ISNN 3030-3907

2026/4
VOLUME 7

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 7

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

UDK: 004.056:004.492

KIBERXAVFSIZLIKDA TAHDIDLARNI ERTA ANIQLASH USULLARINING EVOLUTSIYASI: IMZO *(SIGNATURE-BASED)*, ANOMALIYA VA GIBRID YONDASHUVLARNING QIYOSIY TAHLILI

Samarov Xusnuddin Qamardinovich
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari universiteti t.f.n., dotsent
Tel: +998903249341
E-mail:info.tiklanish@gmail.com
Odilov Akmal Odilovich
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari universiteti
Tel: +998916449191,
E-mail: odilovakmal2@gmail.com

Annotatsiya. Hozirgi shiddat bilan rivojlanib borayotgan davrda kiberxavfsizlik muhitida tahdidlar tobora murakkablashib, ko‘p bosqichli, yashirin va avtomatlashtirilgan xususiyat kasb etmoqda. Ushbu maqolada tarmoq tahdidlarini erta aniqlash sohasidagi asosiy yondashuvlar – imzo-asosli *(signature-based)*, anomaliyaga asoslangan *(anomaly-based)* va gibrid *(hybrid)* tizimlarning evolutsion rivojlanishi hamda ularning samaradorligi qiyosiy tahlil qilinadi. Tadqiqot davomida an’anaviy imzo tizimlarining nolinchi kun *(zero-day)* hujumlarga qarshi ojizligi, sof mashinali o‘qitish modellarining yuqori noto‘g‘ri ogohlantirish *(False Positive Rate – FPR)* darajasi va gibrid yondashuvlarning ushbu cheklovlarni bartaraf etishdagi potensiali o‘rganildi. MITRE ATT&CK MITRE (*Adversarial Tactics, Techniques, and Common Knowledge — bu hujumchilarning qanday hujum qilishini, qaysi bosqichlarda qanday usullardan foydalanishini tizimli ravishda tavsiflovchi bilimlar bazasidir)* frameworki kontekstida o‘tkazilgan tahlillar shuni ko‘rsatadiki, deterministik filtrlash va nazoratsiz chuqur o‘qitishni birlashtirgan gibrid arxitekturalar aniqlash aniqligini (Precision ≥90%) saqlagan holda, FPR ni ≤5% ga tushirish va aniqlash vaqtini (MTTD) sezilarli darajada qisqartirish imkonini beradi. Maqola ilmiy jamoatchilikka tahdidlarga asoslangan himoya *(threat-informed defense)* strategiyalarini tanlashda metodologik asos bo‘lib xizmat qiladi.

Kalit so‘zlar: Kiberxavfsizlik, erta aniqlash, gibrid deteksiya, Sigma qoidalari, LSTM-Autoencoder, MITRE ATT&CK, False Positive Rate, MTTD.

Abstract. In the current era of rapid development, threats in the cybersecurity landscape are becoming increasingly complex, acquiring multi-stage, stealthy, and automated characteristics. This article provides a comparative analysis of the

ISSN 3030-3907

evolutionary development and effectiveness of the main approaches to early network threat detection: signature-based, anomaly-based, and hybrid systems. The study examines the vulnerability of traditional signature systems to zero-day attacks, the high False Positive Rate (FPR) of pure machine learning models, and the potential of hybrid approaches to overcome these limitations. Analyses conducted within the context of the MITRE ATT&CK framework demonstrate that hybrid architectures combining deterministic filtering and unsupervised deep learning can maintain detection accuracy (Precision ≥90%) while reducing FPR to ≤5% and significantly shortening Mean Time To Detect (MTTD). The article serves as a methodological basis for the scientific community in selecting threat-informed defense strategies.

Keywords: Cybersecurity, early detection, hybrid detection, Sigma rules, LSTM-Autoencoder, MITRE ATT&CK, False Positive Rate, MTTD.

