**O‘ZBEKISTON MILLIY UNIVERSITETI
HUZURIDAGI ILMIY DARAJALAR BERUVCHI
DSc.03/2025.27.12.FM.01.03 RAQAMLI ILMIY KENGASH**

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI

BOZOROV OBIDJON NORQOBILOVICH

KONFIDENSIAL AXBOROTLARNI CHIQIB KETISHINI BASHORATLASH VA BARTARAF QILISH MEXANIZMLARINI ISHLAB CHIQISH

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot va kiberxavfsizlik (fizika-matematika fanlari)

**FIZIKA-MATEMATIKA FANLARI
BO‘YICHA FALSAFA DOKTORI (PHD) DISSERTATSIYASI AVTOREFERATI**

Toshkent – 2026

UO‘K: 004.056.53

Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора философии (PhD) по физико-математическим наукам

Contents of dissertation abstract of doctor of philosophy (PhD) on physical and mathematical science

**O‘ZBEKISTON MILLIY UNIVERSITETI
HUZURIDAGI ILMIY DARAJALAR BERUVCHI
DSc.03/2025.27.12.FM.01.03 RAQAMLI ILMIY KENGASH**

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI

BOZOROV OBIDJON NORQOBILOVICH

KONFIDENSIAL AXBOROTLARNI CHIQIB KETISHINI BASHORATLASH VA BARTARAF QILISH MEXANIZMLARINI ISHLAB CHIQISH

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot va kiberxavfsizlik (fizika-matematika fanlari)

**FIZIKA-MATEMATIKA FANLARI
BO‘YICHA FALSAFA DOKTORI (PHD) DISSERTATSIYASI AVTOREFERATI**

Toshkent – 2026

Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasining mavzusi O‘zbekiston Fanlar Akademiyasi huzuridagi Oliy attestatsiya komissiyasida B2019.2.PhD/FM389 raqam bilan ro‘yxatga olingan.

Dissertatsiya Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasida (http://ik-fizmat.nuu.uz) va «ZiyoNet» axborot-ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Jurayev Gayrat Umarovich** fizika-matematika fanlari doktori, professor
Rasmiy opponentlar:	**Tuychiyev G‘ulom Numonovich** fizika-matematika fanlari doktori, dotsent
	G‘ulomov Sherzod Rajabboyevich texnika fanlari doktori, professor
Yetakchi tashkilot:	**Toshkent davlat texnika universiteti**

Dissertatsiya himoyasi O‘zbekiston Milliy universiteti huzuridagi DSc.03/2025.27.12.FM.01.03 raqamli Ilmiy kengashning “_____”_____ 2026-yil soat_____ dagi majlisida bo‘lib o‘tadi (Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 227-12-24; faks: (+99871) 246-53-21, 246-02-24; e-mail: nauka@nuu.uz).

Dissertatsiya bilan O‘zbekiston Milliy universitetining Axborot-resurs markazida tanishish mumkin (_____ raqami bilan ro‘yxatga olingan). Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 246-02-24.

Dissertatsiya avtoreferati 2026-yil “_____” _____ kuni tarqatildi.
(2026-yil “_____” _____ dagi _____ raqamli reestr bayonnomasi)

M.M. Aripov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, f.-m.f.d., professor

Z.R. Raxmonov
Ilmiy darajalar beruvchi Ilmiy kengash ilmiy kotibi, f.-m.f.d.

B.F. Abduraximov
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, f.-m.f.d., professor

Kirish (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Bugungi kunda jahon miqyosida axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi sharoitida konfidensial axborotlarni himoyalash, ularning ruxsatsiz chiqib ketishini bashoratlash va bartaraf etishga oid tadqiqotlar dolzarb va zarur hisoblanib, fan-texnikaning ko‘plab sohalarida, xususan, davlat boshqaruvi, mudofaa, moliya-bank, sog‘liqni saqlash, ta’lim va boshqa turli sohalarga keng joriy etilmoqda. Axborot-kommunikatsiya tizimlari rivojining hozirgi zamon bosqichida axborot xavfsizligi holatini baholashning asosiy mexanizmlaridan biri axborot konfidensialligi ta’minlanganligi hisoblanadi. Axborot tizimlariga bo‘lgan tahdidlar soni va xilma-xilligi ortib borayotgan hozirgi sharoitda konfidensial axborotlarning ruxsatsiz chiqib ketishini oldindan aniqlash (bashoratlash) va samarali tarzda bartaraf etish bo‘yicha mexanizmlarni ishlab chiqish, ularning samarali usul va algoritmlarini qurish hamda dasturiy ta’minotini yaratish muhim vazifalardan biri bo‘lib qolmoqda.

Jahonda konfidensial axborotlarning ruxsatsiz chiqib ketishini aniqlash va oldini olishga mo‘ljallangan DLP tizimlarini ishlab chiqish hamda takomillashtirishga yo‘naltirilgan ilmiy-tadqiqot ishlari olib borilmoqda. Bu borada axborot tizimlarida saqlanayotgan, qayta ishlanayotgan va uzatilayotgan konfidensial ma’lumotlarni avtomatik aniqlash va tasniflash, fayllar harakatini real vaqt rejimida nazorat qilish hamda ularning ruxsatsiz chiqib ketish xavfini oldindan bashoratlash dolzarb vazifa sifatida qaralmoqda. Mavjud DLP yechimlarining aksariyati ingliz va boshqa keng tarqalgan tillardagi ma’lumotlar bilan ishlashga mo‘ljallangan bo‘lib, o‘zbek tilining leksik, morfologik va alifbo xususiyatlarini yetarli darajada hisobga olmaydi. Shu sababli o‘zbek tilidagi konfidensial matnlarni intellektual tasniflash, yashirilgan yoki o‘zgartirilgan axborotlarni aniqlash, vujudga kelishi mumkin bo‘lgan xavflarni oldindan baholash hamda ularni bartaraf qilish mexanizmlari va amaliy dasturiy vositalar majmuini ishlab chiqishga alohida e’tibor berilmoqda.

Respublikamizda axborot xavfsizligini ta’minlash, davlat axborot tizimlari va resurslarini himoyalash hamda konfidensial ma’lumotlarning ruxsatsiz chiqib ketishining oldini olish kabi dolzarb yo‘nalishlarga katta e’tibor qaratib kelinmoqda. Jumladan, davlat axborot tizimlari va resurslarini uzluksiz monitoring qilish, kiberxavfsizlik hodisalarini aniqlash hamda ularning oqibatlarini bartaraf etish yuzasidan keng qamrovli chora-tadbirlar amalga oshirilmoqda. Biroq aniqlanayotgan insayderlik hodisalarining ko‘lami mazkur yo‘nalishda hali yechimini kutayotgan muammolar mavjudligini ko‘rsatmoqda. “Kiberxavfsizlik markazi” davlat unitar korxonasi tomonidan taqdim etilgan “O‘zbekiston Respublikasi kiberxavfsizligi. 2022-yil hisoboti”da jami 1 869 684 ta xavfsizlik hodisasi aniqlangani, ulardan 9 709 tasi konfidensial ma’lumotlarga ruxsatsiz kirish hamda ularning sizib chiqishiga olib kelishi mumkin bo‘lgan hodisalar ekanligi qayd etilgan. O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-

tadbirlar to‘g‘risida”gi PQ-167-son Qarorida muhim axborot infratuzilmasi obyektlarining kiberxavfsizlik holatini baholash, monitoring qilish va nazorat mexanizmlarini takomillashtirish kabi muhim vazifalar belgilab berilgan[1]. Ushbu vazifalarni amalga oshirishda, jumladan, axborot tizimlarida harakatlanayotgan o‘zbek tilidagi matnlardan maxfiy va konfidensial ma’lumotlarni yuqori aniqlikda aniqlash, ularning ruxsatsiz chiqib ketishini bashoratlash va bartaraf qilish mexanizmlari hamda amaliy dasturiy vositalar majmuini yaratish muhim ahamiyat kasb etmoqda.

O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi Farmoni, 2007-yil 3-apreldagi PQ-614-son “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida”gi va 2023-yil 31-maydagi PQ-167-son “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarorlari hamda mazkur sohaga oid boshqa normativ-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga bog‘liqligi. Dissertatsiya O‘zbekiston Respublikasi fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Respublikamizda axborotlarning konfidensialligini ta’minlash maqsadida kriptografik himoyalash usullari va vositalarini ishlab chiqish, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash masalalari bilan M.M.Aripov, B.F.Abduraximov, A.K.Kabulov, G.U.Jurayev, G.N.Tuychiyev, D.M.Kuryazov, S.K.G‘aniyev, M.M.Karimov, Sh.R.G‘ulomov, Sh.N.Turapov, O.P.Axmedova, A.Ruziyev kabi olimlar va ularning shogirdlari shug‘ullanishgan. Ular tomonidan axborotlarni himoyalashning nazariy asoslari ishlab chiqilib, amaliy natijalar olingan va tahlillari keltirilgan.

MDH davlatlari ilmiy tadqiqotlarida asosiy e’tibor tarmoq monitoringi va foydalanuvchi xatti-harakatlarini kuzatish orqali axborotlarning chiqib ketishini aniqlashga qaratilgan edi. Bunga A.V.Lukatskiy, O.B.Makarevich, A.S. Romanov, P.D.Zegjda ishlarini misol qilishimiz mumkin. Ular tomonidan ishlab chiqilgan usul va vositalar DLP tizimlarining kompleks himoya mexanizmlarini shakllantirishga xizmat qilgan.

Xorijiy tadqiqotchilar orasida axborotlarni monitoring qilish, DLP tizimlarining arxitekturasi va ularning mashinaviy o‘rganish algoritmlariga asoslangan modellari A.Shabtai, Y.Elovici va L.Rokach tomonidan ishlab

[1] O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-167-son Qarori (Manba: https://lex.uz/docs/6479190).

chiqilgan. Shu bilan birga, konfidensial axborotlarni tahlil qilish va matnlar ustida latent semantik tahlil (LSA) modellarini ishlab chiqqan S.Deerwester, T.K.Landauer, G.W.Furnas, S.T.Dumais, R.A.Harshman kabi olimlarning ishlari DLP tizimlarining semantik asoslarini yaratishda muhim o‘rin egallaydi. Shu bilan birga, milliy til xususiyatlarini hisobga olgan holda konfidensial axborotlarning chiqib ketishini bashorat qilish mexanizmlari, real vaqt rejimida fayllar harakatini tahlil qilish va potensial xavflarni oldindan aniqlash modellari, shuningdek, o‘zbek tilidagi matnlarda maxfiy va konfidensial ma’lumotlarni yuqori aniqlik bilan ajratib olish imkonini beruvchi sun’iy intellekt usullariga asoslangan DLP tizimlarini yaratish masalalari yetarli darajada tadqiq etilmagan. Bu esa mazkur yo‘nalishda nazariy va amaliy muammolarni yanada chuqur va har tomonlama o‘rganishga xizmat qiladigan yangi yondashuvlarni ishlab chiqishni taqozo qiladi.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti ilmiy-tadqiqot rejasiga muvofiq Uzb-Ind-2021-98-“Oqimli shifrlash algoritmlarini tadqiq qilish va ishlab chiqish” mavzusidagi amaliy loyihasi doirasida bajarilgan.

Tadqiqotning maqsadi konfidensial axborotlarni ruxsatsiz chiqib ketishini bashoratlash hamda ularni bartaraf qilishning samarali usullari, algoritmlari va vositalarini ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

axborot tizimlarida harakatlanayotgan matnlarning o‘zbek tiliga mansublik darajasini tezkor aniqlash hamda axborotlarni filtrlash aniqligini oshirish imkonini beruvchi harflar va maxsus belgilar uchrashish chastotasiga asoslangan matnlarning moslik indeksini hisoblash modelini ishlab chiqish;

konfidensial ma’lumotlarni ruxsatsiz yashirin ravishda olib chiqish maqsadida matn tarkibidagi belgilar va so‘zlar o‘rnini qasddan almashtirish orqali amalga oshiriladigan insayderlik hujumlarini aniqlash imkonini beruvchi TF-IDF usuli va moslik indeksiga asoslangan semantik tahlil algoritmini takomillashtirish;

katta hajmdagi axborot oqimida konfidensial matnlarni real vaqt rejimida inson omilisiz avtomatik aniqlash va konfidensiallik darajasi bo‘yicha tasniflash imkonini beruvchi Bayes modeli, chuqur o‘rganish (BERT) hamda nomlangan obyektlarni aniqlash (NER) algoritmlariga asoslangan intellektual tasniflash mexanizmini ishlab chiqish;

tashqi axborot tashuvchi qurilmalar ulanishlarini dinamik boshqarish hamda ruxsatsiz fayl nusxalanishini nazorat qilish imkonini beruvchi qurilmalarning ishonchlilik darajasini avtomatik baholashga asoslangan tizim arxitekturasini ishlab chiqish.

Tadqiqotning obyekti sifatida axborot-kommunikatsiya tizimlarida konfidensial ma’lumotlarni qayta ishlash, saqlash va uzatish hamda ularning xavfsizligini ta’minlash jarayonlari xizmat qiladi.

Tadqiqotning predmeti axborot tizimlarida konfidensial axborotlarning ruxsatsiz chiqib ketishini bashoratlash hamda bartaraf qilish usul, algoritmlari va dasturiy vositalarini yaratishdan iborat.

