TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

BOZOROV SUHROBJON MUMIN O‘G‘LI

AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA TARMOQ HUJUMLARINI ANIQLASH USULI VA ALGORITMLARI

05.01.05 – Axborotni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2025

UO‘K 004.056.57

Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

Contents of dissertation abstract of doctor of philosophy (PhD) on technical science

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

BOZOROV SUHROBJON MUMIN O‘G‘LI

AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA TARMOQ HUJUMLARINI ANIQLASH USULI VA ALGORITMLARI

05.01.05 – Axborotni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2025

Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasining mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestasiya komissiyasida B2025.1.PhD/T5294 raqam bilan ro‘yxatga olingan.

Dissertatsiya Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida bajarilgan.

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

Ilmiy rahbar:	**G‘ulomov Sherzod Rajaboyevich** texnika fanlar doktori, dotsent
Rasmiy opponentlar:	**Kerimov Komil Fikratovich** texnika fanlar doktori, professor
	Kadirov Mirxusan Mirpo‘latovich texnika fanlari bo‘yicha falsafa doktori (PhD), dotsent
Yetakchi tashkilot:	**“UNICON.UZ” MCHJ - Fan-texnika va marketing tadqiqotlari markazi.**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 2025-yil “_18_”.__oktabr__. soat _11:30_ dagi majlisida bo‘lib o‘tadi. (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (+99871) 238-64-15; e-mail: info@tuit.uz).

Dissertatsiya bilan Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (_368_ – raqam bilan ro‘yxatga olingan).
(Manzil: 100084, Toshkent, Amir Temur ko‘chasi, 108-uy. Tel.: (+99871) 238-64-15).

Dissertatsiya avtoreferati 2025 yil “_08_” _oktabr_da tarqatildi.
(2025-yil “__” _____dagi _____ - raqamli reestr bayonnomasi).

B.Sh. Maxkamov
Ilmiy darajalar beruvchi ilmiy kengash raisi, iqtisodiyot fanlari doktori, professor

M.S. Saitkamolov
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, iqtisodiyot fanlari doktori, dotsent

D.Ya. Irgasheva
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi ilmiy seminar raisi, texnika fanlari doktori, professor

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. So‘nggi yillarda butun dunyo miqyosida axborot-kommunikatsiya tizimlarida yuzaga keluvchi moliyaviy, texnik va axborot xavfsizligiga oid zararlarni kamaytirish yoki butunlay oldini olish maqsadida, hujumlarni aniqlash (Intrusion Detection System – IDS) hamda ularni bartaraf etish tizimlarining (Intrusion Prevention System – IPS) aniqligi va samaradorligini oshirish, mavjud zaifliklarni bartaraf etish ustuvor yo‘nalishlardan biri sifatida ko‘rilmoqda. 2024-yil noyabr oyida respublikamiz axborot-kommunikatsiya tizimlariga 10 500 dan ortiq turli hujumlar amalga oshirilganligi qayd etilgan. Xususan, “Kasperskiy” laboratoriyasining ma’lumotlariga ko‘ra, 2024-yil dekabr oyida kiberhujumlar eng ko‘p uyushtirilgan davlatlar orasida O‘zbekiston 46-o‘rinni egallagan[1]. Bu o‘z navbatida, axborot-kommunikatsiya tizimlari xavfizlik darajasini oshirish uchun hujumlarni aniqlash tizimlarini, xususan, mavjud va yangi hujumlarni samarali aniqlashga imkon beruvchi usul va algoritmlarni takomillashtirishni taqozo etadi. Yevropa mamlakatlari, AQSH, Xitoy, Rossiya Federatsiyasi, Yaponiya va Janubiy Koreya kabi rivojlangan davlatlarda hujumlarni aniqlash tizimlarini sun’iy intellekt usullari yordamida takomillashtirish, yangi usul va algoritmlar ishlab chiqish, shuningdek, ularni real tizimlarda joriy etish borasidagi ilmiy-tadqiqot ishlari ham nazariy, ham amaliy jihatdan faol olib borilmoqda.

Jahon tajribasiga ko‘ra, hozirgi kunda kiberhujumlardan himoya vositalarini ishlab chiqish, tarmoq paketlaridagi anomaliyalarni real vaqtda aniqlash, hujumlarni aniqlash tizimlarini qurish usul va algoritmlarni intellektual tizimlar yordamida takomillashtirish uchun ishlar olib borilmoqda. Ushbu sohada, jumladan signaturaga asoslangan aniqlashdan voz kechgan holda paketlarni sun’iy intellekt usullari yordamida tahlillash orqali hujumlarni aniqlash usullarini ishlab chiqish asosiy vazifalardan biri hisoblanmoqda. Shu bilan birga, axborot-kommunikatsiya tizimlarida almashinuvchi va saqlanuvchi axborotni himoyalash jarayonida foydalanilayotgan sun’iy intellekt usullaridan to‘g‘ri foydalangan holda hujumlarni aniqlash tizimlarining samaradorligini oshirish va yolg‘ondan tasdiqlash ko‘rsatkichlarini (False Alarm Rate - FAR) pasaytirishga yo‘nalishtirilgan ilmiy ishlarga alohida e’tibor qaratilmoqda.

Respublikamizning davlat va xo‘jalik boshqaruv tashkilotlari axborot-kommunikatsiya tizimlarida axborotni himoyalash maqsadida foydanilayotgan himoya mexanizmlarini takomillashtirishga qaratilgan keng ko‘lamli chora-tadbirlar amalga oshirilmoqda. 2022-2026-yillarga mo‘ljallangan Yangi O‘zbekistonning Taraqqiyot strategiyasida “...“UZ” domen zonasi Internet-makonining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlarini hamda elektron hukumat, energetika, raqamli iqtisodiyot tizimlarini va muhim axborot infratuzilmasiga taalluqli boshqa yo‘nalishlarni himoya qilish” [2] bo‘yicha vazifalar belgilab berilgan Ushbu vazifalarni bajarishda axborot-kommunikatsiya tizimlarida

[1] https://cybermap.kaspersky.com/

[2] 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

sun’iy intellekt usullari yordamida hujumlarni aniqlash usullarini takomillashtirgan holda resurs sarfini kamaytirilgan, samaradorligi oshirilgan vositalarni ishlab chiqish muhim hisoblanadi.

Ushbu dissertatsiya ishi 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, 2020 yildagi 5-oktabrdagi PF-6079-sonli ““Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida” gi Farmonlari, 2023-yil 31-maydagi PQ-167-sonli “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlarining kiberxavfsizlik tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi, 2019-yil 14-sentabrdagi PQ-4452-son “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarorlarida belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya ishi ma’lum darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Axborot xavfsizligini ta’minlash maqsadida hujumlarni aniqlash tizimlarini qurishning anomaliyaga asoslangan neyron tarmoqlar, chuqur o‘rganish va boshqa usullar va algoritmlarni qo‘llash bo‘yicha F.Almasoudya, R.Gautam, M.Darkaie, M.Guan, A.Kribel, I.Alekseyev, J.Faysal, R.Gupta va boshqa chet ellik olimlar tomonidan ilmiy izlanishlar olib borilmoqda. Sun’iy neyron tarmoqlar arxitekturalaring hujumlarni aniqlash tizimlaridagi ahamiyatini ko‘rsatish uchun J.Doe, L.Gonzalez,V.Kuzmin, P.Thomas, A.Dridi, J.Klein kabi ilmiy izlanuvchilar bir qancha tadqiqot ishlarini olib borishmoqda. Bundan tashqari, Bro Zeek, RiskWatch, Kasperskiy Lab va Trend Micro tashkilotlari tomonidan axborot-kommunikatsiya tizimlarida axborotni himoyalashning intellektual tizimlarni qo‘llagan holda dasturiy-apparat vositalarini ishlab chiqish bo‘yicha injinerlik-tadqiqot ishlari olib borilmoqda.

O‘zbekistonda S.K.Ganiyev, M.M.Karimov, K.A.Tashev, SH.R.G‘ulomov, N.B.Nasrullayev, F.B.Botirovlar boshchiligidagi ilmiy jamoalar tomonidan axborotni himoyalashning intellektual tizimlari, paketlarni filtrlash, axborot xavfsizligi risklari, hujumlarni aniqlashning usul va algoritmlari ustida ilmiy izlanishlar olib borilgan.

Shu bilan birga, axborot-kommunikatsiya tizimlarida hujumlarni aniqlash tizimlarini qurishning mashinali o‘qitish (machine learning) usullari asosida aniqlash samaradorligini oshirish, yolg‘ondan tasdiqlash ko‘rsatkichini pasaytirish kabi usul va algoritmlari yetarlicha tadqiq etilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim yoki ilmiy tadqiqot muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy tadqiqot ishlari rejasining 598661-EPP-12018-1-

RO-EPPKA2-CBHE-JP “Developing Services for Individuals with Disabilities–DECIDE” (2019-2022) mavzusidagi ilmiy loyihalar doirasida bajarilgan.

Tadqiqotning maqsadi axborot-kommunikatsiya tizimlarida tarmoq hujumlarini aniqlashning samarali usul va algoritmlarini ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

axborot-kommunikatsiya tizimlarida hujumlarni aniqlashning mavjud tizimlarini tahlillash orqali tahdidning umumiy modelini ishlab chiqish;

yolg‘ondan tasdiqlash darajasini kamaytirish va aniqlashning yuqori samaradorligini ta’minlash maqsadida tarmoq hujumlarini aniqlash tizimlarini yaratish usulini takomillashtirish;

axborot-kommunikatsiya tizimlarida tarmoq hujumlarini aniqlashda tarmoq paketlarining o‘qitish uchun xususiyatlarini tanlash algoritmlarini ishlab chiqish;

sun’iy neyron tarmoqlaridan foydalanilganda yashirin qatlam va neyronlarning tarmoq hujumlarini aniqlash tizimining ishlashiga ta’sirini o‘rganish va ularning muvozanatini ta’minlagan holda aniqlash samaradorligini oshirish.

Tadqiqotning obyekti sifatida axborot-kommunikatsiya tizimlarida tarmoq orqali uzatiladigan ma’lumotlar oqimiga qaratilgan hujumlar olingan.

Tadqiqotning predmetini axborot-kommunikatsiya tarmoqlarida hujumlarni aniqlashning samarali usul va algoritmlari tashkil etadi.

Tadqiqotning usullari. Tadqiqot jarayonida axborotni himoyalash usullari, neyron tarmoqlar, axborot nazariyasi, diskret matematika va obyektga yo‘naltirilgan dasturlash, shuningdek, tajribaviy tadqiqotlar natijalariga asoslangan usullardan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

mavjud tarmoq hujumlarini aniqlash tizimlarini tahlillash uchun STRIDE metodikasi yordamida tahdid modeli ishlab chiqilgan va ehtimoliy xavflarning risk darajalari DREAD modeli asosida baholangan;

hujumlarni aniqlash tizimlarini qurish usuli, ulardagi mavjud kamchiliklarni, yolg‘ondan tasdiqlash darajasini minimallashtirish va aniqlash samaradorligini oshirish uchun tarmoq paketi xususiyatlarini ovoz berish hamda neyron tarmoqlar arxitekturasini avtomatik tanlash jarayonlarini kiritish hisobiga takomillashtirilgan;

tarmoq hujumlarini aniqlash tizimlarini sun’iy intellekt usullari yordamida o‘qitish uchun tarmoq paketi xususiyatlarini tanlashda ularning entropiyasini hisoblash va ko‘plikka asoslangan ovoz berish algoritmlari taklif etilgan;

tarmoq himoyalanganligini ta’minlash maqsadida hujumlarni aniqlash tizimining samaradorligini oshirishga imkon beruvchi neyron tarmoqlar arxitekturasini avtomatik tanlash algoritmi tarmoq paketining tanlangan xususiyatlar soniga ko‘ra hisoblash asosida takomillashtirilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

axborot-kommunikatsiya tizimlarida hujumlarni aniqlash usuli, samaradorlikni oshirish va yolg‘ondan tasdiqlash darajasi pasaytirish maqsadida xususiyatlarni tanlashda ovoz berish usuli orqali takomillashtirilgan;

hujumlarni aniqlashda sun’iy neyron tarmoqlar va mashinali o‘qitish usullarining takomillashtirilgan, arxitekturalarini muvozanatlash, xususiyatlarni entropiyaga asoslangan axborot ustuvorligi darajasiga ko‘ra va ko‘plikka

asoslangan ovoz berish orqali tanlash algoritmlaridan foydalanilgan holda hujumlarni aniqlash dasturiy vositasi ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi tizim asosini tashkil etuvchi takomillashtirilgan usul va taklif etilgan algoritmlar yordamida tarmoq hujumlarini real vaqtda aniqlashda tanlangan ma’lumotlar to‘plamini o‘qitishning samaradorligi, ilmiy va tajribaviy-amaliy tadqiqotlarning natijalarin mutasaddi tashkilotlar, jumladan, “UNICON.UZ – Fan-texnika va marketing tadqiqotlari markazi” MCHJ test serverlarida, “O‘zbektelekom” AK Samarqand filiali telekommunikatsiya tarmoqlarida hamda “Kesh-Total Service” MCHJ lokal tarmog‘ida amaliyotga joriy etilganligi bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati axborot-kommunikatsiya tizimlariga uyushtiriladigan hujumlarni aniqlash tizimlarining ishlash usulini takomillashtirish, ushbu tizimlarda sun’iy neyron tarmoqlar va mashinali o‘qitish usullarini qo‘llashning nazariy asoslarini rivojlantirishga ishlab chiqilgan algoritmlarning hissa qo‘shishi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati takomillashtirilgan nazariy asoslar va algoritmlar yordamida ishlab chiqilgan dasturiy vosita, axborot-kommunikatsiya tizimlarida hujumlarni aniqlash samaradorligini oshirish hamda yolg‘ondan tasdiqlash darajasini pasaytirish muammolarini hal etishda qo‘llanilishi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Axborot-kommunikatsiya tizimlarida tarmoq hujumlarini aniqlash usuli va algoritmlarini amalga oshirish bo‘yicha olingan natijalar asosida:

mavjud tarmoq hujumlarini aniqlash tizimlarini tahlillash orqali zaifliklarni aniqlashga asoslangan STRIDE metodologiyasi yordamida ishlab chiqilgan tahdid modeli va yuqori risk darajalarini ko‘rsatgan ehtimoliy tahdidlarni bartaraf etish choralarini mujassamlashtirgan dasturiy vosita “UNICON.UZ – Fan-texnika va marketing tadqiqotlari markazi” MCHJning “Sun’iy intellekt usullarini tadqiq etish va ularni axborot xavfsizligida qo‘llash” mavzusidagi ilmiy loyiha doirasida va “Kesh-Total Service” MCHJ lokal tarmog‘i amalga oshirilgan (“Kesh-Total Service” MCHJ 2025-yil 7-fevraldagi dalolatnomasi; O‘zbekiston Respublikasi Raqamli texnologiyalarni rivojlantirish vazirligining 2025-yil 9-iyundagi 33-8/3918-sonli ma’lumotnomasi). Sinov jarayonida 3500 ta hujum namunalaridan 3426 tasi to‘g‘ri aniqlangan. Erishilgan ilmiy natijalar asosida hujumlarni aniqlash tizimining sun’iy intellekt usullari bilan integratsiyasi mavjud kamchiliklarni bartaraf etish imkonini bergan;

hujumlarini aniqlash tizimlarining mavjud kamchiliklarni, yolg‘ondan tasdiqlash darajasini minimallashtirish va aniqlash samaradorligini oshirish uchun tarmoq paketi xususiyatlarini ovoz berish hamda neyron tarmoqlar arxitekturasini avtomatik tanlash jarayonlarini kiritish orqali takomillashtirilgan qurish usuli asosida ishlab chiqilgan “VIDSA” dasturiy vositasi “O‘zbektelekom” AK Samarqand filiali telekommunikatsiya tarmoqlarida DDoS, portlarni skanerlash va boshqa turdagi hujumlarni aniqlash uchun amaliyotga joriy qilingan (O‘zbekiston Respublikasi Raqamli texnologiyalarni rivojlantirish vazirligining 2025-yil 9-iyundagi 33-8/3918-sonli ma’lumotnomasi). Testlash natijasida axborot-

