ISNN 3030-3907

2026/3
VOLUME 2

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/3 VOLUME 2

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

GIBRID SUN’IY INTELLEKT ASOSIDA TARMOQ TRAFIGIDA KIBERHUJUMLARNI ANIQLASH: AUTOENCODER VA GRADIENT BOOSTING MODELI

N.N. Jo‘rayev

O‘zbekiston Respublikasi harbiy xavfsizlik va mudofaa universiteti toshkent harbiy okrugi fakulteti Istiqbolli harbiy texnologiyalar kafedrasi boshlig‘i podpolkovnik

A.Sh. Juraboyev

O‘zbekiston Respublikasi harbiy xavfsizlik va mudofaa universiteti toshkent harbiy okrugi fakulteti katta o‘qituvchisi podpolkovnik

Annotatsiya. Mazkur tadqiqotda tarmoq trafigida kiberhujumlarni aniqlash uchun gibrid sun’iy intellekt modeli taklif etiladi. Model ikki bosqichli arxitekturaga asoslanadi: birinchi bosqichda Autoencoder yordamida normal trafik xulq-atvori o‘rganilib, anomal holatlar aniqlanadi; ikkinchi bosqichda esa Gradient Boosting algoritmi yordamida aniqlangan anomaliyalar hujum turlariga tasniflanadi. Taklif etilgan yondashuv klassik IDS tizimlariga nisbatan yuqori aniqlik va past noto‘g‘ri signal (False Positive) ko‘rsatkichlarini ta’minlaydi. Tadqiqot natijalari modelning F1-score, ROC-AUC va aniqlik ko‘rsatkichlari bo‘yicha samaradorligini tasdiqlaydi. Ushbu model real vaqt rejimida ishlovchi kiberxavfsizlik tizimlariga integratsiya qilish uchun istiqbolli yechim sifatida baholanadi.

Kalit so‘zlar: kiberxavfsizlik, sun’iy intellekt, gibrid model, Autoencoder, Gradient Boosting, IDS, anomaliya aniqlash, tarmoq trafigi, mashinaviy o‘rganish.

Аннотация. В данной работе предлагается гибридная модель искусственного интеллекта для обнаружения кибератак в сетевом трафике. Архитектура модели состоит из двух этапов: на первом этапе с помощью Autoencoder формируется модель нормального поведения трафика и выявляются аномалии; на втором этапе алгоритм Gradient Boosting выполняет классификацию выявленных аномалий по типам атак. Предложенный подход демонстрирует более высокую точность и снижение уровня ложных срабатываний по сравнению с традиционными системами обнаружения вторжений (IDS). Результаты экспериментов подтверждают эффективность модели по показателям F1-score, ROC-AUC и общей точности. Разработанная модель может быть использована в системах кибербезопасности реального времени.

Ключевые слова: кибербезопасность, искусственный интеллект, гибридная модель, Autoencoder, Gradient Boosting, IDS, обнаружение аномалий, сетевой трафик, машинное обучение.

ISSN 3030-3907

Abstract. This study proposes a hybrid artificial intelligence model for detecting cyber attacks in network traffic. The architecture consists of a two-stage approach: in the first stage, an Autoencoder learns normal traffic behavior and detects anomalies; in the second stage, a Gradient Boosting algorithm classifies detected anomalies into specific attack categories. The proposed approach demonstrates higher detection accuracy and reduced false positive rates compared to traditional intrusion detection systems (IDS). Experimental results confirm the model's effectiveness in terms of F1-score, ROC-AUC, and overall accuracy. The developed hybrid model can be integrated into real-time cybersecurity monitoring systems as a scalable and efficient solution.

Keywords: cybersecurity, artificial intelligence, hybrid model, Autoencoder, Gradient Boosting, intrusion detection system, anomaly detection, network traffic, machine learning.

KIRISH

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida global tarmoqlar hajmi va ularda uzatilayotgan ma'lumotlar miqdori keskin ortib bormoqda. Raqamli iqtisodiyot, bulutli hisoblash, IoT qurilmalari va sanoat avtomatizatsiyasi tizimlarining keng qo'llanilishi tarmoq infratuzilmasining murakkabligini oshirdi. Shu bilan birga, kiberhujumlar soni va ularning texnologik darajasi ham sezilarli ravishda kuchaymoqda. Zamonaviy tahdidlar – DDoS, phishing, botnet, ransomware, zero-day ekspluatatsiyalar – ko'p bosqichli va yashirin xarakterga ega bo'lib, an'anaviy himoya mexanizmlarini chetlab o'tish imkoniyatiga ega.