Tadqiqotning usullari. Mazkur dissertatsiya ishida matematik mantiq va ehtimollar nazariyasi, statistik tahlil usullari, axborot xavfsizligini modellashtirish va loyihalashtirish usullari, mashinali o‘qitish va ma’lumotlarni intellektual tahlil qilish usullari, DREAD metodologiyasiga asoslangan xavflarni tahlil qilish usuli, shuningdek, zamonaviy dasturlash tillari va dasturiy ta’minotlarni ishlab chiqish texnologiyalaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

axborot tizimlarida harakatlanayotgan matnlarning o‘zbek tiliga mansublik darajasini tezkor aniqlash hamda axborotlarni filtrlash aniqligini oshirish imkonini beruvchi harflar va maxsus belgilar chastotasiga asoslangan matnlarning moslik indeksini hisoblash modeli ishlab chiqilgan;

konfidensial ma’lumotlarni ruxsatsiz yashirin ravishda olib chiqish maqsadida matn tarkibidagi belgilar va so‘zlar o‘rnini qasddan almashtirish orqali amalga oshiriladigan insayderlik hujumlarini aniqlash imkonini beruvchi TF-IDF usuli va moslik indeksiga asoslangan semantik tahlil algoritmi takomillashtirilgan;

katta hajmdagi axborot oqimida konfidensial matnlarni real vaqt rejimida inson omilisiz avtomatik aniqlash va konfidensiallik darajasi bo‘yicha toifalash imkonini beruvchi Bayes modeli, chuqur o‘rganish (BERT) hamda nomlangan obyektlarni aniqlash (NER) algoritmlariga asoslangan intellektual tasniflash mexanizmi ishlab chiqilgan;

tashqi axborot tashuvchi qurilmalar ulanishlarini dinamik boshqarish hamda ruxsatsiz fayl nusxalanishini nazorat qilish imkonini beruvchi qurilmalarning ishonchlilik darajasini avtomatik baholashga asoslangan tizim arxitekturasi ishlab chiqilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

o‘zbek tilidagi matnlarning konfidensiallik darajasini avtomatik aniqlash va filtrlash imkonini beruvchi dasturiy modul ishlab chiqilgan;

tashqi axborot tashuvchi qurilmalar orqali fayllarning ruxsatsiz nusxalanishini dinamik nazorat qiluvchi “KARCHKOOT” (Konfidensial axborotlarni ruxsatsiz chiqib ketishini nazorat qilish va oldini olish tizimi) dasturiy kompleksi yaratilgan;

yaratilgan intellektual modellar va algoritmlar yordamida konfidensial hujjatlarni qo‘lda tekshirish vaqtini sezilarli darajada qisqartirish va amaliyotda foydalanish uchun tezkorlikka erishilgan.

Tadqiqot natijalarining ishonchliligi foydalanilgan matematik statistika va mashinaviy o‘rganish usullarining ilmiy asoslanganligi, nazariy xulosalarning amaliy sinov natijalari bilan mos kelishi, ishlab chiqilgan algoritmlarning amaliyotda yuqori aniqlikda (92-96%) ishlashi tasdiqlanganligi, shuningdek, olingan ilmiy natijalarning tegishli vazirlik va idoralar axborot tizimlariga muvaffaqiyatli joriy etilganligi hamda ilmiy nashrlarda chop etilganligi bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati sodir bo‘lishi mumkin bo‘lgan ruxsatsiz axborot chiqib ketish holatlari to‘g‘risidagi ma’lumotlarni yig‘ish va tahlil qilishga asoslangan axborot xavfsizligi monitoringi tizimlarida ma’lumotlarni qayta ishlash sxemasi taklif etilganligi, konfidensial axborotlarni statistik tahlil qilish usullari ishlab chiqilganligi hamda katta hajmdagi axborot oqimida konfidensial matnlarni aniqlash va ularni toifalash jarayonida chuqur o‘rganish (BERT) modeli va nomlangan obyektlarni

aniqlash (NER) algoritmlaridan foydalanishga asoslangan intellektual tahlil usuli taklif etilganligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati olingan nazariy natijalar, sun’iy intellekt modellari va moslik indeksi asosida konfidensial ma’lumotlar ruxsatsiz chiqishini real vaqt rejimida inson omilisiz avtomatik aniqlash va bartaraf qilish dasturiy vositasi ishlab chiqilganligi hamda ular asosida insayderlik hujumlarini proaktiv bloklash orqali axborot xavfsizligi monitoringi tizimlarining ishlash samaradorligi yaxshilanganligi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Konfidensial axborotlarni chiqib ketishini bashoratlash va bartaraf qilish mexanizmlari bo‘yicha olingan ilmiy natijalar amaliyotda quyidagi yo‘nalishlarda joriy etilgan:

o‘zbek tilidagi matnlarning moslik indeksini hisoblash orqali axborot tizimlarida mavjud matnlarning o‘zbek tiliga oidligini avtomatik aniqlash hamda konfidensial axborotlarni kiberhujumchi tomonidan matndagi so‘zlar yoki belgilarning o‘rnini almashtirish orqali ruxsatsiz olib chiqib ketilishining oldini olishga xizmat qiluvchi algoritmdan OT-Atex-2018-486 raqamli “Mantiqiy boshqaruv va axborot xavfsizligi tizimlarini dasturlashtirilgan mantiqiy kontrollerlar va ularni loyihalovchi avtomatlashtirilgan CAD mantiqiy tizimi asosida amalga oshirish” loyihasida ma’lumotlarni tasniflashda va ruxsatsiz chiqib ketishini aniqlashda foydalanilgan (Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining 2022-yil 17-maydagi 04/11-2806-son ma’lumotnomasi). Natijada, dastlabki qayta ishlash jarayonida suvli belgilar, regulyar ifodalar hamda statik so‘rovlar yordamida qidirish imkoniyatlaridan foydalanish tasniflash aniqligini oshirish imkonini bergan;

konfidensial axborotlarni ruxsatsiz chiqib ketishini aniqlash va bartaraf qilishning statistik hamda intellektual usullari, o‘zbek tilidagi matnlarning moslik indeksini hisoblash algoritmi va TF–IDF statistik tahlil mexanizmidan Iqtisodiyot va moliya vazirligi huzuridagi Bojxona qo‘mitasining axborot tizimlarida ma’lumotlarni tasniflash va ularning ruxsatsiz chiqib ketishini aniqlashda foydalanilgan (Iqtisodiyot va moliya vazirligi huzuridagi Bojxona qo‘mitasining 2023-yil 30-martdagi 6/05-23-00108-son ma’lumotnomasi). Natijada, o‘zbek tilidagi matnlar uchun moslik indeksi algoritmi yordamida ma’lumotlarni tasniflashning aniqlik ko‘rsatkichini 92-96 foizgacha oshirish imkonini bergan;

tashqi axborot tashuvchilarni nazorat qilish moduli, o‘zbek tilidagi matnlarning moslik indeksini hisoblash algoritmi, TF–IDF statistik tahlil usuli hamda intellektual tasniflash algoritmlaridan O‘zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti Axborot-kommunikatsiya texnologiyalari va harbiy aloqa institutining axborot tizimida konfidensial matnlarni tasniflash, tashqi qurilmalar orqali uzatilishini nazorat qilish va ularning ruxsatsiz chiqib ketishini aniqlashda foydalanilgan (O‘zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti Axborot-kommunikatsiya texnologiyalari va harbiy aloqa institutining 2025-yil 23-maydagi 1027-son ma’lumotnomasi). Natijada, ishlab chiqilgan tizim USB va boshqa portativ qurilmalar orqali konfidensial ma’lumotlarning ruxsatsiz chiqib ketishini 95% aniqlikda aniqlash va bloklash imkonini bergan;

TF–IDF statistik tahlil usuli va Bayes klassifikatori asosida ishlab chiqilgan konfidensial hujjatlarni tasniflash algoritmlari, tashqi axborot tashuvchi vositalarga nusxalashga ruxsatlarni boshqarish moduli hamda “KARCHKOOT” DLP tizimidan

O‘zbekiston Respublikasi Mudofaa vazirligining kriptografik vositalarni ishlab chiqish, ishlab chiqarish va realizatsiya qilish faoliyati bilan shug‘ullanish uchun litsenziyaga ega sinov laboratoriyasida konfidensial axborotlarni real vaqt rejimida monitoring qilish, aniqlash, tasniflash va bloklashda foydalanilgan (O‘zbekiston Respublikasi Mudofaa vazirligining 2025-yil 27-maydagi 295-son ma’lumotnomasi). Natijada, yaratilgan tizim konfidensial hujjatlarni avtomatik aniqlash va tasniflash jarayonini 3-4 marta tezlashtirgan, konfidensial ma’lumotlarni ruxsatsiz chiqib ketishini 92.1% aniqlikda bartaraf eta olgan, bu esa xodimlarning qo‘lda tahlil qilish vaqtini kamaytirib, ish samaradorligini oshirish imkonini bergan.

Tadqiqot natijalarining aprobatsiyasi. Tadqiqot natijalari 10 ta ilmiy-amaliy, jumladan, 5 ta xalqaro va 5 ta respublika miqyosidagi ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 21 ta ilmiy ish chop etilgan, shulardan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining falsafa doktori dissertatsiyalari asosiy ilmiy natijalarini chop etishga tavsiya etilgan ilmiy nashrlarda 7 ta maqola, jumladan, 2 tasi xorijiy va 5 tasi respublika jurnallarida nashr etilgan. Shuningdek, EHM uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risida 3 ta guvohnoma olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va 2 ta ilovadan iborat. Dissertatsiyaning hajmi 117 betdan tashkil topgan.

DISSERTATSIYA ISHINING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi, tadqiqot maqsadi va vazifalari, ilmiy yangiligi, amaliy natijalari hamda ishning tuzilmasi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiya ishining “**Axborot tizimlarida konfidensial axborotlarning chiqib ketish xavfi va undan himoyalanish mexanizmlari**” deb nomlangan birinchi bobida davlat tashkilotlarining axborot tizimlarida konfidensial ma’lumotlar harakatini nazorat qilish, ularning ruxsatsiz tarqalishining oldini olish hamda mavjud DLP tizimlarining imkoniyatlari tahlil qilingan. Milliy axborot resurslarida konfidensial ma’lumotlarning xavfsizligini ta’minlash, ulardan ruxsatli foydalanishni tashkil etish va axborot oqib chiqishi xavfini kamaytirish maqsadida DLP tizimlarining vazifalari, qo‘llanish sohasi va cheklovlari ko‘rib chiqilgan.

Bobda konfidensial axborotlarni ruxsatsiz uzatish holatlarini aniqlash va bartaraf etishga qaratilgan axborot xavfsizligi siyosatining formal modeli ishlab chiqilgan. Bunda U – foydalanuvchilar, D – hujjatlar yoki fayllar, K – axborot uzatish kanallari, jumladan USB, elektron pochta, HTTP/HTTPS, FTP va printerlar to‘plami sifatida qaraladi. Foydalanuvchining muayyan hujjat bilan ma’lum kanal orqali ishlash huquqi quyidagi ruxsatlar munosabati orqali ifodalanadi: $G \subseteq U \times D \times K$

Ruxsatni tekshirish funksiyasi esa quyidagicha aniqlanadi:

$$L\left(u_i, d_j, k_r\right) = \begin{cases} 1, \text{ agar} \left(u_i, d_j, k_r\right) \in G \text{ bo‘lsa,} \\ 0, \text{ aks holda} \end{cases} \quad (1)$$

Shu asosda xavfsizlik siyosatining umumiy formal modeli quyidagi ko‘rinishda ifodalanadi: $\Pi = \langle U, D, K, G, T, \Omega \rangle$

Bu yerda T – ehtimoliy tahdidlar, Ω esa tahdid aniqlanganda bajariladigan javob choralari, ya’ni ogohlantirish, bloklash, karantinga olish va audit qilish amallarini bildiradi. Mazkur model foydalanuvchi harakatlari, axborot obyektlari va uzatish kanallarini yagona xavfsizlik siyosati doirasida boshqarish imkonini beradi.

Shuningdek, bobda ma’lumotlarning uch holati – data-at-rest, data-in-use va data-in-motion bo‘yicha himoya mexanizmlari o‘rganilgan. McAfee DLP, SearchInform, Sophos, InfoWatch Traffic Monitor va Kiber Protego kabi DLP yechimlari qiyosiy tahlil qilinib, ularning o‘zbek tilidagi matnlar bilan ishlashda samaradorligi cheklanganligi ko‘rsatib berilgan.

Ichki tahdidlarning axborot tizimlari uchun yuqori xavf tug‘dirishini hisobga olgan holda, DREAD metodologiyasi asosida konfidensial ma’lumotlar sizib chiqishi bilan bog‘liq xavflarni baholash modeli ishlab chiqilgan. Tahlil natijalariga ko‘ra, “USB orqali konfidensial fayllarni ruxsatsiz ko‘chirish” 39 ball, “Tizimdagi zaiflik orqali API kalitini olish va soxta agent o‘rnatish” 38 ball hamda “Insayder tomonidan maxfiy matnni yashirin olib chiqish” 37 ball bilan eng yuqori xavf darajasiga ega tahdidlar sifatida aniqlangan.

Birinchi bob yakunida mavjud DLP tizimlarini takomillashtirishda soxta ijobiy va soxta salbiy holatlarni kamaytirish muhim vazifa ekanligi asoslangan. Kalit so‘zlar va qat’iy qoidalarga tayanuvchi an’anaviy mexanizmlar obfuskatsiyalangan yoki kontekstga bog‘liq matnlarni aniqlashda yetarli natija bermasligi ko‘rsatildi. Shu bois o‘zbek tili xususiyatlarini hisobga olgan holda statistik, mashinaviy o‘qitish va chuqur o‘rganish mexanizmlarini integratsiyalashga asoslangan DLP tizimini ishlab chiqish zarurati asoslab berildi.

Dissertatsiya ishining **“Konfidensial axborotlarni tasniflash”** deb nomlangan ikkinchi bobida tabiiy tilda yozilgan konfidensial matnlarni tasniflash amalga oshirildi. Tasniflashni amalga oshirish uchun dastlabki qayta ishlash, statistik tahlillashni amalga oshirish, Bayes modeliga asoslangan konfidensial matnlarni tasniflash usuli hamda o‘zbek tilidagi axborotlarni dastlabki qayta ishlash va statistik tahlilini amalga oshirish bosqichlari ishlab chiqildi.

Konfidensial axborotni avtomatik tahlil qilishning birinchi bosqichi - matnni dastlabki qayta ishlash, ya’ni identifikatsiyalovchi elementlarni (shaxs ismlari, joy nomlari, bank raqamlari) ajratish, belgilarni standartlashtirish va vektorli ko‘rinishga keltirishdan iborat.

Konfidensial matnlarni dastlabki qayta ishlash "hujjat–termin" matritsasini hosil qilish, terminlar chastotasini hisoblash, teskari matn chastotasini hisoblash, terminlar chastotasi – teskari matn chastotasini hisoblash bosqichlaridan iborat.

TF-IDF bu matnlar to‘plami yoki til korpusining bir qismi bo‘lgan matn tarkibidagi terminning vaznini baholash uchun ishlatiladigan statistik o‘lchov hisoblanadi:

$$tf\text{-}idf(t,d,D) = tf(t,d) \cdot idf(t,D) \quad (2)$$

O‘zbek tilidagi matnlarning moslik indeksi (CI) harflar va maxsus belgilar

uchrash chastotasiga asoslanib quyidagicha aniqlanadi:

$$I(\vec{X}) = \sum_{i=0}^{L} \left(\frac{K_i}{M} \right)^2 , \quad (3)$$

bu yerda A - tahlil qilingan ochiq matnlar to‘plami.