kommunikatsiya tizimlarida hujumlarni aniqlash samaradorligi 98.5% ni, yolg‘ondan tasdiqlash ko‘rsatgichi 1,5% ni tashkil qildi. Mazkur yondashuv hujumlarni aniqlash tizimlarining samaradorligini oshirish va yolg‘ondan tasdiqlash darajasini kamaytirish imkonini bergan;

tarmoq hujumlarini aniqlash tizimlarini sun’iy intellekt usullari yordamida o‘qitish uchun taklif etilgan tarmoq paketi xususiyatlarini tanlashda ularning entropiyasini hisoblash va ko‘plikka asoslangan ovoz berish algoritmlarini qo‘llagan holda ishlab chiqilgan dasturiy vosita “UNICON.UZ – Fan-texnika va marketing tadqiqotlari markazi” MCHJning “Ishonchli uchinchi tomon xizmatini rivojlantirish va ekspluatatsiya qilish bo‘limi” hamda “Kesh-Total Service” MCHJ lokal tarmog‘iga joriy qilingan (“Kesh-Total Service” MCHJ 2025-yil 7-fevraldagi dalolatnomasi; O‘zbekiston Respublikasi Raqamli texnologiyalarni rivojlantirish vazirligining 2025-yil 9-iyundagi 33-8/3918-sonli ma’lumotnomasi). Bunda o‘qitish uchun sarflanuvchi vaqt 15% gacha kamaytirilgan. Ilmiy tadqiqot natijasida tarmoq paketi xususiyatlarining to‘g‘ri tanlanishi vaqt sarfini kamaytirishi aniqlangan;

tarmoq himoyalanganligini ta’minlash maqsadida hujumlarni aniqlash tizimining samaradorligini oshirishga imkon beruvchi va tarmoq paketining tanlangan xususiyatlar soniga ko‘ra neyron tarmoqlar arxitekturasini avtomatik tanlashning takomillashtirilgan algoritmi “UNICON.UZ – Fan-texnika va marketing tadqiqotlari markazi” MCHJning “Ishonchli uchinchi tomon xizmatini rivojlantirish va ekspluatatsiya qilish bo‘limi”da joriy etilgan (O‘zbekiston Respublikasi Raqamli texnologiyalarni rivojlantirish vazirligining 2025-yil 9-iyundagi 33-8/3918-sonli ma’lumotnomasi). Ushbu jarayonda, 24 soatlik kuzatuv jarayonida tashkil etilgan 3 ta hujum to‘g‘ri aniqlangan. Natijada, real vaqt rejimida hujumlarni aniqlashning yuqori samaradorligi va past yolg‘ondan tasdiqlash ko‘rsatkichiga erishish imkonini bergan.

Tadqiqot natijalarining aprobatsiyasi. Tadqiqotlar natijalari 3 ta xalqaro, 11 ta respublika ilmiy-amaliy konferensiyalar hamda ilmiy seminarlarda muhokama qilingan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 21 ta ilmiy ishlar, ulardan 4 ta maqolalar O‘zbekiston Respublikasi Oliy attestatsiya komissiyasi tomonidan tavsiya etilgan jurnallarda, shu jumladan 1 ta xorijiy va 3 ta respublika jurnallarida nashr etilgan hamda EHM uchun yaratilgan 3 ta dasturiy vositalarga O‘zbekiston Respublikasi Adliya vazirligi tomonidan rasman ro‘yxatdan o‘kazilganlik guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya ishi o‘zbek tilida yozilgan bo‘lib, uning hajmi 112 bet, jumladan, kirish, to‘rtta bob, xulosalar, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat.

DISSERTATSIYA ISHINING ASOSIY MAZMUNI

Kirishda dissertatsiya mavzusining dolzarbligi va zarurati asoslangan, maqsad va vazifalar shakllantirilgan, tadqiqot obyektlari va predmetlari aniqlangan, tadqiqotning O‘zbekiston Respublikasi ilm-fan va texnologiyalarni

rivojlantirishning ustuvor yo‘nalishlariga mosligi aniqlashtirilgan, tadqiqotning ilmiy yangiligi va amaliy natijalari bayon etilgan, olingan natijalarining ishonchliligi asoslangan, olingan natijalarning nazariy va amaliy ahamiyati ochib berilgan, amaliyotga joriy etilgan tadqiqot natijalari, nashr etilgan ishlar va dissertatsiya ishining tuzilmasi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **“Tarmoq hujumlari, tasnifi va ularni aniqlashdagi muammolar”** deb nomlangan birinchi bobida axborot-kommunikatsiya tarmoqlarida amalga oshiriluvchi hujum turlari, ularni aniqlashdagi muammolar, mavjud vositalar hamda usul va algoritmlarining qiyosiy tahlili keltirilgan. Tahlillar natijasida, hujumlarni aniqlash tizimlarida aniqlash usulini sun’iy intellekt usullari yordamida takomillashtirish, yolg‘ondan tasdiqlash ko‘rsatgichini kamaytirish maqsadida paket xususiyatlarini aniq va to‘g‘ri tanlash, sun’iy neyron tarmoqlar arxitekturalarini muvozanatlash zaruriyati ko‘rsatilgan.

Dissertatiya ishining birinchi bobida to‘rtta kategoriya mansub hujumlar ko‘rib chiqilgan bo‘lib, bular: Probe, DoS/DDOS, U2R va R2L kategoriyalari. Ushbu hujumlardan himoyalanishda Firewall, Honeypot, IDS kabi turli vositalar mavjud va ushbu vositalar ichida IDS lar moslashuvchanligi, qulayligi, kam resurs talab qilishi va tarafikni turli usullarda tahlil qila olishi bilan ajralib turadi.

Yolg‘ondan tasdiqlash ko‘rsatgichi – yolg‘ondan tasdiqlangan holatlarning umumiy holatlar soniga nisbati bilan o‘lchanadi. Shu bilan birga u yolg‘ondan aniqlash ehtimolligi deb ham ataladi va quyidagicha aniqlanadi.

$$FAR = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \quad (1)$$

IDS ni takomillashtirishdagi eng muhim jihatlardan biri ma’lumotlardan muhim xususiyatlarni ajratib olish va ularni qayta ishlashga tayyorlashdir. 1 va 2-jadvallarda xususiyatlarni tanlash amalga oshirilmaganda va oshirilganda klassifikatorlarning samaradorlik natijalari keltirilgan.

1-jadval

Xususiyatlarni tanlash amalga oshirilmaganda klassifikatorlar samaradorligi

Klassifika-torlar	Vaqt (sek)	To‘g‘ri klassifikatsiyalangan (%)	Noto‘g‘ri klassifikatsiyalangan (%)	TPR samaradorligi (%)	FPR samaradorligi (%)
NaïveBayes	7.79	85.24	14.61	45.6	13.4
J-48	49.73	89.73	11.33	96.7	0.3
REPTree	21.22	90.07	9.03	89.2	2.5

Klassifikatorlar samaradorligini baholashda xususiyatlarni tanlashning bir qancha usullaridan foydalaniladi. Masalan, CFS + Best First, Info Gain + Ranker va Gain Ratio + Ranker.

2-jadval

Xususiyatlarni tanlash amalga oshirilganda klassifikatorlar samaradorligi

Xususiyat-larni tanlash algoritmi	Klassifikat-siya algoritmi	Vaqt (sek)	To‘g‘ri klassifikatsi-yalangan (%)	Noto‘g‘ri klassifikatsi-yalangan (%)	TPR samarador-ligi (%)	FPR samarador-ligi (%)
CFS + Best First	Naïve Bayes	5.22	93.5	6.95	93.7	13.4
	J-48	17.04	95.56	4.44	95.1	10.5
	REPTree	7.5	96.40	3.60	96.6	12.1
Info Gain + Ranker	Naïve Bayes	2.25	94.15	5.85	97.5	9.7
	J-48	6.47	97.77	2.34	97.0	12.0
	REPTree	4.24	96.12	3.88	96.0	4.6
Gain Ratio + Ranker	Naïve Bayes	3.46	97.99	2.00	97.4	1.1
	J-48	8.46	98.18	1.82	97.4	0.7
	REPTree	6.34	95.78	4.06	95.0	12.6

Yashirin sathlarda juda ko‘p neyronlardan foydalanish ham bir qancha muammolarga sabab bo‘ladi. Yashirin sathdagi neyronlar sonini to‘g‘ri tanlashning bir qancha usullari mavjud. Masalan, yashirin neyronlar soni kiruvchi sath o‘lchami va chiquvchi sath o‘lchami oralig‘ida bo‘lishi, yashirin neyronlar soni kiruvchi sath o‘lchamining 2/3 qismi va chiquvchi sath o‘lchamiga teng bo‘lishi yoki yashirin neyronlar soni kiruvchi sath o‘lchami ikkilanganidan kichik bo‘lishi kerak.

Birinchi usul bo‘yicha tarmoq konfiguratsiyasi l-m-n bo‘ladi (l - kirish, m - yashirin va n - chiqish neyronlari). 3 va 4-jadvallarda $l = 17$, $m = 17$, $n = 1$ va $l = 17$, $m_1 = 8$, $m_2 = 8$, $n = 1$ arxitekturalarning natijalari keltirilgan.

3-jadval

Yashirin sath=1 va yashirin neyronlar=17

Baholash mezonlari	O‘qitish	Tasdiqlash
To‘g‘ri klassifikatsiyalash darajasi (CCR, %)	100	-
Tarmoq xatoligi (%)	0.0298	0
Iteratsiyalar (ta)	501	
O‘qitish tezligi (ta/sek)	47.264	
Neyron tarmoq arxitekturasi	[17-17-1]	

Ikkinchi arxitekturada bitta kirish, ikkita yashirin va bitta chiqish sathlari mavjud bo‘lib, neyronlar soni mos ravishda 17, 8, 8 va 1 holatida kiritiladi.

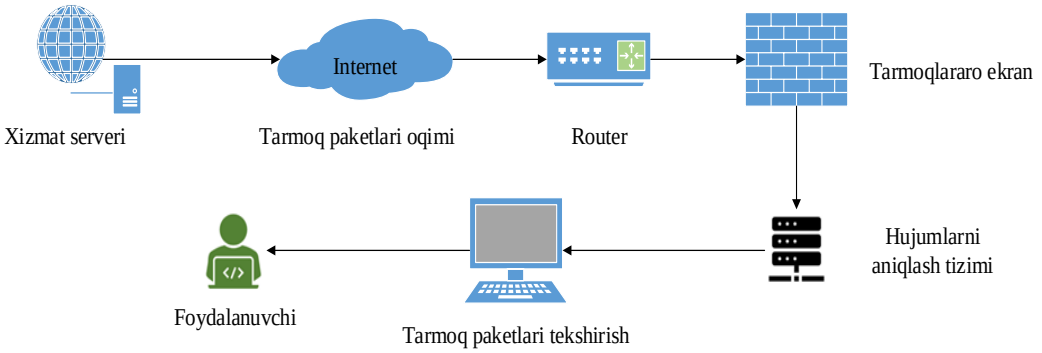
4-jadval

Yashirin sath=2 va yashirin neyronlar =8 tadan

Baholash mezonlari	O‘qitish	Tasdiqlash
To‘g‘ri klassifikatsiyalash darajasi (CCR, %)	100	-
Tarmoq xatoligi (%)	0.0298	0
Iteratsiyalar (ta)	501	
O‘qitish tezligi (ta/sek)	52.187	
Neyron tarmoq arxitekturasi	[17-8-8-1]	

Yuqoridagi jadvallardan ko‘rish mumkinki 17-17-1 arxitektura va 17-8-8-1 arxitektura bir xil xatolik bersa ham o‘qitish tezligiga nisbatan ikkinchi arxitektura ustunlik qiladi.

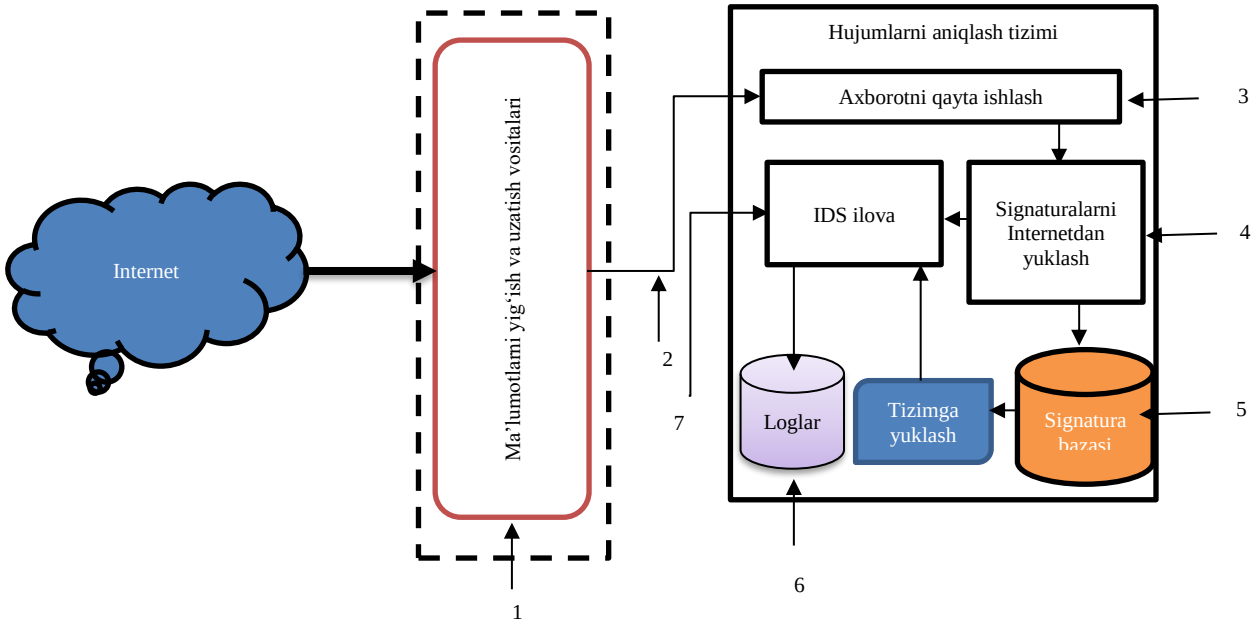
Kiber tahdidlarning eksponensial o‘sishi bilan tashkilotlar real vaqt rejimida xavfsizlik buzilishlarini aniqlash, tahlil qilish va oldini olish uchun hujumlarni aniqlash tizimlari tizimlariga tayanmoqda.



1-rasm. Hujumlarni aniqlash tizimlari bilan tarmoq arxitekturasi

Dissertatsiyaning **“Hujumlarni aniqlash tizimlarining tahdid modeli”** deb nomlangan ikkinchi bobida hujumlarni aniqlash tizimlari uchun tahdid modeli ishlab chiqilgan hamda ularni zamonaviy tendensiyalarga mos qilib qurishda yuqori samaradorlikka erishuvchi sun’iy neyron tizimlardan foydalanish va xususiyatlarni tashlash kabi bajarilishi kerak bo‘lgan vazifalar keltirib o‘tilgan. Shuningdek, hujumlarni aniqlash tizimlarida sun’iy neyron tarmoqlarining qo‘llanilish va xususiyatlar hamda ularni tanlash usullari ham yoritilgan.

Ma’lumotlar va ularni saqlaydigan tizimlar xavfsizligi uchun himoyani ta’minlashda hujumlarni aniqlash tizimi asosiy vositalardan biri hisoblanadi. Lekin mavjud IDS tizimlari uchun tahdid modelini qurish undagi mavjud kamchiliklarni aniqlash va takomillashtirish imkonini beradi. Quyidagi 2-rasmda hujumlarni aniqlashning mavjud tizimlari uchun ishlab chiqilgan tahdid modelini ko‘rish mumkin.

