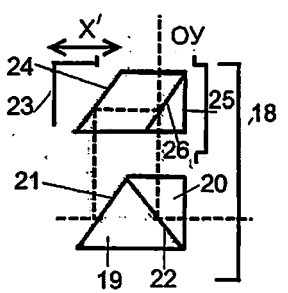
шаффоф кўзгу (29) билан оптик ўқ орқали боғланган. Ньютон ҳалқаларини шакллантиргич (27), (31) монохроматик ёруғлик манбаи, (32) линза, (33) ярим шаффоф кўзгу, (35) қайтарувчи пластинага ўрнатилган (34) ясси қаварик линза, (36) ярим шаффоф ўтказувчи кўзгидан ташкил топган.

Объект юзаси суратини таққослаш икки усулда: биринчи усул, нуқсонли ва деформацияланган объект юзаси натижавий нуқсонсиз объект юзаси билан реал эталон объекти мавжуд бўлмаганда таққослаш, иккинчи усул, мураккаб рельефли объект юзасини реал эталон объекти мавжуд бўлган ҳолда таққослаш орқали амалга оширилади.

Объект юзасини сурати бўйича уни қиёсий анализ учун қурилма (1-расм)да, 1 биринчи таққослаш тармоғи, 2, 3 объективлар, 4 оғдирувчи кўзгу. Биринчи тармоққа параллел жойлашган иккинчи таққослаш тармоғи 5, 6 ва 7 предмет столчаларидан иборат. Таққослаш микроскопи 8 кузатиш блоки, 9 объективни ўз ичига олади, 10 телевизион канал, 11 объектив, 12 телекамера, 13 компьютер мониторидан иборат ва кўриш канали 14, 15 объективдан, 16 бинокуляр оптик тизим 17 ўзгарувчи кўзгулардан иборат эканлиги кўрсатилган.




**1- расм. Объект юзасини суръати бўйича уни қиёсий анализ учун қурилманинг схемаси**




**2- расм. Ньютон ҳалқаларини ҳосил қилувчи бўлувчи призмалар**

қонуний фойдаланувчисига таъсир ўтказадилар ва қалтисликларни қўллайдилар.

$a_i = g_j(f_i, q_{j,1}, \ldots)$ – қалтисликлар воситасида тизим функционалларига таъсир ўтказиш орқали АТ бойликларини олишга имкон берадилар.

$q_m = g_j(f_i, q_{j,1}, \ldots)$ – АТ функционаллари ва бошқа қалтисликлар орқали АТ (янги қалтисликлар) тўғрисидаги айрим маълумотларни олишга имкон берадилар.

Ушбу функционалларнинг кириш учун қулайлигини ҳисобга олиб, АТ функционалларини кўплик остига ажратган ҳолда *ташқи ва ички бузғунчи*ни тавсифлаш мумкин.

$F_1 \subset F$ тўплми остида улардан фақат назоратдаги ҳудуд (НҲ) ичидагина фойдаланиш имконига эга бўлиш мумкин бўлган функционаллар ажратилади.

Шунда бундай $G_j = \{g_{j,1}, g_{j,2}, \ldots\} \subset G$ га эга бўлган кўплаб бузғунчиларда $\forall g \in G_j \forall x \in F_2 \forall q_1, \ldots \in Q_j\ g(x, q_1, \ldots) = NO$ бўлади ва улар қатъий ташқи функционаллар деб аталади. Бу ерда *NO* функционалнинг воз кечишига мос келади. Бу ерда $Q_j$ маълумотларидаги фақат ушбу бузғунчи фойдаланиши мумкин қалтисликлари назарда тутилмоқда.

Функционаллари $G_j = \{g_{j,1}, \ldots\} \subset G$, $\exists g \in G_j\ \exists x \in F_2\ \exists q_1, \ldots \in Q_j\ g(x, q_1, \ldots) = a_i \in A$ бўлган бузғунчи ички деб аталади. Бу ерда $Q_j$ маълумотларидаги фақат ушбу бузғунчи фойдаланиши мумкин қалтисликлари назарда тутилмоқда.

Агар $a_i$ ахамияти ички бузғунчи томонидан $x \in F_1$бўлган жойдан $g(x, q_1, \ldots)$, $x \in F_1(x, q_1, \ldots)$, ёрдамида олинган бўлса, бундай ҳолда мазкур бузғунчи ташқи (бироқ қатъий ташқи эмас) бузғунчи деб аталади.

Диссертациянинг **«Очиқ кодли операцион тизимлар учун ҳимояланган қурилмалар драйверларини жорий этиш усуллари»** деб номланган иккинчи бобида оддий белгили драйвер мисолида «HUMO» ОТ тизимида драйверларни амалга ошириш тамойилари кўрсатилган. Ускуналар билан ўзаро боғланиш ёки тизимдаги имтиёзли ахборотдан фойдаланиш ҳаракатларини амалга ошириш учун драйвер ядролари керак бўлади. «HUMO» ОТ ядросининг модули – бу компилятсияланган иккилик коди бўлиб, ички ва бирмунча кам ҳимояланган қобиғида x86-64 процессоридаги буйруқни бажаришда бевосита «HUMO» ОТ ядросига қўйилади. Бу ерда мутлақо ҳеч бир текширувларсиз, юқори тезликда ва тизимдаги ҳар қандай ресурсларга кириш ҳуқуқига эга бўлган код ижро этилади. Ядрони ўзгартиришда маълумотларни йўқотиш хавфи юзага келади. Ядро кодида «HUMO» ОТ иловаларидаги каби стандарт ҳимоя мавжуд эмас.

Қурилмалар билан ўзаро боғланиш ёки ҳаракатларни амалга ошириш учун қурилма драйвери зарур. Қурилмалар билан хавфсиз муомалада бўлиш ва хавфсиз ишлашни таъминлаш мақсадида дастур талаб қилинади. Ядро қурилмалар билан мос драйверлар орқали ўзаро ҳаракатланади. Қурилма драйвери – бу хизмат кўрсатиш учун қўлланилувчи функциялар йиғиндисидир. «HUMO» ОТнинг муҳим хоссаларидан бири – драйверларнинг динамик равишда юклаш имкониятидир. Бу каби ташкиллаштиришда

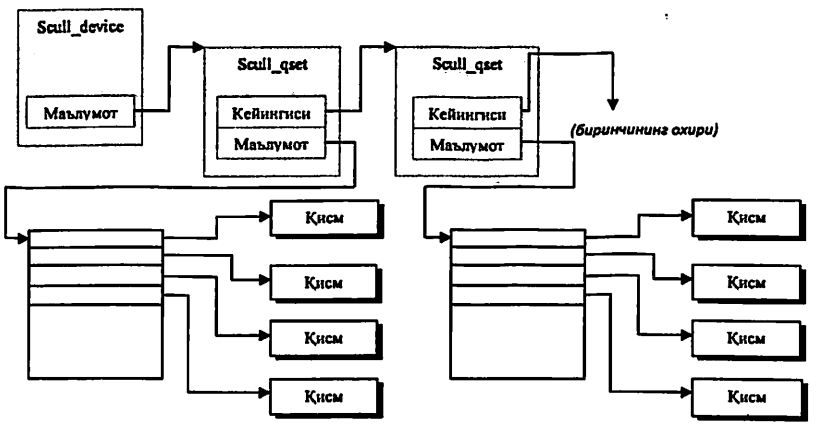
драйвер модули ядронинг бир қисмига айланади ва унинг функцияларига бемалол мурожаат қилиши мумкин. Бундан ташқари, динамик равишда юкланган драйвер, ўз навбатида динамик равишда бўшаши мумкин. Агар драйвер очиқдан-очиқ тарзда бўшамаган бўлса, бу ҳолда у тизимда доимий – кейинги қайта юклашга қадар қолади.

Белгили драйвер – бу белгили қурилмалар билан ишловчи драйвер. Белгили қурилмалар – бу мурожаат қилиш мумкин бўлган байтлар каби қурилма. /dev/ttyS0, /dev/tty1 белгили қурилмага мисол бўлади. Кўргазмалилик учун 1-расмга қаранг.

*Инициализациялаштириш методи.* «alloc_chrdev_region»ни чақирар эканмиз, қурилманинг белгили диапазонини қайд этамиз ва қурилма номини кўрсатамиз. Шундан сўнг MAJOR(dev) чорловига кўра катта сонни оламиз.

Кейинроқ агар у хатоликлар коди бўлса, қайтган қиймати текширилади ҳамда функциядан чиқиш амалга оширилади. Таъкидлаш жоизки, қурилманинг ҳақиқий драйверини ишлаб чиқишда ҳар доим қайтувчи қийматларини ҳамда ҳар қандай элементлар кўрсаткичини текшириши зарур. Агар қайтувчи қиймат хатолик коди бўлмаса, инициализация-лаштиришни бажаришда давом этамиз.

*Ўчириш методи.* Қурилма модулини ядродан олиб ташлашда «scull_cleanup» функцияси чақирилади. Инициаллаштиришнинг тескари жараёнида қурилма тузилмалари олиб ташланади, хотира бўшатилади ва ядро томонидан белгиланган кичик ва катта рақамлар олиб ташаланади.



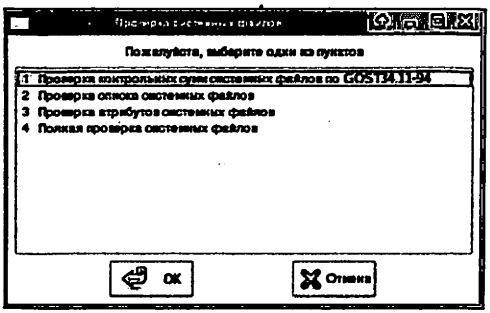

**1-расм. Кўрсаткичларнинг рўйхатини боғловчи чизма**

Диссертациянинг **«Очиқ кодли операцион тизимларининг хавфсизлик воситалари»** дея номланган учинчи бобида асосий вазифаси тизимдаги ташқи қурилмаларни ва фойдаланувчиларни тартиб билан қайд этиш ҳамда шу каби қайд этувчи маълумотлар билан ишлаш учун воситаларни тақдим этиш, тизим файлларининг яхлитлигини текшириш

ҳамда тизимдаги ҳодисаларни таҳлил қилиш ва вақтни белгилашдан иборат бўлган маълумотларни ҳимоялаш учун дастурлар ишлаб чиқилган.