Ishlab chiqilgan dastur yordamida ochiq manbalar (lex.uz, kun.uz va daryo.uz) ni o‘zbek tilidagi matnlarining 70 millionga yaqin belgilari tahlil qilib chiqildi. Hisoblash natijasiga ko‘ra o‘zbek tilining moslik indeksi 0,071698945 qiymatiga teng bo‘ldi. Ushbu natijani ochiq manbalardagi boshqa tabiiy tillarning moslik indekslari bilan taqqoslanganda quyidagi natijaga erishildi (1-jadval).

1-jadval.

Tabiiy tillarning moslik indekslari.

Til	**Moslik indeksi**
Hind tili	0,041837864
Rus tili	0,0553
Urdu	0,057535302
Ingliz tili	0,0644–0,0667
O‘zbek tili	**0,071698945**
Italyan tili	0,0738
Nemis tili	0,0762
Ispan tili	0,0775
Fransuz tili	0,0778

Tadqiqot ishi davomida tarkibida shaxsga doir ma’lumotlar, bank siri va boshqa himoyalanishi zarur ma’lumotlar mavjud hujjatlarning moslik indekslari hisoblab chiqildi va natijalar 2-jadvalda keltirilgan.

2-jadval.

Umumiy til va sohalar bo‘yicha moslik indekslari.

№	**Tahlil turi**	**Matnlar manbasi**	**Belgilar soni (M)**	**Moslik indeksi**	**Izoh**
1	Umumiy o‘zbek tili	kun.uz, daryo.uz, lex.uz	70 000 000	0,0717	Neytral, standart til
2	Ommaviy maqolalar	yangiliklar, bloglar	2 000 000	0,0701	Umumiy tilga yaqin, xilma-xil
3	Bank sohasi	bank hujjatlari, tranzaksiya loglari	1 200 000	**0,0762**	Maxfiy, ko‘p terminli
4	Shaxsga doir ma’lumotlar	pasport, shaxsiy identifikatorlar	950 000	**0,0788**	O‘xshash belgilar ko‘p, yuqori konfidensiallik
5	Harbiy sohaga doir	buyruqlar, harbiy protokollar	800 000	**0,0794**	Cheklangan lug‘at, takroriy so‘zlar ko‘p
6	Tibbiyot sohasi	epikriz, analiz natijalari	850 000	0,0741	Texnik va terminlashgan
7	Yuridik sohasi	qonunlar, nizomlar, qarorlar	930 000	0,0734	Formal, standart tuzilgan

2-jadvaldan ko‘rinib turibdiki, konfidensial axborot turlariga tegishli sohalar (masalan, bank, harbiy, shaxsiy ma’lumotlar) uchun moslik indekslari yuqoriroq. Ya’ni, 0,076 dan yuqori qiymatga ega. Bu shuni anglatadiki, ushbu matnlar ichida takrorlanuvchi belgilar va terminlar ustunlik qiladi.

Bayes qarorlar nazariyasiga asoslangan tasniflashda hujjatning sinfga tegishlilik aposterior ehtimoli quyidagicha (4) hisoblanadi:

$$P(c \mid d) = \frac{P(d \mid c)P(c)}{P(d)}. \quad (4)$$

Ikkinchi bobda taklif etilgan tasniflash va moslik indeksi usullarini nazariy asoslash maqsadida bir qator matematik natijalar isbotlandi. Bayes qarorlar nazariyasiga asoslangan tasniflashda kutilayotgan tavakkalchilikni minimallashtiruvchi qaror chegarasi quyidagi teorema bilan aniqlanadi.

2.1-teorema. Agar konfidensial hujjatning sizib chiqishidan kelib chiqadigan zarar (CFN) ochiq hujjatni adashib bloklash zararidan (CFP) qat’iy katta (CFN > CFP) bo‘lsa, u holda kutilayotgan Bayes xavfini minimallashtiruvchi optimal qaror qabul qilish chegarasi τ* quyidagicha aniqlanadi:

$$\tau^* = \frac{C_{\mathrm{FP}}}{C_{\mathrm{FP}} + C_{\mathrm{FN}}}. \quad (5)$$

Taklif etilgan o‘zaro moslik indeksining insayder kiritgan qisman o‘zgarishlarga (begona matn aralashtirish yoki belgilarni almashtirish) turg‘unligi quyidagi teorema bilan asoslanadi.

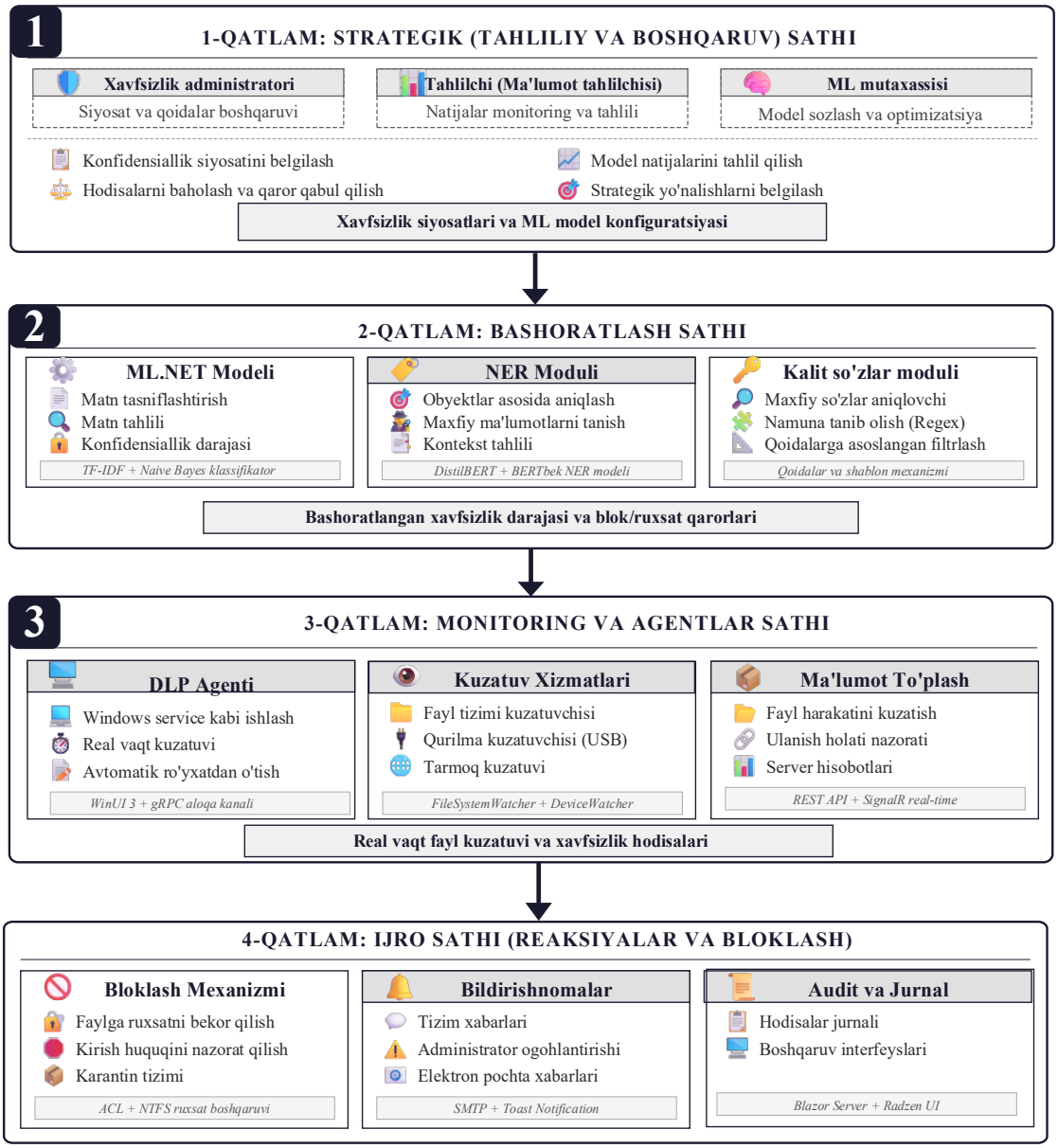
2.2-teorema. Yuqoridagi belgilashlarda gibrid matn va tayanch soha profili o‘rtasidagi o‘zaro moslik indeksining asl qiymatdan og‘ishi ΔMI quyidagi tengsizlik bilan chegaralanadi:

$$\Delta MI = \left| MI\left(X_{\alpha}, Y\right) - MI\left(X, Y\right) \right| \le \alpha \cdot \| r - p \|_2 \cdot \| q \|_2 \quad (6)$$

bu yerda $\|\cdot\|_2$ — vektorning Yevklid normasi, p - asl maxfiy matn, r - o‘zgartirilgan matn, q - tayanch soha profili chastotasi vektori, α ($0 \le \alpha \le 1$) esa o‘zgartirilgan matn ulushini bildiradi. Mazkur teorema o‘zaro moslik indeksining obfuskatsion o‘zgartirishlarga nisbatan turg‘unligini asoslab beradi. Bunda matn tarkibi sun’iy ravishda qisman o‘zgartirilgan taqdirda ham hujjatning statistik belgilar majmui saqlanib qoladi va uning tegishli soha maxfiy ma’lumotlariga yaqinligini aniqlash imkoniyati yo‘qolmaydi.

Dissertatsiya ishining **“Konfidensial axborotlarni chiqib ketishini aniqlash tizimining algoritmlari va strukturasini ishlab chiqish”** deb nomlangan uchinchi bobida konfidensial axborotlarni chiqib ketishini aniqlash tizimining modeli va strukturalari tahlili keltirilgan. Shuningdek, konfidensial axborotlarni chiqib ketishidan himoyalash va bartaraf qilish tizimining funksional tuzilmasi ishlab chiqilgan.

Funksional jihatdan konfidensial axborotlarni chiqib ketishini aniqlash va bartaraf qilish tizimi quyidagi modullardan iborat: ish stansiyasini boshqarish; uzatish kanallarini nazorat qilish; konfidensial ma’lumotlarni saqlash va nusxalashni boshqarish; ularni yig‘ish, qayta ishlash va saqlash; nazorat va boshqaruv moduli (1-rasm).



1-rasm. DLP tizimining umumiy tuzilishi.

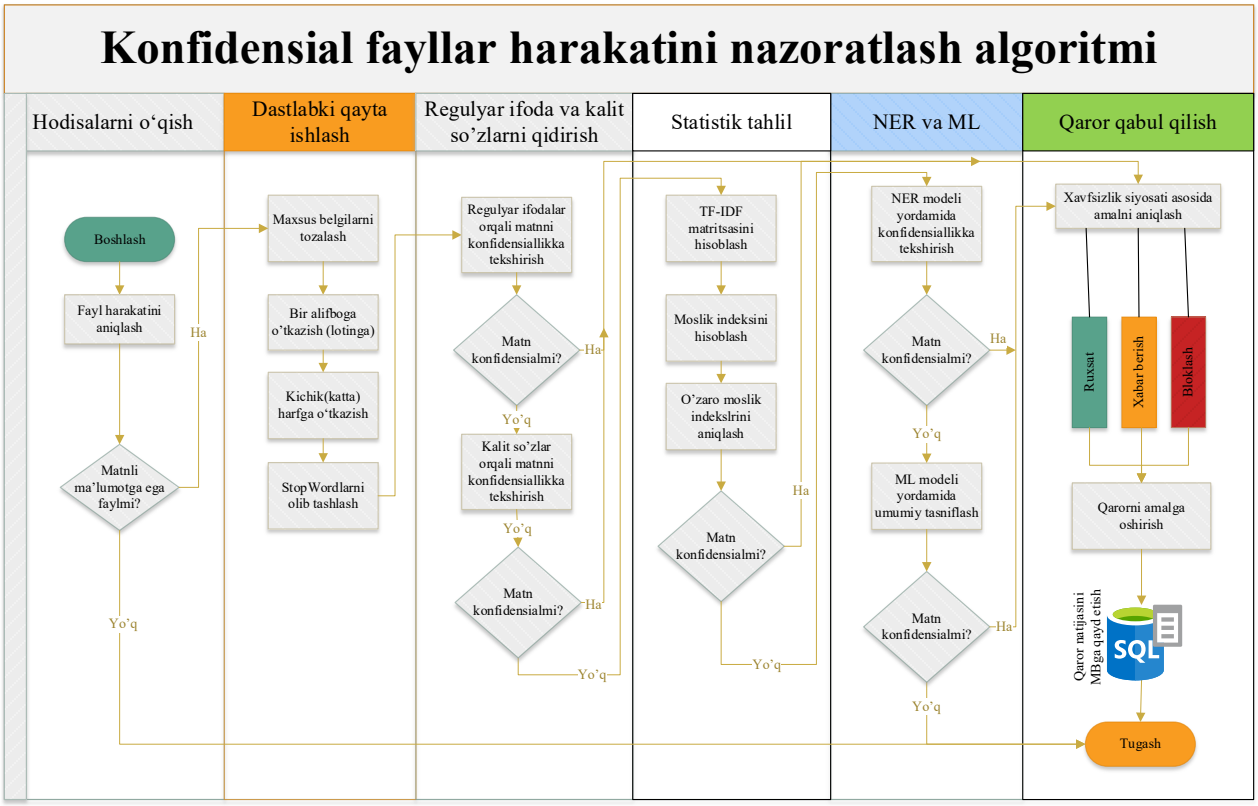
Tashqi axborot tashuvchi qurilmalar orqali ruxsatsiz nusxalashni oldini olish uchun dinamik TrustScore mexanizmi ishlab chiqildi.

Har bir qurilma uchun boshlang‘ich ishonch bali belgilanib, fayllar bilan bog‘liq xavfsizlik hodisalari, fayl konfidensialligi va qurilmaning foydalanish tarixi asosida u dinamik yangilanadi. Qurilmaning yangilangan ishonch bali quyidagicha aniqlanadi:

$$T_{t+1} = \text{clip}\left((1-\rho)T_0 + \rho T_t + \sum_{f \in F_t} \sum_{i=1}^{m} a_i z_i(t,f) r(f), 0, 100 \right), \qquad (7)$$

bu yerda TrustScore_t - qurilmaning joriy ishonch bali; w_i - i-hodisaning musbat yoki manfiy vazni; r_o - faylning konfidensiallik darajasiga bog‘liq xavf koeffitsiyenti; λ - oldingi holat ta’sirining saqlanish koeffitsiyenti. Hisoblangan ishonch bali asosida qurilmaga ruxsat berish, cheklangan nazorat o‘rnatish yoki uni bloklash qarori shakllantiriladi; bir martalik ijobiy hodisa xavfli qurilmani darhol ishonchli holatga o‘tkazmaydi, takroriy buzilishlar esa ishonch balini tezroq pasaytiradi.