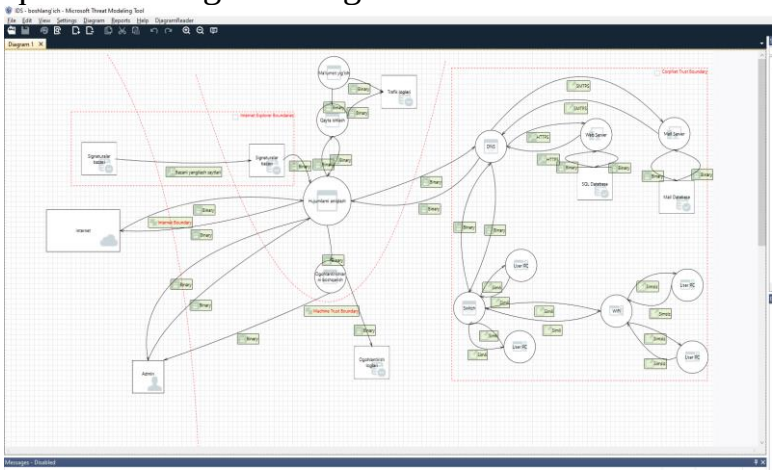


2-rasm. Hujumlarni aniqlash tizimi tahdid modeli

Ushbu tahdid modeliga asosan tizim arxitekturasida bir qancha tahdidlar mavjud bo‘lib, ular quyidagicha:

1. Ma’lumotlarni yig‘ish va uzatish vositalariga nisbatan yolg‘on obyekt kiritish yoki ulardagi ma’lumotlarni qalbakilashtirish imkoniyati;
2. Yig‘ilgan ma’lumotlarni aloqa kanali orqali hujumlarni aniqlash tizimiga uzatish jarayonida ushlab qolinishi, o‘zgartirilishi yoki yo‘q qilinishi mumkinligi;
3. Axborotni qayta ishlash jarayonida o‘zgartirilgan yoki qalbakilashtirilgan ma’lumotlar xususiyatlarini aniqlash va ularni baholash;
4. Hujum signaturalarini internet tarmog‘idan yuklash;
5. Signaturalar bazasining ichki yoki tarmoqqa ulangan tashqi hujumchi tomonidan o‘zgartirib qo‘yilishi;
6. Ilova tomonidan aniqlangan va log fayllarga yozilgan hujum yoki hujumchi haqidagi ma’lumotlarni o‘zgartirilishi yoki yo‘q qilinishi;
7. Ilovani ishdan chiqarish, ma’mur huquqlarini olish, natijalarni kechiktirish yoki o‘zgartirish maqsadida ilovaga hujum uyushtirish.

Ishlab chiqilgan tahdid modeli Microsoft Threat Modelling Tools yordamida amalga oshirildi va mavjud hujumlarni aniqlash tizimlaridagi bir qancha zaiflik va kamchiliklar aniqlandi. Amalga oshirilgan tahdid modeli 3-rasmda keltirilgan.

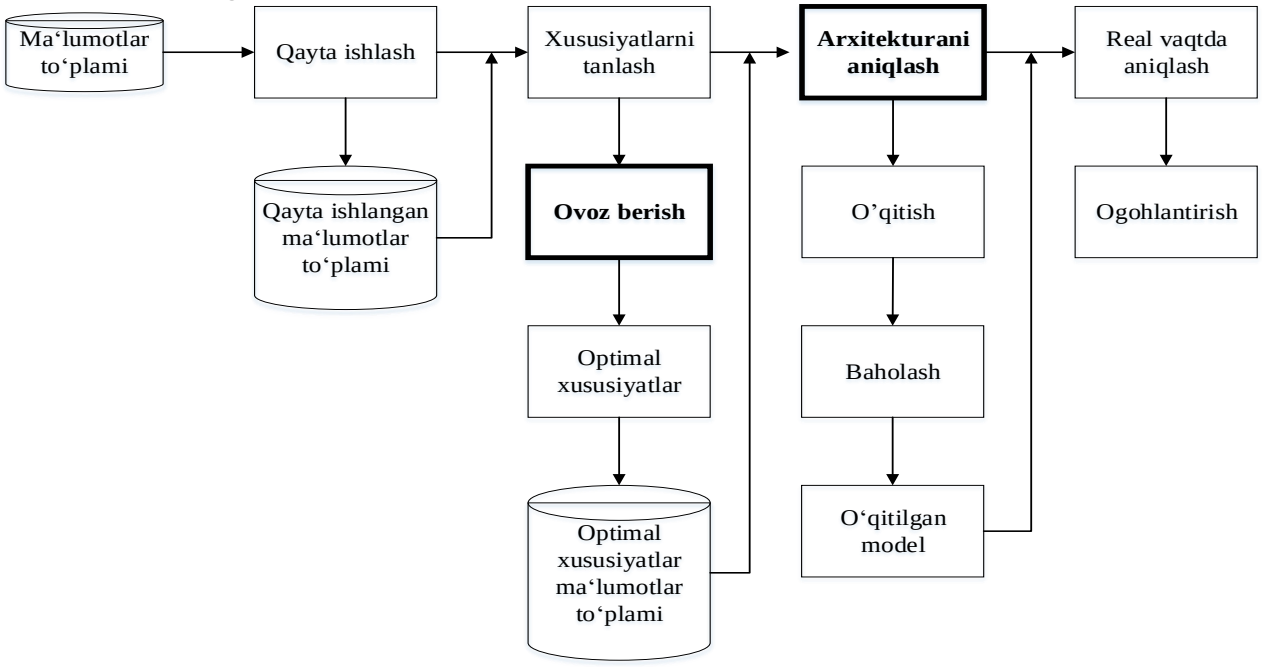


3-rasm. Microsoft Threat Modelling Tools yordamida amalga oshirilgan tahdid modeli

Tahlil natijalari axborot-kommunikatsiya tizimlarida mavjud tahdidlarni yaqqol namoyon bo‘lishini ko‘rsatadi. Ularni hal etish maqsadida sun’iy intellektli usullardan foydalanish maqsadga muvofiq hisoblanadi. Yuqoridagi tahlil natijalaridan kelib chiqgan holda:

1. Axborotni qayta ishlash jarayonida o‘zgartirilgan yoki qalbakilashtirilgan ma’lumotlar xususiyatlarini aniqlash va ularni baholashni oldini olish zarur. Buning uchun, ishonchli xususiyatlar to‘plamini avtomatlashtirilgan holda aniqlash va faqat tizim yoki ilovaning o‘ziga ruxsat berilishi;
2. Hujum signaturalarini internet tarmog‘idan yuklashda ishonchliligi xavfi borligi sababli hujumlarni aniqlash tizimlarini mashinali o‘qitish va sun’iy intellekt usullari orqali tarmoq trafigi anomaliyalarini aniqlash uchun sozlash va ulardan foydalanish;
3. Tarmoq trafigi anomaliyalarini aniqlashda mavjud tizimlardagi yuqori yolg‘ondan tasdiqlash ko‘rsatgichini kamaytirish lozim.

Dissertatsiyaning **“Axborot-kommunikatsiya tizimlarida hujumlarni aniqlashning samarali usul va algoritmlari”** deb nomlangan uchinchi bobida axborot-kommunikatsiya tizimlarida hujumlarni aniqlash tizimlarini qurishning sun’iy neyron tarmoqlari asosida takomillashtirish haqida so‘z yuritiladi (4-5-rasmlar). Hujumlarni aniqlash tizimlarida xususiyatlar sonini belgilash (6-7-rasmlar) hamda yashirin qatlamlar va neyronlarni tanlash algoritmlari ham shu bobdan o‘rin olgan.



4-rasm. Hujumlarni aniqlash tizimlarini qurishning takomillashtirilgan usulining ishlash prinsipi

Ushbu usulning mavjudlaridan farqlari quyidagilardan iborat:

1. Usul yolg‘ondan tasdiqlash ko‘rsatgichini kamaytirish talablariga mos holatda samaradorlikni oshirish uchun mos keladi.

2. Ma’lumotlar to‘plami qayta ishlanganidan so‘ng optimal xususiyatlar to‘plamini aniqlash maqsadida ajratilgan o‘qitish ma’lumotlar to‘plamidan Ovoz berish usuli yordamida aniqlab olinadi.

3. Optimal xususiyatlar sonidan kelib chiqqan holda sun’iy intellekt usullari uchun arxitektura shakllantiriladi, ya’ni yashirin qatlamlar va neyronlar soni aniqlanadi.

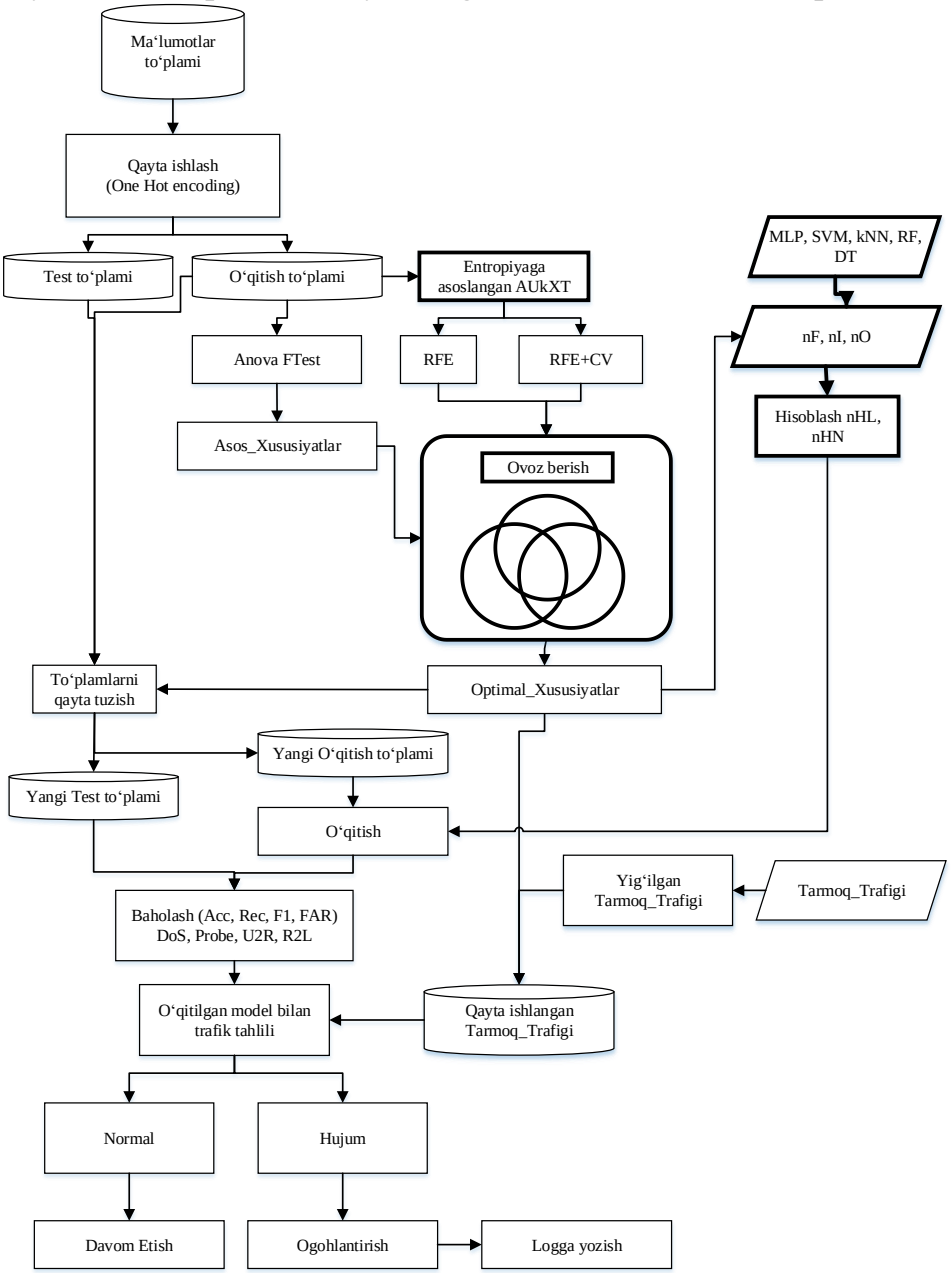
4. Axborot-kommunikatsiya tizimlarida hujumlarni aniqlash uchun model ansambl usulidan foydalanadi. Bu bir vaqtning o‘zida MLP, SVM, DT va RF usullaridan foydalanish imkonini beradi.

5. O‘qitilgan modelni saqlash, uzatish va qayta yuklash imkoniyatini beradi.

Taklif qilingan modelning ishlash usuli 5-rasmda keltirilgan va ishlash algoritmi yoritilgan.

Tarmoq hujumini aniqlash zararli harakatlar bilan bog‘liq murakkab namunalarni samarali qo‘lga kiritadigan xususiyatlarni sinchkovlik bilan tanlash va chiqarishga asoslanadi. Ushbu xususiyatlar normal tarmoq xatti-harakatlarini

potensial zararli anomaliyalardan ajratish uchun mashinani o‘rganish modellari, xususan, neyron tarmoqlar uchun yaratilgan asos bo‘lib xizmat qiladi.



5-rasm. Taklif qilinayotgan usul arxitekturasi

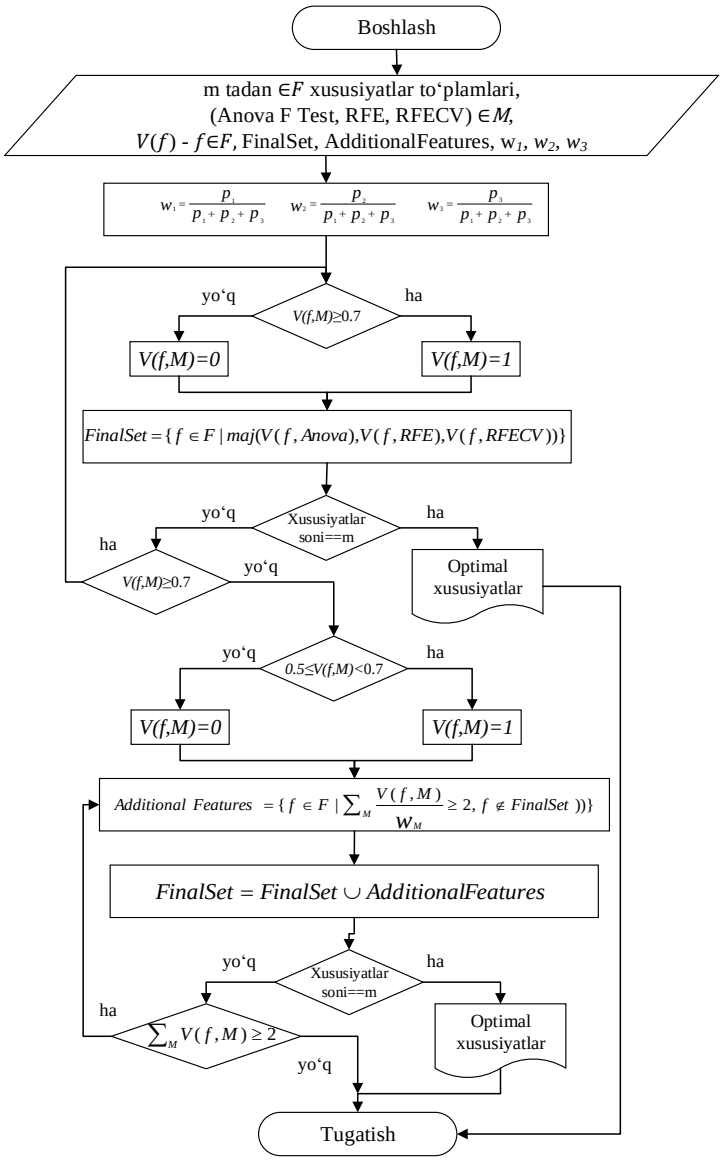
Xususiyatlarni tanlashda ovoz berish algoritmi

Har bir xususiyatni tanlash usuliga uning unumdorligiga ko‘ra w_1, w_2, w_3 vazn berilgan. Ovoz berish jarayoni uchun “majority” funksiyasidan foydalaniladi:

$$\mathrm{maj}(x, y, z) = (x \vee y) \oplus (x \vee z) \oplus (y \vee z) \quad (2)$$

Xususiyatlarni tanlashda ishlab chiqilgan ovoz berish algoritmi blok sxemasi 6-rasmda keltirilgan.