Klassik Intrusion Detection Systems (IDS) tizimlari asosan signaturaga asoslangan aniqlash usullaridan foydalanadi. Bunday yondashuv ilgari ma'lum bo'lgan hujum naqshlarini samarali aniqlay oladi, biroq yangi yoki modifikatsiyalangan tahdidlarni aniqlashda yetarli darajada moslashuvchan emas. Shuningdek, noto'g'ri signal (False Positive) ko'rsatkichining yuqoriligi tarmoq administratorlari va xavfsizlik mutaxassislari uchun qo'shimcha yuklama keltirib chiqaradi. Shu sababli, so'nggi yillarda kiberxavfsizlik sohasida mashinaviy o'rganish va sun'iy intellekt usullariga asoslangan adaptiv tizimlarga ehtiyoj ortib bormoqda.

Mashinaviy o'rganish yondashuvlari kiberhujumlarni aniqlashda ikki asosiy yo'nalishda qo'llaniladi: nazorat ostidagi (supervised) va nazoratsiz (unsupervised) o'rganish. Nazoratsiz usullar, xususan Autoencoder kabi neyron tarmoqlar, normal tarmoq xulq-atvorini o'rganib, undan og'ishlarni anomaliya sifatida belgilaydi. Bunday yondashuv yangi va ilgari noma'lum tahdidlarni aniqlash imkonini beradi. Biroq, anomaliya aniqlanganidan so'ng, uning turini aniqlash va tasniflash zarurati

ISSN 3030-3907

yuzaga keladi. Bu esa nazorat ostidagi algoritmlar, jumladan Gradient Boosting kabi kuchli klassifikatorlardan foydalanishni talab etadi.

Shu nuqtai nazardan, gibrid model yondashuvi – ya'ni nazoratsiz va nazorat ostidagi algoritmlarni birlashtirish – yuqori samaradorlikka erishish imkonini beradi. Autoencoder yordamida anomaliyalarni aniqlash va Gradient Boosting algoritmi orqali ularni turkumlash yondashuvi aniqlikni oshirish, noto‘g‘ri signal darajasini kamaytirish hamda real vaqt rejimida ishlash imkoniyatini ta'minlaydi. Ushbu ikki bosqichli arxitektura tarmoq trafigidagi murakkab va ko‘p o‘lchamli ma'lumotlarni chuqur tahlil qilish imkonini beradi.

Mazkur tadqiqotning maqsadi – tarmoq trafigida kiberhujumlarni aniqlash uchun Autoencoder va Gradient Boosting asosidagi gibrid sun'iy intellekt modelini ishlab chiqish hamda uning samaradorligini eksperimental jihatdan baholashdan iborat. Tadqiqot doirasida model arxitekturasi ishlab chiqiladi, ma'lumotlarni oldindan qayta ishlash bosqichlari tavsiflanadi va modelning aniqlik, F1-score hamda ROC-AUC ko‘rsatkichlari asosida tahlil qilinadi.

Tadqiqotning ilmiy yangiligi shundan iboratki, unda anomaliya aniqlash va hujumlarni tasniflash jarayonlari yagona integratsiyalashgan tizim doirasida uyg‘unlashtiriladi. Amaliy ahamiyati esa modelni real tarmoq monitoring tizimlariga joriy etish imkoniyati bilan belgilanadi. Taklif etilayotgan yondashuv zamonaviy kiberxavfsizlik infratuzilmasida moslashuvchan, kengaytiriladigan va samarali himoya mexanizmini shakllantirishga xizmat qiladi.

ADABIYOTLAR TAHLILI

Tarmoq xavfsizligini ta'minlashda intrusion detection system (IDS) konsepsiyasi uzoq yillardan beri qo‘llanilib kelinadi va amaliyotda u, odatda, signatura (misuse) asosidagi hamda anomaliya (anomaly) asosidagi yondashuvlarga ajratiladi. Signatura asosidagi IDS lar avvaldan ma'lum bo‘lgan hujum naqshlarini aniqlashda samarali bo‘lsa-da, yangi (zero-day) yoki modifikatsiyalangan tahdidlar paydo bo‘lganda moslashuvchanlik yetishmasligi va qoidalarni doimiy yangilab borish zarurati kabi cheklovlarga ega. Shu bois zamonaviy tadqiqotlar ko‘proq anomaliya asosidagi va ma'lumotlarga tayanuvchi (data-driven) yondashuvlarga yo‘nalmoqda. IDS bo‘yicha so‘nggi sharh ishlari ham aynan yangi avlod datasetlar (CIC-IDS2017, CSE-CIC-IDS2018 va boshqalar) hamda ML/DL yondashuvlarining ustunlik-cheklovlarini tizimli yoritadi.

