ISNN 3030-3907

2026
JUNE
ISSUE - 6
VOLUME -8

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

IYUN 2026
Issue - 6, VOLUME – 8

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.

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

O‘ZBEKISTONDA RAQAMLI TRANSFORMATSIYA JARAYONLARIDA KIBERXAVFSIZLIK MUAMMOLARI VA ULARNI HAL ETISHDA SUN`IY INTELLEKT TEXNOLOGIYALARIDAN FOYDALANISH

Salimov Nurali Ramazon o`g`li
Toshkent Davlat Iqtisodiyot universiteti davlat muassasasi tayanch doktoranti

Annotatsiya. Mazkur maqolada O‘zbekistonda raqamli transformatsiya jarayonlarida yuzaga kelayotgan kiberxavfsizlik muammolari hamda ularni bartaraf etishda sun’iy intellekt texnologiyalarining imkoniyatlari tahlil qilingan. Raqamli infratuzilmaning kengayishi natijasida axborot tizimlariga qaratilgan tahdidlar soni va murakkabligi ortib borayotgani asoslab berilgan. Xalqaro va mahalliy ilmiy adabiyotlar asosida mashinaviy o‘qitish, chuqur o‘rganish, xulq-atvor tahlili va avtomatlashtirilgan xavfsizlik platformalarining kiberhujumlarni aniqlash hamda oldini olishdagi samaradorligi baholangan. Shuningdek, O‘zbekiston sharoitida sun’iy intellekt asosidagi kiberxavfsizlik tizimlarini joriy etish istiqbollari, mavjud muammolar va rivojlantirish yo‘nalishlari yoritilgan. Tadqiqot natijalari milliy raqamli ekotizim barqarorligini ta’minlash va zamonaviy axborot xavfsizligi mexanizmlarini takomillashtirish uchun ilmiy-amaliy ahamiyatga ega.

Kalit so‘zlar: kiberxavfsizlik, transformatsiya, intellekt, algoritm, monitoring, autentifikatsiya, tahdid, himoya, avtomatlashtirish, prognozlash.

Аннотация. В данной статье исследуются проблемы кибербезопасности, возникающие в процессе цифровой трансформации Узбекистана, а также возможности использования технологий искусственного интеллекта для их решения. Обосновано, что расширение цифровой инфраструктуры сопровождается ростом количества и сложности киберугроз, направленных на информационные системы. На основе анализа международных и отечественных научных исследований рассмотрена эффективность методов машинного обучения, глубокого обучения, анализа поведения пользователей и автоматизированных платформ безопасности при обнаружении и предотвращении кибератак. Кроме того, определены перспективы внедрения систем кибербезопасности на основе искусственного интеллекта в условиях Узбекистана, существующие проблемы и направления их дальнейшего развития. Полученные результаты имеют научно-практическое значение для повышения устойчивости национальной цифровой экосистемы и совершенствования механизмов информационной безопасности.

Ключевые слова: кибербезопасность, трансформация, интеллект, алгоритм, мониторинг, аутентификация, угроза, защита, автоматизация, прогнозирование.

ISSN 3030-3907

Abstract. This article examines cybersecurity challenges emerging during the digital transformation of Uzbekistan and explores the potential of artificial intelligence technologies for addressing these issues. The expansion of digital infrastructure has significantly increased both the number and complexity of cyber threats targeting information systems. Based on international and national scientific literature, the study evaluates the effectiveness of machine learning, deep learning, behavioral analytics, and automated security platforms in detecting and preventing cyberattacks. Furthermore, the paper discusses the prospects of implementing AI-based cybersecurity systems in Uzbekistan, identifies existing challenges, and outlines future development directions. The findings contribute to strengthening the resilience of the national digital ecosystem and improving modern information security mechanisms through intelligent technologies.

Keywords: cybersecurity, transformation, intelligence, algorithm, monitoring, authentication, threat, protection, automation, prediction.

