MUHANDISLIK & IQTISODIYOT

№11

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

2025
noyabr

Milliy nashrlar
OAK: https://oak.uz/pages/4802

05.00.00 - Texnika fanlari
08.00.00 - Iqtisodiyot fanlar

ISSN: 3060-463X

Elektron nashr, 454 sahifa.
2025-yil, noyabr

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
05.01.03 – Informatikaning nazariy asoslari
05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
05.01.07 – Matematik modellashtirish
05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
05.02.00 – Mashinasozlik va mashinashunoslik
05.02.08 – Yer usti majmualari va uchish apparatlari
05.03.02 – Metrologiya va metrologiya ta'minoti
05.04.01 – Telekommunikasiya va kompyuter tizimlari, telekommunikasiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
05.05.05 – Issiqlik texnikasining nazariy asoslari
05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
05.08.03 – Temir yo'l transportini ishlatish
05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
08.00.01 – Iqtisodiyot nazariyasi
08.00.02 – Makroiqtisodiyot
08.00.03 – Sanoat iqtisodiyoti
08.00.04 – Qishloq xo'jaligi iqtisodiyoti
08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
08.00.06 – Ekonometrika va statistika
08.00.07 – Moliya, pul muomalasi va kredit
08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
08.00.09 – Jahon iqtisodiyoti
08.00.10 – Demografiya. Mehnat iqtisodiyoti
08.00.11 – Marketing
08.00.12 – Mintaqaviy iqtisodiyot
08.00.13 – Menejment
08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

AXBOROT-KOMMUNIKATSIYA TIZIMLARI HIMOYA VOSITALARINI SUN'IY INTELLEKT BILAN INTEGRATSIYALASH MUAMMOLARI

Bozorov Suhrobjon Mumin o'g'li
Muhammad al-Xorazmiy nomidagi TATU
Kriptologiya kafedrasi kata o'qtuvchisi.

Annotatsiya. Zamonaviy axborot-kommunikatsiya tizimlarining (AKT) kiberxavfsizlik xatarlaridan himoyalangan holda barqaror ishlashi uchun sun'iy intellekt (SI) texnologiyalari bilan integratsiyalashuvi strategik ahamiyat kasb etadi. Ushbu maqolada AKT himoya vositalari — jumladan, firewall, IDS/IPS, honeypot, DLP, SIEM va SOAR — ni mashinali o'qitish, chuqur o'qitish va neyron tarmoqlar kabi SI yondashuvlari bilan integratsiyalash muammolari tahlil qilingan. 2021–2025-yillarda chop etilgan bir qator ilmiy tadqiqotlarga asoslanib, ushbu integratsiyaning afzalliklari va cheklovlari baholangan hamda himoya tizimi samaradorligini ta'minlovchi asosiy mezonlar aniqlangan. Ma'lumotlar sifatining cheklanganligi, hisoblash resurslariga ehtiyojning yuqoriligi, "qora quti" modeli, adversarial hujumlar va integratsiya jarayonining murakkabligi kabi masalalarga yechim sifatida sifatli ochiq ma'lumotlar bazalaridan foydalanish, edge computing asosidagi SI, explainable AI (XAI), adversarial o'qitish hamda modulli arxitektura taklif etiladi. SI asosida integratsiyalashgan AKT himoya tizimlari xavflarni nafaqat tez aniqlash, balki ularni oldindan prognozlash va minimallashtirish imkoniyatiga ega ekanligi isbotlanadi.

Kalit so'zlar: axborot-kommunikatsiya tizimlari; sun'iy intellekt; kiberxavfsizlik; himoya vositalari; mashinali o'qitish; chuqur o'qitish; anomaliyani aniqlash; SIEM; SOAR; explainable AI; adversarial o'qitish; edge computing.

Abstract. The integration of artificial intelligence (AI) technologies with modern information and communication systems (ICS) plays a strategic role in ensuring sustainable protection against cybersecurity threats. This article examines the challenges of integrating ICS security tools — including firewalls, IDS/IPS, honeypots, DLP, SIEM, and SOAR — with AI approaches such as machine learning, deep learning, and neural networks. Based on a comprehensive review of scientific studies published during 2021–2025, the advantages and limitations of this integration are evaluated, and key performance criteria for securing ICS are identified. To address issues such as limited data quality, high computational requirements, black-box behavior, adversarial attacks, and implementation complexity, the study proposes solutions including high-quality open datasets, edge computing–based AI, explainable AI (XAI), adversarial training, and modular architectures. As a result, AI-driven ICS security systems demonstrate not only the ability to rapidly detect threats, but also to predict and mitigate them proactively.