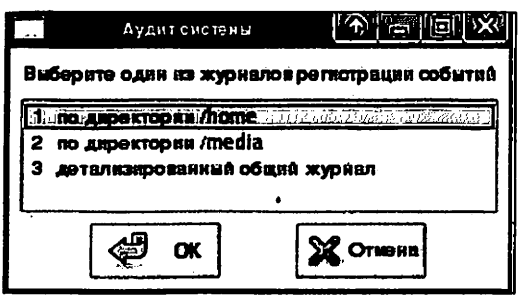
Бошқарув учун утилиталар йиғиндиси тизимдаги қайд этиш журналларини юритиш, ОТнинг яхлитлик контекстидаги ҳолатини текшириш, каби тизимдаги муҳим вазифаларни бажаришга имкон берувчи интерфейс орқали қўшимча созламаларни талаб қилмайдиган, тушунарли ОТда хавфсизликни таъминлаш учун яратилган. Утилиталарнинг ҳар бир йиғиндисидаги дастурлар қуйидаги вазифаларни бажаради:

*Тизимдаги файллар яхлитлигини текшириш дастури* – ОТ хавфсизлигини таъминлашнинг қўшимча механизми саналади. ОТдаги шу каби файллар ва директорияларни ва, шу жумладан, улар белгиларининг ўзгариш ҳодисалари ҳолатини кўл бошқаруви тартибида текширишга имкон беради (2-расм).




**2-расм. Тизим файллари яхлитлигини текшириш дастуридан лавҳа**

*Тизим аудити дастури* – ўтган ҳафтада /home и /media директорияларида юз берган ҳодисалар таҳлили учун график (ёзма) интерфейсни намоён қилади (3-расм.).

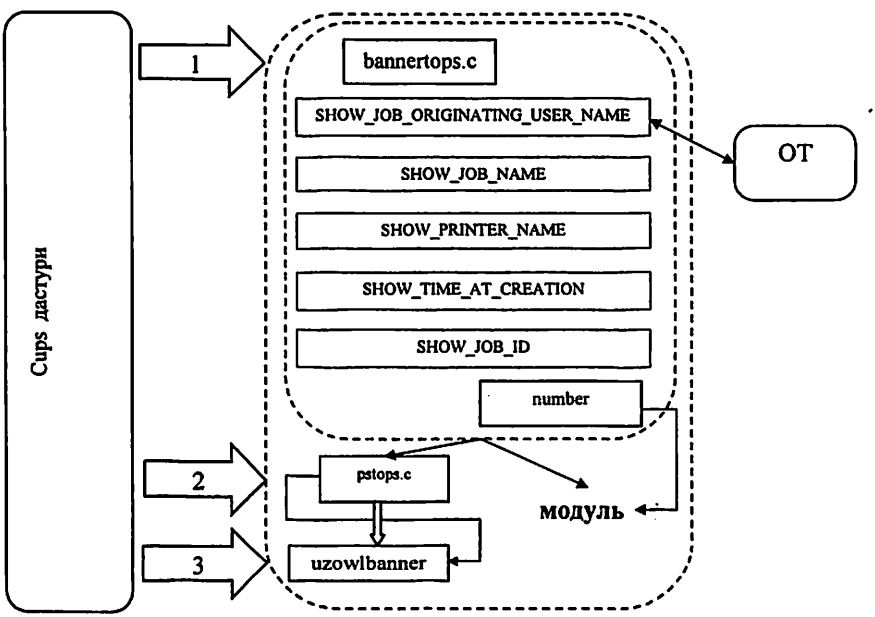



**3-расм. Тизим аудити дастури лавҳаси**

*Оператив (тезкор) хотирани тозалаш учун дастур* – оператив хотирадаги маълумотларнинг тарқалиб кетиш ҳолатига барҳам бериш мақсадида оператив хотирани тозалаш учун график интерфейсни намоён қилади.

*Файллар тизими объектларининг махфийлик даражасини ўзгартириш учун дастур* – график қобиқнинг контекстли менюсини қўллаган ҳолда файллар тизими объектларини уларнинг қайта тиклаш имкониятини қолдирмай туриб махфийлик даражасини ўзгартириш учун график интерфейсни намоён қилади.

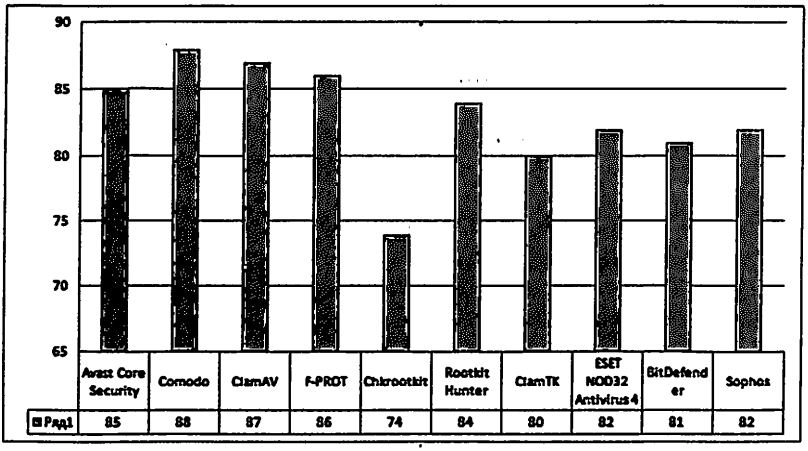
*Босмадан чиқарилаётган ҳужжатларни маркировкалаш дастури* – тегишли реквизитларга эга бўлган жўнатилувчи ахборот билан ҳужжатларни босмадан чиқаришда маркировкалаш учун дастур: ходимнинг Ф.И.Ш ни қўйиш, ҳужжатни (файл номини) номлаш, принтернинг ёки компьютернинг қайд этиш рақами, чоп этилаётган сахифалар сони, ҳужжатни чоп этишнинг вақти ва санаси (5-расм).




1, 2, 3 – файлларни бажариш кетма-кетлиги

**5-расм. Чоп этилаётган ҳужжатларни маркировкалаш дастури схемаси**

Ҳимояланаётган «HUMO» ОТ учун антивирус дастури тавсия қилинди. Тест натижаларига кўра элликдан ортиқ тестларда очиқ кодли «Comodo» антивируси танланди. Натижалар диаграмма кўринишида келтирилган (4-расм).




**4-расм. Антивирус дастурларини қиёсий таққослаш диаграммаси**

Диссертациянинг **««HUMO» операцион тизимининг киришни назорат қилиш воситалари»** дея номланувчи тўртинчи бобида киришни чекловчи қоидалар модели учун дастурлар ишлаб чиқилган.

*Чекловнинг дискрецион назорати асосида:*

• Файлни яратишда тизим бошқарувчисига автоматик равишда фойдаланувчи ва унинг гуруҳи учун ўқиш ва ёзиш ҳуқуқи берилади ва ушбу барча ҳуқуқлар бошқалар учун таъқиқланади.

• Агар фойдаланувчи бир нечта қайд этувчи ёзувларга эга бўлса, у ҳолда улар фойдаланувчининг турли қайд этувчи ёзувлар орқали яратилган ўзининг барча файлларига киришини осонлаштириш учун уларни ягона гуруҳга бирлаштириш мумкин.

• Қайд этувчи ёзувларига эга бўлган турли фойдаланувчилар ўртасида файлларни узатиш учун тизимда барча фойдаланувчилар учун файлларга кириш бирдек бўлган махсус умумий каталоглар ажратилиши мумкин.

• Турли фойдаланувчиларнинг қайд этувчи ёзувлари ўртасида файлларни узатиш учун тизимдаги барча фойдаланувчиларнинг файлларга кириши бир хил бўладиган махсус умумий каталогларга ажратилиши мумкин.