Arxitekturaning yashirin qatlamlari va neyronlari tarmoqning ma’lumotlar ichidagi murakkab munosabatlarni o‘rganish qobiliyatini belgilaydi. Neyron tarmoq arxitekturasini optimallashtirish hujumlarni aniqlash imkoniyatlarini oshirishda hal qiluvchi rol o‘ynaydi. To‘g‘ri sonli xususiyatlarni, yashirin qatlamlarni va yashirin neyronlarni tanlash orqali tarmoq yuqori aniqlik va samaradorlik bilan hujumlarni samarali aniqlashi va tasniflashi mumkin.



6-rasm. Ovoz berish jarayoni algoritmi blok-sxemasi

Neyron tarmog‘ining arxitekturasini optimallashtirish murakkablik va umumlashtirish o‘rtasidagi to‘g‘ri muvozanatni topishni o‘z ichiga oladi.

$$OH5 = \frac{\mathrm{SF} * (\mathrm{NI} + \mathrm{NO}) * \mathrm{Log10}(\mathrm{NI} + \mathrm{NO})}{2} \quad (3)$$

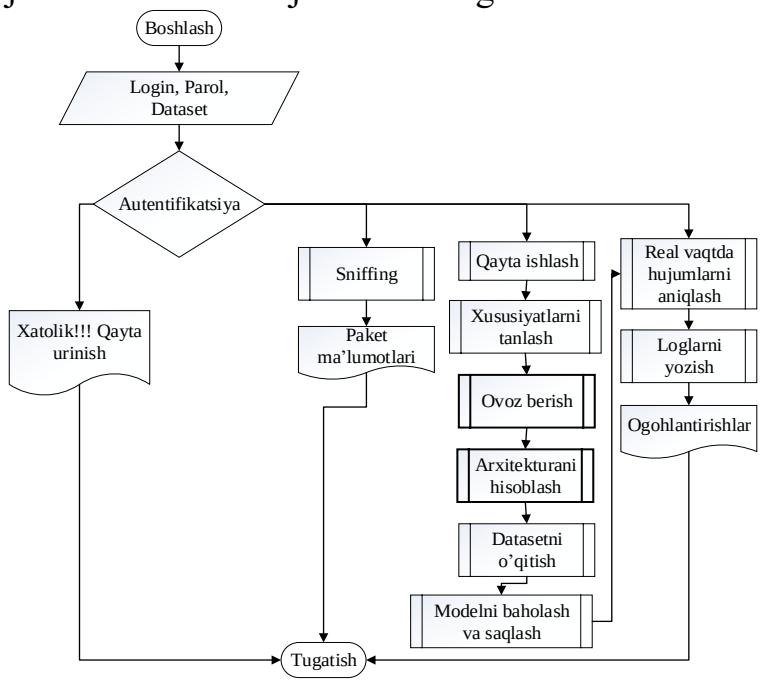
5-jadval

Yashirin neyronlar soni va qatlamlar sonini hisoblash natijalari

Hisoblash formulasi	Bitta yashirin qatlam	Ikkita yashirin qatlam	Uchta yashirin qatlam
OH1 = (NI+ NO)* (1-(1/(NI+NO)))	15	-	-
OH2 = 2/3*(NI+NO)	11	-	-
OH3 = SF*(NI+ NO)^Exp	16	32	768
OH4 = (NI+ NO)*log10(NI+NO)/2	10	-	-
OH5 = SF*(NI+ NO)*log10(NI+NO)/2	10	19	29
OH6 = SF*(NI+ NO)^ Exp*log10(NI+NO)/2	10	19	462
OH7 = SF*(NI+ NO)^Exp*log10(NI+NO)^Exp/2	10	19	558

Yuqoridagi jadval natijalari shuni ko‘rsatadiki, keltirilgan OH5 formula orqali neyron qatlamlarining soni ortishi bilan hisoblagan yashirin neyronlar soni orasida mutanosiblikni saqlaydi.

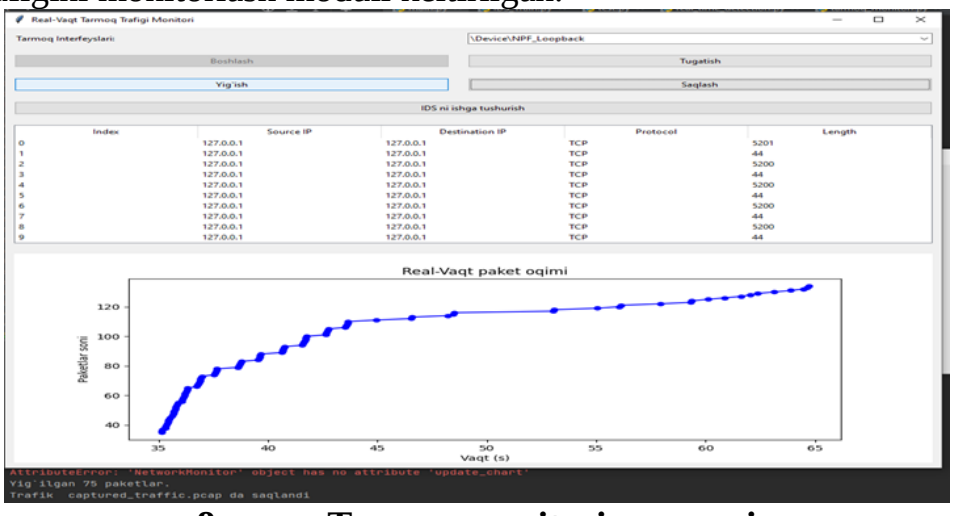
Dissertatsiyaning **“Hujumlarni aniqlashning takomillashtirilgan usulining dasturiy vositasi va tajriba hisoblash natijalari”** deb nomlangan to‘rtinchi bobida yuqoridagi boblarda taklif etilgan takomillashtirilgan usul va algoritmlar asosida ishlab chiqilgan dasturiy vosita, uning modullari hamda ishlash prinsipi keltirilgan. Shu bilan birga, amaliy masalalarni yechishda dasturiy vositani qo‘llash va tajriba hisoblash natijalari keltirilgan.



7-rasm. Dasturiy vositaning ishlash algoritmi

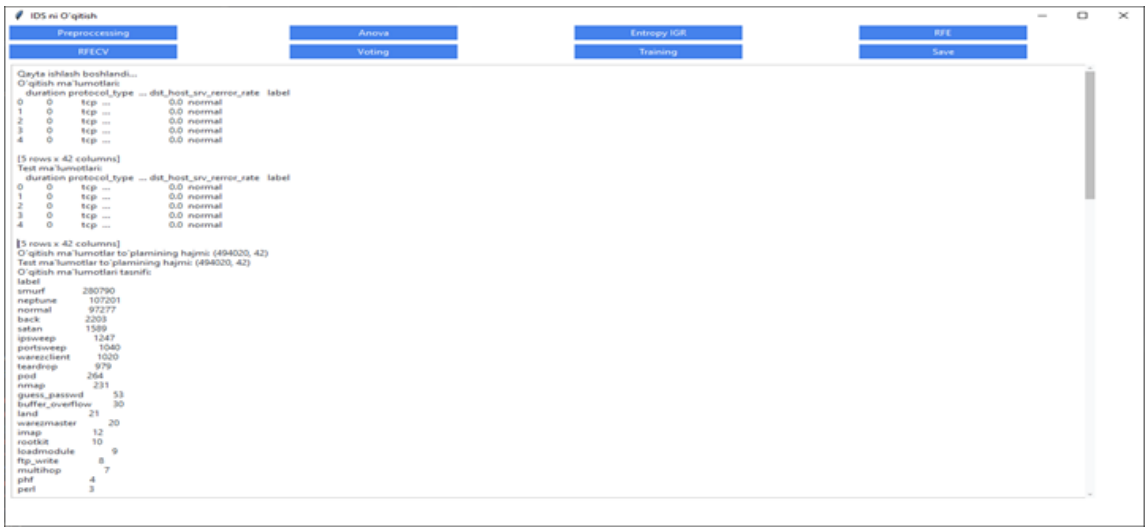
Mashinali o‘qitish va sun’iy neyron tarmoq usullarini o‘qitish va baholash maqsadida KDD-CUP va NSL-KDD datasetlaridan foydalanilgan.

Dissertatsiya ishida keltirilgan usul va algoritmlar asosida ishlab chiqilgan dasturiy vosita modullarga bo‘lingan holda ishlaydi. 8-rasmda real vaqt rejimida tarmoq trafigini monitorlash moduli keltirilgan.



8-rasm. Tarmoq monitoring oynasi

Quyidagi 9-rasmda datasetdagi ma’lumotlarni ishlash, xususiyatlarni tanlash, o‘qitish, baholash hamda modellarni saqlash oynasi ko‘rsatilgan.



9-rasm. O‘qitish jarayoni

10-rasmda saqlangan modelni yuklagan holda axborot-kommunikatsiya tizimiga real vaqt rejimida kiruvchi trafikni tahlil qilgan holda hujumlarni aniqlash jarayoni keltirilgan.

10-rasm. Real vaqt rejimida hujumlarni aniqlash jarayoni

6-7-jadvallarda yolg‘ondan tasdiqlash ko‘rsatgichining tajribaviy natijalari keltirilgan.

6-jadval

Bitta yashirin qatlam uchun yolg‘ondan tasdiqlash ko‘rsatgichi natijalari

Dataset	Hujum turi	MLP (%)	SVM (%)	DT (%)	RF (%)
KDD_CUP	DoS	1.10	1.27	1.00	1.03
	Probe	1.06	2.03	2.00	1.00
	R2L	1.30	2.07	2.01	2.02
	U2R	1.00	1.00	1.20	1.30
NSL_KDD	DoS	1.78	1.13	2.03	2.08
	Probe	1.34	2.27	2.10	2.02
	R2L	1.05	2.00	2.00	3.00
	U2R	1.00	2.30	2.30	2.50

Yuqoridagi jadvalda keltirilgan natijalarning ikkinchi yashirin qatlam ishga tushirilgandan so‘ng o‘zgarish holati quyida ko‘rsatilgan.

7-jadval

Ikkinchi yashirin qatlam ishga tushirilgandan keyin yolg‘ondan tasdiqlash ko‘rsatgichi natijalari

Dataset	Hujum turi	MLP (%)	SVM (%)	DT (%)	RF (%)
KDD_CUP	DoS	1.00	1.05	1.00	1.00
	Probe	1.05	1.04	2.00	2.10
	R2L	1.13	2.07	2.01	2.02
	U2R	1.00	1.80	2.40	2.50
NSL_KDD	DoS	1.20	1.25	2.20	2.09
	Probe	1.26	2.30	2.20	2.30
	R2L	1.06	2.00	2.40	2.50
	U2R	1.01	2.10	2.40	2.60

6 va 7-jadvallarda yashirin qatlamlar soni ko‘payganda, yolg‘ondan tasdiqlash ko‘rsatgichi biroz pasayganini ko‘rish mumkin. Eng past yolg‘ondan tasdiqlash ko‘rsatgichi 2 ta yashirin qatlam uchun olingan.

O‘qitilgan model ishlash samaradorligini ifodalovchi baholash me’zonlaridan yana bir bu F1 baho hisoblanadi. F1 baho aniqlik va to‘g‘rilik orasidagi mutanosiblikni ko‘rsatadi.

$$\mathrm{F1} = \frac{2 * \text{aniqlik} * \text{to‘g‘rilik}}{\text{aniqlik} + \text{to‘g‘rilik}} \qquad (4)$$

8-jadvalda F1 bahoni hisoblash natijalari keltirilgan.

8-jadval

Kdd-Cup va NSL-Kdd datasetlarini o‘qitish va baholash natijasida F1 baho

Datasetlar		KDD-CUP		NSL-KDD	
Hujum turi	O‘qitish usuli	Bitta yashirin qatlam uchun (%)	Ikkinchi yashirin qatlamni ishga tushurilgandan so‘ng (%)	Bitta yashirin qatlam uchun (%)	Ikkinchi yashirin qatlamni ishga tushurilgandan so‘ng (%)
DOS	MLP	99.42	99.80	98.29	99.26
	SVM	99.02	99.17	98.82	98.86
	DT	99.96	99.99	99.70	99.72
	RF	99.96	99.99	99.70	99.72
Probe	MLP	99.27	99.27	98.50	98.82
	SVM	99.37	99.22	98.80	98.58
	DT	99.91	99.89	99.93	99.87
	RF	99.91	99.89	99.93	99.87
R2L	MLP	93.27	93.45	91.85	92.25
	SVM	93.50	93.50	90.82	90.82
	DT	98.97	98.97	99.07	99.07
	RF	98.98	98.99	99.07	99.07
U2R	MLP	64.05	53.62	79.26	78.74
	SVM	65.61	51.87	81.24	81.24
	DT	94.00	93.00	93.47	93.47
	RF	94.00	93.00	93.47	93.61

Yuqoridagi jadvalda Kdd-Cup va NSL-Kdd datasetlarini turli usullar hamda turli neyron arxitekturali asosida o‘qitish va baholash natijalari keltirilgan. Ushbu jadval natijalari har ikki ma’lumotlar to‘plamida ham aniqlik va to‘g‘rilik orasidagi mutanosiblik yuqori darajada ekanligini ko‘rsatadi.

XULOSA

“Axborot-kommunikatsiya tizimlarida tarmoq hujumlarini aniqlash usuli va algortmlari” mavzusidagi dissertatsiya ishi bo‘yicha olib borilgan tadqiqotlar natijasida quyidagi xulosalar taqdim etildi:

1. Hujumlarni aniqlash tizimlaridagi mavjud kamchiliklar qator omillar asosida tahlil qilinishi natijasida ularnining aniqlash samaradorligini oshirish, yolg‘ondan tasdiqlash ko‘rsatgichini kamaytirishning dolzarbligi ko‘rsatildi. Bu, signaturali aniqlash usullarini sun’iy intellektli usullarga almashtirish orqali hujumlarni aniqlashning takomillashtirilgan tizimini ishlab chiqish lozimligini ko‘rsatdi.
2. Mavjud hujumlarni aniqlash usul va vositalarining qiyosiy tahlil natijalaridan kelib chiqgan holda ushbu tizimlar uchun tahdid modeli taklif qilindi. Bu o‘qitiluvchi xususiyatlar to‘plamini aniq tanlash va ularning arxitekturalarini muvozanatlashni avtomatlashtirish hamda yuqori samaradorlikni ta’minlash maqsadida mashinali o‘qitish va neyron tarmoq usullarini ansambllashgan holda qo‘llash lozimligini ko‘rsatdi.
3. Hujumlarni aniqlash tizimlarining ishlash usuli, ovoz berish hamda mashinali o‘qitish va neyron tarmoqlarning arxitekturalarini avtomatik hisoblash orqali takomillashtirildi. Ushbu usul yordamida ishlab chiqilgan hujumlarni aniqlash tizimining mavjudlaridan afzalliklari va samaradorligi jihatdan ustun ekanligi ko‘rsatildi.
4. Mashinali o‘qitish usullaridan foydalanishda tarmoq paketi xususiyatlarini tanlashning entropiyaga va ko‘plikka asoslangan ovoz berish funksiyasi orqali tanlash algoritmi ishlab chiqildi. Tajribalar natijasida tarmoq hujumlarini aniqlashda, tanlanuvchi xususiyatlar sonini belgilash orqali, yolg‘ondan tasdiqlash ko‘rsatgichini 2.1% gacha kamaytirishga erishildi.
5. Mashinali o‘qitish va neyron tarmoq usullarini ansambllashgan holda o‘qitish jarayonida qo‘llash uchun ularning arxitekturalarini muvozanatlash algoritmi ishlab chiqildi. Ilmiy tadqiqot natijasida hujumlarni aniqlash tizimini o‘qitish vaqtini 15% gacha qisqartirish imkoniyati yaratildi.
6. Ishlab chiqilgan algoritmlarni modul sifatida foydalanishni ko‘zda tutgan holda, hujumlarni aniqlash tizimining dasturiy vositasi yaratildi. Ishlab chiqilgan dasturiy vosita tegishli soha korxonalarining tarmoqlarida hujumlarni aniqlash jarayonida qo‘llanilib, o‘rtacha 98% aniqlikga va 2% ga yaqin yolg‘ondan tasdiqlash ko‘rsatgichiga erishildi.