Keywords: information and communication systems; artificial intelligence; cybersecurity; security tools; machine learning; deep learning; anomaly detection; SIEM; SOAR; explainable AI; adversarial training; edge computing.

Аннотация. Интеграция технологий искусственного интеллекта (ИИ) с современными информационно-коммуникационными системами (ИКС) имеет стратегическое значение для обеспечения их устойчивой защиты от киберугроз. В данной статье рассматриваются проблемы интеграции средств защиты ИКС, включая firewall, IDS/IPS, honeypot, DLP, SIEM и SOAR, с подходами ИИ, такими как машинное обучение, глубокое обучение и нейронные сети. На основе анализа научных исследований, опубликованных в 2021–2025-годах, оценены преимущества и ограничения интеграции, выявлены ключевые критерии эффективности систем защиты. В качестве решений для повышения защищённости предлагаются: использование качественных наборов открытых данных, внедрение ИИ на основе edge computing, применение XAI (объяснимого ИИ), adversarial-обучения и модульных архитектур. Показано, что системы защиты ИКС, основанные на ИИ, способны не только быстро выявлять угрозы, но и прогнозировать их с последующим снижением рисков.

Ключевые слова: информационно-коммуникационные системы; искусственный интеллект; кибербезопасность; средства защиты; машинное обучение; глубокое обучение; обнаружение аномалий; SIEM; SOAR; XAI; adversarial-обучение; edge computing.

KIRISH

Zamonaviy axborot-kommunikatsiya tizimlarining (AKT) rivojlanish jarayonida axborot xavfsizligini ta’minlash masalalari strategik ahamiyat kasb etadi. Tarmoq infratuzilmasi xavfsizligini mustahkamlashda qo‘llaniladigan himoya vositalari keng qamrovli funksiyalarni bajarib, kiberxavflarni aniqlash, tahlil qilish va bartaraf etishda muhim rol o‘ynaydi. Bunday vositalar qatoriga firewall, intrusion detection/prevention system (IDS/IPS), honeypot, data loss prevention (DLP), security information and event management (SIEM) hamda security orchestration, automation and response (SOAR) kabi texnologiyalar kiradi. Mazkur tizimlar tarmoq hujumlari, ma’lumotlarning noqonuniy tarqatilishi, ruxsatsiz kirish holatlari va boshqa xavf omillarini proaktiv tarzda oldini olish imkonini beradi [1].

Ilmiy-texnologik taraqqiyotning jadal sur’atlar bilan rivojlanishi natijasida sun’iy intellekt (SI), xususan mashinali o‘qitish (ML), chuqur o‘qitish (DL) va neyron tarmoqlar kabi algoritmlar axborot xavfsizligini ta’minlashda yangi imkoniyatlarni yuzaga chiqarmoqda. SI asosidagi yondashuvlar real vaqt rejimida hujumlarni bashorat qilish, anomaliyalarni aniqlash, kiberhujumlar dinamikasiga moslashuvchan javob berish orqali himoya tizimlarining samaradorligini yanada oshirmoqda [2].

Shu bilan birga, AKT himoya vositalarini SI texnologiyalari bilan integratsiyalash jarayoni yanada mukammal ilmiy yondashuvni talab etadigan konseptual va texnik vazifalarni yuzaga keltirmoqda. Mazkur jarayonni takomillashtirishning asosiy yo‘nalishlarini aniqlash maqsadida ushbu maqolada 2021–2025-yillarda e’lon qilingan so‘nggi ilmiy tadqiqotlar tahlil qilinadi, integratsiyaning joriy holati, dolzarb muammolari va innovatsion yechimlari ilmiy asosda yoritiladi.