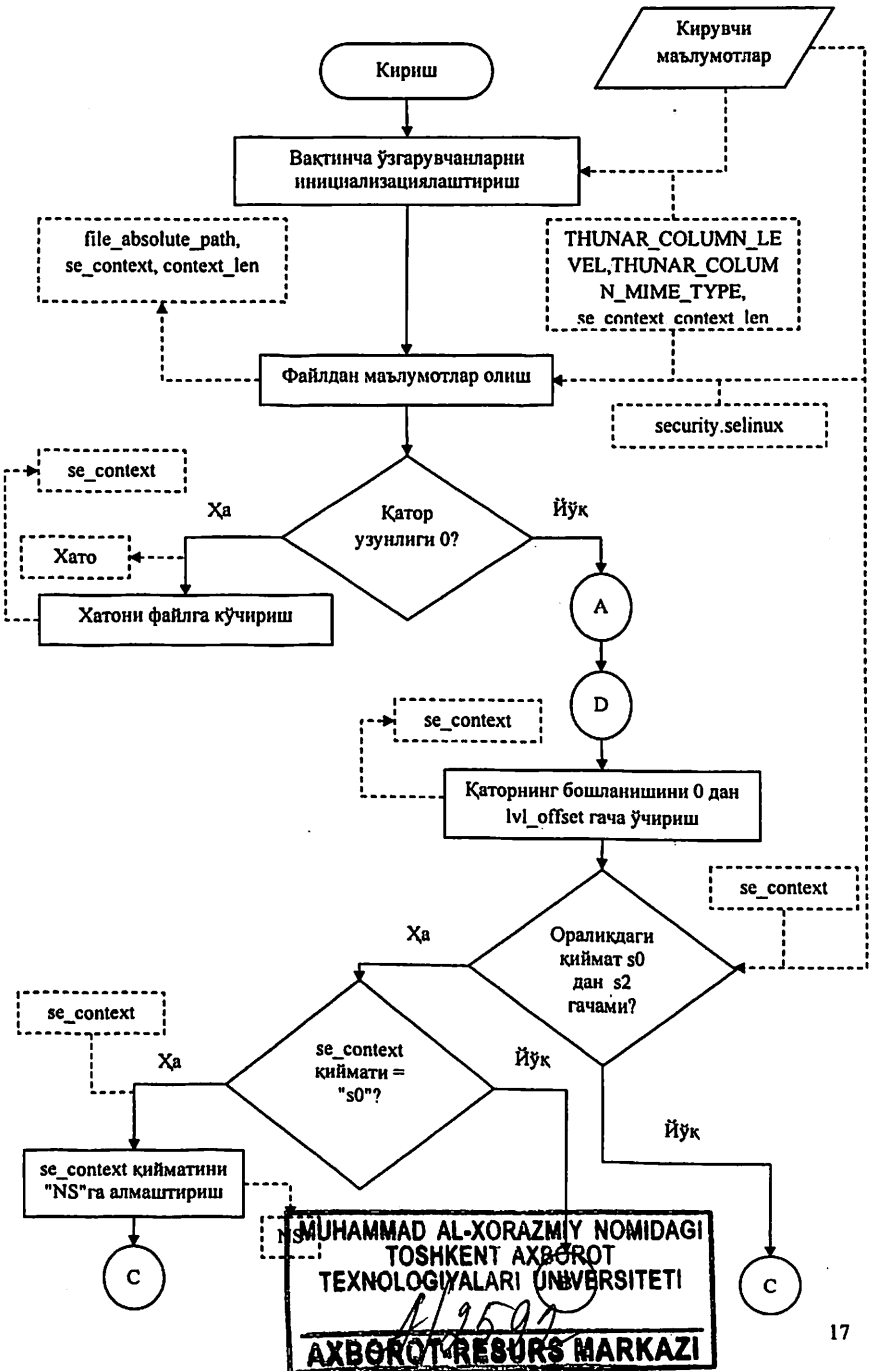
• Фойдаланувчи шахсий файлларига кириш ҳуқуқини ўзгартириш ҳуқуқига эга.

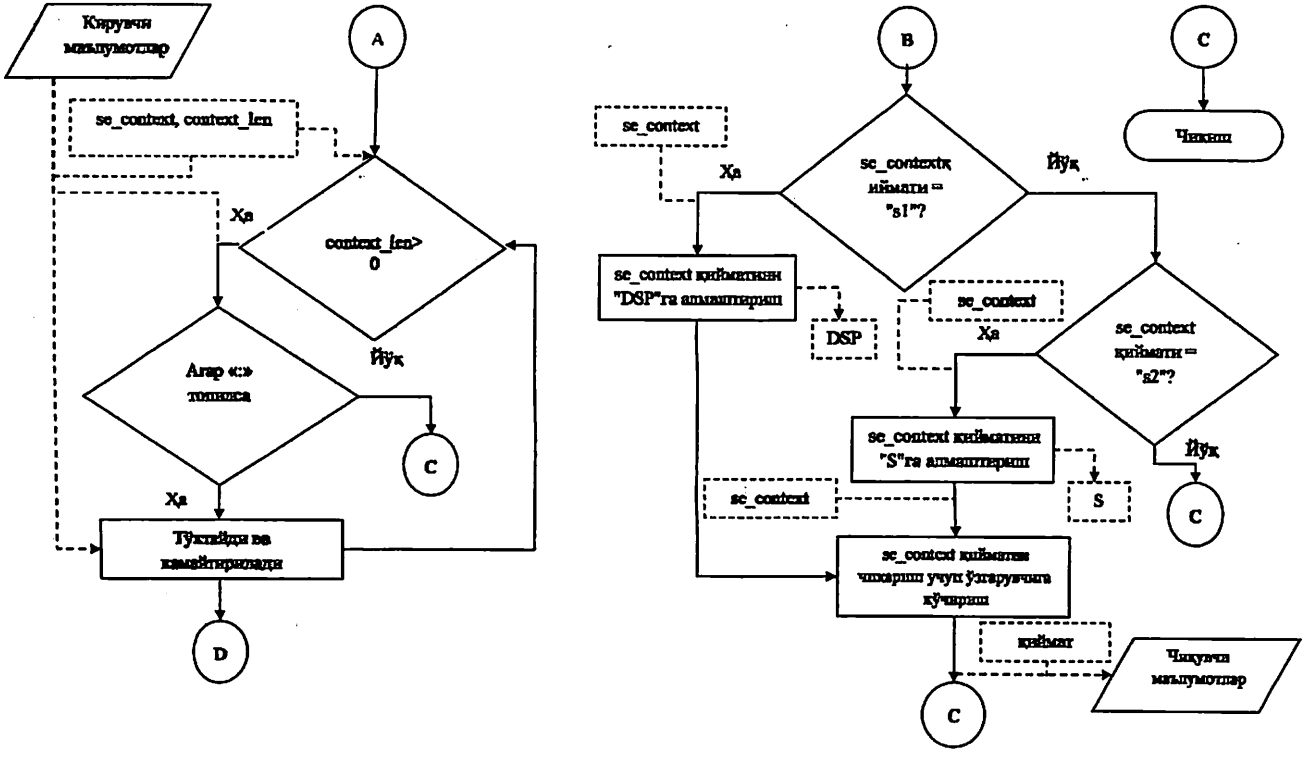
• Тизим бошқарувчиси (администратори) кириш чекловига эга эмас.

*Чекловнинг мандат назорат қилиш асосида:*

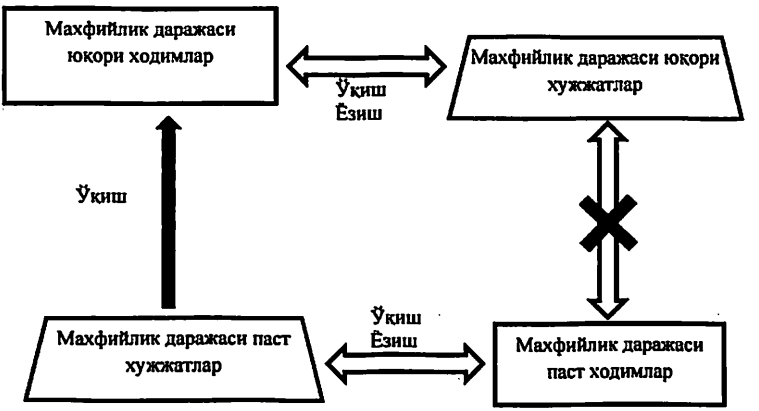
• Фойдаланувчининг қайд этувчи ёзувлари киришнинг фақат биргина даражасига эга.

• Тизимдаги фойдаланувчининг қайд этувчи ёзувлари мандат таксимотига кўра учта даражага бўлинади: s0 (махфийликнинг паст даражаси), s1 (ўрта даражаси), s2 (баланд даражаси).






**6-расм. «HUMO» ОТнинг мандат назорати дастурининг блок-схемаси**




**7-расм. «HUMO» ОТнинг киришнинг мандат назорати алгоритми схемаси**

• Кириш даражасидан келиб чиққан ҳолда бир фойдаланувчида учтагача қайд этувчи ёзувлар бўлиши мумкин. Жумладан, s0 биргина қайд этувчи ёзувга, s1 – иккита қайд этувчи ёзувга, s2 – эса учта қайд этувчи ёзувга эга (6-расм).

• Фойдаланувчи қайд этувчи ёзув остида махфийлик даражаси ушбу қайд этувчи ёзувга кириш даражасига тенг бўлган файлларни яратиш, таҳрир қилиш ва ўқиш ҳуқуқига эга.

• Фойдаланувчи қайд этувчи ёзув остида махфийлик даражаси ушбу қайд этувчи ёзувга кириш даражасига тенг ёки паст даражадаги файлларни ўқиш ҳуқуқига эга (7-расм).

• Бошқа барча ҳолатларда кириш рад этилиши керак.

• Янги файлни яратишда унга фойдаланувчининг ушбу қайд этувчи ёзувига кириш даражасига мос бўлган махфийлик даражаси берилади.

• Ахборотни хавфсизликнинг бошқа даражасига узатиш зарур бўлган ҳолларда файлларнинг махфийлик нишонини ўзгартириш учун хавфсизлик маъмури (администратори) жалб этилиши лозим.

• Иловалар ва сервисларга мурожаат Linux ОТнинг стандарт дискрецион модели, тизимга киришни бартараф қилувчи илова (мослама)лар ва созлаш қурилмалари асосида амалга оширилади. Шу тариқа фойдаланувчи кириш ёки махфийликнинг ҳамда файллар махфийликларининг ўзига тегишли ёки бошқа даражаларига ўзгартириши мумкин эмас.

# ХУЛОСА

"Очиқ кодли операцион тизимларнинг ахборот хавфсизлигини таъминлаш воситалари ва усуллари" мавзуидаги диссертация бўйича қуйидаги натижалар намоён қилинган:

1. Ахборот хавфсизлиги соҳасига асос бўлувчи миллий ва халқаро стандартлар ҳамда ахборот хавфсизлиги борасидаги бошқа ҳужжатларни таҳлил қилиш натижасида, АТ қадриятлари таснифи, таҳдидлар таснифи, шакллантирилган, таянч модели (ОТ томонидан ишлаб чиқилган) асосида таҳдидлар манбаларига тасниф берилган, бузғунчининг таянч модели ва унинг имкониятлари шакллантирилган ҳамда АТ хавфсизлик таҳдидларини аниқловчи бузғунчининг математик модели ишлаб чиқилган. Математик модел АТ хавфсизлик таҳдидларини аниқлашга имкон берган.