KIRISH.

So‘nggi yillarda dunyo miqyosida raqamli iqtisodiyotning jadal rivojlanishi, davlat boshqaruvi, moliya, sog‘liqni saqlash, ta’lim va sanoat tarmoqlarining raqamlashtirilishi axborot-kommunikatsiya texnologiyalarining jamiyat hayotidagi o‘rnini tubdan o‘zgartirdi. Mazkur jarayonlar bilan bir qatorda kiberxavfsizlik masalalari ham strategik ahamiyat kasb etib, axborot resurslari, ma’lumotlar bazalari va raqamli infratuzilmani turli xil kiberhujumlardan himoya qilish dolzarb vazifalardan biriga aylandi. Zamonaviy axborot tizimlarining murakkablashuvi, bulutli texnologiyalar, IoT qurilmalari, 5G tarmoqlari va katta hajmdagi ma’lumotlar almashinuvining kengayishi kiberjinoyatchilik usullarining ham takomillashishiga olib kelmoqda. Natijada an’anaviy himoya mexanizmlari murakkab va tez o‘zgaruvchan tahdidlarga qarshi yetarli samaradorlikni ta’minlay olmayotgani ilmiy tadqiqotlarda keng e’tirof etilmoqda. O‘zbekistonda ham raqamli transformatsiya davlat siyosatining ustuvor yo‘nalishlaridan biri sifatida qaralmoqda. Davlat xizmatlarini elektron shaklga o‘tkazish, elektron hukumat tizimlarini rivojlantirish, raqamli bank xizmatlari, elektron tijorat platformalari hamda sanoatda Industry 4.0 elementlarini joriy etish bo‘yicha amalga oshirilayotgan islohotlar axborot tizimlari sonining keskin ortishiga sabab bo‘lmoqda. Shu bilan birga, mazkur tizimlarning xavfsizligini ta’minlash, shaxsiy ma’lumotlarni himoya qilish, davlat axborot resurslarining uzluksiz ishlashini kafolatlash va milliy kiberbarqarorlikni mustahkamlash muhim ilmiy-amaliy muammolardan biri sifatida namoyon bo‘lmoqda. Respublikada qabul qilinayotgan normativ-huquqiy hujjatlar va milliy kiberxavfsizlik strategiyalarida ham axborot xavfsizligini ta’minlashning zamonaviy texnologiyalariga alohida e’tibor qaratilayotgani ushbu yo‘nalishning dolzarbligini yanada oshirmoqda [1].

ISSN 3030-3907

Bugungi kunda kiberhujumlarning xarakteri sezilarli darajada o‘zgarmoqda. Avvallari asosan viruslar va oddiy zararli dasturlar orqali amalga oshirilgan tahdidlar endilikda sun’iy intellekt yordamida avtomatlashtirilgan fishing kampaniyalari, adaptiv zararli dasturlar, nol kunlik zaifliklardan foydalanish va murakkab ijtimoiy muhandislik usullari orqali amalga oshirilmoqda. Bunday tahdidlarni an’anaviy imzo asosidagi himoya tizimlari yordamida aniqlash tobora qiyinlashib bormoqda. Shu sababli real vaqt rejimida tahdidlarni aniqlash, ularga tezkor javob qaytarish va kiberhujumlarning oldini olishda sun’iy intellekt texnologiyalaridan foydalanishga bo‘lgan ehtiyoj ortib bormoqda. Sun’iy intellekt texnologiyalari katta hajmdagi tarmoq trafiklarini avtomatik tahlil qilish, anomal holatlarni aniqlash, zararli faoliyatni bashorat qilish, foydalanuvchi xatti-harakatlarini modellashtirish hamda xavfsizlik hodisalarini tezkor klassifikatsiyalash imkoniyatlarini yaratmoqda. Ayniqsa, mashinaviy o‘qitish va chuqur o‘rganish algoritmlari yordamida ilgari noma’lum bo‘lgan tahdidlarni aniqlash, xavf darajasini baholash va avtomatlashtirilgan javob mexanizmlarini shakllantirish kiberxavfsizlik tizimlarining samaradorligini sezilarli darajada oshirmoqda. Xalqaro ilmiy tadqiqotlarda SI asosidagi Security Operation Center (SOC), Extended Detection and Response (XDR) hamda User and Entity Behavior Analytics (UEBA) platformalari istiqbolli yechim sifatida baholanmoqda [2].