Konfidensial fayllarni aniqlash algoritmi fayl hodisasini o‘qish, matnni dastlabki qayta ishlash, konfidensial terminlarni aniqlash (regulyar ifodalar va kalit so‘zlar), kontekstual tahlil (NER va ML.NET) hamda qaror qabul qilish bosqichlaridan iborat (2-rasm).



2-rasm. Fayllarni konfidensialligini aniqlash algoritmi blok-sxemasi.

Regulyar ifodalar, kalit so‘zlar, NER va ML modullarining natijalarini birlashtirish uchun ierarxik tasniflash mexanizmi taklif etildi. Tahlil ustuvorlik ketma-ketligida amalga oshirilib, modullarning ustuvorligiga asoslangan yakuniy tasniflash natijasi $\hat{y}(x)$ quyidagicha aniqlanadi:

$$\hat{y}(x)=\begin{cases}\hat{y}_R(x), & \hat{y}_R(x)\in\{1,2\},\\ \hat{y}_N(x), & \hat{y}_R(x)=0\wedge\hat{y}_N(x)\in\{1,2\},\\ \hat{y}_M(x), & \hat{y}_R(x)=0\wedge\hat{y}_N(x)=0.\end{cases} \tag{8}$$

Agar regulyar ifoda yoki kalit so‘z orqali konfidensiallik aniqlansa, qoidaga asoslangan modul natijasi qabul qilinadi. Aks holda NER moduli, undan keyin esa ML modelining semantik tahlili asosida sinf belgilanadi. Faylga nisbatan bajariladigan yakuniy xavfsizlik amali tasniflash natijasi va hodisaning umumiy xavf darajasiga bog‘liq holda quyidagicha aniqlanadi:

$$\omega(x)=\Pi\big(\hat{y}(x),R(x)\big),\qquad \omega(x)\in\Omega.,$$

bu yerda $\hat{y}(x)$ - fayl matnining konfidensiallik sinfi; R - hodisaning umumiy xavf darajasi; A - ruxsat berish, ogohlantirish, qo‘shimcha tekshiruv va bloklash kabi javob choralari to‘plami. Past xavfda faylga ruxsat beriladi, o‘rta xavfda ogohlantirish yoki cheklangan ruxsat qo‘llaniladi, yuqori xavfda esa fayl uzatilishi

bloklanadi va hodisa audit jurnaliga yoziladi.

Real vaqt rejimida yuqori aniqlikdagi aniqlash uchun an'anaviy statistik usullar (TF-IDF, Bayes) bilan bir qatorda Transformer arxitekturasiga asoslangan XLM-RoBERTa modeli tanlanib, uni o'zbek tiliga moslashtirish (fine-tuning) algoritmi ishlab chiqildi.

O'zbek tili agglyutinativ til bo'lgani uchun modelni o'qitishda butun so'zli tokenizatsiya o'rniga SentencePiece algoritmi, xatolikni minimallashtirish uchun esa 15 000 dan ortiq matnli korpusda Kross-Entropiya (Cross-Entropy Loss) yo'qotish funksiyasidan foydalanildi.

Dissertatsiyaning uchinchi bobida konfidensial matnlarni aniqlash mexanizmi nazariy jihatdan asoslab berilgan. Modelning kiritish bosqichida axborot yo'qolishi, o'qitish jarayonining yaqinlashishi hamda umumlashtirish qobiliyati bo'yicha quyidagi fundamental natijalar isbotlangan.

3.1-lemma. Ixtiyoriy $x \in \Sigma^*$ satr (jumladan, korpusda ilgari uchramagan yoki o'zgartirilgan konfidensial atama) chekli o'lchamli V tokenlariga to'liq yoyiladi va lug'atdan tashqari (Out-of-Vocabulary) belgi ehtimoli aynan nolga teng:

$$P_{\text{OOV}}(x)=0, \forall x \in \Sigma^*. \tag{9}$$

3.1-tasdiq (AdamW algoritmining ε-stasionar nuqtaga yaqinlashishi). Agar yo'qotish funksiyasi quyidan chegaralangan, uning gradiyenti K-Lipshits uzluksiz, stoxastik gradiyent siljishsiz (bias'siz) va dispersiyasi bilan chegaralangan hamda o'rganish tezligi bo'lsa, u holda T iteratsiyadan so'ng quyidagi baho o'rinli bo'ladi:

$$\min_{t\le T} \mathrm{E}\left[\|\nabla L(\theta_t)\|_2^2 \right] \le \frac{2\left(L(\theta_0)-L^*\right)}{\eta\sqrt{T}} + \frac{K\eta\sigma^2}{\sqrt{T}} = \mathrm{O}\left(\frac{1}{\sqrt{T}}\right) \to^{\mathrm{T}\to\infty} 0. \tag{10}$$

Ya'ni, o'rtacha gradiyent normasi T ortishi bilan nolga intiladi. Bu natija modelni o'qitish jarayonining barqarorligini ta'minlaydi.

3.1-teorema (XLM-RoBERTa modeli uchun FNR chegarasi). Har qanday $\delta \in (0,1)$ uchun kamida $1-\delta$ ehtimollik bilan, har bir gipoteza $h \in H$ uchun quyidagi tengsizlik o'rinli bo'ladi:

$$\mathrm{FNR}(h) \le \widehat{\mathrm{FNR}}(h) + 2R_{m_c}(H) + \sqrt{\frac{\ln(1/\delta)}{2m_c}}. \tag{11}$$

Bu yerda $R_{m_c}(H)$ — H sinfining konfidensial sinf taqsimoti bo'yicha kutilgan Rademaxer murakkabligi. Mazkur teorema empirik soxta salbiy xatolik (FNR) qiymatining katta namuna hajmida (m_c) barqaror va asimptotik kafolatlangan kattalik ekanligini ko'rsatadi hamda ochiq tarmoqqa konfidensial hujjatni o'tkazib yuborish xavfini matematik jihatdan yuqoridan chegaralaydi.

Dissertatsiya ishining **"Konfidensial axborotlarni chiqib ketishini aniqlash dasturiy ta'minoti samaradorligini baholash va amaliyotga tatbiq etish natijalari"** deb nomlangan to'rtinchi bobida yuqoridagi boblarda taklif etilgan takomillashtirilgan usul va algoritmlar asosida ishlab chiqilgan dasturiy vosita, uning modullari hamda ishlash prinsipi keltirilgan.

Tadqiqot doirasida ishlab chiqilgan dasturiy ta’minot "KARCHKOOT" tizimi konfidensial axborotlarni aniqlash, monitoring qilish va boshqarish imkonini beruvchi agent-server arxitekturasiga ega DLP yechimidir. Tizimning foydalanuvchi interfeysi Blazor Server platformasi asosida ishlab chiqilgan va veb-brauzer orqali qulay boshqaruv muhitini taqdim etadi.

Sun’iy intellekt modelini mijoz qurilmalarida o‘g‘irlash, teskari muhandislik va zararli kod kiritish tahdidlariga qarshi ONNX modeli ko‘p qatlamli himoya bilan ta’minlangan: model shifrlangan kanal orqali uzatiladi, mijoz tomonida raqamli imzosi va xesh qiymati tekshiriladi. Windows DPAPI yordamida aynan shu qurilma va foydalanuvchiga bog‘langan holda shifrlanadi hamda izolyatsiyalangan muhitda (sandbox) bajariladi. Himoya choralari STRIDE tahdid modellashtirish uslubiyati asosida tizimlashtirilib, insidentlarga javob ISO 27035 standartiga muvofiq tashkil etilgan.

To‘liq (FP32) va kvantlangan (INT8/ONNX) XLM-RoBERTa modellarini qiyoslash natijalari 3-jadvalda keltirilgan.

3-jadval.

XLM-RoBERTa model variantlarining qiyosiy tahlili.

Ko‘rsatkich	XLM-RoBERTa (FP32)	XLM-RoBERTa (INT8)	Yaxshilanish
Inferens tezligi	100%	60%	**40% tezroq**
Xotira	1,2–1,4 GB	0,7–0,85 GB	**40% kam**
CPU yuklama	45–55%	25–35%	**35% kam**
Aniqlik	95,2%	94,7%	−0,5%

Ko‘rinib turibdiki, kvantlangan XLM-RoBERTa modeli minimal aniqlik yo‘qotishi (0,5%) evaziga sezilarli tezlik va resurs tejashni ta’minlaydi, bu real vaqt tizimlarida juda muhim.

Ishlab chiqilgan KARCHKOOT tizimining tasniflash aniqligini baholash uchun 1321 ta test faylida sinovdan o‘tkazildi. Test to‘plamining 500 tasi konfidensial, 821 tasi oddiy (ochiq) fayllar edi. Tasniflash natijasi asosida xatoliklari matritsasi qurildi (4-jadval).

4-jadval.

KARCHKOOT tizimi tasniflash natijalari.

Haqiqiy sinf	Bashorat: Konfidensial	Bashorat: Oddiy	Jami
Konfidensial	**474 (TP)**	26 (FN)	500
Oddiy	44 (FP)	**777 (TN)**	821
Jami	518	803	**1321**

Olingan natijalar KARCHKOOT tizimi konfidensial axborotlarni tasniflashda yuqori aniqlikka ega ekanini ko‘rsatadi. Accuracy - 94,7% tizimning umumiy ishonchliligini, Recall – 94,8% konfidensial fayllarni deyarli to‘liq aniqlash qobiliyatini, Precision – 91,5% esa noto‘g‘ri ogohlantirishlarning juda kamligini ko‘rsatmoqda.

Olingan natijalarning tasodifiy emasligi va statistik ahamiyatliligini tasdiqlash maqsadida 5-karra (k = 5) cross-validation o‘tkazildi. Har bir mezon bo‘yicha

o‘rtacha qiymat, standart og‘ish va 95% ishonch oralig‘i hisoblanib, modellar orasidagi farqning ahamiyatliligi McNemar testi yordamida tekshirildi (5-jadval).

5-jadval.

Tasniflash mezonlari va statistik ishonchlilik (k = 5).

Mezon	Qiymat	O‘rtacha ± std (k=5)	95% CI
Accuracy	94,7%	94,5% ± 0,6%	[93,4%; 95,8%]
Precision	91,5%	91,2% ± 0,9%	[89,8%; 92,9%]
Recall	94,8%	94,6% ± 0,7%	[93,3%; 95,9%]
F1-mezon	93,1%	93,0% ± 0,8%	[91,6%; 94,3%]
FPR	5,36%	5,5% ± 0,6%	[4,4%; 6,7%]
FNR	5,2%	5,4% ± 0,7%	[4,1%; 6,8%]

Modullar hissasini baholash (ablation) tahlilida faqat qoida (FNR 22,4%) yoki faqat NER (FNR 25,8%) yondashuvlari yuqori FNR bilan ajralib turdi, faqat ML esa F1 88,3% berdi; to‘liq gibrid (qoida + NER + ML) yondashuv eng yuqori F1 (93,1%) va eng past FNR (5,2%) natijani ko‘rsatib, har bir modulning umumiy samaradorlikka qo‘shgan hissasini tasdiqladi.

Tadqiqot doirasida ishlab chiqilgan tizim ochiq kodli va keng tarqalgan vosita - OpenDLP bilan taqqoslandi. Quyidagi 6-jadvalda ikki tizimning asosiy funksional ko‘rsatkichlari yoritilgan.

6-jadval.

OpenDLP va KARCHKOOT tizimlarining funksional taqqoslanishi

Ko‘rsatkichlar	OpenDLP	Taklif etilgan tizim
Monitoring rejimi	Offline (diskni skanerlash)	**Real vaqtli**
Kontekstual tahlil	Mavjud emas	**Mavjud**
Real vaqtli bloklash	Mavjud emas	**Mavjud**
Fayl kontentini baholash	regex, keywords	**TF-IDF asosida**
Matematik xavf modeli	Mavjud emas	**Mavjud**
Moslashtirish darajasi	Cheklangan	**Moslashuvchan**
Aniqlik (Accuracy)	89%	**94,7%**
Hodisani aniqlash vaqti	Monitoring oralig‘iga bog‘liq	**120 ms**
Operatsion tizim	Windows, Linux	Windows

KARCHKOOT tizimi bir nechta tashkilotlarda amaliy sinovdan o‘tkazildi. KARCHKOOT tizimining umumiy samaradorlik ko‘rsatkichlari 7-jadvalda keltirilgan.

7-jadval.

KARCHKOOT tizimining umumiy samaradorlik ko‘rsatkichlari.

Ko‘rsatkich	Qo‘lda tekshirish	KARCHKOOT	Yaxshilash
Hujjat tahlili vaqti	8–12 daqiqa	2–3 daqiqa	**3–4 marta tez**
Aniqlik	88–91%	92,1–95%	**+4–7%**
False Negative	7–9%	5,2%	**−26…-42%**
False Positive	3–5%	5,36%	+0,4…+2,4
Kunlik qamrov	40–60 hujjat	180–220 hujjat	**3–4,5 marta ko‘p**

Iqtisodiy samaradorlik: har bir xodim uchun kuniga 4–5 soat vaqt tejash; xavfsizlik insidentlarini 67% ga kamaytirishga erishildi hamda ROI (Return on Investment) tizim joriy etilganidan keyin 8–10 oy ichida qaytadi.

Shu tariqa, KARCHKOOT tizimida modelni ONNX formatida tarqatish va C# (.NET) muhitida inferensni tashkil etish orqali o‘zbek tilidagi konfidensial matnlarni avtomatik tasniflash, natijalarni siyosatga mos boshqaruv mexanizmlari bilan bog‘lash, hamda o‘rgatuvchi tanlanmani ishchi muhitga tarqatmasdan foydalanish imkoniyati yaratildi. Bir nechta davlat tashkilotlarida olib borilgan sinovlar tizimning yuqori samaradorligini va o‘zbek tiliga maxsus moslashtirilgan yondashuvning amaliy qiymatini tasdiqladi.

XULOSA

“Konfidensial axborotlarning chiqib ketishini bashoratlash va bartaraf qilish mexanizmlarini ishlab chiqish” mavzusidagi tadqiqot natijasida quyidagi xulosalarga erishildi:

1. Mavjud DLP tizimlarining o‘zbek tilidagi konfidensial matnlarni semantik tahlil qilish imkoniyatlari cheklanganligi va mahalliy ehtiyojlarga to‘liq moslashtirilmaganligi aniqlandi. An’anaviy qoidaviy usullarni mashinaviy va chuqur o‘rganish mexanizmlari bilan takomillashtirish zarurati asoslandi.

2. Harflar va maxsus belgilar chastotasiga asoslangan moslik indeksini hisoblash algoritmi ishlab chiqilib, tajriba matni asosida o‘zbek tili moslik indeksi uchun 0,071698945 qiymat olindi. Usulning obfuskatsiyaga turg‘unligi 2.2-teorema orqali asoslandi, tajribalarda o‘zgartirilgan fayllarni aniqlash ko‘rsatkichi 92–96% ni tashkil etdi.