2. «HUMO» ОТ хавфсиз операцион тизими ядросидаги қурилмаларни ўчириш ва инициализациялаш усулларининг такомиллашган алгоритмлари ишлаб чиқилган. Алгоритм кодидаги ортиқча функциялар миқдорини камайтириш ёрдамида алгоритмнинг иш вақтини 8,3 маротабага камайтиришга имкони яратилган.

3. Дастурлар билан ишлаш учун график воситалар ишлаб чиқилган ҳамда халқаро ва мамлакатимиз стандартлари асосида воқеа-ҳодисаларни ҳисобга олиш ва таркибий тизимни қайд этиш, таркибий тизимнинг яхлитлигини таъминлаш, чоп этилаётган ҳужжатларни маркировка механизмлари, тезкор хотирани тозалаш дастурлари, алгоритмлардан ташкил топган операцион тизимлар хавфсизлиги воситалари ишлаб чиқилган. Ишлаб чиқилган хавфсизлик воситалари Ўзбекистон Республикасининг O'z DSt 2817:2014 асосида 2А даражадаги хавфсизлик талабларига жавоб бериш имкониятини берди.

4. Белла–ЛаПадула классик модели асосида мандатли модель модернизациялаштирилган ҳамда кўп босқичли назорат хоссаларини сақлаган ҳолда, фойдаланишни назорат қилишнинг бирмунча содда сиёсати ишлаб чиқилган. Фойдаланишни назорат қилишнинг бирмунча содда сиёсати кўп босқичли назорат хоссаларини такомиллаштириш имконини беради.

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

**НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА**

**ОЧИЛОВ НИЗОМИДДИН НАЖМИДДИН ЎҒЛИ**

# МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ С ОТКРЫТЫМ КОДОМ

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

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

**Ташкент-2019**

**Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2019.2.PhD/T1107.**

Диссертация выполнена в Национальном университете Узбекистана.

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:** | **Каримов Маджит Маликович**<br>доктор технических наук, профессор |
| **Официальные оппоненты:** | **Мухамедиева Дилноз Тўлкуновна**<br>доктор физико-математических наук, профессор |
| | **Туйчиев Ғулом Нумонович**<br>доктор физико-математических наук |
| **Ведущая организация:** | **«UNICON.UZ» – центр научно-технических и маркетинговых исследований** |

Защита диссертации состоится «8» 10 2019 года в 14:00 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 «31» 10 2019 года.
(протокол рассылки №19 от «8» 10 2019 года.)

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

**К.Ф. Керимов**
Заместитель председателя научного совета по присуждению ученых степеней, к.т.н., доцент

**Р.Ж. Алоев**
Председатель научного семинара при Научном совете по присуждению ученых степеней, д.ф-м.н. проф.

## ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

**Актуальность и востребованность темы диссертации.** В мире особое внимание уделяется разработке и совершенствованию систем информационной безопасности (ИБ). При нынешнем уровне развития информационных и коммуникационных систем становятся особенно актуальными вопросы защиты операционных систем, которые являются одними из наиболее важных механизмов обеспечения эффективной информационной безопасности. «Согласно данным Интерфакса, число киберпреступлений в Германии в 2016 году выросло в 1,8 раза по сравнению с 2017 годом, а раскрытие таких атак в 2016 году увеличилось на 38,7% против 32,8% в предыдущем году»[1]. По данному вопросу в зарубежных странах, таких как США, Нидерланды, Германия, Великобритания, Швеция, Франция, Южная Корея, Китай, Российская Федерация и других государствах были отмечены определенные сферы, где уделяется особое внимание созданию программно-аппаратных средств механизмов защиты операционных систем, обеспечивающих высокую защищенность компьютерных систем.

В мире особую важность приобретает совершенствование эффективных методов и средств защиты операционных систем, повышение их эффективности до уровня классов защищенности операционных систем. В этом отношении в научно-исследовательских работах особое внимание уделяется следующим аспектам: разработка методов, ограничивающих использование определенных категорий ресурсов с целью обеспечения надежной защиты компьютерных систем; разработка методов и программных комплексов защиты системных данных операционной системы на основе комплексов средств защиты (КСЗ), таких как: аудит, изоляция модулей, очистка оперативной памяти, проверки целостности системных файлов и т.д.; создание моделей защиты данных на основе моделей прав доступов.

В республике наряду с развитием информационных технологий в органах государственного и хозяйственного управления особое внимание уделяется защите данных от системных угроз и широкому применению методов и средств защиты информации в компьютерных системах. В связи с этим были достигнуты значимые результаты по обнаружению и предотвращению угроз и атак в компьютерных системах, в частности, с целью обеспечения защищенности компьютерных систем была начата разработка системы обнаружения и предотвращения угроз, системы мониторинга информационной безопасности. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 годах определены задачи, в том числе, «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[2]. Реализации

[1] https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/343228.php

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

таких операционных систем, в том числе создание моделей, методов и алгоритмов средств защиты, снижающих влияние внешних угроз, являются важными задачами, стоящими перед специалистами в области информационных технологий.

Данное диссертационное исследование, в определенной степени, служит выполнению задач, предусмотренных Указом Президента Республики Узбекистан № УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», № УП-5264 от 29 ноября 2017 года «Об образовании Министерства инновационного развития Республики Узбекистан», Постановлением Президента Республики Узбекистан № ПП-1989 от 27 июня 2013 года «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан», а также другими нормативно-правовыми документами, принятыми в данной сфере.

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

**Степень изученности проблемы.** Л.Торвальдс, Р.Херцог, Б.Керниган провели исследования по разработкам операционных систем семейства Linux. Изучены научно-исследовательские работы зарубежных и отечественных ученых, таких как: Р.Пайк, Б.Уорд, Д.Барретт, С.Алапати, А.Робачевский, Д.Н.Колиснеченко, М.Фленов, С.Немнюгин, О.Стесик, Т.Адельштайн, Б.Любанович, С.Л.Скловская в сфере создания систем защиты данных в ОС Linux. В научных разработках стран СНГ, а также Республики Узбекистан были изучены операционные системы, как «Astra Linux», операционные системы (ОС) «Заря», «Альт Linux», «РОСА» по разработке методов и средств защиты информации, теоретико-практической концепции защиты информации, различных моделей, методов и алгоритмов средств защиты, алгоритмов шифрования. «Doppix» изучены графические оболочки, применяющиеся в различных государственных учреждениях.

В научных статьях Х.А. Музаффарова и А. Икрамова рассмотрены метод построения системы защиты, шифрования данных с алгоритмом ГОСТ 28147-89. В научных трудах Д. Н. Колиснеченко, В. Аллена (журнал Linux Format, все номера за 2014, 2015 и 2016) были исследованы структуры и алгоритмы ядра ОС Linux, скорости обработки пакетных данных, модели безопасности, средства обеспечения безопасности.

Вместе с тем не полностью проанализированы методы и средства защиты от сетевых угроз, выявлены недостатки в существующих алгоритмах реализации драйверов устройств, защищающих от несанкционированных воздействий.

**Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация.** Диссертационное исследование выполнено в

рамках научных проектов согласно плану научно-исследовательских работ Национального Университета Узбекистана в рамках научного проекта согласно (2015-2017) № 5/15 «Разработка операционной системы специального назначения для специализированных персональных электронно-вычислительных машин на основе операционной системы с открытым кодом».

**Целью исследования** является разработкой специальных методов и средств обеспечения безопасности в ОС открытым исходным кодом, удовлетворяющих требованиям стандарта Республики Узбекистан в области секретного делопроизводства и отвечающих требованиям безопасности, классу 2А в соответствии с O'zDSt 2817:2014.

**Задачи исследования:**

проанализировать основополагающие международные и национальные стандарты и иные документы в области информационной безопасности, а так же современных безопасных ОС специального назначения с открытом кодом;

разработать модернизированный алгоритм метода инициализации и удаления драйвера устройств в ядре безопасной операционной системы на основе символьного драйвера;

разработать средств безопасности операционных систем с открытым кодом, удовлетворяющих требованиям стандарта Республики Узбекистан на основе модели угроз и нарушителя безопасности, состоящих из очистки оперативной памяти, механизмы маркировки выводимых на печать документов, подсистемы обеспечения целостности, подсистемы регистрации и учета событий по принципу международных и отечественных стандартов, а так же графические инструменты для работы с программами;

разработка системы контроля доступов, с сохранением свойств многоуровневого контроля, для модуля идентификация и аутентификация.

**Объектом исследования** являются программы и модули защиты операционной системы.

**Предметом исследования** являются методы и технологии построения защищённых операционных систем на основе операционной системы Linux.

**Методы исследования.** В процессе исследования использованы методы защиты информации в операционных системах с открытым кодом, теории алгоритмов, методы математического моделирования, процедурно- и объектно-ориентированное программирование.

**Научная новизна исследования** заключается в следующем:

разработана математическая модель нарушителя, его возможности, на основе модели нарушителя (разработанной ФСТЭК (Федеральной службы по техническому и экспортному контролю)), проанализировав основополагающие международные и национальные стандарты;

модернизирован алгоритм метода инициализации и удаления драйвера устройств на основе символьного драйвера;

созданы средств безопасности операционных систем с открытым кодом, удовлетворяющие требованиям стандарта Республики Узбекистан на основе модели угроз и нарушителя безопасности, состоящих из алгоритма,

программы очистки оперативной памяти, механизмы маркировки выводимых на печать документов, подсистемы обеспечения целостности, подсистемы регистрации и учета событий, а так же разработаны графические инструменты для работы с программами на основе модели угроз и нарушителя безопасности;

усовершенствованы системы контроля доступов, с сохранением свойств многоуровневого контроля, для модуля идентификация и аутентификация.