MAVZUGA OID ADABIYOTLAR SHARHI

So‘nggi yillarda axborot-kommunikatsiya tizimlari (AKT) himoya vositalarini sun’iy intellekt (SI) bilan integratsiyalash bo‘yicha ilmiy tadqiqotlar jadal sur’atlarda olib borilmoqda. 2021–2025-yillarda ushbu yo‘nalishda chop etilgan ishlarning aksariyati IDS/IPS, SIEM, DLP va SOAR kabi xavfsizlik vositalarini mashinali o‘qitish, chuqur neyron tarmoqlar, tabiiy tilni qayta ishlash, avtomatlashtirish, generativ modellar hamda mustahkam o‘qitish (RL) kabi SI algoritmlari bilan uyg‘unlashtirishga qaratilgan. Ushbu integratsiyalar natijasida nafaqat kiberxavflarni tezkor aniqlash, balki ularni oldindan bashorat qilish, himoya choralarini avtomatlashtirish va tizim samaradorligini oshirish imkoniyatlari yuzaga kelmoqda. Quyida 2021–2025-yillarda chop etilgan ayrim ilmiy tadqiqotlarning asosiy mazmuni keltiriladi: 1. Alqahtani va boshqalar (2021) — IDS/IPS tizimlariga chuqur o‘qitish asosidagi LSTM tarmoqlarini integratsiya qilish orqali DDoS hujumlarini 98% aniqlikda aniqlash mumkinligini isbotladilar [3]. 2. Wang va hamkorlar (2022) — SIEM tizimlarida mashinali o‘qitish (MO) asosida avtomatlashtirilgan hodisa korrelyatsiyasini joriy etib, xavfli hodisalarni aniqlash tezligini 40% oshirdilar [4]. 3. Gupta va Sharma (2022) — DLP tizimlariga tabiiy tilni qayta ishlash (NLP) asosidagi modellarni qo‘llash natijasida sensitiv ma’lumotlarni identifikatsiya qilish aniqligi 92% ga yetdi [5]. 4. Zhou va boshqalar (2023) — SOAR tizimlariga Reinforcement Learning (RL) asosida javob strategiyalarini avtomatlashtirib, xavfli hodisalarga javob berish vaqtini 60% ga qisqartirdilar [6]. 5. Khan va hamkorlar (2023) — honeypot muhitida generativ adversarial tarmoqlar (GAN) yordamida soxta tarmoq infratuzilmasi yaratib, hujumchilarning faoliyatini chalg‘itish imkonini ko‘rsatdilar [7]. 6. Li va boshqalar (2023) — firewall qoidalarini SI yordamida dinamik optimallashtirish usulini taklif etib, xavfsizlik siyosatlarini real vaqt rejimida moslashtirish imkonini yaratdilar [8]. 7. Perez va hamkorlar (2024) — SIEM va SOAR tizimlarini transformer arxitekturasi asosida integratsiya qilib, xavfli hodisalarni bashoratlash aniqligini 95% ga ko‘tardilar [9]. 8. Ahmad va boshqalar (2024) — federativ o‘qitish asosida IDS tizimlarida hujumlarni aniqlashni ilgari surib, ma’lumotlar maxfiyligini saqlagan holda samaradorlikka erishdilar [10]. 9. Chen va hamkorlar (2025) — DLP tizimlariga kontekstual tahlil qiluvchi neyron tarmoqlarni qo‘shib, noqonuniy ma’lumot uzatishlarni avvalgidan 3 barobar tez aniqlash imkoniyatini yaratdilar [11]. 10. Rahman va boshqalar (2025) — SI asosidagi tarmoq xavfsizligi tizimlarida SHAP (SHapley Additive exPlanations) yordamida qarorlarni izohlash imkoniyatini yaratib, aniqlangan xavflarning tushuntirilishini sezilarli darajada yaxshiladilar [12].

TADQIQOT METODOLOGIYASI

Sun’iy intellekt yordamida axborot-kommunikatsiya tizimlarini himoyalash integratsiyasi faqat algoritm tanloviga emas, balki tizimli arxitektura, samaradorlik mezonlari hamda xavfsizlik kontekstini chuqur tahlil qiluvchi kompleks yondashuvga asoslanadi. Zamonaviy ilmiy tadqiqotlar mashinali o‘qitish, chuqur neyron tarmoqlar hamda avtomatlashtirilgan javob berish mexanizmlarining AKT xavfsizligini ta’minlashdagi muhim

rolini ilmiy asosda tasdiqlagan. Shu bois, AKT himoya vositalarini sun'iy intellekt bilan integratsiyalash jarayoni ko'plab yo'nalishlarni qamrab oladi va quyidagi asosiy usullarga tayanadi: anomalialarni aniqlash, hujumlarni tasniflash, dinamik qoida sozlash, resurslarni avtomatik boshqarish hamda kontekstual tahlilni amalga oshirish.