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

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

БОЗОРОВ СУҲРОБЖОН МУМИН УГЛИ

МЕТОДЫ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

05.01.05-Методы и системы защиты информации. Информационная безопасность

АВТОРЕФЕРАТ
ДИССЕРТАЦИИ ДОКТОРА ФИЛОСОФИИ (PHD) ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент – 2025

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан под номером B2025.1.PhD/T5294.

Диссертация выполнена в Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб странице (www.tuit.uz) и на Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

Научный руководитель:	**Гуломов Шерзод Раджабоевич** Доктор технических наук, доцент
Официальные оппоненты:	**Керимов Комил Фикратович** Доктор технических наук, профессор
	Кадиров Мирхусан Мирпўлатович Доктор философии по техническим наукам (PhD), доцент
Ведущая организация:	**ООО «UNICON.UZ» - Центр научно-технических и маркетинговых исследований.**

Защита диссертации состоится «_18_». _октября_ . в _11:30_ часов на заседании научного совета DSc.13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (+99871) 238-64-15; e-mail: info@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий (регистрационный номер №_368_). (Адрес: 100084, г. Ташкент, ул. Амира Темура, 108. Тел.: (+99871) 238-64-15).

Автореферат диссертации разослан «_08_» _октября_ 2025 года.
(протокол рассылки №__ от _____ 2025г.).

Б.Ш.Махамов
Председатель научного совета по присуждению ученых степеней, доктор экономических наук, профессор

М.С.Саиткамолов
Ученый секретарь научного совета по присуждению ученых степеней, доктор экономических наук, доцент

Д.Я.Иргашева
Председатель научного семинара при научном совете по присуждению ученых степеней, доктор технических наук, профессор

Введение (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В последние годы на глобальном уровне одной из приоритетных задач считается повышение точности и эффективности систем обнаружения атак (Intrusion Detection System – IDS) и их предотвращения (Intrusion Prevention System – IPS), а также устранение существующих уязвимостей с целью снижения или полного предотвращения финансового, технического и информационно-безопасностного ущерба, возникающего в информационно-коммуникационных системах. В ноябре 2024 года было зафиксировано более 10 500 различных атак на информационно-коммуникационные системы нашей республики. В частности, по данным лаборатории «Касперского», в декабре 2024 года Узбекистан занял 46-е место среди стран, на которые совершено наибольшее количество кибератак. Это, в свою очередь, требует совершенствования систем обнаружения атак, в частности методов и алгоритмов, обеспечивающих эффективное выявление как существующих, так и новых угроз, с целью повышения уровня безопасности информационно-коммуникационных систем. В развитых странах, таких как государства Европы, США, Китай, Российская Федерация, Япония и Республика Корея, научно-исследовательские работы по совершенствованию систем обнаружения атак с применением методов искусственного интеллекта, разработке новых методов и алгоритмов, а также их внедрению в реальные системы ведутся активно как в теоретическом, так и в практическом аспектах.

По мировому опыту, в настоящее время в результате проводимых научных исследований в области разработки средств защиты от кибератак ведутся работы по выявлению аномалий в сетевых пакетах в реальном времени, а также по совершенствованию методов и алгоритмов построения систем обнаружения атак с использованием интеллектуальных технологий. В данной сфере, в частности, одной из основных задач является отказ от методов обнаружения, основанных на сигнатурах, и разработка методов выявления атак посредством анализа пакетов с применением методов искусственного интеллекта. При этом в нашей стране также уделяется особое внимание повышению эффективности систем обнаружения атак и снижению показателей ложных срабатываний (False Alarm Rate — FAR) за счёт правильного применения методов искусственного интеллекта в процессе защиты информации, передаваемой и хранящейся в информационно-коммуникационных системах.

В информационно-коммуникационных системах государственных и хозяйственных органов управления нашей республики реализуются масштабные меры, направленные на совершенствование используемых механизмов защиты информации. В Указе Президента Республики Узбекистан № 158 от 11 сентября 2023 года «О стратегии “Узбекистан – 2030”» определены задачи: «…создание необходимых условий для беспрепятственного доступа к сети Интернет, обеспечение кибербезопасности в национальном интернет-пространстве, а также

повышение уровня грамотности граждан в вопросах использования Интернета». Кроме того, в Стратегии развития «Новый Узбекистан» на 2022–2026 годы установлены задачи по «…определению основных направлений обеспечения кибербезопасности интернет-пространства в доменной зоне “UZ”, а также комплексных мер по защите систем электронного правительства, энергетики, цифровой экономики и других сфер, относящихся к критически важной информационной инфраструктуре…». В выполнении этих задач особое значение имеет разработка усовершенствованных средств обнаружения атак в информационно-коммуникационных системах с применением методов искусственного интеллекта, позволяющих снизить затраты ресурсов и повысить эффективность защиты.

Данное исследование в определенной степени служит выполнению задач, предусмотренных в Законе Республики Узбекистан № ЗРУ-764 от 15 апреля 2022 года «О кибербезопасности»; Указом Президента Республики Узбекистан № УП-60 от 28 января 2022 года «О Стратегии развития “Новый Узбекистан” на 2022–2026 годы»; Указом Президента № УП-6079 от 5 октября 2020 года «Об утверждении Стратегии “Цифровой Узбекистан — 2030” и мерах по её эффективной реализации»; Постановлением Президента № ПП-167 от 31 мая 2023 года «О дополнительных мерах по совершенствованию системы кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» и Постановлением Президента № ПП-4452 от 14 сентября 2019 года «О дополнительных мерах по контролю внедрения, а также совершенствованию системы защиты информационных технологий и коммуникаций».

Соответствие исследования с приоритетными направлениями развития науки и технологий республики. Данное исследование выполнено в соответствии с приоритетными направлениями развития науки и технологий республики IV. «Информатизация и развитие инфокоммуникационных технологий».

Степень изученности проблемы. О применении нейронных сетей на основе аномалий, глубокого обучения и других методов, а также алгоритмов, направленных на построение систем обнаружения атак, с целью обеспечения информационной безопасности, проводятся научные исследования F.Almasoudya, R.Gautam, M.Darkaie, M.Guan, А.Крибеля, И.Алексеева, J.Faysal, R.Gupta и других зарубежных учёных. Чтобы проиллюстрировать важность архитектур искусственных нейронных сетей в системах обнаружения атак, зарубежные ученые, такие как, J.Doe, L.Gonzalez, В.Кузьмин, P.Thomas, A.Dridi, J.Klein проводят ряд исследований. Кроме того, организациями Bro Zeek, RiskWatch, Kaspersky Lab и Trend Micro ведутся научно-исследовательские работы по разработке программно-аппаратных средств с применением интеллектуальных систем защиты информации в информационно-коммуникационных системах.

В Узбекистане научными коллективами под руководством С.К.Ганиева, М.М.Каримова, К.А.Ташева, С.Р.Гуломова, Н.Б.Насруллаева, Ф.Б.Ботирова проводились научные исследования по интеллектуальным системам защиты

информации, пакетной фильтрации, рискам информационной безопасности, методам и алгоритмам обнаружения атак.

В то же время методы и алгоритмы построения систем обнаружения атак в информационно-коммуникационных системах на основе методов машинного обучения, такие как повышение эффективности обнаружения и снижение числа ложных срабатываний, изучены недостаточно.

Связь диссертационного исследования с планами научно исследовательских работ высшего исследовательского учреждения, где выполнена диссертация. Диссертационная работа выполнена в рамках проекта 598661-EPP-12018-1-RO-EPPKA2-CBHE-JP по теме «Развитие услуг для лиц с ограниченными возможностями – DECIDE» (2019-2022 гг.) Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий.

Целью исследования является разработка эффективных методов и алгоритмов обнаружения сетевых атак на информационные и коммуникационные системы.

Задачи исследования:

разработка общей модели угрозы путём анализа существующих систем обнаружения атак в информационно-коммуникационных системах;

улучшение метода создания систем обнаружения сетевых атак с целью снижения уровня ложных срабатываний и обеспечения высокой эффективности обнаружения;

разработка алгоритмов выбора признаков сетевых пакетов для обучения при обнаружении сетевых атак в информационно-коммуникационных системах;

изучение влияния скрытого слоя и нейронов на работу системы обнаружения сетевых атак при использовании искусственных нейронных сетей и повышение эффективности обнаружения за счёт обеспечения их баланса.

Объектом исследования являются атаки, направленные на потоки данных, передаваемые по сети в информационно-коммуникационных системах.

Предметом исследования являются эффективные методы и алгоритмы обнаружения атак в информационно-коммуникационных сетях.

Методы исследования. В ходе исследования были использованы методы защиты информации, нейронные сети, теория информации, дискретная математика и объектно-ориентированное программирование, а также методы, основанные на результатах экспериментальных исследований.

Научная новизна исследования:

На основе анализа существующих систем обнаружения сетевых атак с использованием методологии STRIDE разработана модель угроз, а уровни риска потенциальных опасностей оценены по модели DREAD.

Метод построения систем обнаружения атак усовершенствован путём внедрения процедур выбора признаков сетевых пакетов на основе голосования и автоматического выбора архитектуры нейронных сетей, что

позволяет минимизировать показатель ложных срабатываний и повысить эффективность обнаружения.

Для обучения систем обнаружения сетевых атак с применением методов искусственного интеллекта предложены алгоритмы выбора признаков сетевых пакетов с использованием расчёта их энтропии и голосования на основе множественности.

С целью обеспечения защищённости сети усовершенствован алгоритм автоматического выбора архитектуры нейронных сетей, который рассчитывается в зависимости от числа выбранных признаков сетевого пакета и способствует повышению эффективности систем обнаружения атак.

Практические результаты исследования:

метод обнаружения атак в информационных и коммуникационных системах, улучшенный с применением метода голосования при выборе признаков с целью повышения эффективности и снижения уровня ложных срабатываний;

при обнаружении атак было разработано программное средство обнаружения атак с использованием усовершенствованных искусственных нейронных сетей и методов машинного обучения, обеспечивающих баланс архитектуры, определяющих признаков в соответствии с уровнем приоритета информации на основе энтропии, и алгоритмов выбора путём голосования на основе множественности.

Достоверность результатов исследования. Достоверность результатов исследования заключается в эффективности обучения выбранного набора данных по обнаружению сетевых атак в реальном времени с использованием усовершенствованного метода и предложенных алгоритмов, составляющих основу системы, а также в том, что результаты научных и экспериментальных исследований могут быть воспроизведены ответственными организациями, в том числе на тестовых серверах ООО «UNICON.UZ - Центр научно-технических и маркетинговых исследований», Самаркандский филиал АО «Узбектелеком» а также внедрены в практику телекоммуникационных сетей и в локальной сети ООО «Kesh-Total Service».

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования объясняется с совершенствованием способов работы систем обнаружения организованных атак на информационно-коммуникационные системы, а также во вкладе разработанных алгоритмов в развитие теоретических основ применения искусственных нейронных сетей и методов машинного обучения в этих системах.

Практическая значимость результатов исследования объясняется тем, что разработанные программные средства, основанные на усовершенствованных теоретических основах и алгоритмах, используются для решения задач повышения эффективности обнаружения атак в информационно-коммуникационных системах и снижения уровня ложных срабатываний.

Внедрение результатов исследования. На основе полученных результатов по реализации методов и алгоритмов обнаружения сетевых атак в информационно-коммуникационных системах показало:

разработанная на основе методологии STRIDE модель угроз, ориентированная на выявление уязвимостей существующих систем обнаружения сетевых атак, а также программное средство, интегрирующее меры по нейтрализации потенциальных угроз с высокими уровнями риска, были реализованы в рамках научного проекта ООО «UNICON.UZ – Центр научно-технических и маркетинговых исследований» по теме «Исследование методов искусственного интеллекта и их применение в информационной безопасности», а также в локальной сети ООО «Kesh-Total Service» (протокол ООО «Kesh-Total Service» от 7 февраля 2025 года; справка Министерства цифровых технологий Республики Узбекистан № 33-8/3918 от 9 июня 2025 года). В ходе испытаний из 3500 образцов атак было корректно выявлено 3426. Полученные научные результаты показали, что интеграция систем обнаружения атак с методами искусственного интеллекта позволила устранить существующие недостатки.

на основе усовершенствованного метода построения систем обнаружения атак, предусматривающего внедрение процедур выбора признаков сетевых пакетов с применением голосования и автоматического определения архитектуры нейронных сетей, что позволило минимизировать уровень ложных срабатываний и повысить эффективность обнаружения, было разработано программное средство «VIDSA». Оно прошло экспериментальные испытания в телекоммуникационных сетях Самаркандского филиала АО «Uzbektelecom» для выявления атак типа DDoS, сканирования портов и других разновидностей угроз (справка Министерства цифровых технологий Республики Узбекистан № 33-8/3918 от 9 июня 2025 года). В результате тестирования эффективность обнаружения атак в информационно-коммуникационных системах составила 98,5%, а показатель ложных срабатываний — 1,5%. Данный подход позволил повысить результативность систем обнаружения атак и сократить количество ложных оповещений.

программное средство, разработанное с использованием предложенных алгоритмов расчёта энтропии признаков сетевых пакетов и голосования на основе множественности для их выбора при обучении систем обнаружения сетевых атак методами искусственного интеллекта, было протестировано в подразделении «Развитие и эксплуатация службы доверенной третьей стороны» ООО «UNICON.UZ – Центр научно-технических и маркетинговых исследований» и в локальной сети ООО «Kesh-Total Service» (протокол ООО «Kesh-Total Service» от 7 февраля 2025 года; справка Министерства цифровых технологий Республики Узбекистан № 33-8/3918 от 9 июня 2025 года). В результате время, затрачиваемое на обучение, было сокращено до 15 %. Научное исследование показало, что корректный выбор признаков сетевых пакетов позволяет значительно уменьшить временные затраты.

усовершенствованный алгоритм автоматического выбора архитектуры нейронных сетей в зависимости от количества выбранных признаков сетевого пакета, позволяющий повысить эффективность системы обнаружения атак с целью обеспечения защищённости сети, был внедрён в отдел «Развитие и эксплуатация службы доверенной третьей стороны» ООО «UNICON.UZ – Центр научно-технических и маркетинговых исследований» (справка Министерства цифровых технологий Республики Узбекистан № 33-8/3918 от 9 июня 2025 года). В ходе 24-часового мониторинга было корректно выявлено 3 атаки. Результаты показали, что данный подход обеспечивает высокую эффективность обнаружения атак в режиме реального времени и низкий уровень ложных срабатываний.

Апробация результатов исследования.

Результаты исследований обсуждались на 3 международных, 11 республиканских научно-практических конференциях и научных семинарах.

Публикация результатов исследования.

Всего по теме исследования опубликована 21 научная работа, из них 4 статей – в журналах, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе в 1 зарубежных и 3 республиканских журналах, а также получены свидетельства об официальной регистрации Министерством юстиции Республики Узбекистан на 3 программных средства, созданных для СЭС.

Структура и объем диссертации. Диссертационная работа написана на узбекском языке, ее объем составляет 112 страниц, включая введение, четыре главы, выводы, Список использованной литературы и приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обоснованы актуальность и необходимость темы диссертации, приведено соответствие исследования приоритетным направлениями развития науки и техники Республики Узбекистан, определены–цель и задачи, объект и предмет исследования, обоснованы достоверность полученных результатов, их теоретическая и практическая значимость, состояние внедрения результатов исследования в практику, перечислены опубликованные работы и представлена информация о структуре диссертации.

В первой главе диссертации, озаглавленной **«Сетевые атаки, их классификация и проблемы обнаружения»**, представлен сравнительный анализ видов атак, осуществляемых в информационно-коммуникационных сетях, проблем их обнаружения, существующих средств, а также методов и алгоритмов. В результате проведенного анализа показана необходимость совершенствования метода обнаружения в системах обнаружения атак с помощью методов искусственного интеллекта, точного и правильного выбора признаков сетевых пакетов, балансировки архитектуры искусственных нейронных сетей с целью снижения показателя ложных срабатываний.