**Практические результаты исследования** заключаются в разработке математического моделя автоматизированных систем (АС) и нарушителя на основе базовой модели нарушителя;

модернизирован алгоритм метода инициализации и удаления устройств на основе символьного драйвера;

разработаны систем безопасности операционных систем с открытым кодом, удовлетворяющих требованиям стандарта Республики Узбекистан на основе модели угроз и нарушителя безопасности, состоящих из очистки оперативной памяти, механизмы маркировки выводимых на печать документов, подсистемы обеспечения целостности, подсистемы регистрации и учета событий на основе отечественных стандартов;

разработана система контроля доступов, с сохранением свойств многоуровневого контроля, для модуля идентификация и аутентификация.

**Достоверность результатов исследования.** Обеспечена обоснованностью методологии работы; проведением исследования на теоретическом и практическом уровнях; методами, адекватными предмету, цели и задачам исследования; использованием качественной и количественной оценки результатов.

**Научная и практическая значимость** результатов исследования заключается в практической апробации предложенных в работе алгоритмов и программных средств, позволяющих существенно расширить функциональные возможности информационной безопасности системы на основе реализации концепции разделения и совместного использования логической и физической защиты данных. Разработаны модели и предложены механизмы функционирования универсальной инфраструктуры для обработки и защиты информации. На основе предложенных алгоритмов разработаны системы безопасности для операционных систем с открытым кодом в соответствии с законодательством Республики Узбекистан, отвечающая требованиям безопасности.

Практическая значимость темы исследования заключается в разработке системы обеспечения информационной безопасности, которая может быть применена в коммерческих или государственных учреждениях, связанных с использованием его выводов государственными и силовыми органами, для обеспечения защиты информации в области секретного делопроизводства и отвечающих требованиям безопасности, классу 2A в соответствии с O'zDSt 2817:2014. Реализация результатов исследования на практике способна обеспечить проведение более обоснованной и целенаправленной политики

информационной безопасности в министерствах и ведомствах Республики Узбекистан, связанных с использованием информационных систем и технологий.

**Внедрение результатов исследования.** На основе результатов созданных алгоритмов по применению методов и средств обеспечения информационной безопасности внедрены:

средства контроля доступов, с сохранением свойств многоуровневого контроля, для модуля идентификация и аутентификация внедрена в деятельности в отделе Сурхандарьинской области Государственного центра тестирования при Кабинете Министров Республики Узбекистан (справка Государственного центра тестирования при Кабинете Министров Республики Узбекистан от 25 сентября 2019 года №104). Дает возможность для усовершенствования средств многоуровневого контроля доступов, с сохранением свойств многоуровневого контроля;

модернизация алгоритма метода инициализации и удаления драйвера устройств в ядре безопасной операционной системы на основе символьного драйвера внедрена в деятельности ООО "Infoteka" (справка Государственного центра тестирования при Кабинете Министров Республики Узбекистан от 25 сентября 2019 года №104). В результате разработанный программный метод инициализации и удаления устройств в ядре безопасной операционной системы позволяет сократить время работы устройств до 8,3 раза;

на основе разработанных специальных систем защиты, программы и алгоритмов защиты данных в ОС «HUMO» прошли положительную экспертизу в Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан, и принята для ввода в эксплуатацию (справка Государственного центра тестирования при Кабинете Министров Республики Узбекистан от 25 сентября 2019 года №104). Применение разработанного на основе результатов проведенного исследования программного комплекса и методов защиты информации в ОС с открытом кодом позволяет повысить уровень защищенности данных от несанкционированного обращения к объектам и определить их эффективность при построении защищенных операционных систем.

**Апробация результатов исследования.** Результаты данного исследования были обсуждены в 2-х международных и в 2-х тезисах республиканской научно-практической конференции.

**Публикация результатов исследования.** По теме исследования опубликованы всего 14 научных работ, из которых 4 статьи в журнальных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 2 иностранных и 3 статьи в журнальных изданиях с

грифом ДСП, а также получены 3 свидетельства о регистрации программных продуктов для ЭВМ.

**Структура и объем диссертации.** Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 114 страниц.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

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

Первая глава диссертации, озаглавленная как **«Модели угроз и нарушителя безопасности»**, посвящена основным понятиям, необходимым для определения модели угроз и модели нарушителя. Был изучен достаточно широкий набор международных и национальных стандартов и иных документов в области информационной безопасности (ИБ).

Предлагаются базовая модель угроз и базовая модель нарушителя.

Результаты анализа возможностей, которыми может обладать нарушитель, приводится в рамках модели нарушителя.

При разработке модели нарушителя использованы следующие положения:

1. Безопасность автоматизированных систем (АС) обеспечивается средствами защиты информации, и используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемыми в соответствии с законодательством Республики Узбекистан[3].

2. Средства защиты информации (СЗИ) функционируют в сочетании с аппаратным и программным обеспечением, которое влияет на выполнение требований.

3. СЗИ не может обеспечить защиту от действий, совершаемых в рамках полномочий, предоставленных субъекту действий.

Для определения модели угроз и модели нарушителя нужно определить следующее:

*Описание нарушителей:* К контролируемой зоне (КЗ) относятся все конструкции, здания и помещения, из которых может быть осуществлен доступ к АС.

Модель АС содержит множество ценной информации $A = \{a_1, a_2, \ldots\}$.

[3] O'z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»

АС также содержит множество функционалов $F = \{f_0, f_1, f_2, \ldots, f_m, \ldots\}$, позволяющих получать ценную информацию АС (обрабатывать, изменять, получать информацию).

Операции с АС выполняют пользователи, которые составляют конечное множество $U = \{u_0, u_1, \ldots, u_n\}$.

Каждому из пользователей соответствует множество разрешений и ограничений, задаваемых $R_i = \{r_{i,1}, r_{i,2}, \ldots\}$, где $r_{i,j}$ определяет, какой доступ имеет пользователь $u_i$ к ценности $a_j$.

Каждый пользователь для авторизации имеет свой ключ (пароль), все ключи всех пользователей составляют вместе множество $K = \{k_1, k_2, \ldots, k_n\}$ (индекс ключа соответствует индексу своего пользователя). $f_0(x, y)$ - особый функционал, позволяющий проверять соответствие пароля и имени пользователя: $f_0(u_i, k_i) = 1$, во всех остальных случаях функционал равен 0 (неверное имя пользователя или пароль).

Многие из функционалов системы при использовании запрашивают подтверждение через $f_0$. Это происходит, например, когда пользователь хочет получить доступ к $a_j$, которое принадлежит другому пользователю, но по иерархии доступа первый пользователь имеет на это право (должен лишь подтвердить это). Применительно к ОС, $f_0$ – это функционал авторизации в системе.

Таким образом, набор <A, F, U, K, R> называется моделью АС.

АС называется безопасной, если все действия пользователей и функционирование АС полностью соответствует ограничениям R.

Уязвимостями называется множество значений данных $Q = \{q_1, q_2, \ldots\}$, которые содержат некоторую информацию, позволяющую в определенных условиях выполнять действия, противоречащие ограничениям R. Эти уязвимости могут относиться не только к АС.

После описания системы можно перейти к описанию злоумышленников.

Злоумышленник задаётся множеством функционалов $G = \{g_1, g_2, \ldots\}$, которые используя данные Q позволяют выполнять некоторые угрозы.

Указанные выше подмножества могут иметь непустые пересечения, что свидетельствует о вложенности некоторых функционалов в возможности нескольких видов злоумышленников. Так как некоторые злоумышленники могут одновременно удовлетворять условиям нескольких нарушителей, то далее это разделение явно не будет описываться при построении модели, тем самым полученная модель будет максимально общей и охватывать все возможные случаи.

Функционалы действуют следующим образом:

$k_i = g_j(u_i, q_{j,1}, \ldots)$ – позволяют получить пароль пользователя $u_i$. Такие функционалы соответствуют, в конечном счёте, внутренним злоумышленникам, так как использование пароля вне АС не даст никаких результатов.

$a_i = g_j(u_t, q_{j,1}, \ldots)$ – позволяют получить ценности АС. Действуют на законного пользователя АС и используют уязвимости.

$a_i = g_j(f_t, q_{j,1}, \ldots)$ – позволяют получить ценности АС, действуя на

функционалы системы через уязвимости.

$q_m = g_j(f_i, q_{j,1}, \ldots)$ – позволяют получить некоторые данные о АС (новые уязвимости) через функционалы АС и другие уязвимости.

Разделяя функционалы АС на подмножества, учитывая доступность этих функционалов, можно описать *внешнего и внутреннего злоумышленника.*

В подмножество $F_1 \subset F$ выделяются функционалы, доступ к которым можно получить извне контролируемой зоны (КЗ) (например, электросеть, сети коммуникаций).

В подмножество $F_2 \subset F$ выделяются функционалы, доступ к которым можно получить только внутри КЗ.

Тогда злоумышленники, у которых множество $G_j = \{g_{j,1}, g_{j,2}, \ldots\} \subset G$ такое, что $\forall g \in G_j \; \forall x \in F_2 \; \forall q_1, \ldots \in Q_j$, $g(x, q_1, \ldots) = NO$, называются строго внешними. Здесь NO соответствует отказу функционала. Подразумевается, что используются только доступные данному злоумышленнику уязвимости из данных $Q_j$.

Злоумышленники, у которых функционалы $G_j = \{g_{j,1}, \ldots\} \subset G$ такие, что $\exists g \in G_j \; \exists x \in F_2 \; \exists q_1, \ldots \in Q_j$ $g(x, q_1, \ldots) = a_i \in A$, называются внутренними. Подразумевается, что используются только доступные данному злоумышленнику уязвимости из $Q_j$.

В случае, если ценность $a_i$ получена внутренним злоумышленником с помощью $g(x, q_1, \ldots)$, где $x \in F_1$, данный злоумышленник также называется внешним (но не строго внешним).