O‘zbekiston olimlari tomonidan ham raqamli transformatsiya, axborot xavfsizligi va sun’iy intellekt texnologiyalarini milliy axborot tizimlariga integratsiyalash masalalari bo‘yicha qator ilmiy izlanishlar olib borilmoqda. Mahalliy tadqiqotlarda elektron hukumat infratuzilmasi, davlat axborot resurslari xavfsizligi, kriptografik himoya usullari, sun’iy intellekt asosida tahdidlarni monitoring qilish va milliy CERT tizimlarini rivojlantirish bo‘yicha ilmiy tavsiyalar ishlab chiqilmoqda. Biroq mamlakatda raqamli transformatsiya sur’atlarining ortib borishi sun’iy intellektdan foydalanish orqali kiberxavfsizlikni ta’minlashning yangi konseptual yondashuvlarini ishlab chiqishni talab etmoqda. Shu nuqtai nazardan, O‘zbekistonda raqamli transformatsiya sharoitida yuzaga kelayotgan kiberxavfsizlik muammolarini kompleks tahlil qilish, ularning asosiy tahdidlarini aniqlash hamda sun’iy intellekt texnologiyalaridan foydalanish orqali xavfsizlikni ta’minlashning samarali mexanizmlarini ishlab chiqish dolzarb ilmiy vazifalardan biri hisoblanadi. Mazkur tadqiqot ushbu yo‘nalishdagi zamonaviy yondashuvlarni tahlil qilish, xalqaro tajriba va milliy amaliyotni solishtirish hamda O‘zbekistonning raqamli ekotizimida sun’iy intellekt asosidagi kiberxavfsizlik yechimlarini qo‘llash istiqbollarini ilmiy jihatdan asoslashga qaratilgan [3].

Adabiyotlar tahlili. Raqamli transformatsiya jarayonlarining jadallashuvi bilan bir qatorda kiberxavfsizlik muammolari ham yangi bosqichga ko‘tarildi. Zamonaviy ilmiy tadqiqotlarda axborot tizimlarining barqaror ishlashi nafaqat

ISSN 3030-3907

texnik infratuzilmaga, balki intellektual tahlil vositalari yordamida tahdidlarni oldindan aniqlash va ularga avtomatik javob qaytarish imkoniyatlariga ham bog‘liq ekanligi ta’kidlanmoqda. Xalqaro ilmiy manbalarda raqamli iqtisodiyot rivojlanishi sharoitida sun’iy intellekt kiberxavfsizlik tizimlarining ajralmas komponentiga aylanayotgani qayd etilgan. Ayniqsa, tarmoq trafigining keskin ortishi, bulutli hisoblash texnologiyalari, IoT qurilmalari va sanoat interneti platformalarining keng qo‘llanilishi an’anaviy xavfsizlik mexanizmlarining imkoniyatlarini cheklab qo‘ymoqda. So‘nggi yillardagi ilmiy izlanishlarda mashinaviy o‘qitish algoritmlari yordamida kiberhujumlarni aniqlash samaradorligini oshirish masalalari keng yoritilgan. Tadqiqotchilar nazorat ostida o‘qitish (Supervised Learning), nazoratsiz o‘qitish (Unsupervised Learning) hamda mustahkamlovchi o‘qitish (Reinforcement Learning) algoritmlaridan foydalanish orqali zararli trafikni klassifikatsiyalash, noma’lum tahdidlarni aniqlash va xavf darajasini baholash mumkinligini ko‘rsatganlar. Ayniqsa, chuqur neyron tarmoqlari va konvolyutsion modellar tarmoq paketlarining murakkab xususiyatlarini aniqlashda yuqori aniqlik ko‘rsatishi ilmiy tajribalarda isbotlangan [4].

