O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami

2026-yil 25-26-sentabr

(2-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2026-yil 25-26-sentabr. 315-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., т.f.f.d.(PhD), dots. Abdumalikov A.A, p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O‘ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

[2] M. Bethany et al., “Large Language Model Lateral Spear Phishing: A Comparative Study in Large-Scale Organizational Settings,” arXiv, 2024.

[3] F. Heiding et al., “Evaluating Large Language Models’ Capability to Launch Fully Automated Spear Phishing Campaigns,” arXiv, 2024.

[4] M. Weinz et al., “The Impact of Emerging Phishing Threats,” ASIA CCS, 2025.

[5] G. Desolda et al., “APOLLO: A GPT-based Tool to Detect Phishing Emails,” Proc. ACM Hum.-Comput. Interact., 2025.

[6] Y. Li et al., “KnowPhish: Large Language Models Meet Multimodal Knowledge Graphs,” USENIX Security, 2024.

[7] R. Liu et al., “PiMRef: Detecting and Explaining Ever-evolving Spear Phishing Emails,” arXiv, 2025.

[8] R. Meléndez et al., “Comparative Investigation of Transformer Models for Phishing Email Detection,” Electronics, 2024.

[9] M. Ibrahim and R. Elhafiz, “Phishing Email Detection Using BERT and RoBERTa,” Computation, 2026.

[10] H. Jiang et al., “D-PhishNet: URL and HTML Feature Fusion in Phishing Detection,” Computer Networks, 2025.

TARMOQ TRAFIGIDAGI ANOMALIYALARNI ANIQLASH VA KIBERHUJUMLARNING OLDINI OLISH

Axmedov Juraboy Raxmonberdiyevich
O‘zbekiston Milliy universitetining Jizzax filiali Axborot tizimlari va texnologiyalari kafedrasi professori v.b, pedagogika fanlari doktori (DSc),
Boboyev Akbarshoh Ibrohim o’g’li
Magistrant
E-mail: akbarshohboboyev79@gmail.com

Annotatsiya: Mazkur tezisda sun’iy intellekt va mashinaviy o‘qitish algoritmlari yordamida kompyuter tarmoqlaridagi anomal faoliyatni aniqlash va zamonaviy kiberhujumlarning oldini olish masalalari ko‘rib chiqilgan. Zararli trafikni an’anaviy signatura asosidagi tizimlardan farqli ravishda real vaqt rejimida aniqlashga imkon beruvchi neyron tarmoqlar, tasodifiy o‘rmon (Random Forest) va chuqur o‘rganish (Deep Learning) modellarining afzalliklari tahlil qilingan. Tadqiqot natijalari sun’iy intellektga asoslangan yondashuvlarning aniqlik darajasini oshirishda samarali ekanligini ko‘rsatadi.

Kalit so‘zlar: sun’iy intellekt, axborot xavfsizligi, kiberhujum, anomaliyalarni aniqlash, mashinaviy o‘qitish, neyron tarmoqlar, tarmoq trafigi, kiberxavfsizlik.

Kirish. Sun’iy intellekt asosida tarmoq trafigini intellektual monitoring qilishda asosiy e’tibor faqat mavjud kiberhujumlarni aniqlashga emas, balki tarmoqdagi normal xatti-harakatlarni modellashtirish, yangi va ilgari noma’lum hujumlarni aniqlash hamda aniqlangan tahdidga real vaqt rejimida avtomatik javob qaytarish mexanizmlarini ishlab chiqishga qaratilishi lozim. Zamonaviy raqamli iqtisodiyot

sharoitida axborot tizimlari va kompyuter tarmoqlarining hajmi tobora ortib bormoqda, bu esa o‘z navbatida kiberxavfsizlik muammolarini yanada dolzarblashtirmoqda. An’anaviy xavfsizlik devorlari va signatura asosidagi tizimlar allaqachon ma’lum bo‘lgan hujum turlarini aniqlashda samarali bo‘lsa-da, kun sayin paydo bo‘layotgan yangi turdagi (zero-day) hujumlarni aniqlashda ular yetarli darajada samarasiz hisoblanadi. Shu sababli, so‘nggi yillarda sun’iy intellekt (SI) va mashinaviy o‘qitish (Machine Learning) texnologiyalarini axborot xavfsizligi tizimlariga tatbiq etish borasidagi ilmiy-amaliy tadqiqotlar sezilarli darajada faollashdi[1].