В второй главе диссертации **«Методы реализации драйверов устройств защищенных операционных систем»** показаны принципы реализации драйверов устройств в операционных системах с открытым кодом, на примере простого символьного драйвера. Для взаимодействия с оборудованием или осуществления операций с доступом к привилегированной информации в системе нужен драйвер ядра. Модуль ядра в операционных системах с открытым кодом – это скомпилированный двоичный код, который вставляется непосредственно в ядро ОС, внутренней и наименее защищённой оболочке при выполнения команд в процессоре x86-64. Здесь код исполняется совершенно без всяких проверок, на высокой скорости и с доступом к любым ресурсам системы. Изменяя ядро, есть риск потерять данные. В коде ядра нет стандартной защиты, как в обычных приложениях ОС.

Для взаимодействия с оборудованием или осуществления операций необходим драйвер устройств. С целью обеспечения безопасной работы и безопасного обращения с устройствами требуется программа. Ядро операционной системы взаимодействует с устройствами ввода / вывода через драйверы. Драйвер устройства - это набор функций, используемых для его поддержки. Одной из наиболее важных особенностей операционной системы HUMO является возможность динамической загрузки драйверов. При таком расположении модуль драйвера становится частью ядра и может свободно обращаться к его функциям. Кроме того, динамически загружаемый драйвер

также может быть динамически выгружен. Если драйвер не выгружен, он будет оставаться в системе постоянно - до следующей перезагрузки ОС.

Символьный драйвер – это драйвер устройства, который взаимодействует с символьными устройствами. Символьные устройства – это устройства, с которым можно работать как поток байтов. Пример символьного устройства - /dev/ttyS0, /dev/tty1. Для наглядности см. рис. 1.

*Метод инициализация.* При вызове assign_chrdev_region регистрируется диапазон номеров символов драйвера устройства, а затем мы указываем имя устройства. После этого, вызывая функцию MAJOR (dev), мы получаем наибольший номер элемента.

Далее проверяется возвращаемое значение, если это код ошибки, функция закрывается. Видно, что при разработке безопасного драйвера устройства всегда необходимо проверять возвращаемые значения, а также указатели на любой элемент. Если возвращенные элементы не являются кодом ошибки, продолжите инициализацию.

*Метод удаление.* Когда модуль устройства удаляется из ядра, вызывается функция «scull_cleanup». При обратной инициализации структуры устройства очищаются, память освобождается, а меньшие и большие номера элементов устройства, назначенные ядром, удаляются.

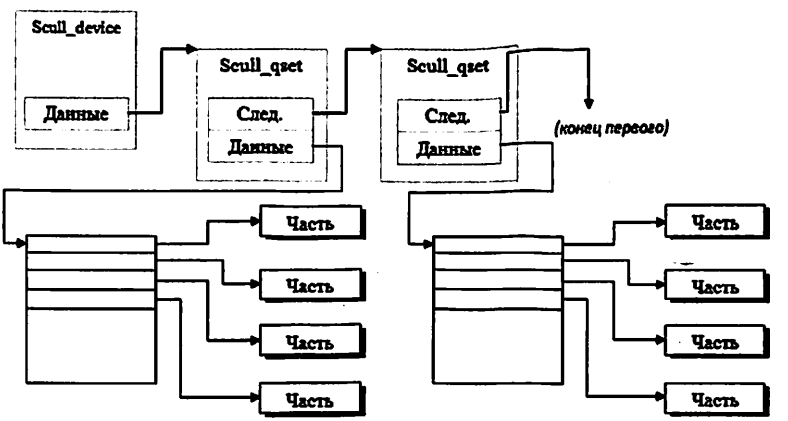



**Рис. 1. Схема связного списка указателей**

Во третьей главе диссертации **«Средства безопасности операционных систем с открытым кодом»** разработаны программы для защиты данных, в которых основной задачей является корректная регистрация пользователей и внешних устройств в системе, а также предоставление инструмента для работы с такими регистрационными данными, проверки на целостность системных файлов, а также инструментов для задания времени и анализа системных событий.

Набор утилит для администрирования был создан для того, чтобы обеспечить ОС понятным, не требующим дополнительной настройки интерфейсом, позволяющим выполнять такие важные функции системы, как ведение регистрационных журналов, проверку состояния ОС в контексте целостности, изменение даты и времени. Каждая программа из набора утилит выполняет следующие функции:

*Программа проверки целостности системных файлов* – является дополнительным механизмом обеспечения безопасности ОС. Позволяет в ручном режиме проверить состояние системных файлов ОС на предмет изменения таких файлов и директорий, в том числе и их атрибутов (рис.2).

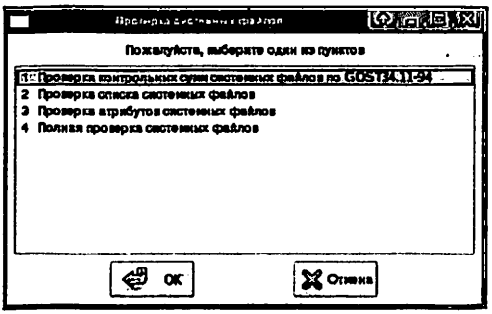



**Рис.2. Заставка программы проверки целостности системных файлов**

*Программа аудита системы* – предоставляет графический интерфейс для анализа событий, произошедших в директориях /home и /media за прошедшую неделю (рис.3).

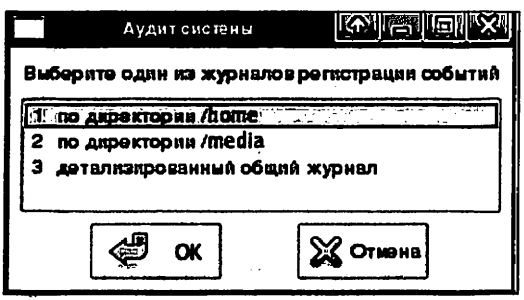
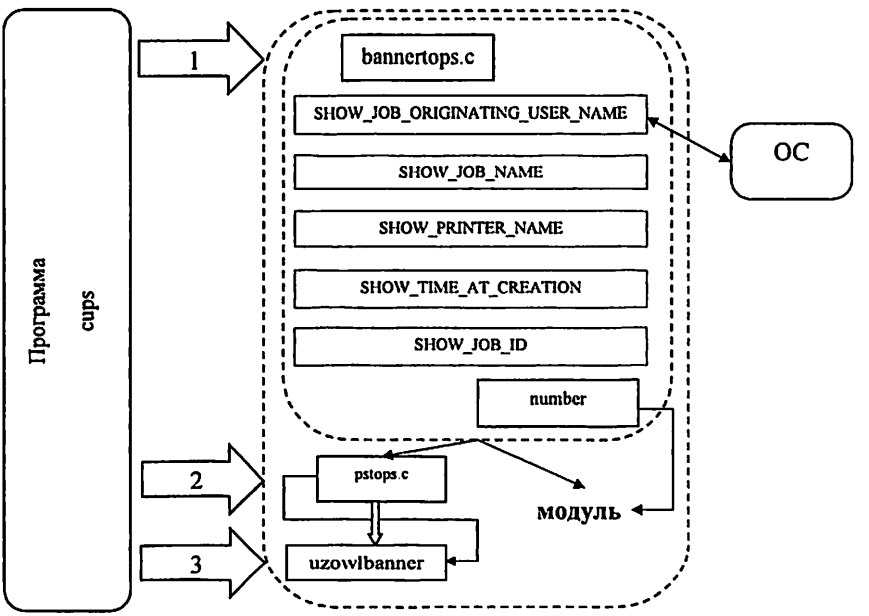



**Рис.3. Заставка программы аудита системы**

*Программа для очистки оперативной памяти* – предоставляет графический интерфейс для очистки оперативной памяти с целью исключения случаев утечки оперативной памяти.

*Программа изменения уровня конфиденциальности объектов файловой системы* – утилита для задания уровня конфиденциальности заданных объектов файловой системы посредством выбора соответствующего пункта контекстного меню в графическом рабочем окружении.

*Программа маркировки выводимых на печать документов* – программа для маркировки выводимых на печать документов с сопроводительной информацией с соответствующими реквизитами: вставка Ф.И.О. сотрудника, наименование документа (имя файла), учетного номера принтера или компьютера, количества печатаемых страниц, дата и время печати документа (рис.5).




1, 2, 3 – очередность выполнения файлов

**Рис. 5. Схема программы маркировки выводимых на печать документов**

Для защищенных ОС «HUMO» с открытом кодом предложена антивирусная программа. По результатам тестирования в более пятидесятых тестах был выбран антивирус с открытым кодом «Comodo». Результаты приведены в виде диаграммы (рис.4).

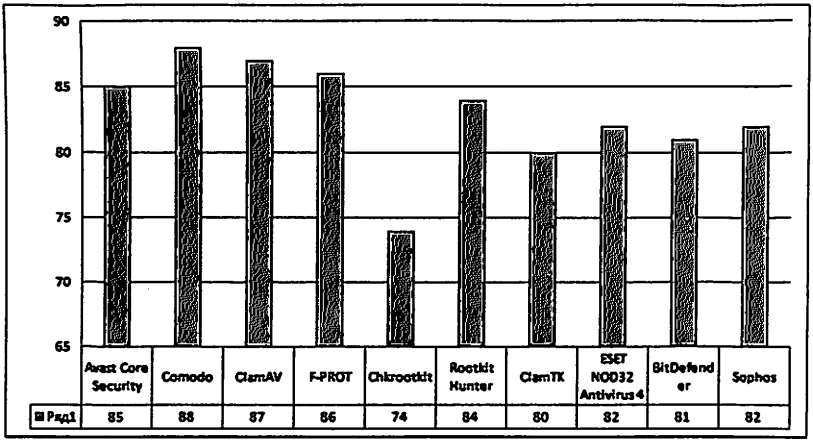



**Рис.4. Диаграмма сравнительного анализа антивирусных программ**

В четвертой главе диссертации «**Средства контроля доступа операционной системы «HUMO»**» разработаны программы для модели правил разграничения доступа.

*На основе дискреционного контроля доступа:*

• При создании файла администратору системы автоматически выставляются права на запись и чтение для владельца и его группы, и запрещаются все права для остальных.