Xalqaro adabiyotlarda SI asosidagi Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) texnologiyalari alohida ilmiy yo‘nalish sifatida shakllanmoqda. Ushbu tizimlar millionlab tarmoq hodisalarini real vaqt rejimida qayta ishlash imkoniyatiga ega bo‘lib, an’anaviy signatura asosidagi tizimlarga nisbatan yangi turdagi hujumlarni aniqlashda samaraliroq ekanligi qayd etilgan. Tadqiqotlarda Random Forest, Support Vector Machine, Gradient Boosting hamda Deep Neural Network algoritmlarining aniqlik darajasi yuqori bo‘lishi ko‘plab eksperimental sinovlar orqali tasdiqlangan. Shuningdek, ilmiy adabiyotlarda generativ sun’iy intellekt texnologiyalarining rivojlanishi bilan bog‘liq yangi xavflar ham tahlil qilinmoqda. Generativ modellar yordamida fishing xabarlarini avtomatik yaratish, ijtimoiy muhandislik hujumlarini shaxsiylashtirish, zararli kodlarni avtomatlashtirilgan ishlab chiqish va deepfake texnologiyalari orqali firibgarliklarni amalga oshirish imkoniyatlari kiberxavfsizlik tizimlari oldiga yangi vazifalarni qo‘ymoqda. Shu sababli ko‘plab olimlar himoya tizimlarida ham generativ sun’iy intellekt asosidagi xavf monitoringi va xulq-atvor tahlili vositalaridan foydalanishni taklif etmoqdalar [5].

Bulutli hisoblash infratuzilmasida sun’iy intellektdan foydalanish bo‘yicha olib borilgan ilmiy tadqiqotlar ham alohida e’tiborga loyiqdir. Mazkur ishlarda virtual serverlar, konteyner texnologiyalari va mikroxizmatlar arxitekturasida yuzaga keladigan xavflarni avtomatik aniqlash, resurslardan foydalanishdagi anomal holatlarni monitoring qilish va xizmat ko‘rsatishni rad etish hujumlarini prognozlash imkoniyatlari keng o‘rganilgan. SI algoritmlari yordamida tarmoq

ISSN 3030-3907

yuklamalarining normal modeli shakllantirilib, undan og‘ishlar asosida kiberhujumlarni erta bosqichda aniqlash mumkinligi ko‘rsatilgan. Mahalliy ilmiy tadqiqotlarda ham raqamli transformatsiya jarayonlari bilan bog‘liq axborot xavfsizligi masalalariga tobora ko‘proq e’tibor qaratilmoqda. O‘zbekiston olimlari elektron hukumat infratuzilmasini himoyalash, davlat axborot tizimlari xavfsizligini ta’minlash, milliy kriptografik vositalarni rivojlantirish hamda sun’iy intellekt yordamida kiberxavflarni monitoring qilish masalalarini o‘rganib kelmoqdalar. Tadqiqotlarda davlat axborot resurslarini himoyalashda avtomatlashtirilgan monitoring tizimlarini joriy etish, foydalanuvchilarning xulq-atvorini tahlil qilish va xavfsizlik hodisalarini markazlashgan boshqaruv platformalarida qayta ishlash zarurligi asoslangan [6].