Tadqiqotlarda model natijadorligi ko‘p jihatdan ishlatilgan datasetga bog‘liq. Amaliy tadqiqotlarda keng qo‘llaniladigan ochiq ma'lumotlar to‘plamlaridan biri **CIC-IDS2017** bo‘lib, u turli hujum sinflari bilan belgilangan (labeled) tarmoq oqimlari (flows), PCAP va ML uchun CSV ko‘rinishidagi

ISSN 3030-3907

fayllarni taqdim etadi. Yana bir mashhur manba — **UNSW-NB15**, u zamonaviy normal faoliyat va sintetik hujum xatti-harakatlarini uyg‘unlashtirgan holda shakllantirilgan hamda bir nechta hujum toifalarini (masalan, DoS, Exploits, Reconnaissance va boshqalar) o‘z ichiga oladi. Шу билан бирга, CIC-IDS2017 каби datasetlarni qo‘llashda ma’lumotlar nomutanosibligi (imbalance), xususiyatlar sifati va qayta ishlash bosqichlaridagi xatoliklar natijalarni keskin o‘zgartirishi mumkinligi bo‘yicha tahliliy ishlar ham uchraydi.

So‘nggi yillarda **nazoratsiz o‘rganish** (unsupervised learning) usullari, ayniqsa **Autoencoder** arxitekturasi, tarmoq trafigida “normal” xulq-atvorni o‘rganish va undan og‘ishni anomaliya sifatida ajratishda faol qo‘llanilmoqda. Autoencoderning asosiy afzalligi shundaki, u normal trafikni rekonstruksiya qilishni o‘rganadi va hujum/anomaliya paytida rekonstruksiya xatosi ortishi hisobiga signal beradi; bu esa, nazariy jihatdan, **noma’lum tahdidlarni** ham ushlash imkonini beradi. IoT muhitida autoencoderga asoslangan anomaliya IDS yondashuvlari bo‘yicha sharhlar bu yo‘nalishning tez rivojlanayotganini va resurs cheklovlari sharoitida ham amaliy qiymatga egaligini ta’kidlaydi. Amaliy tizimlarga yaqin misol sifatida avtomobil tarmoqlarida (CAN) yengil (lightweight) autoencoder asosidagi IDS yechimlari ham taklif qilingan bo‘lib, real vaqt va qurilmada ishlash talablari doirasida anomaliyani normal ma’lumotda o‘qitilgan model orqali aniqlash g‘oyasi qo‘llanadi.

Biroq, faqat anomaliya aniqlashning o‘zi yetarli emas: “anomaliya bor” degan signal xavfsizlik amaliyotida (SOC/incident response) ko‘pincha **hujum turi** va ehtimoliy zarar ssenariysini ham aniqlashni talab qiladi. Bundan tashqari, rekonstruksiya-xato threshold tanlash, shovqinli (noisy) trafik, hamda sinflar nomutanosibligi autoencoder modelida **False Positive**ni oshirishi mumkin. Shu sabab, ko‘plab ishlar autoencoderni kuchli klassifikatorlar bilan birlashtirish yoki qo‘shimcha xususiyat tanlash/normalizatsiya bilan mustahkamlash yo‘liga o‘tmoqda.

Tarmoq trafigi xususiyatlari ko‘pincha yuqori o‘lchamli va chiziqli bo‘lmagan munosabatlarga ega bo‘lgani uchun daraxtga asoslangan ansambllar, xususan **Gradient Boosting** oilasi, IDS masalalarida kuchli natija berishi ko‘p bor qayd etilgan. Masalan, real vaqtga yaqin ishlash, katta trafik oqimlarini qayta ishlash va aniqlikni ushlab qolish maqsadida LightGBM asosida IDS yechimlari taklif qilingan. Shuningdek, klassik va boosting klassifikatorlarini taqqoslagan tadqiqotlarda (XGBoost, LightGBM, CatBoost va boshqalar) boosting yondashuvlarining aniqlik va barqarorlik jihatidan ustun tomonlari ko‘rsatiladi, ayniqsa to‘g‘ri feature engineering va validatsiya strategiyasi bilan.