• В случае, если у пользователя несколько учетных записей, то они могут быть объединены одной группой для упрощения доступа пользователя из любой своей учетной записи ко всем своим файлам, созданным под разными учетными записями.

• Для передачи файлов между учетными записями различных пользователей в системе могут выделяться специальные общие каталоги, доступ к файлам, которых будет одинаковым для всех пользователей.

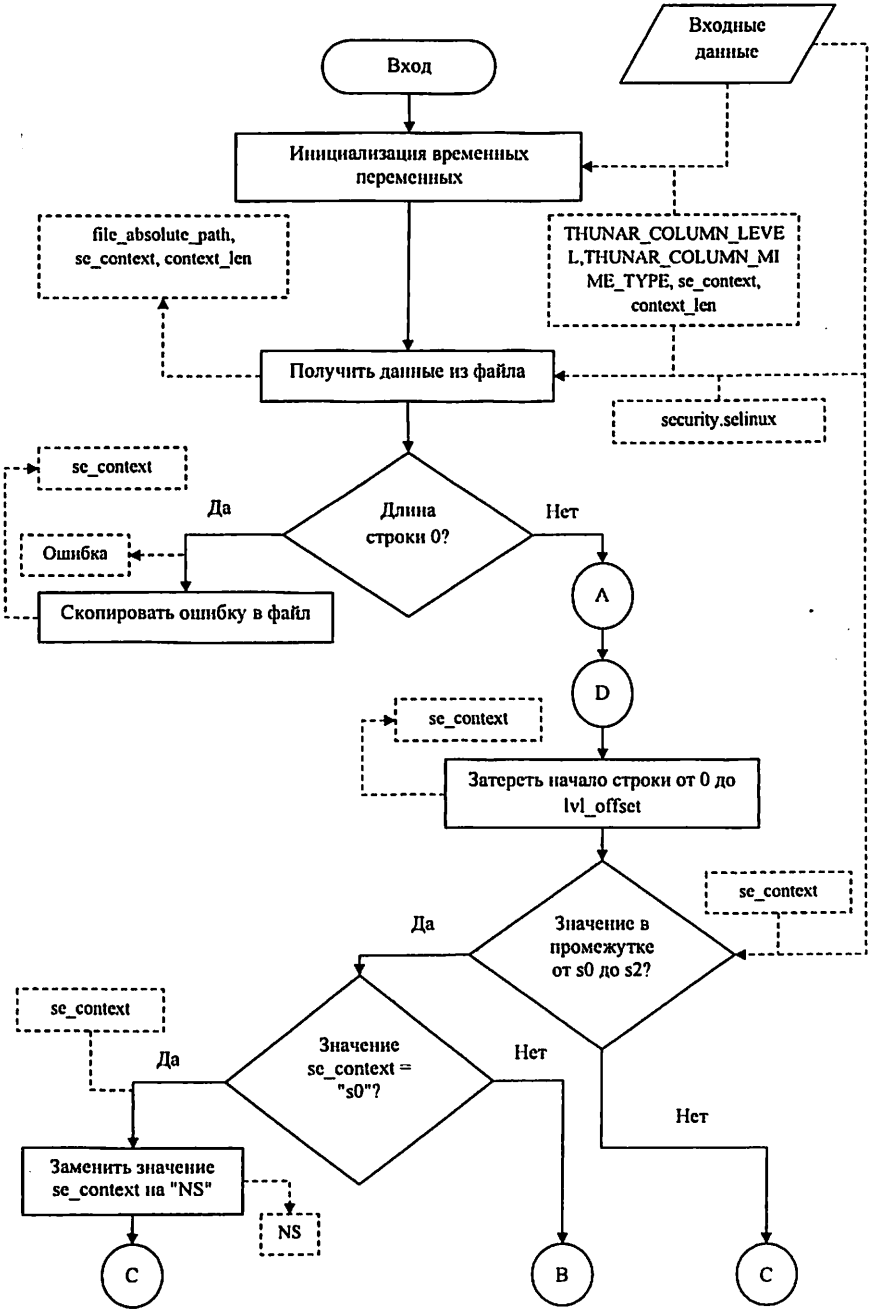
• Пользователь имеет право изменять права доступа к собственным файлам.

• Системный администратор не имеет ограничений в доступе.

*На основе мандатного контроля доступа:*

• Учетная запись пользователя имеет только один уровень доступа.

• В системе учетные записи пользователей по мандатному распределению делятся на три уровня: s0 (низкий уровень), s1 (средний уровень), s2 (высокий уровень секретности).


Входные данные
Вход
Инициализация временных переменных
file_absolute_path, se_context, context_len
THUNAR_COLUMN_LEVEL,THUNAR_COLUMN_MIME_TYPE, se_context, context_len
Получить данные из файла
security.selinux
se_context
Да
Длина строки 0?
Нет
Ошибка
Скопировать ошибку в файл
A
D
se_context
Затереть начало строки от 0 до lvl_offset
se_context
Да
Значение в промежутке от s0 до s2?
se_context
Да
Значение se_context = "s0"?
Нет
Нет
Заменить значение se_context на "NS"
NS
C
B
C

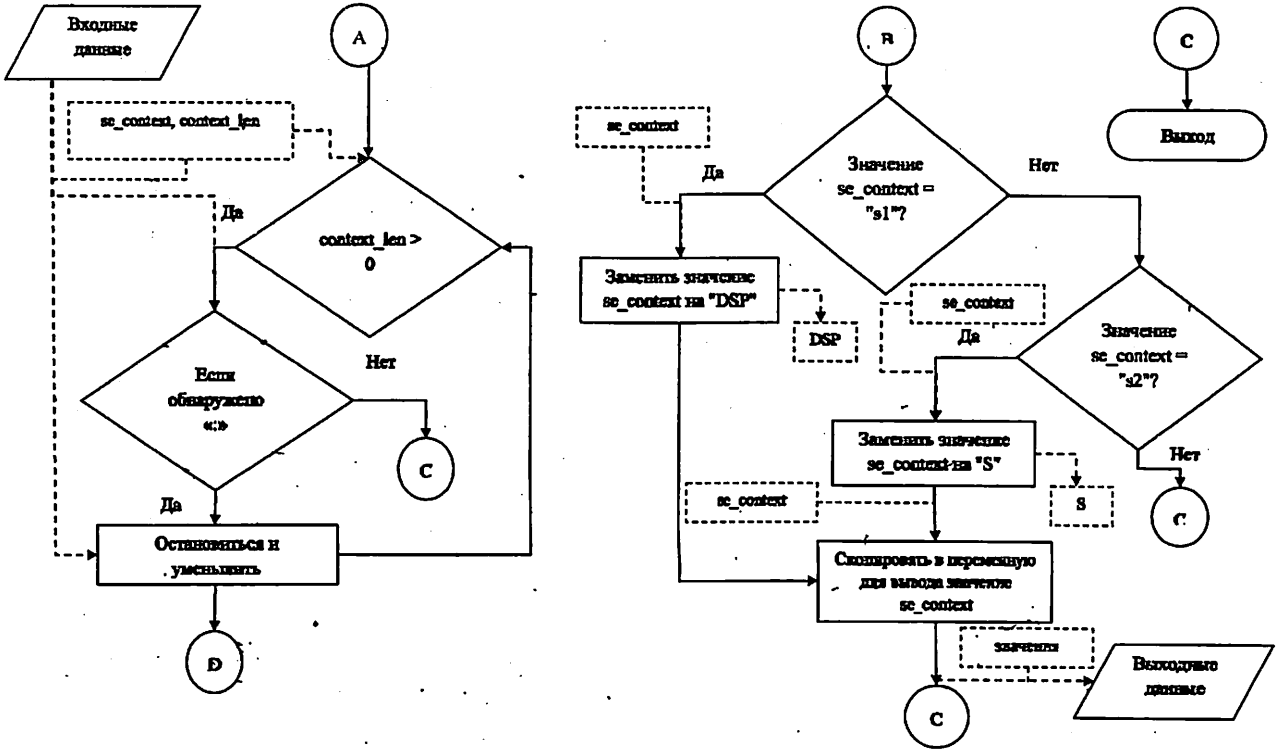



**Рис. 6. Блок схема алгоритма мандатного контроля доступа в ОС «HUMO»**

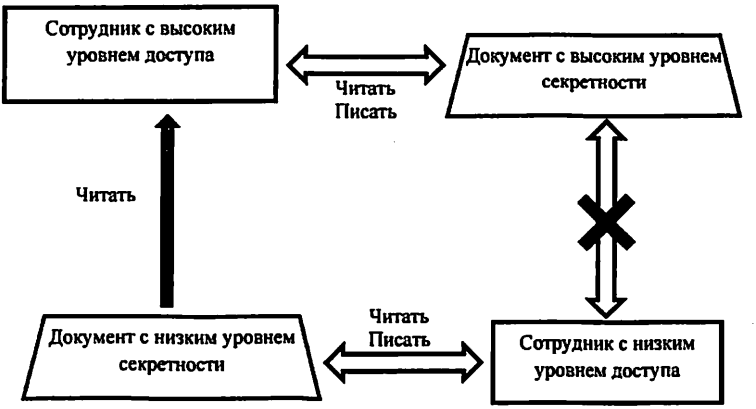



**Рис. 7. Схема алгоритма мандатного контроля доступа в ОС «HUMO»**

• У одного пользователя может быть до трех учетных записей в зависимости от уровня доступа. Например, s0 имеет одну учетную запись, s1 – две учетной записи, s2 – три учетной записи (рис.6).

• Пользователь под учетной записью имеет право создавать, редактировать и читать файлы, уровень конфиденциальности которых равен уровню доступа данной учетной записи.

• Пользователь под учетной записью имеет право читать файлы, уровень конфиденциальности которых равен или ниже уровня доступа данной учетной записи (рис.7).