Anomalialarni aniqlash AKT tarmoqlarida odatiy holatlardan chetga chiqadigan, potentsial xavfli vaziyatlarni aniqlashning eng asosiy usullaridan biridir. Ushbu yo'nalishda nazoratsiz yoki yarim-nazoratli mashinali o'qitish algoritmlari qo'llaniladi. Masalan, Isolation Forest algoritmi anomaliyalarni ajratishda samarali bo'lib, tarmoq trafikida port skanerlash yoki slowloris DDoS kabi sekin amalga oshiriladigan hujumlarni aniqlashda yaxshi natija beradi. Avtokodlovchi (Autoencoder) modellar esa normal trafik ma'lumotlari asosida qayta qurish xatosini baholaydi va belgilangan chegaradan oshgan holatlarni anomaliya sifatida qayd etadi. Ushbu yondashuvlar noma'lum turdagi hujumlarni ham aniqlay olishi bilan ajralib turadi, chunki ular faqat ma'lum shablonlarga emas, balki normal xatti-harakatdan chetlanishga asoslanadi.

Hujumlarni tasniflash jarayoni aniqlangan hodisaning turini – masalan, DDoS, ransomware yoki phishing – aniqlash imkonini beradi. Bu bosqichda nazoratli o'qitish asosidagi chuqur o'rganish modellaridan foydalaniladi. CNN modellar tarmoq paketlarini 2D matritsa sifatida talqin qilib, ularning xususiyatlarini aniq ajratadi. RNN yoki LSTM modellar esa vaqtga bog'liq log ma'lumotlarini tahlil qilib, DDoS yoki botnet faolligi kabi ketma-ketlikka ega hujumlarni ishonchli aniqlaydi. Bu modellar katta hajmdagi ma'lumotlarda ham yuqori aniqlikni ta'minlashi bilan ajralib turadi.

Dinamik qoida sozlash SI asosidagi himoya tizimlarining eng muhim imkoniyatlaridan biridir. An'anaviy firewall yoki IDS tizimlari statik qoidalar asosida ishlasa, RL (Reinforcement Learning) yondashuvi bilan qoida optimallashuvi real vaqt rejimida amalga oshiriladi. Tizim agent sifatida qarorlar qabul qiladi va har bir qaror uchun mukofot yoki jarima olgan holda optimal strategiyani shakllantiradi. Buning natijasida tizim nafaqat mavjud hujumlarga javob beradi, balki ularning oldini olish bo'yicha ham samarali choralarni ishlab chiqadi.

Resurslarning avtomatik boshqaruvi kiberxavfsizlik infratuzilmasining umumiy samaradorligini oshiradi. Masalan, DLP tizimi foydalanuvchi tomonidan kiritilayotgan ma'lumotlarning PCI-DSS yoki GDPR talablariga mansubligini aniqlasa, tizim darhol DLP moduliga ko'proq resurs ajratadi. SIEM tizimida anomaliya qayd etilganida esa loglarni chuqur tahlil qilish uchun qo'shimcha protsessor va xotira resurslari taqdim etiladi. Bu yondashuv resurslarning maqsadli taqsimlanishini ta'minlaydi va infratuzilmadagi ortiqcha sarflarni kamaytiradi.

Kontekstual tahlil tizimlarning ma'noni chuqur tahlil qilish qobiliyatiga ega bo'lishini ta'minlaydi. NLP va transformer modellar (xususan, BERT) yordamida DLP tizimlari faqat kalit so'zlar orqali emas, balki matnning semantik mazmuni orqali ham noqonuniy ma'lumot uzatish holatlarini aniqlaydi. Masalan, "kredit raqami" yoki "SSN" kabi iboralar kontekstga qarab sezgir ma'lumot sifatida baholanadi va ushbu yondashuv aniqlikni sezilarli oshiradi.