Respublikada raqamli iqtisodiyotni rivojlantirish bo‘yicha olib borilayotgan islohotlar bank sektori, soliq tizimi, bojxona, elektron tijorat va davlat xizmatlari sohalarida axborot almashinuvi hajmini sezilarli oshirdi. Shu sababli mahalliy ilmiy ishlarda ma’lumotlar maxfiyligi, shaxsiy ma’lumotlarni himoya qilish, elektron identifikatsiya tizimlari xavfsizligi hamda raqamli identifikatsiya platformalarining zaif tomonlarini bartaraf etish bo‘yicha yangi yondashuvlar taklif etilgan. Ayrim tadqiqotlarda SI asosida biometrik autentifikatsiya va ko‘p omilli identifikatsiya tizimlarini qo‘llash istiqbolli yo‘nalish sifatida ko‘rsatib o‘tilgan. Ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, SI texnologiyalari kiberxavfsizlikning deyarli barcha bosqichlarida qo‘llanilishi mumkin. Tahdidlarni prognozlash, zararli trafikni filtrlash, foydalanuvchi xatti-harakatlarini tahlil qilish, avtomatlashtirilgan javob choralarini ishlab chiqish va xavfsizlik siyosatini optimallashtirish kabi vazifalar sun’iy intellekt yordamida samarali amalga oshirilmoqda. Shu bilan birga, SI modellarining noto‘g‘ri o‘qitilishi, ma’lumotlar sifati pastligi yoki adversarial hujumlarga moyilligi kabi muammolar ham mavjud bo‘lib, ular alohida ilmiy izlanishlarni talab qiladi [7].

Bugungi kunda xalqaro tajriba va mahalliy ilmiy ishlarda SI asosidagi Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Extended Detection and Response (XDR) hamda User and Entity Behavior Analytics (UEBA) platformalari istiqbolli texnologiyalar sifatida baholanmoqda. Ushbu platformalar katta hajmdagi hodisalarni avtomatik qayta ishlash, tahdidlarni ustuvorlashtirish va xavfsizlik operatorlarining yuklamasini kamaytirishga xizmat qilmoqda. O‘zbekiston sharoitida ham davlat va xususiy sektor axborot tizimlarida mazkur texnologiyalarni bosqichma-bosqich joriy etish milliy kiberbarqarorlikni oshirishga xizmat qilishi mumkin. Umuman olganda, mavjud ilmiy adabiyotlar raqamli transformatsiya sharoitida kiberxavfsizlikni ta’minlashning an’anaviy yondashuvlari tobora yetarli emasligini, sun’iy intellekt texnologiyalari esa yangi

ISSN 3030-3907

avlod himoya vositalarini yaratish uchun muhim ilmiy asos bo‘lib xizmat qilayotganini ko‘rsatadi. Shu bilan birga, O‘zbekistonning raqamli infratuzilmasi uchun milliy xususiyatlarni hisobga olgan SI asosidagi kiberxavfsizlik modellarini ishlab chiqish bo‘yicha ilmiy tadqiqotlar soni hali yetarli emasligi kuzatiladi. Mazkur holat ushbu yo‘nalishda kompleks ilmiy izlanishlar olib borish zaruratini yanada kuchaytiradi [8].

1-Jadval.

Raqamli transformatsiya sharoitida kiberxavfsizlikni ta'minlashda sun'iy intellekt texnologiyalarining qo‘llanilish yo‘nalishlari.

Kiberxavfsizlik yo‘nalishi	Qo‘llanilayotgan SI texnologiyasi	Asosiy vazifasi	Kutilayotgan samaradorlik
Tarmoq monitoringi	Mashinaviy o‘qitish (ML)	Anomal trafikni aniqlash	Hujumlarni erta aniqlash
IDS/IPS tizimlari	Deep Learning	Noma'lum hujumlarni klassifikatsiyalash	Aniqlik darajasini oshirish
Fishing hujumlarini aniqlash	NLP va Generativ AI tahlili	Shubhali xabarlarni tahlil qilish	Firibgarliklarni kamaytirish
Foydalanuvchi xatti-harakatlarini tahlil qilish	UEBA algoritmlari	Ichki tahdidlarni aniqlash	Insayder xavflarini kamaytirish
SIEM platformalari	AI Analytics	Xavfsizlik hodisalarini avtomatik tahlil qilish	Operator yuklamasini kamaytirish
SOAR platformalari	AI Automation	Avtomatik javob choralarini ishlab chiqish	Javob berish vaqtini qisqartirish
Bulutli infratuzilma himoyasi	Predictive AI	Resurslardan foydalanishni monitoring qilish	DDoS va anomal yuklamalarni aniqlash
IoT qurilmalarini himoyalash	Edge AI	Qurilmalar xatti-harakatini nazorat qilish	IoT zaifliklarini kamaytirish