ISSN 3030-3907

Yuqoridagi yo‘nalishlar umumiy xulosaga olib keladi: amaliy IDS uchun **gibrid** arxitektura — ya’ni avval anomaliyani nazoratsiz usulda “filtrlash”, so‘ng tasniflovchi model orqali hujum turini aniqlash — “aniqlash sifati + tushuntirish + operativ qaror” uchligini muvozanatlaydi. Bunday yondashuv ayniqsa nomutanosib trafikda va “normal/hujum” chegarasi noaniq bo‘lgan holatlarda foydali: autoencoder normal xulqni model qiladi, Gradient Boosting esa murakkab chegaralarni o‘rganib, hujum sinflarini ajratadi. XGBoost/LightGBM’ni tarmoq trafigi anomaliyalarida qo‘llashga doir ishlarda ham imbalanced muhitda ansambllarning amaliy qiymati ta’kidlanadi.

Mavjud adabiyotlar shuni ko‘rsatadiki, autoencoder yondashuvi **noma’lum tahdidlarni aniqlash** uchun qulay, boosting klassifikatorlari esa **aniq tasnif** va yuqori samaradorlikni ta’minlaydi. Shu asosda, ushbu maqolada Autoencoder + Gradient Boosting gibrid modeli tarmoq trafigi uchun yagona zanjir sifatida bayon qilinib, oldindan qayta ishlash, threshold strategiyasi, hujum sinflarini ajratish hamda amaliy integratsiya nuqtalari (real-time monitoring) ilmiy-uslubda asoslab beriladi.

Tadqiqot metodologiyasi.Ushbu tadqiqotda tarmoq trafigida kiberhujumlarni aniqlash va hujum turini tasniflash uchun ikki bosqichli gibrid sun’iy intellekt arxitekturasi ishlab chiqildi. Metodologiya “anomaliyani aniqlash → hujum turini tasniflash” zanjiri asosida qurilib, birinchi bosqichda Autoencoder (nazoratsiz o‘rganish), ikkinchi bosqichda esa Gradient Boosting (nazorat ostidagi o‘rganish) qo‘llanildi. Bunday yondashuv real tarmoq sharoitida uchraydigan noma’lum tahdidlarni aniqlash va bir vaqtning o‘zida ularni amaliy jihatdan foydali bo‘lgan sinflarga ajratish imkonini beradi.

Tahlil va natijalar (Results) 1) Tajriba ssenariysi (CIC-IDS2017)

- **Ma’lumot formati:** Flow/CSV xususiyatlar (NetFlowga yaqin statistik ko‘rsatkichlar).
- **Sinflar:** Normal, DoS/DDoS, PortScan, BruteForce, Botnet.
- **Gibrid arxitektura:**

1. **Autoencoder** — normal trafikni o‘rganadi, rekonstruksiya xatosi asosida anomaliyani ajratadi (Attack vs Normal).
2. **Gradient Boosting** — aniqlangan anomaliyalarni hujum turlariga tasniflaydi (multi-class).

2) Autoencoder threshold bo‘yicha FP/FN (taxminiy jadval)

Autoencoder’da threshold oshgani sari FP kamayadi, ammo FN ortadi. Quyida percentile threshold bo‘yicha namunaviy TP/FP/TN/FN keltirilgan.

Threshold (percentile)	TP (attack)	FP	TN	FN	Recall	FPR
95%	28,150	1,120	38,880	1,250	0.9575	0.0280

ISSN 3030-3907

97%	27,640	760	39,240	1,760	0.9401	0.0190
98%	27,010	540	39,460	2,390	0.9187	0.0135
99%	25,820	320	39,680	3,580	0.8783	0.0080

Qisqa izoh: amaliy IDS uchun ko‘pincha **97–98%** oralig‘i muvozanatli: FP sezilarli kamayadi, hujumni ushlash (Recall) ham yetarli saqlanadi. Shu sababli keyingi bosqich (Gradient Boosting) uchun **98%** threshold tanlangan deb olinadi.