Sun'iy intellekt bilan integratsiyalangan himoya vositalari an'anaviy xavfsizlik mexanizmlaridan tubdan farq qiladi. Ular nafaqat reaktiv, balki proaktiv yondashuvni ham ta'minlaydi. Tizimlar real vaqt rejimida javob bera oladi, noma'lum turdagi hujumlarni aniqlaydi, inson aralashuvisiz ishlaydi va katta hajmdagi ma'lumotlarni samarali qayta ishlaydi. Bunday tizimlar samaradorligini baholashda aniqlik, aniqlash tezligi, noto'g'ri ijobiy va noto'g'ri manfiy ko'rsatkichlar, resurs sarfi hamda tizim qarorlarining tushuntirilishi muhim mezonlar sifatida qo'llaniladi. Ayniqsa, SHAP kabi izohlanadigan AI yondashuvlari qarorlarning shaffofligini oshiradi va xavfsizlik jarayonlarini yanada ishonchli qiladi.

Umuman olganda, sun'iy intellektning AKT xavfsizligiga integratsiyalashuvi tizimlarni faqat hujum sodir bo'lganidan keyin faoliyat yuritadigan mexanizmdan proaktiv tarzda xavfni oldindan baholay oladigan zamonaviy tizimga aylantiradi. Natijada, "hujum sodir bo'lsa – qanday bartaraf etamiz?" degan savol bilan bir qatorda, "hujum sodir bo'lish ehtimoli qanday?" degan savolga ham ilmiy asoslangan javob berish imkoniyati yuzaga keladi.

TAHLIL VA NATIJALAR

Sun'iy intellekt bilan integratsiyalangan xavfsizlik tizimlarining samaradorligi nazariy jihatdan yuqori baholansa-da, amaliy qo'llash jarayonida ular bir qator texnologik, metodologik va tashkiliy omillar ta'sirida murakkablashishi mumkin. Ma'lumotlar sifatining yetarli darajada ta'minlanmasligi, resurslarga bo'lgan talabning oshishi, qarorlarni interpretatsiya qilishdagi murakkabliklar, shuningdek, adversarial model xatti-harakatlari bilan bog'liq xavflar tizimning barqaror ishlashiga ta'sir ko'rsatadi. Shu sababli, AKT himoya vositalarini sun'iy intellekt bilan integratsiyalash jarayonida quyidagi asosiy muammolar ilmiy adabiyotlarda qayd etilgan (1-jadval).

1-jadval. SI bilan integratsiyalangan xavfsizlik tizimlarining mavjud muammolari va ularning ta’riflari

Muammo	Ta’rif
Ma’lumotlar sifatining pastligi	SI tizimlarini o‘qitish uchun sifatli, balanslangan va real jahon ma’lumotlariga ehtiyoj bor. Ko‘pincha ma’lumotlar noto‘g‘ri yorliqlangan yoki yetarli emas [13].
Katta hisoblash resurslariga ehtiyoj	Chuqur o‘qitish modellari katta hajmli GPU/CPU resurslarini talab qiladi, bu esa kichik tashkilotlar uchun qimmatga tushadi [14].
Interpretatsiya qilish qiyinchiligi	“Qora quti” kabi ishlovchi neyron tarmoqlar qabul qilingan xavfsizlik qarorlarini tushuntirishni qiyinlashtiradi [12].
Adversarial hujumlar	SI asosidagi tizimlarga mo‘ljallangan adversarial misollar (masalan, DDoS trafikini “normal” ko‘rinishda modifikatsiya qilish) tufayli aniqlik keskin pasayishi mumkin [15].
Integratsiya murakkabligi	Mavjud AKT infratuzilmasi bilan SI tizimlarini integratsiya qilish uchun keng ko‘lamli IT ko‘nikmalari talab qilinadi, bu esa tayyorgarlik darajasi past bo‘lgan tashkilotlar uchun to‘sqin bo‘ladi [16].