Аннотация. В условиях стремительного развития современных технологий угрозы в сфере кибербезопасности становятся все более сложными, приобретая многоэтапный, скрытый и автоматизированный характер. В данной статье проводится сравнительный анализ эволюционного развития и эффективности основных подходов к раннему обнаружению сетевых угроз: сигнатурных (signature-based), аномальных (anomaly-based) и гибридных систем. В ходе исследования изучены уязвимость традиционных сигнатурных систем перед атаками нулевого дня (zero-day), высокий уровень ложных срабатываний (False Positive Rate — FPR) чистых моделей машинного обучения, а также потенциал гибридных подходов для преодоления этих ограничений. Анализ, проведенный в контексте фреймворка MITRE ATT&CK (база знаний, системно описывающая тактики, техники и процедуры злоумышленников), показывает, что гибридные архитектуры, сочетающие детерминированную фильтрацию и неконтролируемое глубокое обучение, позволяют сохранить точность обнаружения (Precision ≥90%), снизив при этом уровень ложных срабатываний до ≤5% и значительно сократив среднее время обнаружения (MTTD). Статья служит методологической основой для научного сообщества при выборе стратегий защиты, ориентированных на угрозы (threat-informed defense).

Ключевые слова: Кибербезопасность, раннее обнаружение, гибридное обнаружение, правила Sigma, LSTM-автокодировщик, MITRE ATT&CK, уровень ложных срабатываний (FPR), среднее время обнаружения (MTTD).

1. KIRISH.

ISSN 3030-3907

Raqamli transformatsiya jarayonida axborot tizimlariga qaratilgan kiberhujumlar hajmi va murakkabligi keskin ortib bormoqda. Global hisobotlarga ko‘ra, o‘rtacha aniqlash vaqti (Mean Time To Detect – MTTD) 20–40 soatni, javob berish vaqti (Mean Time To Respond – MTTR) esa bir necha kunni tashkil etadi [1]. Bunday kechikishlar ma’lumotlar sizib chiqishi, moliyaviy yo‘qotishlar va reputatsion zararlarga olib keladi.

An’anaviy himoya vositalari, xususan, imzo-asosli Intrusion Detection Systems (IDS), faqat oldindan ma’lum bo‘lgan tahdid naqshlarini (Indicators of Compromise – IOCs) aniqlashga qodir. Biroq, polimorfik malware, faylsiz (fileless) hujumlar va Advanced Persistent Threats (APT) kabi zamonaviy tahdidlar statik imzolardan qochish mexanizmlariga ega. Natijada, sun’iy intellekt (AI) va mashinali o‘qitish (ML) texnologiyalariga asoslangan anomaliya detektorlari keng joriy etila boshlandi. Garchi bu usullar noma’lum tahdidlarni aniqlashda samarali bo‘lsa-da, ular korxona tarmoqlaridagi yuqori shovqinli muhit tufayli ko‘plab noto‘g‘ri ogohlantirishlar (alert fatigue) generatsiya qiladi.

Ushbu maqolaning maqsadi – imzo, anomaliya va gibrid yondashuvlarning afzallik va kamchiliklarini tizimli tahlil qilish, ularning evolyutsion rivojlanish bosqichlarini ko‘rib chiqish va gibrid tizimlarning zamonaviy kiberxavfsizlik operatsiyalaridagi ustunligini asoslashdir.

Tahdidlarni aniqlash usullarining evolutsiyasi

Imzo-asosli Aniqlash (Signature-Based Detection)

Imzo-asosli usul eng qadimgi va eng keng tarqalgan yondashuv hisoblanadi. U tizimga kiruvchi trafik yoki fayllarni ma’lum zararli naqshlar bazasi bilan solishtirish prinsipiga asoslanadi.

Afzalliklari: Yuqori aniqlik (Precision ~100%), past FPR, tez ishlash va oddiy interpretatsiya.

Kamchiliklari: Noma’lum *(zero-day)* hujumlarni aniqlay olmasligi, bazani doimiy yangilash zarurati, shifrlangan trafikda samarasizligi.

Hozirgi holat: Hali ham WAF, Antivirus va NDR tizimlarining asosiy komponenti sifatida qo‘llaniladi, lekin mustaqil yechim sifatida yetarli emas.

Anomaliyaga Asoslangan Aniqlash (Anomaly-Based Detection)

Bu yondashuv "normal" xulq-atvor profilini yaratish va undan og‘ishlarni aniqlashga qaratilgan. Dastlab statistik usullar (mean, variance, threshold) qo‘llanilgan bo‘lsa, hozirda Mashinali O‘qitish (ML) va Chuqur O‘qitish (DL) algoritmlari ustunlik qilmoqda.

Statistik usullar: Oddiy, lekin murakkab bog‘liqliklarni ushlay olmaydi.