• Во всех остальных случаях в доступе должно быть отказано.

• При создании нового файла ему будет присвоена метка конфиденциальности, соответствующая уровню доступа данной учетной записи пользователя.

• Для изменения меток конфиденциальности файлов в случае необходимости передачи информации на другой уровень безопасности должен привлекаться администратор безопасности.

• Обращение к приложениям и сервисам осуществляется на основе стандартной дискреционной модели Linux, предотвращающей доступ к системным приложениям и настройкам, так что пользователь не сможет изменить собственные или чужие уровни доступа или конфиденциальности, а также метки файлов.

## ЗАКЛЮЧЕНИЕ

Представлены следующие результаты по теме диссертации «Методы и средства обеспечения информационной безопасности операционных систем с открытым кодом»:

1. Проанализировав основополагающие международные и национальные стандарты и иные документы в области информационной безопасности, сформулирована классификация ценностей АС, классификация угроз, дана характеристика источникам угроз, на основе базовой модели (разработанной ОС) – сформулирована базовая модель нарушителя, его возможностей, а также разработана математическая модель АС и нарушителя. Данная математическая модель позволила выявлять угроз безопасности в АС.

2. Разработан модернизированный алгоритм метода инициализации и удаления драйвера устройств в ядре безопасной операционной системы ОС «HUMO». Данный алгоритм позволяет уменьшить время работы алгоритма в 8,3 раза засчёт сокращения количества лишних функций в коде.

3. Разработаны средств безопасности операционных систем, состоящих из алгоритмов, программы очистки оперативной памяти, механизмы маркировки выводимых на печать документов, подсистемы обеспечения целостности, подсистемы регистрации и учета событий на основе международных и отечественных стандартов, а так же разработаны графические инструменты для работы с программами. Разработанные средства безопасности позволяют отвечать требованиям безопасности, классу 2А в соответствии с O'z DSt 2817:2014.

4. Разработана более простая политика контроля доступов, с сохранением свойств многоуровневого контроля, а так же модернизирована мандатная модель на основе классической модели Белла – ЛаПадулы. Простая политика контроля доступов дает возможность усовершенствовать средств многоуровневого контроля доступов.

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

NATIONAL UNIVERSITY OF UZBEKISTAN

OCHILOV NIZOMIDDIN NAJMIDDIN O'G'LI

# METHODS AND MEANS OF ENSURING THE INFORMATION SECURITY OF OPEN SOURCE OPERATING SYSTEMS

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 doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2019.2.PhD/T1107.**

The dissertation has been prepared at National University of Uzbekistan.

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:** | **Karimov Madjit Malikovich**<br>Doctor of Technical Sciences, Professor |
| **Official opponents:** | **Muxamedieva Dilnoz Tulkunovna**<br>Doctor of Physical-Mathematical Sciences, Professor |
| | **Tuychiev Gulom Numonovich**<br>Doctor of Physical-Mathematical Sciences |
| **Leading organization:** | **Scientific-Engineering and Marketing researches Center «UNICON.UZ»** |

The defense will take place "9" november 2019 at 14:00 the meeting of 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 can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No. _____). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on "31" october 2019 y.
(mailing report No. 19 on "8" october 2019 y.).

**R.Kh. Khamdamov**
Chairman of the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

**K.F. Kerimov**
Scientific secretary of scientific council awarding scientific degrees, Candidate of Technical Sciences, Docent

**R.J. Aloev**
Chairman of the academic seminar under the scientific council awarding scientific degrees, Doctor of Physical-Mathematical Sciences, Professor

## INTRODUCTION (abstract of PhD dissertation)

**The aim of the research work** is to develop special methods and security tools in the open source operating system that meets the requirements of the standard of the Republic of Uzbekistan in the field of secret office work and meets the security requirements, class 2A in accordance with O'zDSt 2817: 2014.

**The object of the research work** is the programs and modules of the operating system protection.

**The scientific novelty of the research work** is as follows:

formulated the basic model of the offender, its capabilities, based on the model of the offender (developed by FSTEC (Federal Service for Technical and Export Control)), analyzing the fundamental international and national standards;

the algorithm of the method for initializing and deleting a device driver based on a character driver has been modernized;

security tools for open source operating systems have been created that meet the requirements of the standard of the Republic of Uzbekistan based on the threat model and the security violator, consisting of an algorithm, a memory cleaning program, marking mechanisms for printed documents, an integrity subsystem, an event registration and recording subsystem, and graphical tools for working with programs based on the threat and security violator model have been developed;

access control systems have been improved with the preservation of multi-level control properties for the identification and authentication module.

**Implementation of the research results.** Based on the results of the created algorithms for the application of methods and means of ensuring information security, the following have been introduced:

access control tools, while maintaining the properties of multi-level control, for the module identification and authentication was introduced in the activities in the department of the Surkhandarya region of the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan (certificate of the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan dated September 25, 2019 No. 104). It makes it possible to improve the means of multi-level access control, while maintaining the properties of multi-level control;

modernization algorithm for the method of initializing and removing device drivers in the core of a secure operating system based on a symbolic driver was introduced in the activities of « Infoteka» LLC (certificate from the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan dated September 25, 2019 No. 104). As a result, the developed software method for initializing and deleting devices in the core of a secure operating system allows reducing the device up to 8.3 times;

based on the developed special protection systems, programs and data protection algorithms in the HUMO OS, they passed a positive examination at the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan and were accepted for commissioning (certificate of the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan of September 25 2019 No. 104). The application of the software package and information protection methods developed on the basis of the results

of the study conducted in the open source operating system allows you to increase the level of data protection from unauthorized access to objects and determine their effectiveness in building secure operating systems.

**Structure and volume of the dissertation.** The structure of the dissertation consists of an introduction, four chapters, conclusion, references and appendices. The volume of the thesis is 114 pages.

## ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
## СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
## LIST OF PUBLISHED WORKS

1. Каримов М.М., Очилов Н.Н. Принцип реализации драйверов устройств, защищенных ОС Linux //Доклады УзА. г. Ташкент, 2017. №5. С.49-51. (05.00.00; № 9)

2. Каримов М.М., Очилов Н.Н. Модуль ядра, защищенного ОС Linux // Вестник ТГТУ. г. Ташкент, 2017. №4. С.39-46. (05.00.00; № 16)

3. Очилов Н.Н. Антивирусные программы для защищенных ОС Linux // Вестник ТУИТ. г. Ташкент, 2017. №4(44). С.70-80. (05.00.00; № 31)

4. Очилов Н.Н. Драйвер функции открытия SCULL_OPEN, чтения/записи SCULL_READ/SCULL_WRITE для защищенного ОС Linux // Узбекский журнал "Проблемы информатики и энергетики" Ташкент: Фан ва технология, 2017 №5. С.85-91. (05.00.00; № 5)

5. Жураев Г.У., Очилов Н.Н. О линейном криптоанализе алгоритма ГОСТ 28147-89 //Вестник информационной безопасности. г. Ташкент, 2014. №7. С.18. гриф - ДСП.

6. Икрамов А.А., Очилов Н.Н. О реализации шифрования в операционной системе HUMO с учетом стандарта Республики Узбекистан и современного криптоанализа //Вестник информационной безопасности. г. Ташкент, 2017. №16. С.19. гриф - ДСП.

7. Каримов М.М., Очилов Н.Н. Маркировка выводимых на печать документов средствами ОС семейства Linux //Вестник информационной безопасности. г. Ташкент, 2018. №18. С.38. гриф - ДСП.

8. Музаффаров Х.А., Саблин Д.П., Очилов Н.Н. Регистрация событий в защищенных операционных системах. Аудит в операционных системах // Вестник УзМУ. г. Ташкент, 2017. №2/2. С.166-173. (01.00.00; № 8)

9. Nizomiddin Najmiddin ugli Ochilov THE PRINCIPLE OF THE IMPLEMENTATION OF DRIVERS FOR DEVICES PROTECTED BY LINUX OS //International Scientific Journal Theoretical & Applied Science. Philadelphia, USA., 2019. Vol - Issue: 74-01. 11 июнь, P. 186-192. (Scientific Journal Impact Factor; № 23; IF = 5.667)

10. Ochilov Nizomiddin Najmiddin Ugli The Driver for the Scull_Open Discovery Function, Read / Write Scull_Read / Scull_Write For a Protected Linux OS //International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR). Индия, 2019. Vol - Issue: 9-1. 30 июнь, P. 31-42.

11. Очилов Н.Н. Маркировка выводимых на печать документов / Н.Н. Очилов //Инновационные подходы в современной науке: сборник статей по материалам XLV Международной научно-практической конференции «Инновационные подходы в современной науке». – № 9(45). – 2019, май, Россия, Москва. С.60-66.

12. Очилов Н.Н. МАНДАТНЫЙ ПРИНЦИП КОНТРОЛЯ ДОСТУПА В ЗАЩИЩЕННЫХ ОС LINUX //Научный форум: Технические и физико-

математические науки: сборник статей по материалам XXV международная научно-практическая конференция – № 6(25). – 2019, май, Россия, Москва. С.19-24.

13. Каримов М.М., Очилов Н.Н. Анализ журнальных файлов событий в защищенных
операционных системах //«Проблемы информационной безопасности и кибербезопасности в сфере информационно-коммуникационной технологии» Республиканская научно-техническая конференция. г. Ташкент, 2018. 22-23 ноября. С.100-102.

14. Очилов Н.Н. Мандатный принцип контроля доступа в защищенных ОС Linux //«Проблемы информационной безопасности и кибербезопасности в сфере информационно-коммуникационной технологии» Республиканская научно-техническая конференция. г. Ташкент, 2018. 22-23 ноября. С.246-248.

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: 2,75. Адади 100. Буюртма № 83.

Гувохнома № 10-3719
“Тошкент кимё технология институти” босмахонасида чоп этилган.
Босмахона манзили: 100011, Тошкент ш., Навоий кўчаси, 32-уй.