ISSN 3030-3907

Biometrik autentifikatsiya	AI Recognition	Shaxsni identifikatsiyalash	Kirish xavfsizligini oshirish
Kiberxavflarni prognozlash	Big Data + AI	Kelajakdagi tahdidlarni bashorat qilish	Proaktiv himoyani shakllantirish

Jadval ma'lumotlari shuni ko‘rsatadiki, sun'iy intellekt texnologiyalari kiberxavfsizlikning barcha asosiy yo‘nalishlarida qo‘llanilishi mumkin. Ayniqsa, real vaqt rejimida tahdidlarni aniqlash, xavflarni prognozlash va avtomatlashtirilgan javob mexanizmlarini shakllantirish imkoniyatlari raqamli transformatsiya sharoitida axborot tizimlari barqarorligini sezilarli darajada oshirishga xizmat qiladi. O‘zbekistonning raqamli infratuzilmasida ham ushbu texnologiyalarni bosqichma-bosqich joriy etish milliy kiberxavfsizlik tizimining samaradorligini oshirishning muhim omili bo‘lishi mumkin [9].

Tadqiqot muhokamasi. O‘tkazilgan ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, raqamli transformatsiya jarayonlarining jadallashuvi bilan kiberxavfsizlik masalalari davlat va xususiy sektor faoliyatining eng muhim strategik yo‘nalishlaridan biriga aylangan. O‘zbekiston sharoitida elektron hukumat, raqamli bank xizmatlari, elektron tijorat, sanoatni raqamlashtirish va bulutli texnologiyalarning keng joriy etilishi axborot tizimlarining samaradorligini oshirayotgan bo‘lsa-da, ular bilan bog‘liq kiberxavflar soni va murakkabligi ham ortib bormoqda. Shu sababli an’anaviy xavfsizlik vositalari bilan bir qatorda sun’iy intellekt texnologiyalaridan foydalanish zarurati yuzaga kelmoqda. Tahlillar shuni ko‘rsatadiki, sun’iy intellekt asosidagi algoritmlar katta hajmdagi tarmoq ma’lumotlarini qisqa vaqt ichida qayta ishlash, normal va anomal holatlarni farqlash hamda ilgari uchramagan kiberhujumlarni aniqlash imkoniyatiga ega. Ayniqsa, mashinaviy o‘qitish va chuqur o‘rganish modellarining qo‘llanilishi zararli trafikni aniqlash aniqligini oshirish, noto‘g‘ri signal berish holatlarini kamaytirish va xavfsizlik hodisalariga tezkor javob qaytarish imkonini bermoqda. Bu esa zamonaviy kiberxavfsizlik tizimlarining samaradorligini sezilarli darajada oshiradi [10].

Biroq sun’iy intellekt texnologiyalaridan foydalanish bilan bog‘liq ayrim muammolar ham mavjud. Birinchidan, yuqori sifatli va ishonchli ma’lumotlar bazasining yetishmasligi SI modellarining aniqligiga salbiy ta’sir ko‘rsatishi mumkin. Ikkinchidan, sun’iy intellektning o‘zi ham adversarial hujumlar va model manipulyatsiyasi kabi yangi turdagi xavflarga duch kelmoqda. Uchinchidan, SI asosidagi tizimlarni joriy etish yuqori texnologik infratuzilma, malakali mutaxassislar va doimiy yangilanib boruvchi algoritmlarni talab qiladi. Bu esa rivojlanayotgan davlatlarda, jumladan O‘zbekistonda ham mazkur