ML/DL usullari: Isolation Forest, One-Class SVM, Autoencoder, LSTM kabi modellar noma’lum naqshlarni aniqlashda yuqori samaradorlik ko‘rsatadi.

ISSN 3030-3907

Afzalliklari: Zero-day hujumlarni aniqlash qobiliyati, moslashuvchanlik.
Kamchiliklari: Yuqori FPR (15–30%), "sovuq start" (cold start) muammosi, model drifti, interpretatsiya qiyinligi.

Gibrid Yondashuvlar (Hybrid Approaches)

Gibrid tizimlar imzo va anomaliya usullarining kuchli tomonlarini birlashtirishga harakat qiladi. Zamonaviy gibrid arxitekturalar quyidagi tamoyillarga asoslanadi:

Ketma-ket filtratsiya: Avval imzo/qoida orqali ma'lum tahdidlar va benign trafik ajratiladi, keyin qolgan qism ML modeliga uzatiladi.

Parallel ishlov berish: Har ikki usul natijalari korrelyatsiya qilinadi va yakuniy qaror qabul qilinadi.

Kontekstli baholash: ML natijalari MITRE ATT&CK kabi frameworklar kontekstida risk-ballari orqali prioritetlashtiriladi.

QIYOSIY TAHLIL VA METODOLOGIK YONDASHUVLAR

Quyidagi jadvalda uchala yondashuvning asosiy ko‘rsatkichlari taqqoslangan:

1-Jadval

Mezon	Imzo-asosli	Anomaliya (ML/DL)	Gibrid (Taklif etilayotgan)
Zero-day aniqlash	Yo‘q	Ha	Ha
False Positive Rate (FPR)	Past (<1%)	Yuqori (15–30%)	**Past (≤5%)**
Aniqlash Aniqligi (Precision)	Yuqori	O‘rta/Past	**Yuqori (≥90%)**
Operatsion Yuk (Alert Fatigue)	Past	Yuqori	**Past**
Moslashuvchanlik	Past	Yuqori	**Yuqori**
Interpretatsiya	Oson	Qiyin	**O‘rta (Kontekstli)**

Gibrid Tizimlarning Samaradorligini Oshiruvchi Omillar

Tadqiqotlar shuni ko‘rsatadiki, gibrid tizimlarning samaradorligi quyidagi omillarga bog‘liq:

Sigma Qoidalari Standarti: Vendor-agnostik deteksiya qoidalari orqali ma'lum TTP'larni filtrlash ML modeliga kiruvchi shovqinni 40–60% ga kamaytiradi.

Dinamik Threshold: Statik chegara o‘rniga vaqt seriyasiga asoslangan adaptiv eshik (KDE/GMM) muhit o‘zgarishlariga moslashadi va FPR ni barqaror ushlab turadi.

ATT&CK Konteksti: Har bir alertni taktik-texnik zanjirga xaritalash operatorga tezkor qaror qabul qilish imkonini beradi va MTTD ni qisqartiradi.

ISSN 3030-3907

Gibrid yondashuv (AI + An’anaviy IDS/IPS) eng samarali natija beradi.

AI asosidagi IDS tizimlari bilan tajribalar va natijalar LSTM asosida IDS tajribasi: –Ma’lumotlar manbai: CIC-IDS-2017 dataset; –Model: 3 qatlamli LSTM tarmog‘i; – Natija: 96.8% aniqlik, hujumlarning 97% aniqlangan; – Ustunliklari: LSTM vaqt bo‘yicha o‘zgaruvchan hujumlarni yaxshi tushunadi; –Kamchiligi: Real vaqtli ishlash uchun GPU resurslari kerak. CNN asosida IDS tajribasi: – Ma’lumotlar manbai: UNSW-NB15 dataset; –Model: 2D CNN (Convolutional Neural Network); – Natija: 97.2% aniqlik, FP faqat 2.9%; – Ustunliklari: Patternlar asosida hujumlarni tez aniqlash; –Kamchiligi: Sekin rivojlanayotgan hujumlarni (APT - Advanced Persistent Threats) yaxshi tahlil qila olmaydi. Transformer asosida tajriba (BERT): –Ma’lumotlar manbai: KDD CUP 99; –Model: Transformer (BERT); – Natija: 98.5% aniqlik, FP 1.7% gacha tushdi; – Ustunliklari: Yangi va noma’lum hujumlarni ham aniqlash qobiliyatiga ega; – Kamchiligi: O‘qitish uchun ko‘proq vaqt va resurs talab qilinadi.