3. TF-IDF va Bayes qarorlar nazariyasiga asoslangan tasniflash modeli ishlab chiqildi. 2.1-teorema asosida xatoliklar zararini hisobga oluvchi optimal chegara τ^* aniqlandi. Bu chegara Bayes tavakkalchiligini minimallashtirish va tasniflashni xavfsizlik talablariga moslashtirish imkonini berdi.

4. Konfidensial fayllarni aniqlash uchun $\text{Regex/kalit so'z} \rightarrow \text{NER} \rightarrow \text{ML}$ ketma-ketligida ishlaydigan gibrid algoritm ishlab chiqildi. Transformer modelini o‘qitish va optimallashtirish jarayonlari 3.1-lemma, 3.1-tasdiq va 3.1-teorema orqali nazariy asoslandi.

5. Tashqi qurilmalar ulanishi va fayl nusxalanishini nazorat qiluvchi KARCHKOOT tizimi ishlab chiqildi. USB qurilmalar uchun dinamik ishonch modeli taklif etildi. Agent, server va tahlil modullarining gRPC orqali integratsiyasi fayl harakati va foydalanuvchi konteksti asosida real vaqtli qaror qabul qilishni ta’minladi.

6. Tizim 1 321 ta faylda sinovdan o‘tkazilib, Accuracy - 94,7%, Precision - 91,5%, Recall - 94,8%, F1-mezon - 93,1%, FNR - 5,2% va FPR - 5,36% natijalar olindi. Qaror qabul qilish vaqti 120 ms ni tashkil etdi.

**НАУЧНЫЙ СОВЕТ DSc.03/2025.27.12.FM.01.03
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ
НАЦИОНАЛЬНОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА**

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ МИРЗО УЛУГБЕКА

БОЗОРОВ ОБИДЖОН НОРКОБИЛОВИЧ

РАЗРАБОТКА МЕХАНИЗМОВ ПРОГНОЗИРОВАНИЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

05.01.05 – Методы и системы защиты информации. Информационная и кибербезопасность (физико-математические науки)

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА ФИЛОСОФИИ (PhD)
ПО ФИЗИКО-МАТЕМАТИЧЕСКИМ НАУКАМ**

Ташкент – 2026

Тема диссертации доктора философии (PhD) по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Академии наук Республики Узбекистан за № B2019.2.PhD/FM389.

Диссертация выполнена в Национальном университете Узбекистана имени Мирзо Улугбека.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице Научного совета (http://ik-fizmat.nuu.uz) и на Информационно-образовательном портале «ZiyoNet» по адресу (www.ziyonet.uz).

Научный руководитель:	**Жураев Гайрат Умарович** доктор физико-математических наук, профессор
Официальные оппоненты:	**Туйчиев Гулом Нумонович** доктор физико-математических наук, доцент
	Гуломов Шерзод Раджаббоевич доктор технических наук, профессор
Ведущая организация:	**Ташкентский государственный технический университет**

Защита диссертации состоится «_____» _____2026 года в ____ часов на заседании Научного совета DSc.03/2025.27.12.FM.01.03 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-12-24; факс: (+99871) 246-53-21, 246-02-24; e-mail: nauka@nuu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за № ____). Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 246-02-24.

Автореферат диссертации разослан «____» _____ 2026 года.

(протокол рассылки № _____ от «____» _____ 2026 года).

М.М.Арипов
Председатель Научного совета поприсуждению научных степеней, д.ф.-м.н., профессор

З.Р.Рахмонов
Ученый секретарь Научного совета по присуждению научных степеней, д.ф.-м.н.

Б.Ф. Абдурахимов
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 настоящее время в условиях стремительного развития информационно-коммуникационных технологий в мировом масштабе исследования, посвящённые защите конфиденциальной информации, прогнозированию и предотвращению её несанкционированной утечки, являются актуальными и востребованными и широко внедряются во многие области науки и техники, в частности в государственное управление, оборону, финансово-банковскую сферу, здравоохранение, образование и другие отрасли. На современном этапе развития информационно-коммуникационных систем одним из основных механизмов оценки состояния информационной безопасности является обеспечение конфиденциальности информации. В нынешних условиях, когда количество и разнообразие угроз информационным системам непрерывно растут, разработка механизмов заблаговременного выявления (прогнозирования) и эффективного предотвращения несанкционированной утечки конфиденциальной информации, построение их эффективных методов и алгоритмов, а также создание соответствующего программного обеспечения остаются одной из важных задач.

В мире ведутся научно-исследовательские работы, направленные на разработку и совершенствование DLP-систем, предназначенных для выявления и предотвращения несанкционированной утечки конфиденциальной информации. При этом в качестве актуальной задачи рассматриваются автоматическое выявление и классификация конфиденциальных данных, хранящихся, обрабатываемых и передаваемых в информационных системах, контроль движения файлов в режиме реального времени, а также заблаговременное прогнозирование риска их несанкционированной утечки. Большинство существующих DLP-решений ориентировано на работу с данными на английском и других широко распространённых языках и не учитывает в достаточной степени лексические, морфологические и алфавитные особенности узбекского языка. В связи с этим особое внимание уделяется разработке механизмов интеллектуальной классификации конфиденциальных текстов на узбекском языке, выявления скрытой или изменённой информации, заблаговременной оценки возможных рисков и их предотвращения, а также комплекса прикладных программных средств.

В нашей республике большое внимание уделяется таким актуальным направлениям, как обеспечение информационной безопасности, защита государственных информационных систем и ресурсов, а также предотвращение несанкционированной утечки конфиденциальных данных. В частности, осуществляются широкомасштабные меры по непрерывному мониторингу государственных информационных систем и ресурсов, выявлению инцидентов кибербезопасности и устранению их последствий. Однако масштабы выявляемых инсайдерских инцидентов свидетельствуют о

наличии в данном направлении проблем, всё ещё ожидающих своего решения. В «Отчёте о кибербезопасности Республики Узбекистан за 2022 год», представленном государственным унитарным предприятием «Центр кибербезопасности», отмечено, что в общей сложности выявлено 1 869 684 события безопасности, из которых 9 709 представляли собой события, способные привести к несанкционированному доступу к конфиденциальным данным и их утечке. В Постановлении Президента Республики Узбекистан от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» определены такие важные задачи, как совершенствование механизмов оценки, мониторинга и контроля состояния кибербезопасности объектов критической информационной инфраструктуры[2]. В реализации указанных задач важное значение приобретает, в частности, создание механизмов и комплекса прикладных программных средств, позволяющих с высокой точностью выявлять секретные и конфиденциальные данные в текстах на узбекском языке, циркулирующих в информационных системах, прогнозировать и предотвращать их несанкционированную утечку.

Данное диссертационное исследование в определённой степени служит выполнению задач, предусмотренных в Законе Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности», Указе Президента Республики Узбекистан от 28 января 2022 года № УП-60 «О Стратегии развития Нового Узбекистана на 2022–2026 годы», Постановлениях Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан» и от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан», а также в других нормативно-правовых документах, относящихся к данной сфере.

Связь исследования с приоритетными направлениями развития науки и технологий республики. Диссертация выполнена в рамках IV приоритетного направления развития науки и технологий Республики Узбекистан «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. В нашей республике вопросами разработки криптографических методов и средств защиты в целях обеспечения конфиденциальности информации, а также обеспечения информационной безопасности в компьютерных системах и сетях занимались такие учёные, как М.М.Арипов, Б.Ф.Абдурахимов, А.К.Кабулов, Г.У.Жураев, Г.Н.Туйчиев, Д.М.Курязов, С.К.Ганиев, М.М.Каримов,

[2] Постановление Президента Республики Узбекистан от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» (Источник: https://lex.uz/docs/6479190).

Ш.Р.Гуломов, Ш.Н.Турапов, О.П.Ахмедова, А.Рузиев и их ученики. Ими разработаны теоретические основы защиты информации, получены практические результаты и приведён их анализ.

В научных исследованиях стран СНГ основное внимание уделялось выявлению утечек информации посредством сетевого мониторинга и наблюдения за действиями пользователей. В качестве примеров можно привести работы А.В.Лукацкого, О.Б.Макаревича, А.С.Романова, П.Д.Зегжды. Разработанные ими методы и средства послужили формированию комплексных механизмов защиты DLP-систем.

Среди зарубежных исследователей модели мониторинга информации, архитектуры DLP-систем и их модели, основанные на алгоритмах машинного обучения, были разработаны A.Shabtai, Y.Elovici и L.Rokach. Вместе с тем работы таких учёных, как S.Deerwester, T.K.Landauer, G.W.Furnas, S.T.Dumais, R.A.Harshman, разработавших модели латентно-семантического анализа (LSA) текстов и анализа конфиденциальной информации, занимают важное место в создании семантических основ DLP-систем. Вместе с тем недостаточно исследованы механизмы прогнозирования утечек конфиденциальной информации с учётом особенностей национального языка, модели анализа движения файлов в режиме реального времени и заблаговременного выявления потенциальных рисков, а также вопросы создания DLP-систем на основе методов искусственного интеллекта, позволяющих с высокой точностью выделять секретные и конфиденциальные данные в текстах на узбекском языке. Это обусловливает необходимость разработки новых подходов, способствующих более глубокому и всестороннему изучению теоретических и практических проблем в данном направлении.

Связь темы диссертации с научно-исследовательскими работами высшего образовательного учреждения, где выполнена диссертация.

Диссертационное исследование выполнено в соответствии с планом научно-исследовательских работ Национального университета Узбекистана имени Мирзо Улугбека в рамках прикладного проекта Uzb-Ind-2021-98 «Исследование и разработка алгоритмов потокового шифрования».

Цель исследования заключается в разработке эффективных методов, алгоритмов и средств прогнозирования несанкционированной утечки конфиденциальной информации и её предотвращения.

Задачи исследования:

разработка модели вычисления индекса соответствия текстов на основе частоты встречаемости букв и специальных символов, позволяющей оперативно определять степень принадлежности текстов, циркулирующих в информационных системах, к узбекскому языку и повышать точность фильтрации информации;

совершенствование алгоритма семантического анализа на основе метода TF-IDF и индекса соответствия, позволяющего выявлять инсайдерские атаки, осуществляемые путём преднамеренной перестановки символов и слов в

тексте с целью скрытого несанкционированного вывода конфиденциальных данных;

разработка механизма интеллектуальной классификации на основе модели Байеса, глубокого обучения (BERT) и алгоритмов распознавания именованных сущностей (NER), позволяющего в режиме реального времени без участия человека автоматически выявлять конфиденциальные тексты в большом потоке информации и классифицировать их по уровню конфиденциальности;

разработка архитектуры системы на основе автоматической оценки уровня доверия устройств, позволяющей динамически управлять подключениями внешних носителей информации и контролировать несанкционированное копирование файлов.

Объектом исследования являются процессы обработки, хранения и передачи конфиденциальных данных в информационно-коммуникационных системах, а также процессы обеспечения их безопасности.

Предметом исследования является создание методов, алгоритмов и программных средств прогнозирования и предотвращения несанкционированной утечки конфиденциальной информации в информационных системах.

Методы исследования. В данной диссертационной работе использованы методы математической логики и теории вероятностей, методы статистического анализа, методы моделирования и проектирования информационной безопасности, методы машинного обучения и интеллектуального анализа данных, метод анализа рисков на основе методологии DREAD, а также современные языки программирования и технологии разработки программного обеспечения.

Научная новизна исследования заключается в следующем:

разработана модель вычисления индекса соответствия текстов на основе частоты встречаемости букв и специальных символов, позволяющая оперативно определять степень принадлежности текстов, циркулирующих в информационных системах, к узбекскому языку и повышать точность фильтрации информации;

усовершенствован алгоритм семантического анализа на основе метода TF-IDF и индекса соответствия, позволяющий выявлять инсайдерские атаки, осуществляемые путём преднамеренной перестановки символов и слов в тексте с целью скрытого несанкционированного вывода конфиденциальных данных;

разработан механизм интеллектуальной классификации на основе модели Байеса, глубокого обучения (BERT) и алгоритмов распознавания именованных сущностей (NER), позволяющий в режиме реального времени без участия человека автоматически выявлять конфиденциальные тексты в большом потоке информации и категорировать их по уровню конфиденциальности;

разработана архитектура системы на основе автоматической оценки уровня доверия устройств, позволяющая динамически управлять подключениями внешних носителей информации и контролировать несанкционированное копирование файлов.

Практические результаты исследования заключаются в следующем:

разработан программный модуль, автоматически определяющий уровень конфиденциальности текстов на узбекском языке и позволяющий осуществлять их фильтрацию;

создан программный комплекс «KARCHKOOT» (система контроля и предотвращения несанкционированной утечки конфиденциальной информации), осуществляющий динамический контроль несанкционированного копирования файлов на внешние носители информации;

с помощью созданных интеллектуальных моделей и алгоритмов значительно сокращено время ручной проверки конфиденциальных документов и повышена оперативность на практике.

Достоверность результатов исследования объясняется научной обоснованностью применённых методов математической статистики и машинного обучения, соответствием теоретических выводов результатам практических испытаний, подтверждённой высокой точностью (92-96%) работы разработанных алгоритмов на практике, а также успешным внедрением полученных научных результатов в информационные системы соответствующих министерств и ведомств и их публикацией в научных изданиях.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования объясняется тем, что предложена схема обработки данных в системах мониторинга информационной безопасности, основанная на сборе и анализе сведений о возможных случаях несанкционированной утечки информации, разработаны методы статистического анализа конфиденциальной информации, а также предложен метод интеллектуального анализа, основанный на использовании модели глубокого обучения (BERT) и алгоритмов распознавания именованных сущностей (NER) в процессе выявления конфиденциальных текстов в большом потоке информации и их категорирования.

Практическая значимость результатов исследования объясняется тем, что на основе полученных теоретических результатов, моделей искусственного интеллекта и индекса соответствия разработано программное средство, автоматически выявляющее и предотвращающее несанкционированную утечку конфиденциальных данных в режиме реального времени без участия человека, и на их основе за счёт проактивного блокирования инсайдерских атак повышена эффективность работы систем мониторинга информационной безопасности.