Asosiy qism. Sun’iy intellektga asoslangan kiberxavfsizlik tizimlarining asosiy vazifasi - tarmoq trafigidagi statistik va xatti-harakat naqshlarini o‘rganish orqali normal holatdan chetlanishlarni (anomaliyalarni) aniqlashdan iborat. Bunday tizimlar quyidagi asosiy bosqichlardan iborat bo‘ladi: ma’lumotlarni yig‘ish va oldindan qayta ishlash, xususiyatlarni ajratib olish (feature extraction), modelni o‘qitish va natijalarni baholash.

Zamonaviy ilmiy yondashuvlar

Sun’iy intellekt va mashinaviy o‘qitish algoritmlaridan foydalanib, tarmoqdagi odatiy trafik xatti-harakatlarini o‘rganish va undan chetga chiqadigan holatlarni avtomatik aniqlash mumkin. Bunda nazoratli (supervised), nazoratsiz (unsupervised) va yarim nazoratli (semi-supervised) o‘qitish usullari muhim ahamiyatga ega.

Deep Learning asosida ishlab chiqilgan CNN, LSTM, Transformer kabi modellar tarmoq paketlari va trafik oqimlaridagi murakkab bog‘liqliklarni aniqlash imkonini beradi. Ayniqsa, vaqt bo‘yicha o‘zgaruvchi trafikni tahlil qilishda LSTM va Transformer arxitekturalaridan foydalanish istiqbolli hisoblanadi.

Real vaqt rejimida anomaliyalarni aniqlash zamonaviy kiberxavfsizlikning muhim yo‘nalishlaridan biridir. Tizim faqat hujum sodir bo‘lgandan keyin emas, balki hujumga xos bo‘lgan dastlabki belgilar paydo bo‘lishi bilan xavfni aniqlashi kerak.

Zero Trust konsepsiyasi bilan sun’iy intellektni integratsiya qilish orqali foydalanuvchi, qurilma va tarmoqdagi har bir ulanish doimiy ravishda baholanishi mumkin. AI tizimi qurilmaning odatiy xatti-harakatidan chetlanishni aniqlasa, qo‘shimcha autentifikatsiya yoki kirishni cheklash mexanizmini ishga tushiradi.

Xulq-atvorni tahlil qilish (Behavioral Analysis) orqali foydalanuvchi va qurilmalarning odatiy faoliyati uchun “normal profil” yaratiladi. Masalan, qurilmaning odatdagidan keskin ko‘p ma’lumot yuborishi, noodatiy portlarga murojaat qilishi yoki noma’lum manbalar bilan aloqa o‘rnatishi anomaliya sifatida baholanishi mumkin.

Generativ sun’iy intellekt kiberxavfsizlikda xavfsizlik jurnallarini (logs), tarmoq hodisalarini va ogohlantirishlarni tahlil qilish, ularni umumlashtirish hamda xavfsizlik mutaxassisiga tushunarli shaklda izohlash uchun qo‘llanilishi mumkin.

Federativ o‘qitish (Federated Learning) turli tashkilotlar yoki tarmoq segmentlaridagi ma’lumotlarni markaziy serverga to‘liq uzatmasdan AI modelini o‘qitish imkonini beradi. Bu yondashuv maxfiy ma’lumotlarni himoya qilish nuqtayi nazaridan ayniqsa muhim.