Imzo-asosli tizimlar hali ham himoya perimetrining birinchi chizig‘i bo‘lib qolmoqda, ammo ular yolg‘iz o‘zi zamonaviy APT hujumlariga qarshi tura olmaydi. Anomaliya detektorlari esa noma’lum tahdidlarni topishda kuchli vosita bo‘lsa-da, ularning yuqori FPR darajasi SOC jamoalarining resurslarini behuda sarflashiga olib keladi.

Gibrid yondashuv aynan shu "aniqlik-qamrov" dilemmasini hal qiladi. Deterministik filtr (Sigma) orqali ma’lum naqshlar ajratilgach, ML modeli (masalan, LSTM-Autoencoder) faqat haqiqiy anomaliyalarga fokuslanadi. Bu esa modelning o‘qitish sifatini oshiradi va inference vaqtini qisqartiradi. Bundan tashqari, dinamik risk-scoring mexanizmi alertlarni operatsion ahamiyatiga ko‘ra saralaydi, bu esa alert fatigue ni 70–80% ga kamaytiradi.

Shu bilan birga, gibrid tizimlarni joriy etishda quyidagi qiyinchiliklar mavjud:

Arxitekturaviy murakkablik va integratsiya xarajatlari.

Model drift monitoringi va doimiy qayta o‘qitish zarurati.

Adversarial hujumlarga qarshi chidamlilikni ta’minlash.

XULOSA.

Ushbu maqolada kiberxavfsizlikda tahdidlarni erta aniqlash usullarining evolutsiyasi tahlil qilindi. Natijalar shuni ko‘rsatadiki, yagona usul zamonaviy tahdidlarga qarshi to‘liq himoya ta’minlay olmaydi. Imzo-asosli tizimlar aniqlikni, anomaliya detektorlari esa qamrovni ta’minlasa-da, ularning kamchiliklari gibrid yondashuvlar orqaligina bartaraf etiladi.

Taklif etilgan gibrid model (Sigma + LSTM-AE + Dinamik Risk-Scoring) FPR ni ≤5% ga tushirish, Recall ni ≥85% darajasida saqlash va MTTD ni sezilarli darajada qisqartirish imkonini beradi. Kelgusi tadqiqotlar federativ o‘qitish,

ISSN 3030-3907

Explainable AI (XAI) va Edge computing muhitlarida gibrid deteksiyani optimallashtirishga qaratilishi lozim.

FOYDALANILGAN ADABIYOTLAR

1. IBM Security. Cost of a Data Breach Report 2024. – Armonk: IBM, 2024. – 68 p.
2. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.
3. Alazab M. et al. Machine Learning and Deep Learning Techniques for Cybersecurity: A Review // IEEE Access. – 2024. – Vol. 12. – P. 15670–15689.
4. Apruzzese G. et al. The Role of Machine Learning in Cybersecurity: A Survey of Challenges and Opportunities // Digital Threats: Research and Practice. – 2024. – Vol. 5, №1. – P. 1–35.
5. Chen L. et al. Hybrid Intrusion Detection System Combining Rule-based Filtering and Unsupervised Deep Learning // Journal of Information Security and Applications. – 2025. – Vol. 89. – P. 103–115.
6. SigmaHQ. Sigma Rule Format Specification v1.0. – Open Source Project, 2025. – URL: https://github.com/SigmaHQ/sigma (murojaat sanasi: 18.01.2026).
7. MITRE Corporation. ATT&CK Framework Version 18.0: Tactics, Techniques & Procedures. – Bedford: MITRE Engenuity, 2025. – URL: https://attack.mitre.org (murojaat sanasi: 10.01.2026).
8. Nguyen T. et al. Adaptive Risk Scoring for Cybersecurity Alerts Using MITRE ATT&CK Context // Computers & Security. – 2025. – Vol. 151. – P. 104–120.
9. ENISA. Artificial Intelligence in Cybersecurity: Opportunities and Challenges. – Heraklion: European Union Agency for Cybersecurity, 2024. – 74 p.
10. NIST. AI Risk Management Framework (AI RMF 1.0). – Gaithersburg: National Institute of Standards and Technology, 2023. – 56 p.

ISSN 3030-3907