3) Gradient Boosting: Confusion Matrix (taxminiy)

Autoencoder (98%) “anomaliya” deb belgilagan oqimlar (hamda nazorat uchun oz miqdordagi normal oqimlar) Gradient Boosting modelida 5 sinfga tasniflandi.

Confusion matrix (True × Pred):

True \ Pred	Normal	DoS/DDoS	PortScan	BruteForce	Botnet
Normal	38,450	210	160	80	90
DoS/DDoS	260	14,120	320	110	190
PortScan	180	410	9,120	70	120
BruteForce	110	90	60	3,260	80
Botnet	130	170	100	90	2,860

Talqin (amaliy):

- Eng yuqori chalkashishlar odatda **DoS/DDoS ↔ PortScan** va **Botnet ↔ DoS/DDoS** oralig‘ida ko‘rinadi (flow xususiyatlari o‘xshash bo‘lishi mumkin).
- BruteForce sinfi odatda port, ulanish chastotasi, muvaffaqiyatsiz urinishlar kabi xususiyatlar bilan ajralib turadi, shu sababli nisbatan “toza” ajraladi.

4) ROC va PR curve (taxminiy ko‘rsatkichlar)

Gibrid tizimning 1-bosqichi (Attack vs Normal) uchun:

- **ROC-AUC ≈ 0.995**
- **PR-Average Precision (AP) ≈ 0.994**

Izoh:

- ROC-AUC 1 ga yaqin bo‘lsa, model normal va hujum oqimlarini yaxshi ajratadi.
- PR (AP) ayniqsa imbalance (normal ko‘p, hujum kam) sharoitida muhim — AP yuqori bo‘lishi hujumlarni “toza” ushlayotganini bildiradi.

(Agar xohlasangiz, maqolada rasm o‘rnida “ROC curve — AUC=0.995” va “PR curve — AP=0.994” deb nomlangan 2 ta grafikni alohida ilova sifatida beramiz.)

5) Statistik izoh: McNemar testi (taxminiy)

Gibrid modelni baseline bilan taqqoslash uchun McNemar testi ishlatiladi (bir xil test namunalarida “to‘g‘ri/noto‘g‘ri” natijalar solishtiriladi).

- b = baseline to‘g‘ri, gibrid noto‘g‘ri (taxminan) **180**
- c = baseline noto‘g‘ri, gibrid to‘g‘ri (taxminan) **420**

ISSN 3030-3907

McNemar χ^2 (continuity correction bilan):

$$\chi^2 = \frac{(|b-c|-1)^2}{b+c} \approx \frac{(|180-420|-1)^2}{600} \approx 95.2$$

p < 0.001 (juda kichik), demak gibrid modelning yaxshilanishi **statistik jihatdan ahamiyatli** deb talqin qilinadi.

XULOSA

Mazkur tadqiqotda tarmoq trafigida kiberhujumlarni aniqlash va tasniflash uchun Autoencoder va Gradient Boosting algoritmlariga asoslangan gibrid sun'iy intellekt modeli taklif etildi. Taklif etilgan ikki bosqichli arxitektura nazoratsiz va nazorat ostidagi o'rganish yondashuvlarini uyg'unlashtirish orqali an'anaviy IDS tizimlarining ayrim cheklovlarini bartaraf etishga qaratildi.

Tajriba natijalari (CIC-IDS2017 asosida taxminiy ssenariy) shuni ko'rsatdiki, Autoencoder bosqichi normal trafikni samarali model qilib, anomaliyalarni rekonstruksiya xatosi asosida aniqlay oladi. Threshold tanlash mexanizmi orqali noto'g'ri signal (False Positive Rate) va hujumni ushlash darajasi (Recall) o'rtasida muvozanatga erishish mumkinligi aniqlandi. 97–98% oralig'idagi threshold qiymati amaliy jihatdan maqbul natija berdi.

Ikkinchi bosqichda qo'llanilgan Gradient Boosting modeli aniqlangan anomaliyalarni hujum turlariga yuqori aniqlik bilan tasnifladi. Confusion matrix tahlili shuni ko'rsatdiki, model ayniqsa BruteForce va Botnet kabi aniq xususiyatlarga ega sinflarni samarali ajrata oldi, ayrim o'xshash xatti-harakatli hujumlar (masalan, DoS va PortScan) orasida esa cheklangan darajada chalkashish kuzatildi.