В первой главе диссертации рассматриваются атаки, относящиеся к четырем категориям: Probe, DoS/DDoS, U2R и R2L. Защита от этих атак включает в себя различные инструменты, такие как брандмауэр, honeypot, IDS, и в рамках этих инструментов IDS отличается гибкостью, удобством, низкой ресурсоемкостью и способностью анализировать стороны различными способами.

Показатель ложных срабатываний измеряется отношением количества ложных срабатываний к общему числу проверок. Однако его также называют вероятностью ложного срабатывания и определяют следующим образом.

$$FAR = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \quad (1)$$

Одним из наиболее важных аспектов улучшения IDS является извлечение значимых признаков из данных и их предварительная подготовка к обработке. В таблицах 1 и 2 приведены результаты эффективности классификаторов при отсутствии отбора признаков и при его использовании.

Таблица 1

Эффективность классификаторов без выполнения отбора признаков

Классифика-торы	время (сек)	правильно классифици-ровано (%)	Неправильно классифици-ровано (%)	Эффектив-ность TPR (%)	Эффектив-ность FPR (%)
NaïveBayes	7.79	85.24	14.61	45.6	13.4
J-48	49.73	89.73	11.33	96.7	0.3
REPTree	21.22	90.07	9.03	89.2	2.5

При оценке эффективности классификаторов используются различные методы отбора признаков. Например, CFS + Best First, Info Gain + Ranker и Gain Ratio + Ranker.

Таблица 2

Эффективность классификаторов при выполнении отбора признаков

Алгоритм выбора признаков	Классифика-торы	время (сек)	правильно классифициро-вано (%)	Неправильно классифициро-вано (%)	Эффектив-ность TPR (%)	Эффектив-ность FPR (%)
CFS + Best First	Naïve Bayes	5.22	93.5	6.95	93.7	13.4
	J-48	17.04	95.56	4.44	95.1	10.5
	REPTree	7.5	96.40	3.60	96.6	12.1
Info Gain + Ranker	Naïve Bayes	2.25	94.15	5.85	97.5	9.7
	J-48	6.47	97.77	2.34	97.0	12.0
	REPTree	4.24	96.12	3.88	96.0	4.6
Gain Ratio + Ranker	Naïve Bayes	3.46	97.99	2.00	97.4	1.1
	J-48	8.46	98.18	1.82	97.4	0.7
	REPTree	6.34	95.78	4.06	95.0	12.6

Использование слишком большого количества нейронов в скрытых слоях также приводит к ряду проблем. Существует несколько способов выбора правильного количества нейронов в скрытом слое. Например, количество скрытых нейронов должно быть между размером входного слоя и размером выходного слоя, количество скрытых нейронов должно составлять 2/3 размера входного слоя и быть равным размеру выходного слоя, или количество скрытых нейронов должно быть меньше чем в удвоенный размера входного слоя.

Согласно первому методу, конфигурация сети — l-m-n (где l — чисдо входных, m — скрытых, а n — выходных нейронов). В таблицах 3 и 4 представлены результаты для архитектур $l = 17,\ m = 17,\ n = 1$ и $l = 17,\ m_1 = 8, m_2 = 8, n = 1.$

Таблица 3

Скрытый слой=1, число скрытых нейронов=17

Критерии оценки	Обучение	Подтверждение
Коэффициент правильной классификации (CCR, %)	100	-
Ошибка сети (%)	0.0298	0
Итерации (шт.)	501	
Скорость обучения (шт./сек)	47.264	
Архитектура нейронной сети	[17-17-1]	

Вторая архитектура включает один входной, два скрытых и один выходной слой с числом нейронов 17, 8, 8 и 1 соответственно.

Таблица 4

Скрытых слоёв = 2, число нейронов в каждом скрытом слое = 8

Критерии оценки	Обучение	Подтверждение
Коэффициент правильной классификации (CCR, %)	100	-
Ошибка сети (%)	0.0298	0
Итерации (шт.)	501	
Скорость обучения (шт./сек)	52.187	
Архитектура нейронной сети	[17-8-8-1]	

Из приведенных выше таблиц видно, что хотя архитектура 17-17-1 и 17-8-8-1 демонстрируют одинаковую частоту ошибок, вторая архитектура обладает преимуществом с точки зрения скорости обучения.

Рисунок 1. Архитектура сети с системами обнаружения вторжений

С учётом экспоненциального роста киберугроз, организации всё чаще полагаются на системы обнаружения вторжений для обнаружения, анализа и предотвращения нарушений безопасности в режиме реального времени.

Во второй главе диссертации, озаглавленной **«Модель угроз для систем обнаружения вторжений»** разрабатывается модель угроз для систем обнаружения вторжений и формулируются задачи, которые необходимо решить при их построении в соответствии с современными тенденциями, такими как использование высокопроизводительных искусственных нейронных систем и отбор признаков. Также рассматриваются применение и характеристики искусственных нейронных сетей в системах обнаружения вторжений, а также методы выбора их архитектуры и параметров..

Системы обнаружения вторжений являются одним из основных инструментов обеспечения безопасности данных и систем, в которых эти данные хранятся. Однако построение модели угроз для существующих систем IDS позволяет выявить и устранить имеющиеся уязвимости. На рисунке 2 приведена модель угроз, разработанная для существующих систем обнаружения вторжений.

Исходя из данной модели угроз, можно выделить несколько угроз архитектуре системы, а именно:

1. возможность внедрения ложного объекта в средства сбора и передачи данных либо подделки данных в этих средствах;

2. возможность перехвата, изменения или уничтожения собранных данных при передаче в систему обнаружения вторжений по каналу связи;

3. выявление и оценка характеристик данных, которые были изменены или фальсифицированы в процессе обработки информации;

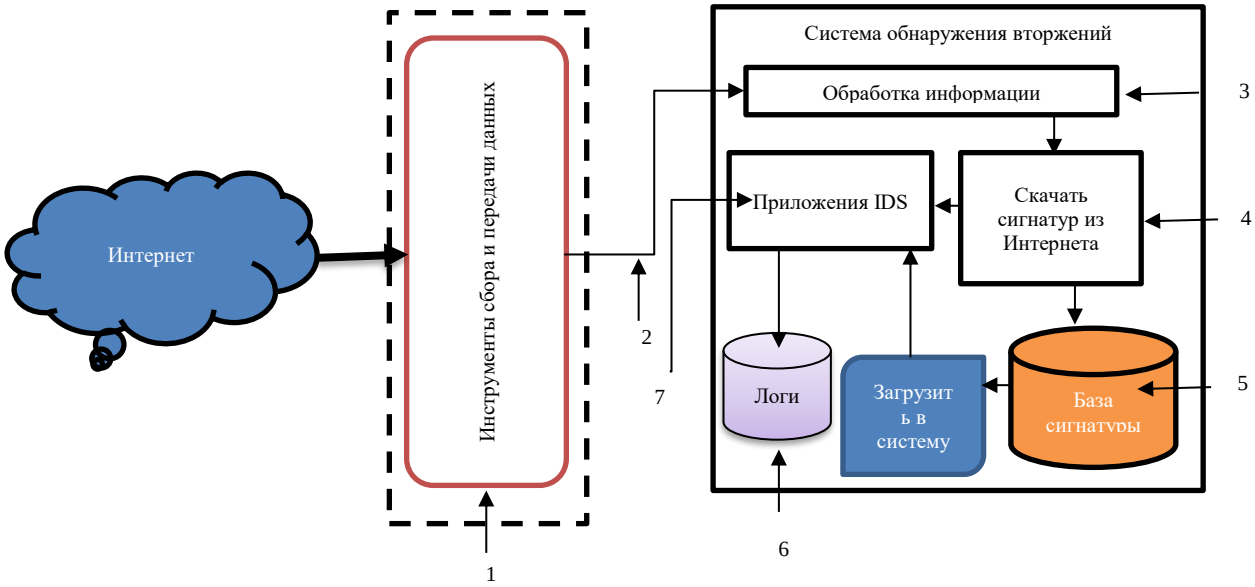


Рисунок 2. Модель угроз системы обнаружения вторжений

4. загрузка сигнатур атак из Интернета;

5. изменение базы данных сигнатур внутренним или внешним злоумышленником, подключённым к сети;

6. изменение или удаление информации об атаке или злоумышленнике, обнаруженной приложением и записанной в файлах журналов;

7. Атака на приложение с целью его отключения приложения, получения прав администратора, задержки или изменения результатов.

Разработанная модель угроз была реализована с использованием Microsoft Threat Modeling Tool и позволила выявить ряд уязвимостей и недостатков в существующих системах обнаружения вторжений. Реализованная модель угроз представлена на рисунке 3.

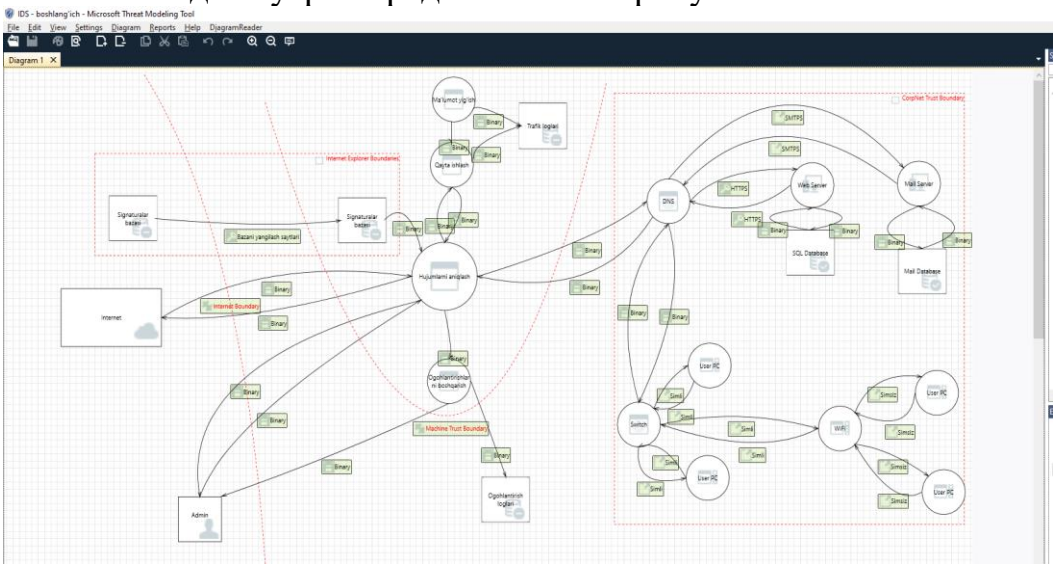


Рисунок 3. Модель угроз, реализованная с использованием Microsoft Threat Modelling Tools

Результаты анализа показывают, что существуют явные угрозы для информационно-коммуникационных систем. Эти угрозы тесно связаны с проблемами, представленными в первой главе. Для их решения целесообразно использовать методы искусственного интеллекта. На основании результатов вышеуказанного анализа:

1. необходимо выявлять и предотвращать оценку признаков данных, которые были изменены или фальсифицированы в процессе обработки информации. Для этого требуется автоматически определять надёжный набор признаков и ограничивать доступ пользователя к ним, то есть только самой системой или приложением;

2. в связи с рисками надёжности при загрузке сигнатур атак из Интернета необходимо настраивать и применять системы обнаружения вторжений, способные выявлять аномалии сетевого трафика с использованием методов машинного обучения и искусственного интеллекта;

3. следует снизить высокий уровень ложных срабатываний, характерный для существующих систем обнаружения аномалий сетевого трафика.

В третьей главе диссертации под названием «**Эффективные методы и алгоритмы обнаружения атак в информационно-коммуникационных системах»** рассматривается совершенствование систем обнаружения атак в информационно-коммуникационных системах на основе искусственных нейронных сетей (рисунки 4-5). Также в главу включены вопросы определения числа признаков в системах обнаружения атак (рисунки 6–7) и алгоритмы выбора скрытых слоёв и нейронов.

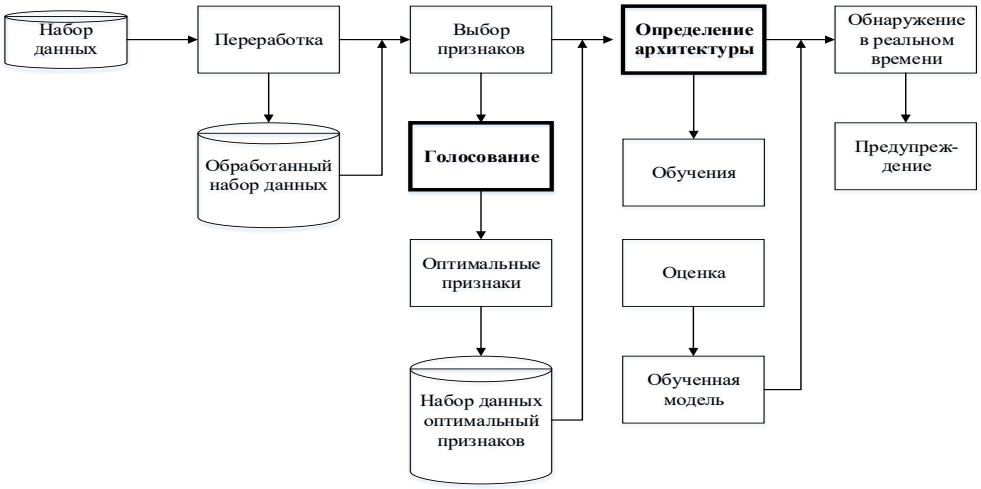


Рисунок 4. Принцип работы усовершенствованного метода построения систем обнаружения вторжений

Отличия данного метода от существующих заключаются в следующем:

1. Метод подходит для повышения эффективности в случае выполнения требований по снижению уровня ложных срабатываний.

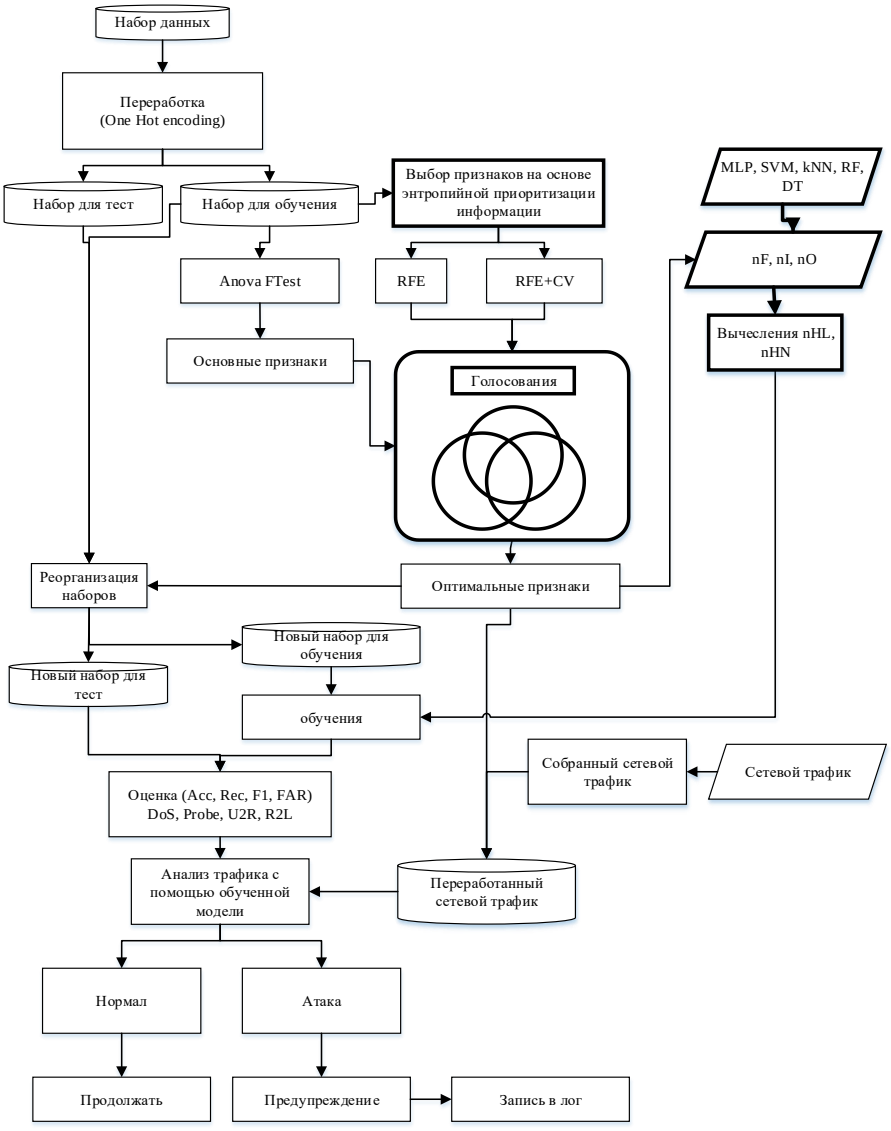


Рисунок 5. Архитектура предлагаемого метода

2. После обработки обучающего набора данных с помощью метода голосования определяется оптимальный набор признаков.