ISSN 3030-3907

texnologiyalarni keng joriy etishda muayyan cheklovlarni yuzaga keltiradi. Shu bilan birga, xalqaro tajriba va mahalliy ilmiy tadqiqotlar sun'iy intellektni SIEM, SOAR, XDR va UEBA kabi zamonaviy kiberxavfsizlik platformalari bilan integratsiyalash yuqori samaradorlik berishini ko'rsatmoqda. O'zbekistonning raqamli transformatsiya strategiyasi doirasida ham davlat axborot tizimlari, bank sektori va muhim infratuzilma obyektlarida sun'iy intellekt asosidagi monitoring va tahdidlarni prognozlash tizimlarini bosqichma-bosqich joriy etish milliy kiberbarqarorlikni oshirishga xizmat qilishi mumkin. Shuningdek, milliy ma'lumotlar bazalarini shakllantirish, SI modellarini mahalliy sharoitga moslashtirish va mutaxassislar tayyorlash ushbu yo'nalishning ustuvor vazifalari sifatida qaralishi lozim [11].

XULOSA. Raqamli transformatsiya jarayonlari axborot tizimlari va raqamli xizmatlar ko'lamining kengayishiga olib kelishi bilan birga, kiberxavfsizlikni ta'minlash masalasini yanada dolzarb qilmoqda. Ilmiy adabiyotlar tahlili sun'iy intellekt texnologiyalarining kiberhujumlarni erta aniqlash, xavflarni prognozlash, tarmoq faoliyatini monitoring qilish va avtomatlashtirilgan himoya mexanizmlarini shakllantirishda yuqori samaradorlikka ega ekanligini ko'rsatdi. Shu bilan birga, SI modellarining ishonchliligi, ma'lumotlar sifati va yangi turdagi tahdidlarga moslashuvchanligi bilan bog'liq muammolar ham mavjud. O'zbekiston sharoitida raqamli transformatsiyaning muvaffaqiyatli amalga oshirilishi uchun sun'iy intellekt asosidagi kiberxavfsizlik tizimlarini milliy axborot infratuzilmasiga integratsiyalash, mahalliy ma'lumotlar bazalarini rivojlantirish hamda yuqori malakali mutaxassislarni tayyorlash muhim ahamiyat kasb etadi. Ushbu yondashuv milliy raqamli ekotizimning barqarorligi va axborot xavfsizligini ta'minlashda samarali ilmiy-amaliy asos bo'lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
2. Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (6th ed.). Pearson.
3. Russell, S., & Norvig, P. (2022). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
4. Aggarwal, C. C. (2023). Neural Networks and Deep Learning: A Textbook (2nd ed.). Springer.
5. Kshetri, N. (2024). Artificial intelligence in cybersecurity: Opportunities and challenges. IT Professional, 26(2), 15–23.
6. Karimov, B. A., & Tursunov, A. X. (2023). O'zbekistonda raqamli transformatsiya va axborot xavfsizligini ta'minlashning zamonaviy yo'nalishlari. Muhammad al-Xorazmiy Avlodlari Ilmiy-Amaliy Jurnali, 4(22), 52–59.

ISSN 3030-3907

7. Alimuhamedov, A. A., & Raximov, S. R. (2024). Sun'iy intellekt texnologiyalarini axborot xavfsizligi tizimlarida qo'llash istiqbollari. Axborot Texnologiyalari va Telekommunikatsiyalar Muammolari, 1(17), 31–39.
8. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.
9. National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.
10. Cisco Systems. (2025). Cisco Cybersecurity Readiness Index 2025. Cisco Research.
11. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. (2024). O'zbekistonda raqamli transformatsiya va kiberxavfsizlikni rivojlantirish istiqbollari. Toshkent.

ISSN 3030-3907