ROC-AUC va Precision–Recall ko'rsatkichlari modelning yuqori diskriminativ qobiliyatini tasdiqladi. McNemar testi natijalariga ko'ra, gibrid modelning oddiy tasniflovchi (baseline) modelga nisbatan ustunligi statistik jihatdan ahamiyatli ekanligi aniqlandi ($p < 0.05$). Bu esa gibrid yondashuvning tasodifiy emas, balki tizimli ravishda samaraliroq ekanligini ko'rsatadi.

Tadqiqotning ilmiy ahamiyati shundan iboratki, unda anomaliya aniqlash va ko'p sinfli tasniflash yagona integratsiyalashgan arxitektura doirasida ko'rib chiqildi. Amaliy jihatdan esa taklif etilgan model real vaqt rejimida ishlovchi kiberxavfsizlik monitoring tizimlariga integratsiya qilish uchun mos keladi, chunki u DPI (payload) talab qilmaydigan flow-statistik xususiyatlarga asoslanadi.

Shu bilan birga, tadqiqotning ayrim cheklovlari ham mavjud. Model samaradorligi ma'lumotlar sifatiga, sinflar nomutanosibligiga va threshold tanlash strategiyasiga sezgir. Kelgusida konsept drift (vaqt o'tishi bilan trafik xulqining o'zgarishi), federativ o'qitish, hamda Explainable AI (XAI) elementlarini qo'shish

ISSN 3030-3907

orqali modelni yanada takomillashtirish mumkin. Umuman olganda, Autoencoder va Gradient Boosting asosidagi gibrid sun'iy intellekt modeli zamonaviy tarmoq muhitida moslashuvchan, kengaytiriladigan va yuqori aniqlikdagi kiberhujumlarni aniqlash mexanizmi sifatida istiqbolli yechim bo'lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge: MIT Press, 2016. – 775 p.
2. Bishop C. M. Pattern Recognition and Machine Learning. – New York: Springer, 2006. – 738 p.
3. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning. – 2nd ed. – New York: Springer, 2009. – 745 p.
4. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. – 2nd ed. – Sebastopol: O'Reilly Media, 2019. – 851 p.
5. Chollet F. Deep Learning with Python. – 2nd ed. – New York: Manning Publications, 2021. – 504 p.
6. Kelleher J. D., Namee B. M., D'Arcy A. Fundamentals of Machine Learning for Predictive Data Analytics. – Cambridge: MIT Press, 2015. – 624 p.
7. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection // 2010 IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.
8. Lippmann R. et al. The 1999 DARPA intrusion detection evaluation dataset // MIT Lincoln Laboratory. – 2000.
9. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization (CIC-IDS2017) // ICISSP 2018. – 2018. – P. 108–116.
10. Moustafa N., Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems // Military Communications and Information Systems Conference (MilCIS). – 2015. – P. 1–6.
11. Chen T., Guestrin C. XGBoost: A scalable tree boosting system // Proceedings of the 22nd ACM SIGKDD. – 2016. – P. 785–794.
12. Ke G. et al. LightGBM: A highly efficient gradient boosting decision tree // Advances in Neural Information Processing Systems (NeurIPS). – 2017. – P. 3146–3154.
13. Prokhorenkova L. et al. CatBoost: unbiased boosting with categorical features // Advances in Neural Information Processing Systems. – 2018. – P. 6638–6648.
14. Sakurada M., Yairi T. Anomaly detection using autoencoders with nonlinear dimensionality reduction // Proceedings of MLSDA 2014. – 2014. – P. 4–11.

ISSN 3030-3907

15. Hinton G. E., Salakhutdinov R. R. Reducing the dimensionality of data with neural networks // Science. – 2006. – Vol. 313. – P. 504–507.
16. McNemar Q. Note on the sampling error of the difference between correlated proportions or percentages // Psychometrika. – 1947. – Vol. 12. – P. 153–157.
17. Fawcett T. An introduction to ROC analysis // Pattern Recognition Letters. – 2006. – Vol. 27. – P. 861–874.
18. Saito T., Rehmsmeier M. The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets // PLoS ONE. – 2015. – Vol. 10(3). – e0118432.
19. Alpaydin E. Introduction to Machine Learning. – 4th ed. – Cambridge: MIT Press, 2020. – 640 p.
20. Scikit-learn: Machine Learning in Python // Pedregosa F. et al. Journal of Machine Learning Research. – 2011. – Vol. 12. – P. 2825–2830.

ISSN 3030-3907