3. На основе количества оптимальных признаков формируется архитектура для методов искусственного интеллекта, то есть определяется количество скрытых слоёв и нейронов.

4. Модель использует ансамблевый метод для обнаружения атак в информационно-коммуникационных системах. Это позволяет одновременно использовать методы MLP, SVM, DT и RF.

5. Предоставляет возможность сохранения, передачи и перезагрузки обученной модели.

Работа предлагаемой модели представлена на рисунке 5.

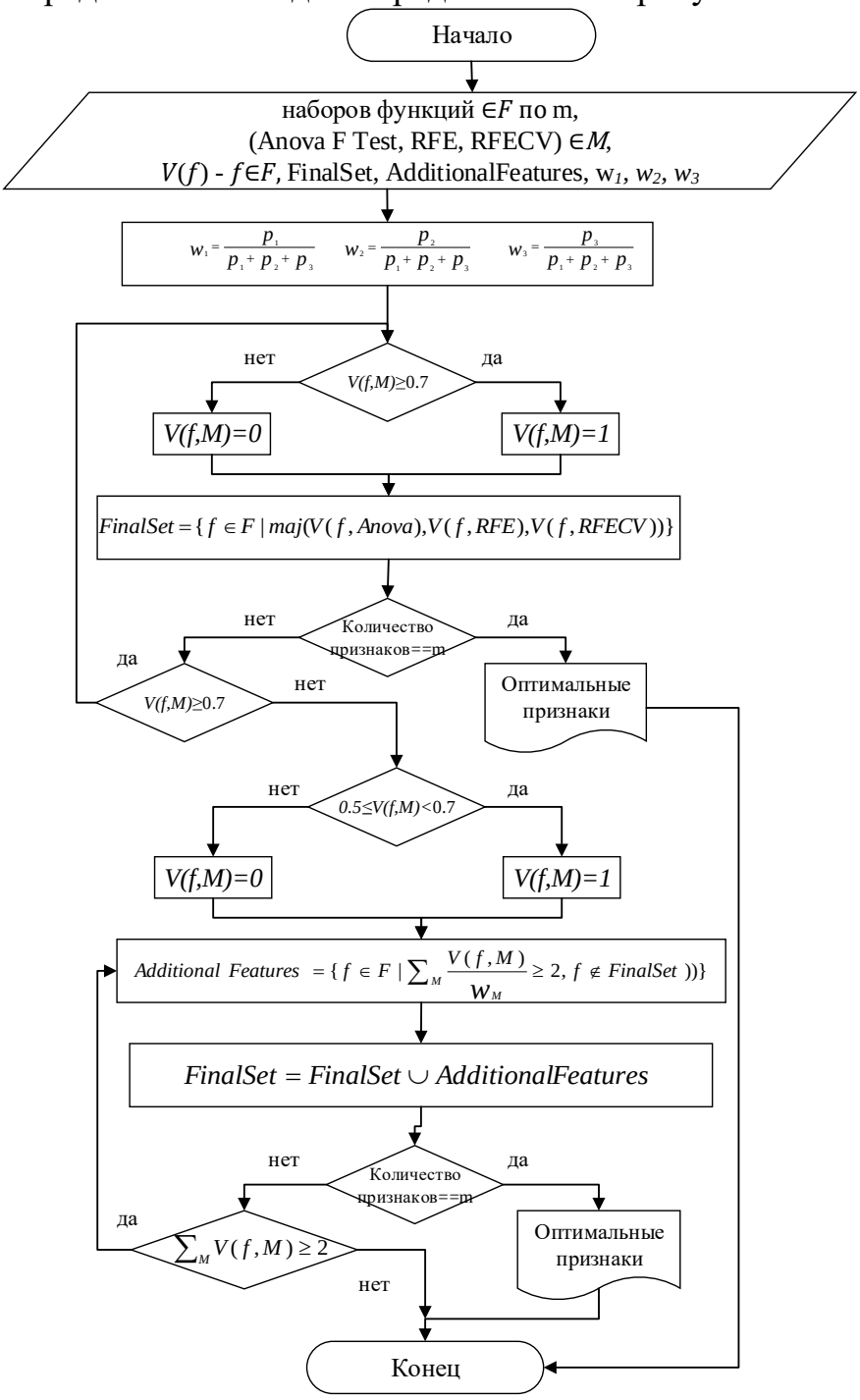


Рисунок 6. Блок-схема алгоритма процесса голосования

Обнаружение сетевых атак основано на тщательном выборе и извлечении признаков, которые эффективно фиксируют сложные закономерности, связанные с вредоносной активностью. Эти признаки служат основой для моделей машинного обучения, в частности нейронных сетей, разработанных для различения нормального поведения сети от потенциально вредоносных аномалий.

Алгоритм голосования для выбора признаков

Каждому методу выбора признаков присваивается вес w_1, w_2, w_3 в соответствии с его производительностью. Процесс голосования использует функцию «большинства» и рассчитывается по следующей формуле:

$$\mathrm{maj}(x, y, z) = (x \vee y) \oplus (x \vee z) \oplus (y \vee z) \quad (2)$$

Блок-схема алгоритма голосования, разработанного для выбора признаков, представлена на рисунке 6.

Скрытые слои и нейроны архитектуры определяют способность нейронной сети изучать сложные взаимосвязи в данных. Оптимизация архитектуры нейронной сети играет решающую роль в повышении её возможностей обнаружения атак. Выбирая правильное количество признаков, скрытых слоев и скрытых нейронов, сеть может эффективно обнаруживать и классифицировать атаки с высокой точностью и эффективностью. Оптимизация архитектуры включает поиск баланса между её сложностью и способностью к обобщению.

$$OH5 = \frac{\mathrm{SF} * (\mathrm{NI} + \mathrm{NO}) * \mathrm{Log10}(\mathrm{NI} + \mathrm{NO})}{2} \quad (3)$$

Таблица 5

Результаты расчета количества скрытых нейронов и количества слоев

Формула расчёта	Один скрытый слой	Два скрытых слоя	Три скрытых слоя
OH1 = (NI+ NO)* (1-(1/(NI+NO)))	15	-	-
OH2 = 2/3*(NI+NO)	11	-	-
OH3 = SF*(NI+ NO)^Exp	16	32	768
OH4 = (NI+ NO)*log10(NI+NO)/2	10	-	-
OH5 = SF*(NI+ NO)*log10(NI+NO)/2	10	19	29
OH6 = SF*(NI+ NO)^ Exp*log10(NI+NO)/2	10	19	462
OH7 = SF*(NI+ NO)^Exp*log10(NI+NO)^Exp/2	10	19	558

Результаты таблицы, представленной выше, показывают, что формула OH5 сохраняет пропорциональность между числом скрытых нейронов при увеличении количества нейронных слоёв.

В четвертой главе диссертации, озаглавленной **«Программное средство и результаты экспериментальных расчётов усовершенствованного метода обнаружения атак»,** представлено программное средство, разработанное на основе усовершенствованных методов и алгоритмов, предложенных в предыдущих главах, его модули и принцип работы. При этом представлено применение программного средства при решении практических задач и результаты экспериментальных расчётов.

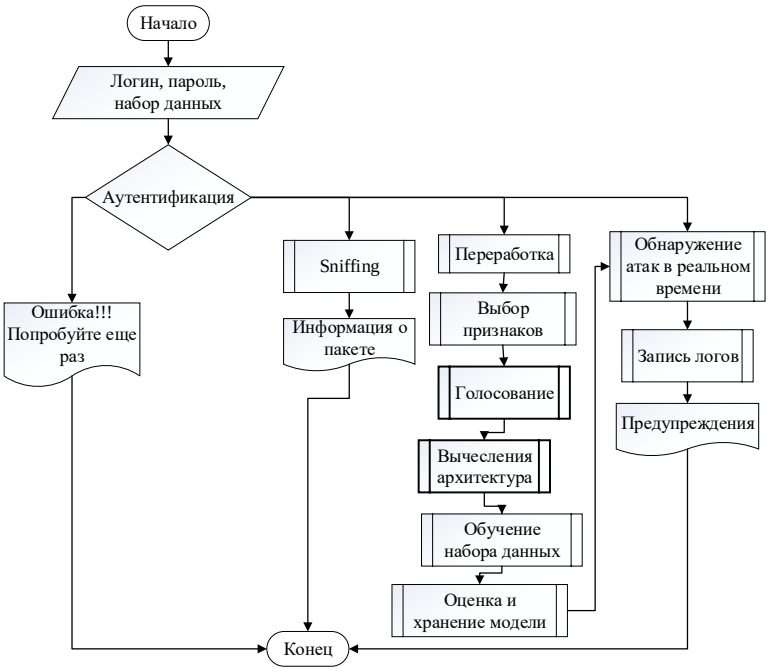


Рисунок 7. Алгоритм работы программного средства

Наборы данных KDD-CUP и NSL-KDD использовались для обучения и оценки методов машинного обучения и искусственных нейронных сетей.

Программный инструмент, разработанный на основе методов и алгоритмов, представленных в диссертации, разделён на модули. На рисунке 8 показан модуль мониторинга сетевого трафика в реальном времени.

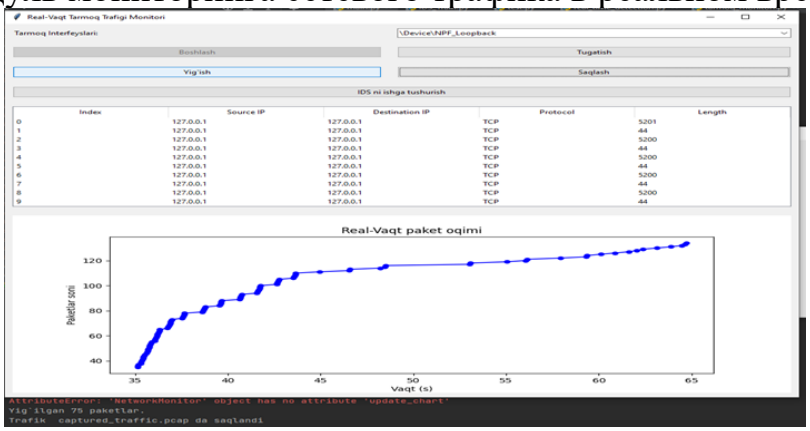


Рисунок 8. Окно мониторинга сети

На рисунке 9 ниже показано окно для обработки данных в наборе данных, выбора признаков, обучения, оценки и сохранения моделей.

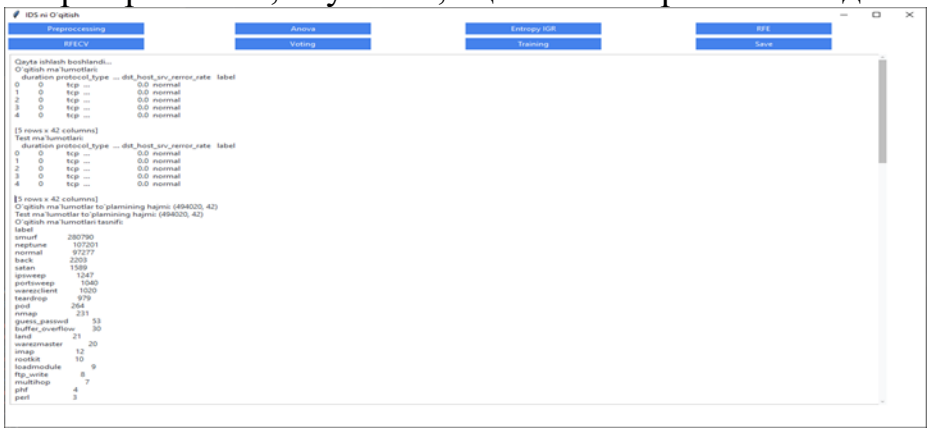


Рисунок 9. Процесс обучения

На рисунке 10 представлен процесс обнаружения атак путём анализа входящего трафика в информационно-коммуникационную систему в режиме реального времени с использованием загруженной сохранённой модели.

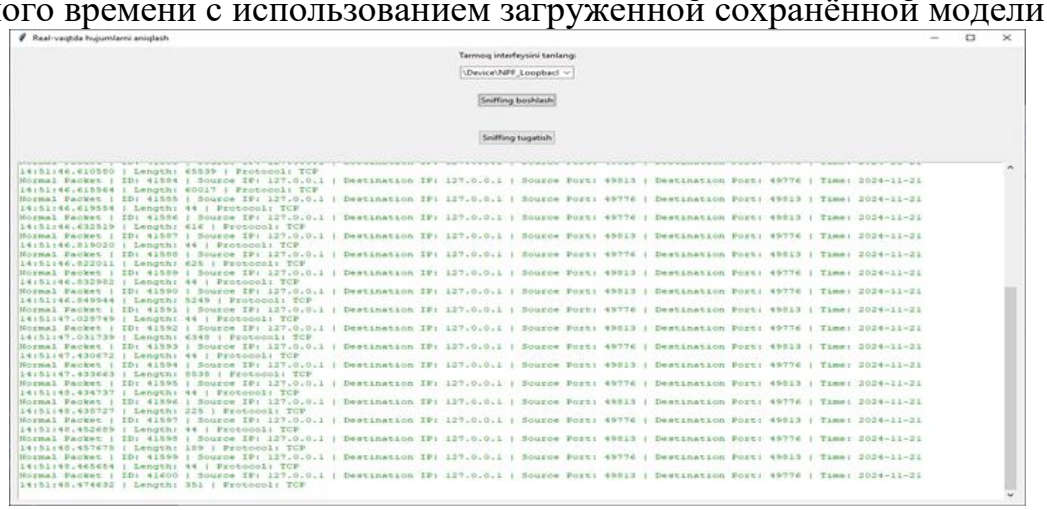


Рисунок 10. Процесс обнаружения атак в реальном времени

В таблицах 6–7 представлены экспериментальные результаты ложноположительных результатов.

Таблица 6

Результаты ложноположительных результатов для одного скрытого слоя

Набор данных	Тип атаки	MLP (%)	SVM (%)	DT (%)	RF (%)
KDD_CUP	DoS	1.10	1.27	1.00	1.03
	Probe	1.06	2.03	2.00	1.00
	R2L	1.30	2.07	2.01	2.02
	U2R	1.00	1.00	1.20	1.30
NSL_KDD	DoS	1.78	1.13	2.03	2.08
	Probe	1.34	2.27	2.10	2.02
	R2L	1.05	2.00	2.00	3.00
	U2R	1.00	2.30	2.30	2.50

Результаты в таблице выше показывают, как они изменяются после включения второго скрытого слоя.

Таблица 7

Результаты ложного подтверждения после включения второго скрытого слоя

Набор данных	Тип атаки	MLP (%)	SVM (%)	DT (%)	RF (%)
KDD_CUP	DoS	1.00	1.05	1.00	1.00
	Probe	1.05	1.04	2.00	2.10
	R2L	1.13	2.07	2.01	2.02
	U2R	1.00	1.80	2.40	2.50
NSL_KDD	DoS	1.20	1.25	2.20	2.09
	Probe	1.26	2.30	2.20	2.30
	R2L	1.06	2.00	2.40	2.50
	U2R	1.01	2.10	2.40	2.60

В таблицах 6 и 7 видно, что частота ложных срабатываний несколько уменьшается с увеличением количества скрытых слоев. Наименьшее значение частоты ложных срабатываний получено при использовании двух скрытых слоёв.