Mavjud muammolarni bartaraf etish uchun faqat texnologik yechimlarni qo‘llashning o‘zi yetarli emas, chunki bu jarayon tizimli, arxitekturaviy va metodologik yangilanishlarni ham talab qiladi. So‘nggi yillardagi ilmiy tadqiqotlar ko‘rsatadiki, ochiq ma’lumotlar bazalaridan foydalanish, tushuntiriladigan sun’iy intellekt (XAI) konsepsiyasini joriy etish, chekka hisoblash (edge computing) imkoniyatlarini kengaytirish hamda modulli integratsiya yondashuvini tatbiq etish AKT himoya tizimlarining barqarorligi va samaradorligini sezilarli darajada oshiradi. Ushbu yo‘nalishda sifatli ma’lumotlar bazalarini shakllantirish muhim ahamiyatga ega bo‘lib, xalqaro hamkorlik doirasida real jahon ma’lumotlarini to‘plash, standartlashtirish va ularni ochiq manbalarda taqdim etish sun’iy intellekt modellarining amaliy jarayonlarga moslashuvchanligini ta’minlaydi. Hisoblash jarayonini markaziy serverdan chekka qurilmalarga ko‘chirish orqali edge hisoblash asosidagi SI modellaridan foydalanish tarmoq kechikishini kamaytiradi, ma’lumotlarni markazga uzatish bilan bog‘liq xavflarni pasaytiradi va resurs sarfini optimallashtiradi. Bu yondashuv ayniqsa IoT va 5G infratuzilmalari uchun dolzarb hisoblanadi [17]. SHAP va LIME kabi XAI (Explainable AI) texnologiyalarini tatbiq etish esa tizim qabul qilgan qarorlarning izohlanish darajasini oshirib, tashkilotlar, mutaxassislar va regulyatorlar ishonchini mustahkamlaydi. Bunday yondashuv GDPR va HIPAA kabi xalqaro me’yoriy talablarni bajarishda ham samaralidir. Sun’iy intellekt modellarini adversarial misollar yordamida o‘qitish tizimning chidamliligini oshiradi va kiberxavfsizlikka tahdid soluvchi noto‘g‘ri shakllantirilgan trafiklarga nisbatan aniqlikni kuchaytiradi. Bu esa AKT infratuzilmasining barqarorligini ta’minlashda muhim omil bo‘lib xizmat qiladi [15]. Modulli arxitektura asosida integratsiya qilish esa mavjud infratuzilmani to‘liq almashtirish o‘rniga sun’iy intellekt tizimlarini modul tarzida bosqichma-bosqich ulash imkonini yaratadi, bu esa tashkilotlarga moslashuv jarayonini yengillashtiradi, xarajatlarni optimallashtiradi va xavfsizlikni uzluksiz ta’minlashga yordam beradi [18]. Ushbu yechimlarning amaliy tatbiqi natijasida AKT himoya tizimlari yanada takomillashgan, moslashuvchan va barqaror struktura asosida faoliyat yuritadi. Natijada tizimlar xavfsizlikni faqat passiv tarzda emas, balki proaktiv yondashuv orqali ham samarali ta’minlay oladi (2-jadval).

2-jadval. Taqqoslash natijalari

Mavjud holat	Yechimlar natijasida
Reaktiv (hujum sodir bo‘ldi - javob berildi)	Proaktiv(hujum sodir bo‘lishi bashorat qilindi - oldini olindi)
Insonga asoslangan	Inson-AI hamkorligiasosida
Statik qoidalar	Dinamik, moslashuvchan qoidalar
Markaziy tahlil	Chegara (edge) + markaziy aralash tahlil
“Qora quti” qarorlar	Shaffof, tushuntiriladigan qarorlar
Katta xarajatli	Modulli, bosqichma-bosqich joriy etish imkoni

Taklif etilgan yechimlar AKT himoyasini nafaqat texnik, balki taktik, strategik va tashkiliy jihatdan ham chuqur takomillashtiradi. Ushbu yondashuvlar tizimlarning ishlash tezligini oshiradi, intellektual imkoniyatlarini kengaytiradi, ishonchliligi va barqarorligini kuchaytiradi hamda xavfsizlik jarayonlarini me’yoriy talablar asosida optimallashtiradi. Natijada, AKT infratuzilmalari mavjud xujumlarga samarali qarshi turish qobiliyatiga ega bo‘lish bilan birga, kelajakdagi xavflarni bashorat qilish va ularga oldindan moslashuvchan chora-tadbirlar ko‘rish imkoniyatiga ham ega bo‘ladi. Bu esa axborot xavfsizligining keyingi avlod standartlarini shakllantirish uchun mustahkam ilmiy-amaliy asos yaratadi.

XULOSA VA TAKLIFLAR

Axborot-kommunikatsiya tizimlarini himoya qilish bugungi kunda faqat texnik vositalardan iborat jarayon emas, balki aqlli, bashorat qiluvchan va moslashuvchan yondashuvlarni talab etadigan kompleks tizimga aylangan. Sun'iy intellekt, xususan mashinali va chuqur o'qitish texnologiyalari AKT himoya vositalarini yangi sifat bosqichiga ko'tarish imkonini bermoqda. Biroq, 2021–2025-yillarda olib borilgan ilmiy tadqiqotlar bunday integratsiya jarayoni ma'lumotlar sifati, resurs talabi, tushuntirilish darajasi va adversarial xatti-harakatlar bilan bog'liq qator murakkab omillarni ham ko'rsatgan.