Внедрение результатов исследования. Научные результаты, полученные по механизмам прогнозирования и предотвращения утечек конфиденциальной информации, внедрены в практику в следующих направлениях:

алгоритм, служащий автоматическому определению принадлежности текстов в информационных системах к узбекскому языку посредством вычисления индекса соответствия текстов на узбекском языке, а также предотвращению несанкционированного вывода конфиденциальной информации киберзлоумышленником путём перестановки слов или символов в тексте, использован при классификации данных и выявлении несанкционированных утечек в проекте OT-Atex-2018-486 «Реализация систем логического управления и информационной безопасности на основе программируемых логических контроллеров и автоматизированной CAD-системы их проектирования» (справка Национального университета Узбекистана имени Мирзо Улугбека от 17 мая 2022 года № 04/11-2806). В результате использование возможностей поиска с помощью водяных знаков, регулярных выражений и статических запросов в процессе предварительной обработки обеспечило повышение точности классификации;

статистические и интеллектуальные методы выявления и предотвращения несанкционированной утечки конфиденциальной информации, алгоритм вычисления индекса соответствия текстов на узбекском языке и механизм статистического анализа TF–IDF использованы при классификации данных и выявлении их несанкционированной утечки в информационных системах Таможенного комитета при Министерстве экономики и финансов (справка Таможенного комитета при Министерстве экономики и финансов от 30 марта 2023 года № 6/05-23-00108). В результате с помощью алгоритма индекса соответствия для текстов на узбекском языке достигнуто повышение показателя точности классификации данных до 92-96 процентов;

модуль контроля внешних носителей информации, алгоритм вычисления индекса соответствия текстов на узбекском языке, метод статистического анализа TF–IDF и алгоритмы интеллектуальной классификации использованы в информационной системе Института информационно-коммуникационных технологий и военной связи Университета военной безопасности и обороны Республики Узбекистан при классификации конфиденциальных текстов, контроле их передачи через внешние устройства и выявлении их несанкционированной утечки (справка Института информационно-коммуникационных технологий и военной связи Университета военной безопасности и обороны Республики Узбекистан от 23 мая 2025 года № 1027). В результате разработанная система обеспечила возможность выявления и блокирования несанкционированной утечки конфиденциальных данных через USB и другие портативные устройства с точностью 95%;

алгоритмы классификации конфиденциальных документов, разработанные на основе метода статистического анализа TF–IDF и классификатора Байеса, модуль управления разрешениями на копирование на внешние носители информации, а также DLP-система «KARCHKOOT» использованы в испытательной лаборатории Министерства обороны Республики Узбекистан, имеющей лицензию на осуществление деятельности по разработке, производству и реализации криптографических средств, при мониторинге, выявлении, классификации и блокировании конфиденциальной информации в режиме реального времени (справка Министерства обороны Республики Узбекистан от 27 мая 2025 года № 295). В результате созданная система ускорила процесс автоматического выявления и классификации конфиденциальных документов в 3-4 раза и обеспечила предотвращение несанкционированной утечки конфиденциальных данных с точностью 92.1%, что позволило сократить время ручного анализа сотрудников и повысить эффективность работы.

Апробация результатов исследования. Результаты исследования обсуждены на 10 научно-практических конференциях, в том числе на 5 международных и 5 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме исследования опубликована в общей сложности 21 научная работа, из них 7 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов диссертаций доктора философии (PhD), в том числе 2 статьи - в зарубежных и 5 - в республиканских журналах. Кроме того, получено 3 свидетельства об официальной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырёх глав, заключения, списка использованной литературы и 2 приложений. Объём диссертации составляет 117 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** приведены сведения об актуальности темы диссертации, цели и задачах, научной новизне, практических результатах и структуре работы.

В первой главе диссертации, озаглавленной **«Риск утечки конфиденциальной информации в информационных системах и механизмы защиты от неё»**, проанализированы вопросы контроля движения конфиденциальных данных в информационных системах государственных организаций, предотвращения их несанкционированного распространения, а также возможности существующих DLP-систем. Рассмотрены задачи, область применения и ограничения DLP-систем в целях обеспечения безопасности конфиденциальных данных в национальных информационных ресурсах, организации санкционированного доступа к ним и снижения риска утечки информации.

В главе разработана формальная модель политики информационной безопасности, направленной на выявление и предотвращение

несанкционированной передачи конфиденциальной информации. Здесь U – пользователи, D – документы или файлы, K – каналы передачи информации, включая USB, электронную почту, HTTP/HTTPS, FTP и принтеры, рассматриваемые как соответствующие множества. Право пользователя работать с определённым документом по определённому каналу выражается следующим отношением разрешений: $G \subseteq U \times D \times K$

Функция проверки разрешения определяется следующим образом:

$$L\left(u_i, d_j, k_r\right) = \begin{cases} 1, \text{ если} \left(u_i, d_j, k_r\right) \in G \\ 0, \text{ иначе} \end{cases} \quad (12)$$

На этой основе общая формальная модель политики безопасности выражается в следующем виде: $\Pi = \langle U, D, K, G, T, \Omega \rangle$

Здесь T – вероятные угрозы, Ω — ответные меры, выполняемые при обнаружении угрозы, то есть предупреждение, блокировка, карантин и аудит. Данная модель позволяет управлять действиями пользователей, информационными объектами и каналами передачи в рамках единой политики безопасности.

Кроме того, в главе изучены механизмы защиты данных в трёх состояниях – data-at-rest, data-in-use и data-in-motion. Проведён сравнительный анализ DLP-решений, таких как McAfee DLP, SearchInform, Sophos, InfoWatch Traffic Monitor и Kiber Protego, и показана их ограниченная эффективность при работе с текстами на узбекском языке.

С учётом высокого риска внутренних угроз для информационных систем на основе методологии DREAD разработана модель оценки рисков, связанных с утечкой конфиденциальных данных. По результатам анализа угрозами с наивысшим уровнем риска определены «Несанкционированное копирование конфиденциальных файлов через USB» (39 баллов), «Получение API-ключа через уязвимость системы и установка поддельного агента» (38 баллов) и «Скрытый вывод секретного текста инсайдером» (37 баллов).

В завершение первой главы обосновано, что снижение ложноположительных и ложноотрицательных срабатываний является важной задачей совершенствования существующих DLP-систем. Показано, что традиционные механизмы, опирающиеся на ключевые слова и жёсткие правила, не дают достаточных результатов при выявлении обфусцированных или контекстно-зависимых текстов. В связи с этим обоснована необходимость разработки DLP-системы, основанной на интеграции статистических механизмов, машинного обучения и глубокого обучения с учётом особенностей узбекского языка.

Во второй главе диссертации, озаглавленной **«Классификация конфиденциальной информации»**, осуществлена классификация конфиденциальных текстов, написанных на естественном языке. Для осуществления классификации разработаны этапы предварительной обработки, проведения статистического анализа, метод классификации

конфиденциальных текстов на основе модели Байеса, а также этапы предварительной обработки и статистического анализа информации на узбекском языке.

Первый этап автоматического анализа конфиденциальной информации - предварительная обработка текста: выделение идентифицирующих элементов, нормализация символов и приведение к векторному виду.

Предварительная обработка конфиденциальных текстов состоит из этапов формирования матрицы «документ–термин», вычисления частоты терминов, вычисления обратной частоты документов, вычисления частоты терминов – обратной частоты документов.

TF-IDF - это статистическая мера, используемая для оценки веса термина в тексте, являющемся частью совокупности текстов или языкового корпуса:

$$tf\text{-}idf(t,d,D) = tf(t,d) \cdot idf(t,D) \tag{13}$$

Индекс соответствия (CI) текстов на узбекском языке на основе частоты встречаемости букв и специальных символов определяется так:

$$I(\vec{X}) = \sum_{i=0}^{L} \left(\frac{K_i}{M} \right)^2 , \tag{14}$$

где A - множество проанализированных открытых текстов.

С помощью разработанной программы проанализировано около 70 миллионов символов текстов на узбекском языке из открытых источников (lex.uz, kun.uz и daryo.uz). По результатам вычислений индекс соответствия узбекского языка составил 0,071698945. При сопоставлении данного результата с индексами соответствия других естественных языков из открытых источников получена следующая картина (таблица 1).

Таблица 1.

Индексы соответствия языков.

Язык	**Индекс соответствия**
Хинди	0,041837864
Русский язык	0,0553
Урду	0,057535302
Английский язык	0,0644–0,0667
Узбекский язык	**0,071698945**
Итальянский язык	0,0738
Немецкий язык	0,0762
Испанский язык	0,0775
Французский язык	0,0778

В ходе исследования вычислены индексы соответствия документов, содержащих персональные данные, банковскую тайну и другие подлежащие защите сведения; результаты приведены в таблице 2.

Из таблицы 2 видно, что для отраслей, относящихся к видам конфиденциальной информации (например, банковская, военная сферы, персональные данные), индексы соответствия выше, то есть имеют значение

выше 0,076. Это означает, что в этих текстах преобладают повторяющиеся символы и термины.

Таблица 2.

Индексы соответствия по общему языку и отраслям.

№	Вид анализа	Источник текстов	Число символов (M)	Индекс соответствия	Примечание
1	Общий узбекский язык	kun.uz, daryo.uz, lex.uz	70 000 000	0,0717	Стандартный язык
2	Массовые статьи	новости, блоги	2 000 000	0,0701	Разнообразные
3	Банковская сфера	банковские документы, логи транзакций	1 200 000	**0,0762**	Секретные
4	Персональные данные	паспорт, личные идентификаторы	950 000	**0,0788**	Высокая конфиденциальность
5	Военная сфера	приказы, военные протоколы	800 000	**0,0794**	Повторяющиеся слова
6	Медицинская сфера	эпикризы, результаты анализов	850 000	0,0741	Терминологизированные
7	Юридическая сфера	законы, положения, постановления	930 000	0,0734	Формальные

В классификации на основе теории байесовских решений апостериорная вероятность принадлежности документа к классу вычисляется так:

$$P(c \mid d) = \frac{P(d \mid c)P(c)}{P(d)}. \tag{15}$$

Во второй главе для теоретического обоснования предложенных методов классификации и взаимного индекса соответствия доказан ряд математических результатов. Граница принятия решения, минимизирующая ожидаемый риск при байесовской классификации, определяется следующей теоремой.

Теорема 2.1. Если ущерб от утечки конфиденциального документа (CFN) строго больше ущерба от ошибочного блокирования открытого документа (CFP) (CFN > CFP), то оптимальная граница принятия решения τ*, минимизирующая ожидаемый байесовский риск, определяется следующим образом:

$$\tau^{*} = \frac{C_{\mathrm{FP}}}{C_{\mathrm{FP}} + C_{\mathrm{FN}}} \tag{16}$$

Устойчивость предложенного взаимного индекса соответствия к частичным изменениям инсайдера (примешивание постороннего текста или замена символов) обосновывается следующей теоремой; здесь p — частоты исходного секретного текста, r — изменённого текста, q — профиля опорной отрасли, а α ($0 \le \alpha \le 1$) — доля изменённого текста.

Теорема 2.2. В приведённых выше обозначениях отклонение ΔMI взаимного индекса соответствия между гибридным текстом X_{α} и профилем опорной отрасли Y от исходного значения ограничивается следующим неравенством:

$$\Delta MI = \left| MI\left(X_\alpha, Y\right) - MI\left(X, Y\right) \right| \le \alpha \cdot \|r - p\|_2 \cdot \|q\|_2, \quad (17)$$

где $\|\cdot\|_2$ - евклидова норма вектора. Данная теорема гарантирует пертурбационную устойчивость взаимного индекса соответствия, то есть сохранение статистического «отпечатка» документа даже при искусственном изменении состава текста и возможность определения его близости к секретным данным соответствующей отрасли.

В третьей главе диссертации, озаглавленной **«Разработка алгоритмов и структуры системы выявления утечек конфиденциальной информации»**, приведён анализ модели и структур системы выявления утечек конфиденциальной информации. Также разработана функциональная структура системы защиты от утечек конфиденциальной информации и их предотвращения.

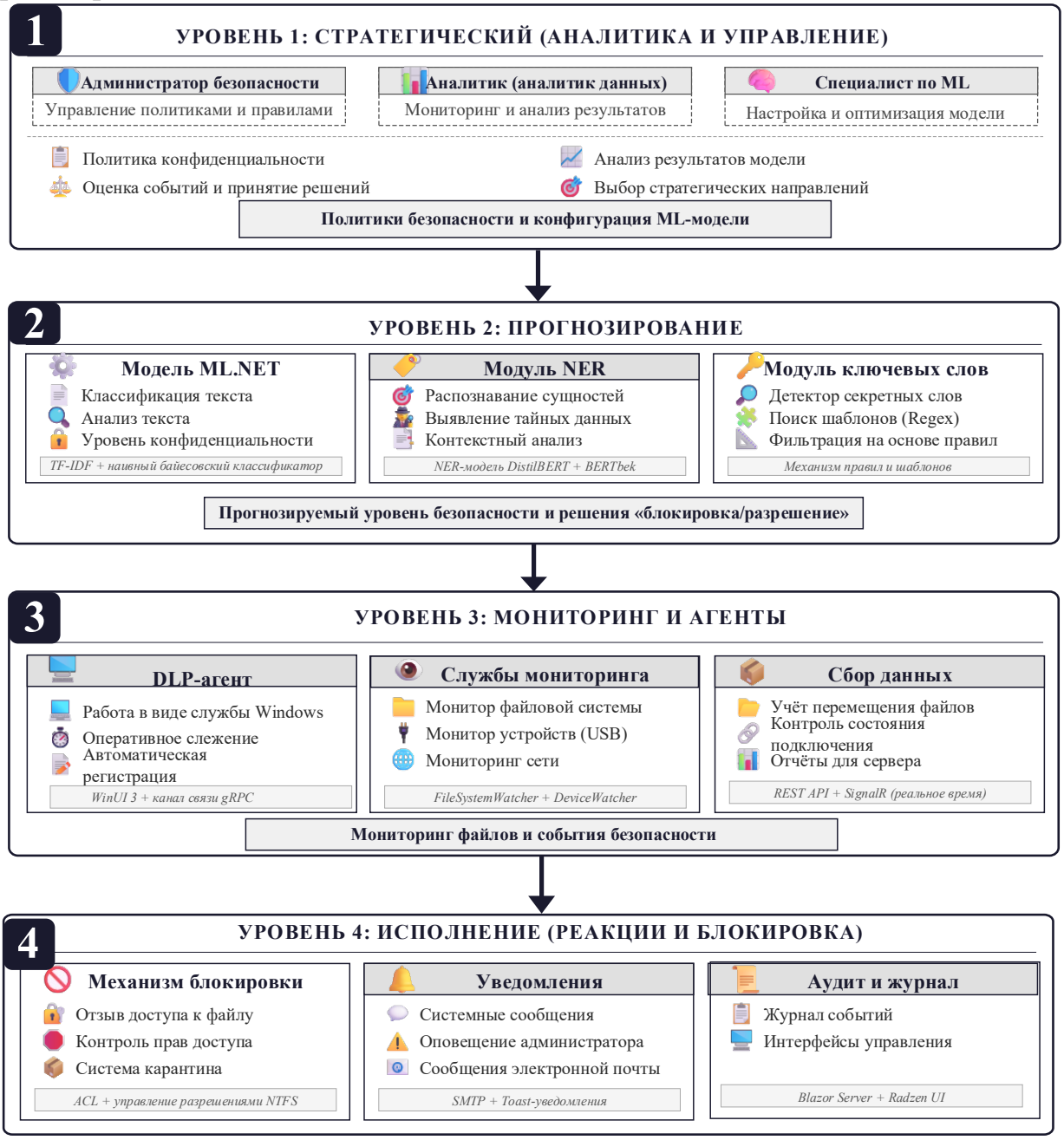


Рис. 1. Общая структура DLP-системы.