Другим критерием оценки, отражающим производительность обученной модели, является оценка F1, которая показывает соотношение между точностью и полнотой.

$$\text{F1} = \frac{2 * \text{точность} * \text{достоверность}}{\text{точность} + \text{достоверность}} \qquad (4)$$

В таблицу 8 представлены результаты расчета оценки F1.

Таблица 8

Оценка F1, полученная в результате обучения наборы данных Kdd-Cup и NSL-KDD

Datasetlar		KDD-CUP		NSL-KDD	
Тип атаки	Метод обучения	Для одного скрытого слоя (%)	После активации второго скрытого слоя (%)	Для одного скрытого слоя (%)	После активации второго скрытого слоя (%)
DOS	MLP	99.42	99.80	98.29	99.26
	SVM	99.02	99.17	98.82	98.86
	DT	99.96	99.99	99.70	99.72
	RF	99.96	99.99	99.70	99.72
Probe	MLP	99.27	99.27	98.50	98.82
	SVM	99.37	99.22	98.80	98.58
	DT	99.91	99.89	99.93	99.87
	RF	99.91	99.89	99.93	99.87
R2L	MLP	93.27	93.45	91.85	92.25
	SVM	93.50	93.50	90.82	90.82
	DT	98.97	98.97	99.07	99.07
	RF	98.98	98.99	99.07	99.07
U2R	MLP	64.05	53.62	79.26	78.74
	SVM	65.61	51.87	81.24	81.24
	DT	94.00	93.00	93.47	93.47
	RF	94.00	93.00	93.47	93.61

В таблице выше показаны результаты обучения и оценки наборы данных Kdd-Cup и NSL-Kdd с использованием различных методов и различных нейронных архитектур. Результаты этого таблица показывают, что корреляция между точностью и достоверностью высока в обоих наборах данных.

ЗАКЛЮЧЕНИЕ

В результате проведенных исследований по диссертационной работе на тему «Метод и алгоритмы обнаружения сетевых атак в информационно-коммуникационных системах» сделаны следующие выводы:

1. В результате анализа существующих недостатков систем обнаружения атак по ряду факторов показана актуальность повышения эффективности их обнаружения и снижения доли ложных срабатываний. Это подтвердило необходимость разработки усовершенствованной системы обнаружения атак путём перехода сигнатурных методов к методам искусственного интеллекта.

2. По результатам сравнительного анализа существующих методов и средств обнаружения атак предложена модель угроз для этих систем. Это показало необходимость использования методов машинного обучения и нейросетей в ансамбле для точного подбора набора обучаемых признаков и автоматизации балансировки их архитектур, а также обеспечения высокой эффективности.

3. Работа систем обнаружения атак была усовершенствована за счёт применения метода голосования и автоматического расчёта архитектур машинного обучения и нейросетей. Показано, что разработанная с использованием данного метода система обнаружения атак превосходит существующие по преимуществам и эффективности.

4. С использованием методов машинного обучения разработан алгоритм выбора признаков сетевых пакетов на основе энтропии и функций множественного голосования. В результате экспериментов удалось добиться снижения уровня ложных срабатываний до 2,1% при обнаружении сетевых атак за счет указания количества выбираемых признаков.

5. Разработан алгоритм балансировки архитектур методов машинного обучения и нейросетей для использования их при ансамблевом обучении. В результате научных исследований удалось сократить время обучения системы обнаружения атак до 15%.

6. Создано программное средство для системы обнаружения атак, предусматривающее использование разработанных алгоритмов в качестве модулей. Разработанное программное средство было использовано в процессе обнаружения атак в сетях предприятий соответствующей отрасли, достигнув средней точности 98% и уровня ложных срабатываний около 2%.

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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

BOZOROV SUHROBJON MUMIN UGLI

METHOD AND ALGORITHMS FOR DETECTING NETWORK ATTACKS IN INFORMATION AND COMMUNICATION SYSTEMS

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

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

Tashkent-2025

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2025.1.PhD/T5294.

The dissertation has been prepared at Tashkent university of information technologies named after Muhammad al-Khwarizmi.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website www.tuit.uz and on the website of «ZiyoNet» Information and educational portal www.ziyonet.uz.

Scientific adviser:	**Gulomov Sherzod Rajaboyevich** doctor of technical sciense, asosiate professor
Official opponents:	**Kerimov Komil Fikratovich** doctor of technical sciense, professor **Kadirov Mirkhusan Mirpulatovich** PhD, assosiate professor
Leading organization:	**“UNICON.UZ” LLC - Center for Scientific, Technical and Marketing Research.**

The defense will take place «_18_» _october_ 2025 at _11:30_ the meeting of Scientific council No. DSc.13/30.12.2019.T.07.02 at Tashkent university of information technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-15, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No._368_). (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-15).

Abstract of dissertation sent out on «_08_» _october_ 2025 y.
(mailing report No. ___ on «____» _____ 2025 y.).

B.Sh.Makhkamov
Chairman of the Scientific Council awarding scientific degrees, doctor of economical sciences, professor

M.S.Saitkamolov
Scientific secretary of the Scientific Council awarding scientific degrees, doctor of economical sciences, associate professor

D.Ya.Irgasheva
Chairman of the academic Seminar under the Scientific Council awarding scientific degrees, doctor of technical sciences, professor

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is to develop effective methods and algorithms for detecting network attacks on information and communication systems.

The object of the research work is attacks aimed at data flows transmitted over the network in information and communication systems.

The scientific novelty of the research work is as follows:

Based on the analysis of existing network attack detection systems, a threat model has been developed using the STRIDE methodology, and the risk levels of potential threats have been assessed according to the DREAD model.

The method for constructing attack detection systems has been enhanced by incorporating feature selection of network packets through voting and the automatic selection of neural network architectures, thereby minimizing the false positive rate and improving detection efficiency.

For training network attack detection systems using artificial intelligence methods, algorithms have been proposed for selecting network packet features based on entropy calculation and majority voting.

To ensure network protection, the algorithm for automatic selection of neural network architectures has been improved by calculating it according to the number of selected network packet features, thereby increasing the efficiency of attack detection systems.

Implementation of the research results. Based on scientific results on the implementation of methods and algorithms for detecting network attacks in information and communication systems:

A threat model, developed using the STRIDE methodology and aimed at identifying vulnerabilities in existing network attack detection systems, along with a software tool that consolidates measures to mitigate potential threats with high-risk levels, was implemented within the framework of the scientific project of LLC “UNICON.UZ – Center for Scientific, Technical, and Marketing Research” on the topic “Research of Artificial Intelligence Methods and Their Application in Information Security,” as well as in the local network of LLC “Kesh-Total Service” (Protocol of LLC “Kesh-Total Service” dated February 7, 2025; Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8/3918 dated June 9, 2025). During testing, 3,426 out of 3,500 attack samples were correctly detected. The obtained scientific results demonstrated that integrating attack detection systems with artificial intelligence methods made it possible to eliminate existing shortcomings.

Based on an improved method for constructing intrusion detection systems, which incorporates network packet feature selection through voting and automatic determination of neural network architecture—thereby minimizing the false positive rate and enhancing detection efficiency—the “VIDSA” software tool was developed. It was experimentally tested in the telecommunications networks of the Samarkand branch of JSC “Uzbektelecom” for detecting DDoS attacks, port scanning, and other types of threats (Certificate of the Ministry of Digital

Technologies of the Republic of Uzbekistan No. 33-8/3918 dated June 9, 2025). The testing results showed that the attack detection efficiency in information and communication systems reached 98.5%, with a false positive rate of 1.5%. This approach has proven effective in improving the performance of intrusion detection systems while reducing false alarms.

A software tool, developed using proposed algorithms for calculating the entropy of network packet features and plurality-based voting for their selection in the training of network attack detection systems using artificial intelligence methods, was tested in the “Trusted Third Party Service Development and Operation Department” of LLC “UNICON.UZ – Center for Scientific, Technical, and Marketing Research” and in the local network of LLC “Kesh-Total Service” (Protocol of LLC “Kesh-Total Service” dated February 7, 2025; Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8/3918 dated June 9, 2025). As a result, the training time was reduced by up to 15%. The research findings demonstrated that the correct selection of network packet features significantly reduces the time required for training.

The improved algorithm for the automatic selection of neural network architectures, based on the number of selected network packet features and designed to enhance the efficiency of attack detection systems for ensuring network security, was implemented in the “Development and Operation of Trusted Third-Party Services” Department of UNICON.UZ – Center for Scientific, Technical and Marketing Research LLC (Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8/3918 dated June 9, 2025). During a 24-hour monitoring period, three attacks were accurately detected. The results demonstrated that this approach ensures high efficiency of real-time attack detection and a low false alarm rate.

Structure and volume of the dissertation. The dissertation consists of an introduction, four chapters, a conclusion, a list of references and appendices. The volume of the dissertation is 112 pages.

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

I bo‘lim (I частъ; I part)

1. Bozorov S.M. DDoS Attack Detection via IDS: Open Challenges and Problems // International Conference on “Information Science and Communications Technologies (ICISCT)”. Tashkent and Urgench, Uzbekistan-2021. -4p. (3) Scopus, (OAK Rayosatining qarori 30.10.2021 y. №308/6).

2. Bozorov S.M. ANN and voting based novel approach for building balanced IDS // Raqamli Transformatsiya va Sun’iy Intellekt” ilmiy jurnali. Volume 2, Issue 6, 2024. –P. 55-63. (OAK rayosat qarori, 04.07.2023, №363).

3. Gulomov Sh.R., Bozorov S.M. Survey on methods and models for reducing false alarm rate of IDS // Journal of “Bulletin of TUIT: Management and Communication Technologies”. Vol. 3(15), 2022. -8p. (OAK Rayosatining 30.07.2023 yildagi qarori bilan “Uzbekistan Research Online” raqamli platformasidagi jurnallarda e’lon qilingan ingliz tilidagi maqolalar dissertatsiyalar asosiy ilmiy natijalarini e’lon qilishga tavsiya etilgan xorijiy ilmiy nashrlarda chop etilgan ilmiy maqolalarga tenglashtirilgan).

4. Bozorov S.M., Usmanbayev D.Sh., Malikova N.T. Machine learning algoritmlari asosida infokommunikatsion tarmoqlarda hujumlarni aniqlash mexanizmlari // “Muhammad al-Xorazmiy avlodlari” ilmiy-amaliy va axborot-tahliliy jurnali. № 3 (17), 2021. –B. 8-12. (05.00.00; №10).

II bo‘lim (II частъ; II part)

5. Bozorov S.M., Akhmedova N.F., Qurbonaliyeva D.V., Kader G. Survey on Honeypot: Detection, Countermeasures and Future with MI // International Scientific Conference on “Modern Problems of Applied Science and Engineering-MPASE-2024”. Samarkand, Uzbekistan-2024. -10p. (3) Scopus.

6. Usmanbayev D.Sh. and Bozorov S.M. Analysis of Algorithm of Binary Classifiers to Improve Attack Detection Systems // 12th World Conference “Intelligent System for Industrial Automation” (WCIS-2022). Volume 1. Tashkent, Uzbekistan-2022. –P. 81-87. (11) Springer.

7. Xoliyarov F.T., Gulomov Sh.R., Bozorov S.M. The Impact of Artificial Neural Network Architecture on Network Attack Detection // Proceedings of the 7th International Conference on “Future Networks and Distributed Systems (ICFNDS-23)”. Association for Computing Machinery, New York, NY, USA-2023. -P. 532–539 https://doi.org/10.1145/3644713.3644792. (3) Scopus.

8. Bozorov Suhrobjon. Voting systems in AI-based Intrusion Detection Systems: enhancing security through consensus mechanisms// International scientific conference on “EDUCATION AND RESEARCH IN THE ERA OF DIGITAL TRANSFORMATION”. Vol. 1 No. 2 (2025). America-2025. –7p.

9. Бозоров С.М. DDOS ҳужумларидан ҳимояланишда Machine Learning технологияси асосида captcha тизимини ишлаб чиқиш // Proceedings of the

Scientific Online International Conference “Actual problems and prospects of the development of intelligent information and communication systems IICS-2020”. Tashkent-2020. –Б. 48-51

10. Bozorov S.M.. Intrusion detection using machine learning on KDDCUP-99 dataset: analysis of feature selection // International scientific conference on “BRIDGING THE GAP: EDUCATION AND SCIENCE FOR A SUSTAINABLE FUTURE”. Vol. 1 No. 1 (2025). Germany-2025. –6p.

11. Bozorov S.M. Infokommunikatsion tarmoqlarda taqsimlangan kiber hujumlarni machine learning asosida oldindan aniqlashda xususiyatlarni tanlash // Сборник докладов международной научнопрактической конференции “Информационные Технологии, Сети И Телекоммуникации-ITN&T-2021”. Ургенч-2021. –B. 251-254

12. Bozorov S.M. Datasets for Intrusion Detection Systems: enhancing network security // “Kompyuter ilmlari va muhandislik texnologiyalari” xalqaro ilmiy-texnik anjuman materiallari to‘plami, 1-qism. Toshkent-2023. -P. 60-62

13. Bozorov S.M. Comparison analysis of feature selection methods and algorithms // “Zamonaviy Axborot, Kommunikatsiya Texnologiyalari va AT-Ta’lim Tatbiqi Muammolari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Samarqand-2023. -P. 198-199

14. S. Bozorov S.M. Building Intrusion Detection Systems: Requirements and Methods // “Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari” Respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Toshkent-2023. –P. 119-124

15. Bozorov S.M. Impact of hidden layers and count of neurons in ANN to improve accuracy on attack detection // “Zamonaviy Axborot, Kommunikatsiya Texnologiyalari va AT-Ta’lim Tatbiqi Muammolari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Samarqand-2023. -P. 202-204

16. Bozorov S.M. Network packet analyzing methods used by Intrusion Detection Systems // “Ilm-Fan va Innovatsiya” ilmiy-amaliy konferensiyasi. Toshkent-2024. –P. 81-88

17. Bozorov S.M. Hujumlarni aniqlash tizimlarida yolg‘ondan tasdiqlash ko‘rsatgichi va uni kamaytirish zarurati // “Iqtisodiyot Tarmoqlarining Innovatsion Rivojlanishida Axborot-Kommunikatsiya Texnologiyalarining Ahamiyati” Respublika ilmiy-texnik anjumani ma’ruzalar to‘plami, 1-qism. Toshkent- 2022. –B. 334-337

18. Bozorov S.M., Usmanbayev D.Sh. Supervized machine learning algoritmlarini hujumlarni aniqlash tizimlarida qo‘llash // «Iqtisodiyotning Tarmoklarining Innovatsion Rivojlanishida Axborot-Kommunikatsiya Texnologiyalarining Ahamiyati» Respublika ilmiy-texnik anjumanining ma’ruzalar to‘plami. 2-qism. Toshkent-2021. -B. 300-302

19. Bozorov S.M., Usmanbayev D.Sh. “DDoSDC” dasturi. O‘zbekiston Respublikasi Adliya Vazirligi huzuridagi Intellektual Mulk Agentligi. EHM uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma. №DGU 16007, 07.05.2022

20. Bozorov S.M., Usmanbayev D.Sh. “Tarmoq trafigi monitori” dasturi. O‘zbekiston Respublikasi Adliya Vazirligi. EHM uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma. №DGU 23693, 29.03.2023

21. Bozorov S.M. “VIDSA” dasturi. O‘zbekiston Respublikasi Adliya Vazirligi. EHM uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma. №DGU 41957, 17.08.2024

Avtoreferat «Muhammad al-Xorazmiy avlodlari» ilmiy jurnali tahririyatida o‘zbek, rus va ingliz tillaridagi matnlarining mosligi tekshirildi.

Bosmaxona litsenziyasi:

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 2,75. Adadi 100 dona. Buyurtma № 31/24.

Guvohnoma № 851684.
«Tipograff» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko‘chasi, 83-uy.