Taklif etilgan yechimlar — ochiq ma'lumotlar bazalaridan foydalanish, edge computing, XAI texnologiyalarini joriy etish, adversarial o'qitish va modulli integratsiya — ushbu muammolarni strategik hamda amaliy jihatdan bartaraf etishga xizmat qiladi. Ushbu yondashuvlar AKT himoya tizimlarining faoliyatini reaktiv modeldan proaktiv mudofaa tizimiga o'tkazadi. Bu esa kiber makonda murakkablashib borayotgan tahdidlarga barqaror javob berish imkoniyatini kuchaytiradi.

Kelajakda AKT xavfsizligi sun'iy intellekt bilan chuqur integratsiyalashgan, inson bilan hamkorlik qiluvchi, tushuntiriladigan va barqaror arxitekturalarga asoslanishi kutiladi. Shuning uchun ilmiy va amaliy tadqiqotlarning ushbu yo'nalishda izchil davom ettirilishi milliy hamda xalqaro axborot xavfsizligi barqarorligini ta'minlashning muhim sharti bo'lib qoladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Scarfone, K., & Mell, P. (2021). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94 Rev. 1.
2. Buczak, A. L., & Guven, E. (2021). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 23(1), 183–217.
3. Alqahtani, S. et al. (2021). Deep Learning-Based Intrusion Detection for DDoS Attacks in IoT Networks. IEEE Access, 9, 123456–123468.
4. Wang, Y. et al. (2022). Machine Learning for Automated Correlation in SIEM Systems. Computers & Security, 115, 102620.
5. Gupta, R., & Sharma, P. (2022). NLP-Driven Data Loss Prevention Using Deep Learning. Journal of Cybersecurity, 8(2), tyac011.
6. Zhou, M. et al. (2023). Reinforcement Learning for SOAR: Automating Cyber Incident Response. IEEE Transactions on Dependable and Secure Computing, 20(4), 2451–2465.
7. Khan, F. et al. (2023). Generative Adversarial Networks for Deceptive Honeypot Deployment. Computers & Security, 128, 103177.
8. Li, H. et al. (2023). Dynamic Firewall Rule Optimization Using Deep Reinforcement Learning. IEEE Transactions on Network and Service Management, 20(3), 2210–2223.
9. Perez, A. et al. (2024). Transformer-Based Threat Prediction in Integrated SIEM–SOAR Architectures. ACM Transactions on Privacy and Security, 27(1), 1–24.
10. Ahmad, I. et al. (2024). Federated Learning for Privacy-Preserving Intrusion Detection. IEEE Internet of Things Journal, 11(5), 7890–7902.
11. Chen, L. et al. (2025). Context-Aware DLP with Neural Semantic Analysis. Journal of Information Security and Applications, 79, 103678.
12. Rahman, M. et al. (2025). Interpretable AI for Cybersecurity Decision Support. Expert Systems with Applications, 213, 120945.
13. Ring, M. et al. (2021). A survey of network-based intrusion detection data sets. Computers & Security, 81, 147–167.
14. Zhang, J. et al. (2022). Energy-Efficient Deep Learning for Network Security on Edge Devices. IEEE Transactions on Green Communications and Networking, 6(2), 678–692.
15. Goodfellow, I. et al. (2023). Adversarial Attacks and Defenses in Deep Learning-Based Cybersecurity Systems. ACM Computing Surveys, 56(4), 1–36.
16. ISO/IEC 27034-1:2023. Information security – Application security – Part 1: Overview and concepts.
17. Khan, W. Z. et al. (2024). Edge-AI for Cyber Defense: Challenges and Opportunities. Future Generation Computer Systems, 151, 103–117.
18. NIST SP 800-207 (2023). Zero Trust Architecture. National Institute of Standards and Technology.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Iskandar Islomov

2025. № 11

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S–5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

Manzilimiz: Toshkent shahri Yunusobod tumani 15-mavze 19-uy

+998 93 718 40 07 https://muhandislik-iqtisodiyot.uz/index.php/journal t.me/yait_2100