Функционально система выявления и предотвращения утечек конфиденциальной информации состоит из модулей: управления рабочей станцией; контроля каналов передачи; управления хранением и копированием конфиденциальных данных; их сбора, обработки и хранения; контроля и управления (рис. 1).

Для предотвращения несанкционированного копирования через внешние носители информации разработан динамический механизм TrustScore.

Для каждого устройства задаётся начальный балл доверия, который динамически обновляется на основе связанных с файлами событий безопасности с учётом конфиденциальности файла, веса события и истории использования устройства. Обновлённый балл доверия определяется так:

$$T_{t+1} = \text{clip}\left((1-\rho)T_0 + \rho T_t + \sum_{f \in F_t} \sum_{i=1}^{m} a_i z_i(t,f) r(f), 0, 100 \right), \qquad (18)$$

где TrustScore$_t$ - текущий балл доверия устройства; w_i - положительный или отрицательный вес i-го события; r_o - коэффициент риска, зависящий от уровня конфиденциальности файла; λ - коэффициент сохранения влияния предыдущего состояния. На основе вычисленного балла формируется решение о разрешении, ограниченном контроле или блокировке устройства; однократное положительное событие не переводит опасное устройство в доверенное мгновенно, а повторные нарушения ускоряют снижение балла доверия.

Алгоритм выявления конфиденциальных файлов включает чтение файлового события, предварительную обработку текста, выявление конфиденциальных терминов (регулярные выражения и ключевые слова), контекстный анализ (NER и ML.NET) и принятие решения (рис. 2).

Рис. 2. Блок-схема алгоритма определения конфиденциальности файлов.

Для объединения результатов модулей регулярных выражений, ключевых слов, NER и ML предложен иерархический механизм классификации. Анализ выполняется в порядке приоритета, и итоговый результат классификации c* определяется так:

$$\hat{y}(x)=\begin{cases}\hat{y}_R(x), & \hat{y}_R(x)\in\{1,2\},\\ \hat{y}_N(x), & \hat{y}_R(x)=0\wedge\hat{y}_N(x)\in\{1,2\},\\ \hat{y}_M(x), & \hat{y}_R(x)=0\wedge\hat{y}_N(x)=0.\end{cases} \tag{19}$$

Если конфиденциальность выявлена регулярным выражением или ключевым словом, принимается результат модуля правил; иначе проверяется модуль NER, а затем класс определяется семантическим анализом ML-модели. Итоговое действие безопасности над файлом определяется в зависимости от результата классификации и общего уровня риска события:

$$\omega(x)=\Pi\big(\hat{y}(x),R(x)\big),\qquad \omega(x)\in\Omega.$$

где c* — класс конфиденциальности текста файла; R - общий уровень риска события; A - набор мер реагирования (разрешение, предупреждение, дополнительная проверка, блокировка). При низком риске доступ разрешается, при среднем применяются предупреждение или ограниченный доступ, при высоком - передача блокируется, а событие фиксируется в журнале аудита.

Для выявления конфиденциальных данных с высокой точностью в реальном времени наряду с традиционными статистическими методами (TF-IDF, Байес) выбрана модель XLM-RoBERTa на архитектуре Transformer и разработан алгоритм её адаптации (fine-tuning) к узбекскому языку.

Поскольку узбекский язык является агглютинативным, при обучении модели вместо пословной токенизации использован алгоритм SentencePiece, а для минимизации ошибки на корпусе из более 15 000 текстов — функция потерь кросс-энтропии (Cross-Entropy Loss).

В третьей главе теоретически обоснован механизм выявления конфиденциальных текстов системы KARCHKOOT. Доказаны следующие фундаментальные результаты, касающиеся потери информации на этапе ввода модели, сходимости процесса обучения и способности к обобщению.

Лемма 3.1. Произвольная $x\in\Sigma^*$ строка (в том числе ранее не встречавшийся в корпусе или изменённый конфиденциальный термин) полностью разлагается на токены конечного словаря V, и вероятность символа вне словаря (Out-of-Vocabulary) в точности равна нулю:

$$P_{\text{OOV}}(x)=0,\ \forall x\in\Sigma^*. \tag{20}$$

Утверждение 3.1 (сходимость алгоритма AdamW к ε-стационарной точке). Если функция потерь $L(\theta)$ ограничена снизу, её градиент K-липшицево непрерывен, стохастический градиент несмещённый (без bias) и

его дисперсия σ^2 ограничена, а скорость обучения $\eta t = \eta / \sqrt{T}$ $(\eta \le 1/K)$, то после T итераций справедлива следующая оценка:

$$\min_{t \le T} \mathrm{E}\left[\|\nabla L(\theta_t)\|_2^2 \right] \le \frac{2\left(L(\theta_0) - L^*\right)}{\eta\sqrt{T}} + \frac{K\eta\sigma^2}{\sqrt{T}} = \mathrm{O}\left(\frac{1}{\sqrt{T}}\right) \to^{T\to\infty} 0. \qquad (21)$$

То есть средняя норма градиента стремится к нулю с ростом T. Этот результат обеспечивает стабильность процесса обучения модели.

Теорема 3.1 (граница генерализации FNR для модели XLM-RoBERTa). Для любого $\delta \in (0,1)$ с вероятностью не менее $1 - \delta$ для каждой гипотезы $h \in H$ справедливо следующее неравенство:

$$\mathrm{FNR}(h) \le \widehat{\mathrm{FNR}}(h) + 2R_{m_c}(H) + \sqrt{\frac{\ln(1/\delta)}{2m_c}}, \qquad (22)$$

где $R_{m_c}(H)$ — H - ожидаемая радемахеровская сложность класса по распределению конфиденциального класса. Данная теорема показывает, что значение эмпирической ложноотрицательной ошибки (FNR) при большом объёме выборки (m_c) является стабильной и асимптотически гарантированной величиной и математически ограничивает сверху риск пропуска конфиденциального документа в открытую сеть.

В четвёртой главе диссертации, озаглавленной **«Оценка эффективности программного обеспечения выявления утечек конфиденциальной информации и результаты внедрения в практику»**, представлено программное средство, разработанное на основе усовершенствованных методов и алгоритмов, предложенных в предыдущих главах, его модули и принцип работы.

Разработанное в рамках исследования программное обеспечение - система «KARCHKOOT» представляет собой DLP-решение с агент-серверной архитектурой, позволяющее выявлять конфиденциальную информацию, осуществлять её мониторинг и управление. Пользовательский интерфейс системы разработан на основе платформы Blazor Server и предоставляет удобную среду управления через веб-браузер.

Для защиты от угроз кражи модели, обратного инжиниринга и внедрения вредоносного кода ONNX-модель обеспечена многоуровневой защитой: модель передаётся по шифрованному каналу, на стороне клиента проверяются её цифровая подпись и хеш, она шифруется с помощью Windows DPAPI с привязкой к данному устройству и пользователю и исполняется в изолированной среде (sandbox). Меры защиты систематизированы на основе методологии STRIDE, а реагирование на инциденты организовано в соответствии со стандартом ISO 27035.

Результаты сравнения полной (FP32) и квантованной (INT8/ONNX) моделей XLM-RoBERTa приведены в таблице 3.

Таблица 3.

Сравнительный анализ вариантов модели XLM-RoBERTa.

Показатель	XLM-RoBERTa (FP32)	XLM-RoBERTa (INT8)	Улучшение
Скорость инференса	100%	60%	**на 40% быстрее**
Память	1,2–1,4 ГБ	0,7–0,85 ГБ	**на 40% меньше**
Загрузка CPU	45–55%	25–35%	**на 35% меньше**
Точность	95,2%	94,7%	−0,5%

Как видно, квантованная модель XLM-RoBERTa ценой минимальной потери точности (0,5%) обеспечивает значительный выигрыш в скорости и экономию ресурсов, что очень важно в системах реального времени.

Для оценки точности классификации разработанной системы KARCHKOOT проведено тестирование на 1321 тестовом файле. Из тестового набора 500 файлов были конфиденциальными, 821 — обычными (открытыми). На основе результатов классификации построена матрица ошибок (таблица 4).

Таблица 4.

Результаты классификации системы KARCHKOOT.

Истинный класс	Прогноз: Конфиденциальный	Прогноз: Обычный	Всего
Конфиденциальный	**474 (TP)**	26 (FN)	500
Обычный	44 (FP)	**777 (TN)**	821
Всего	518	803	**1321**

Полученные результаты показывают, что система KARCHKOOT обладает высокой точностью при классификации конфиденциальной информации. Accuracy - 94,7% свидетельствует об общей надёжности системы, Recall - 94,8% о способности практически полного выявления конфиденциальных файлов, а Precision - 91,5% об очень малом числе ложных предупреждений.

Для подтверждения неслучайности и статистической значимости результатов проведена 5-кратная (k = 5) перекрёстная проверка. По каждому показателю вычислены среднее значение, стандартное отклонение и 95% доверительный интервал, а значимость различий между моделями проверена тестом МакНемара (таблица 5).

Таблица 5.

Показатели классификации и статистическая надёжность (k = 5).

Показатель	Значение	Среднее ± ст. откл. (k=5)	95% ДИ
Accuracy	94,7%	94,5% ± 0,6%	[93,4%; 95,8%]
Precision	91,5%	91,2% ± 0,9%	[89,8%; 92,9%]
Recall	94,8%	94,6% ± 0,7%	[93,3%; 95,9%]
F1-мера	93,1%	93,0% ± 0,8%	[91,6%; 94,3%]
FPR	5,36%	5,5% ± 0,6%	[4,4%; 6,7%]
FNR	5,2%	5,4% ± 0,7%	[4,1%; 6,8%]

При ablation-анализе подходы «только правила» (FNR 22,4%) и «только NER» (FNR 25,8%) показали высокий FNR, «только ML» — F1 88,3%; полный гибрид (правила + NER + ML) обеспечил наивысшую F1 (93,1%) и наименьший FNR (5,2%), подтвердив вклад каждого модуля.

Разработанная в рамках исследования система сопоставлена с открытым и широко распространённым средством — OpenDLP. В таблице 6 ниже освещены основные функциональные показатели двух систем.

Таблица 6.
Функциональное сопоставление систем OpenDLP и KARCHKOOT.

Показатели	**OpenDLP**	**Предлагаемая система**
Режим мониторинга	Offline (сканирование диска)	**В реальном времени**
Контекстный анализ	Отсутствует	**Имеется**
Блокирование в реальном времени	Отсутствует	**Имеется**
Оценка контента файла	regex, keywords	**На основе TF-IDF**
Математическая модель риска	Отсутствует	**Имеется**
Степень адаптируемости	Ограниченная	**Гибкая**
Точность (Accuracy)	89%	**94,7%**
Время выявления события	Зависит от интервала мониторинга	**120 мс**
Операционная система	Windows, Linux	Windows

Система KARCHKOOT прошла практические испытания в нескольких организациях. Общие показатели эффективности системы KARCHKOOT приведены в таблице 7.

Таблица 7.
Общие показатели эффективности системы KARCHKOOT.

Показатель	**Ручная проверка**	**KARCHKOOT**	**Улучшение**
Время анализа документа	8–12 минут	2–3 минуты	**в 3–4 раза быстрее**
Точность	88–91%	92,1–95%	**+4–7%**
False Negative	7–9%	5,2%	**−26…-42%**
False Positive	3–5%	5,36%	**+0,4…+2,4**
Дневной охват	40–60 документов	180–220 документов	**в 3–4,5 раза больше**

Экономическая эффективность: экономия 4–5 часов времени в день на каждого сотрудника; сокращение инцидентов безопасности на 67%; ROI

(Return on Investment) - система окупается в течение 8–10 месяцев после внедрения.

Таким образом, в системе KARCHKOOT за счёт распространения модели в формате ONNX и организации инференса в среде C# (.NET) создана возможность автоматической классификации конфиденциальных текстов на узбекском языке, связывания результатов с механизмами управления, соответствующими политике безопасности, а также использования без передачи обучающей выборки в рабочую среду. Испытания, проведённые в нескольких государственных организациях, подтвердили высокую эффективность системы и практическую ценность подхода, специально адаптированного к узбекскому языку.

ЗАКЛЮЧЕНИЕ

В результате исследования по теме «Разработка механизмов прогнозирования и предотвращения утечек конфиденциальной информации» получены следующие выводы:

1. Установлено, что возможности существующих DLP-систем по семантическому анализу конфиденциальных текстов на узбекском языке ограничены и не в полной мере адаптированы к локальным потребностям. Обоснована необходимость совершенствования традиционных методов, основанных на правилах, с использованием механизмов машинного и глубокого обучения.

2. Разработан алгоритм вычисления индекса соответствия на основе частоты букв и специальных символов; для тестового текста получено значение 0,071698945. Устойчивость метода к обфускации обоснована теоремой 2.2; в экспериментах показатель выявления изменённых файлов составил 92–96%.

3. Разработана модель классификации на основе TF-IDF и теории байесовских решений. На основе теоремы 2.1 определён оптимальный порог τ^*, учитывающий стоимость ошибок. Этот порог позволил минимизировать байесовский риск и согласовать классификацию с требованиями безопасности.

4. Для выявления конфиденциальных файлов разработан гибридный алгоритм, работающий в последовательности «регулярные выражения/ключевые слова → NER → ML». Процессы обучения и оптимизации трансформерной модели теоретически обоснованы леммой 3.1, утверждением 3.1 и теоремой 3.1.

5. Разработана система KARCHKOOT, контролирующая подключение внешних устройств и копирование файлов. Предложена динамическая модель доверия для USB-устройств. Интеграция агентского, серверного и аналитического модулей посредством gRPC обеспечила принятие решений в реальном времени на основе файловых событий и пользовательского контекста.

6. Система испытана на 1 321 файле; получены результаты: Accuracy - 94,7%, Precision - 91,5%, Recall - 94,8%, F1-мера - 93,1%, FNR - 5,2% и FPR - 5,36%. Время принятия решения составило 120 мс.

SCIENTIFIC COUNCIL AWARDING OF THE SCIENTIFIC DEGREES DSc.03/2025.27.12.FM.01.03 NATIONAL UNIVERSITY OF UZBEKISTAN

NATIONAL UNIVERSITY OF UZBEKISTAN NAMED AFTER MIRZO ULUGBEK

BOZOROV OBIDJON NORKOBILOVICH

DEVELOPMENT OF MECHANISMS FOR PREDICTING AND PREVENTING CONFIDENTIAL INFORMATION LEAKAGE

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

ABSTRACT OF DISSERTATION OF THE DOCTOR OF PHILOSOPHY (PhD) ON PHYSICAL AND MATHEMATICAL SCIENCES

Tashkent – 2026

The theme of the dissertation of the Doctor of Philosophy (PhD) on physical and mathematical sciences was registered at the Higher Attestation Commission under the Academy of Sciences of the Republic of Uzbekistan under number B2019.2.PhD/FM389.

The dissertation has been prepared at the National University of Uzbekistan.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (summary)) on the website (http://ik-fizmat.nuu.uz) and the website of "ZiyoNet" Information and educational portal (www.ziyonet.uz).

Scientific supervisor:	**Juraev Gayrat Umarovich** Doctor of Physical and Mathematical Sciences, Professor
Official opponents:	**Gulomov Sherzod Rajabboevich** Doctor of Technical Sciences, Professor
	Tuychiev Gulom Numonovich Doctor of Physical and Mathematical Sciences
Leading organization:	**Tashkent State Technical University**

Defense will take place on «____» _____ 2026 at ____ at the meeting of Scientific council number DSc.03/2025.27.12.FM.01.03 at the National University of Uzbekistan (Address: 100174, Uzbekistan, Tashkent city, Almazar area, University str. 4, Ph.: (99871) 227-12-24, fax: (99871) 246-53-21, 246-02-24, e-mail: nauka@nuu.uz).

The dissertation is possible to review in Information-resource centre at the National University of Uzbekistan (registered № _____) (Address: 100174, Uzbekistan, Tashkent city, Almazar area, University str., 4. Ph.: (99871) 246-02-24).

Abstract of dissertation sent out on «____» _____ 2026.
(mailing report №___ on «____» _____ 2026).

M.M. Aripov
Chairman of Scientific Council on award of scientific degrees, D.F.-M.S., professor

Z.R. Rakhmonov
Scientific secretary of Scientific Council on award of scientific degrees, D.F.-M.S.

B.F. Abdurakhimov
Chairman of the Scientific seminar at the Scientific Council on award of scientific degrees, D.F.-M.S.

INTRODUCTION (Abstract of PhD thesis)

The aim of the research is to develop effective methods, algorithms and tools for predicting and preventing the unauthorized leakage of confidential information.

The object of the research is the processes of processing, storing and transmitting confidential data in information and communication systems, as well as ensuring their security.

The scientific novelty of the research is as follows:

a model for calculating the text conformity index based on the frequency of occurrence of letters and special characters has been developed, which makes it possible to quickly determine the degree to which texts circulating in information systems belong to the Uzbek language and to increase the accuracy of information filtering;

the semantic analysis algorithm based on the TF-IDF method and the conformity index has been improved, which makes it possible to detect insider attacks carried out by deliberately rearranging characters and words in the text in order to covertly exfiltrate confidential data;

an intelligent classification mechanism based on the Bayes model, deep learning (BERT) and named entity recognition (NER) algorithms has been developed, which makes it possible to automatically detect confidential texts in a large information flow in real time without human involvement and to categorize them by confidentiality level;

a system architecture based on automatic assessment of the trust level of devices has been developed, which makes it possible to dynamically manage connections of external storage devices and to control unauthorized file copying.

Implementation of the research results. The scientific results obtained on the mechanisms for predicting and preventing confidential information leakage have been implemented in practice in the following areas:

the algorithm serving to automatically determine whether texts in information systems belong to the Uzbek language by calculating the conformity index of Uzbek-language texts, as well as to prevent the unauthorized exfiltration of confidential information by a cyber attacker through rearranging words or characters in the text, was used for data classification and detection of unauthorized leaks in the project OT-Atex-2018-486 «Implementation of logical control and information security systems based on programmable logic controllers and an automated CAD logic system for their design» (Certificate of the National University of Uzbekistan named after Mirzo Ulugbek No. 04/11-2806 dated May 17, 2022). As a result, the use of search capabilities based on watermarks, regular expressions and static queries during preprocessing ensured an increase in classification accuracy;

statistical and intelligent methods for detecting and preventing the unauthorized leakage of confidential information, the algorithm for calculating the conformity index of Uzbek-language texts and the TF–IDF statistical analysis

mechanism were used for data classification and detection of unauthorized leaks in the information systems of the Customs Committee under the Ministry of Economy and Finance (Certificate of the Customs Committee under the Ministry of Economy and Finance No. 6/05-23-00108 dated March 30, 2023). As a result, using the conformity index algorithm for Uzbek-language texts, the data classification accuracy was increased to 92-96 percent;

the external storage media control module, the algorithm for calculating the conformity index of Uzbek-language texts, the TF–IDF statistical analysis method and intelligent classification algorithms were used in the information system of the Institute of Information and Communication Technologies and Military Communication of the University of Military Security and Defense of the Republic of Uzbekistan for classifying confidential texts, controlling their transfer via external devices and detecting their unauthorized leakage (Certificate of the Institute of Information and Communication Technologies and Military Communication of the University of Military Security and Defense of the Republic of Uzbekistan No. 1027 dated May 23, 2025). As a result, the developed system made it possible to detect and block the unauthorized leakage of confidential data via USB and other portable devices with 95% accuracy;

the confidential document classification algorithms developed on the basis of the TF–IDF statistical analysis method and the Bayes classifier, the module for managing permissions to copy to external storage media, as well as the «KARCHKOOT» DLP system were used in the testing laboratory of the Ministry of Defense of the Republic of Uzbekistan licensed to engage in the development, production and sale of cryptographic tools, for real-time monitoring, detection, classification and blocking of confidential information (Certificate of the Ministry of Defense of the Republic of Uzbekistan No. 295 dated May 27, 2025). As a result, the created system accelerated the process of automatic detection and classification of confidential documents by 3-4 times and prevented the unauthorized leakage of confidential data with 92.1% accuracy, which reduced the time of manual analysis by employees and increased work efficiency.

Structure and scope of the dissertation. The dissertation consists of an introduction, four chapters, a conclusion, a list of references and 2 appendices. The volume of the dissertation is 117 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo‘lim (I часть; I part)

1. Saymanov I., Muxammadiev F., Juraev G., Lu Y., Boiprav O., Alaev R., Bozorov O., Abdullayev T. Detecting Anomalous States Through File Operations Using Unsupervised Learning Algorithms // Advances in Artificial Intelligence and Machine Learning. – 2026. – № 06 (02). – pp.01–14. https://doi.org/10.54364/AAIML.2026.62284 (3, Scopus IF=0.5).
2. Juraev G., Bozorov O. Using TF-IDF in text classification // AIP Conference Proceedings. – 2023. – Vol. 2789, Issue 1. – Article 050017. https://doi.org/10.1063/5.0145520 (3, Scopus IF=0.146).
3. Bozorov O.N. Konfidensial fayllarning harakatini aniqlash va nazorat qilish tizimi // Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali, 2025, T. 3. № 1. 80-84-b. https://doi.org/10.5281/zenodo.20916607 (05.00.00, OAK 340/5-son qarori)
4. Bozorov O.N. O‘zbek tilidagi konfidensial matnlarni qoidaviy, NER va mashinaviy o‘qitish modellari asosida gibrid tasniflash // Texnika fanlarining dolzarb masalalari, vol. 4(6), 2026, 4–14-b. https://doi.org/10.47390/ts-v4is/1y2026N01 (05.00.00, OAK 370-son qarori)
5. Bozorov O.N. Chastotali tahlil usulidan foydalangan holda ochiq matnlarning o‘xshashligni tahlil qilish // Ilm sarchashmalari. 2021. T. 8. № 1. 12–17 b. https://ilmsarchashmalari.urdu.uz/user-media/issues_files/2021-8.pdf (01.00.00, №12)
6. Bozorov O.N. O‘zbek tilidagi konfidensial matnlarni aniqlash uchun transformer modellar va gibrid tasniflash mexanizmlariga asoslangan DLP tizimi// Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali, 2026, T. 4. № 2. 149-158-b. https://doi.org/10.5281/zenodo.20916240 (05.00.00, OAK 340/5-son qarori)
7. Jo‘rayev G., Alayev R.X., Bozorov O., Mukhammadiyev F. Model and Algorithm for Controlling Channels of Confidential Data Leakage in Computer Systems // International Conference on Information Science and Communications Technologies (ICISCT 2023): Applications, Trends and Opportunities. – 2023. pp. 118–123. https://www.researchgate.net/publication/408307398 (05.00.00, OAK 2766/05-3-son qarori)

II bo‘lim (II часть; II part)

8. Bozorov O., Muxammadiyev F., Jurayev G., Alayev R., Insayder tahdidlarini aniqlashda tanlanmani shakllantirish va avtomatik sinflashtirish // Axborot xavfsizligi muammolari, 2025, № 2 (3). 13-25 b. (01.00.00, OAK 347-son qarori)
9. Bozorov O., Mukhammadiyev F., Boltayev S. Analysis of the capabilities of systems for detecting abnormal states in computer systems // DTAI – 2024:

“Digital transformation and artificial intelligence: problems, innovations and trends” I international scientific - practical conference, 2024, pp. 136–144. (05.00.00, OAK 358/3-son qarori)

10. Bozorov O., Muxammadiyev F., Jurayev G., Alayev R., Comparative analysis of software products destined to prevent leaks of confidential information. SCIENTIFIC – TECHNICAL JOURNAL of FerPI, 2023, № 27 (2), pp. 136–144. (05.00.00, №20)

11. Jo‘rayev G.U., Bozorov O.N. Problems of ensuring the confidentiality of data objects of informatization. International Uzbekistan-Malaysia Conference on "COMPUTATIONAL MODELS AND TECHNOLOGIES (CMT2020)”. 24-25 August 2020, Tashkent, 104 p.

12. Бозоров О. Н. Ҳарфлар частоталарини матнлар таҳлилида қўлланилиши // “Ахборот тизимлари ва технологияларининг замонавий жамиятдаги ўрни” мавзусида Республика миқёсидаги илмий-амалий конференция материаллари тўплами. Наманган шаҳри: НамМҚИ, 2021. 28–31 b.

13. Бозоров О.Н., Жўраев Г.У. «Электрон ҳукумат» шароитида Ўзбекистон Республикасида конфиденциал ахборотларни ҳимоялаш муаммолари ва ечимлари // Ўзбекистон Республикаси Президенти ҳузуридаги Давлат бошқаруви академиясида бўлиб ўтган “Давлат бошқарувида рақамлаштириш: муаммо ва ечимлар. Тошкент: , 2019. 108–111 b.

14. Bozorov O. N. Sharofov D.O. “Data Leakage Detection and Prevention Solutions.” International Journal of Advanced Research in Science, Engineering and Technology, 2019, Vol. 6(11), pp. 11764–11772.

15. Berdimurodov M. A., Bozorov O. N. Hamming masofasi va kodi axborot xavfsizligida // Matematik fizika va matematik modellashtirishning zamonaviy muammolari: Xalqaro ilmiy konferensiya materiallari. Qarshi: , 2021. 196–198 b.

16. Bozorov O.N. Axborot tizimlarida foydalanuvchilarning anomal harakatlarini aniqlash // Matematik fizika va matematik modellashtirishning zamonaviy muammolari: Xalqaro ilmiy konferensiya materiallari. Qarshi: QarshiDU, 2021. C. 198–200.

17. Bozorov O.N. Harflar chastotalarini matnlar tahlilida qo‘llanilishi // “Zamonaviy axborot, kommunikatsiya texnologiyalari va at-ta’lim tatbiqi muammolari” mavzusidagi Respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. 2022. 343–345 b.

18. Bozorov O.N. Matnlarning o‘xshashligini tahlil qilish // KOMPYUTER LINGVISTIKASI: MUAMMOLAR, YECHIM, ISTIQBOLLAR. Toshkent: , 2023. 187–189 b.

19. Bozorov Obidjon. Protecting confidential files from corporate network without permission // Technical sciences. 2020. T. 6. № 3. 9–14 b.

20. Gayrat Juraev, Obidjon Bozorov, Dadakhon Sharofov “Protection of System from an Unauthorized Leak of Confidential Information.” *International*

Journal of Advanced Research in Science, Engineering and Technology, 2019, Vol. 6(11), pp. 11795–11798.

21. Bozorov O. N., Muhammadiyev F. R. o‘g‘li. Windowsda fayllarining harakatini aniqlash va nazorat qilish tizimi// “Axborot xavfsizligi sohasida raqamlashtirish muammolari va istiqbollari” mavzusidagi Respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami, Toshkent 2025. 141–144 b.

22. Jo‘rayev G.U., Bozorov O.N. Konfidensial ma’lumotlarni qidirish va klassifikatsiyalash dasturiy ta’minoti. DGU 12391. Dasturiy mahsulotlar davlat reestrida 11.09.2021-yilda ro‘yxatdan o‘tkazilgan.

23. Jo‘rayev G.U., Bozorov O.N. Konfidensial axborotlarni ruxsatsiz chiqib ketishini oldini olish tizimi. DGU 12605. Dasturiy mahsulotlar davlat reestrida 08.10.2021-yilda ro‘yxatdan o‘tkazilgan.

24. Jo‘rayev G.U., Bozorov O.N.’KARCHKOOT’ tizimi. DGU 35108. Dasturiy mahsulotlar davlat reestrida 07.03.2024-yilda ro‘yxatdan o‘tkazilgan.

Avtoreferat «Public Publish Printing» nashriyotida tahrirdan o‘tkazilib,
o‘zbek, rus va ingliz tillaridagi matnlar o‘zaro muvofiqlashtirildi.

Bosishga ruxsat etildi: 10.08.2026-yil
Bichimi 60x84 $^{1}/_{16}$, “Times New Roman”
garniturada raqamli bosma usulida bosildi.
Shartli bosma tabog‘i 3,0. Adadi: 50. Buyurtma: №90.

«Public Publish Printing» MChJ
bosmaxonasida chop etildi.
Toshkent, M.Ulug‘bek tum., Moylisoy, 22.