Explainable AI (XAI) yordamida tizim “hujum mavjud” degan xulosani berish bilan cheklanmay, nima sababdan ushbu trafik shubhali deb topilganini ham ko‘rsatishi mumkin. Bu xavfsizlik mutaxassisining qaror qabul qilish jarayonini yaxshilaydi.

Tadqiqot davomida uch xil yondashuv qiyosiy tahlil qilindi:

1) Klassik mashinaviy o‘qitish algoritmlari (Random Forest, Support Vector Machine) - nisbatan kichik hajmdagi ma’lumotlar to‘plamida yuqori tezlik va tushunarli natijalar beradi, ammo murakkab, ko‘p o‘lchovli hujum turlarini aniqlashda cheklovlarga ega[2].

2) Chuqur o‘rganish (Deep Learning) modellari, xususan, rekurrent neyron tarmoqlar (LSTM) - vaqt bo‘yicha ketma-ket keladigan tarmoq paketlari orasidagi bog‘liqlikni aniqlash imkonini beradi, bu esa DDoS va botnet hujumlarini yuqori aniqlik bilan aniqlashga yordam beradi.

3) Gibrid tizimlar - klassik algoritmlar va chuqur o‘rganishni birlashtirgan yondashuv bo‘lib, hisoblash resurslarini tejash bilan birga yuqori aniqlikni ta’minlaydi[3].

O‘tkazilgan tahlillar shuni ko‘rsatdiki, sun’iy intellekt asosidagi tizimlarni real vaqt rejimida joriy etish uchun ma’lumotlar sifatiga, hisoblash quvvatiga va modelni muntazam yangilab borish mexanizmiga alohida e’tibor qaratish zarur. Bundan tashqari, soxta signal (false positive) darajasini kamaytirish - bunday tizimlarning amaliy foydaliligini belgilovchi muhim omillardan biri hisoblanadi.

Xulosa: Xulosa qilib aytganda, sun’iy intellekt texnologiyalarini axborot xavfsizligi sohasiga tatbiq etish zamonaviy kiberhujumlarga qarshi kurashning samarali vositasi hisoblanadi. Kelajakda ushbu sohadagi tadqiqotlarni ma’lumotlar to‘plamlarining sifatini oshirish, modellarning shaffofligini (explainable AI) ta’minlash va tarmoq infratuzilmasiga real vaqt rejimida integratsiya qilish yo‘nalishlarida davom ettirish tavsiya etiladi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 2016.

2. Ahmad Z., Shahid Khan A., Wai Shiang C. va boshq. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 2021.

3. Vinayakumar R., Soman K.P., Poornachandran P. Applying deep learning approaches for network traffic prediction. International Conference on Advances in Computing, Communications and Informatics, 2017.

АДАПТИВНЫЕ АЛГОРИТМЫ ВЫЧИСЛЕНИЯ ОЦЕНОК В ЗАДАЧАХ ТАКСОНОМИИ И ВЫДЕЛЕНИЯ ОСОБЕННОСТЕЙ ОБЪЕКТОВ ИСТОРИЧЕСКОГО НАСЛЕДИЯ С ИСПОЛЬЗОВАНИЕМ ГРАФОВЫХ МЕТОДОВ ИИ И ЦИФРОВЫХ БАЗ ДАННЫХ

Эшанкулов Т

Актуальность темы исследования. В эпоху глобальной цифровизации гуманитарного знания и формирования парадигмы *Digital Humanities* критически важной задачей становится сохранение, систематизация и глубокий анализ объектов, имеющих историческую и культурную ценность. Цифровые архивы, базы данных музеев и археологические реестры содержат гетерогенные, слабоструктурированные и зачастую фрагментарные данные о материальных и нематериальных памятниках прошлого. Традиционные методы классификации и атрибуции, опирающиеся исключительно на экспертные знания, сталкиваются с проблемой субъективизма, низкой пропускной способности при обработке больших массивов данных, а также с невозможностью выявить скрытые нелинейные зависимости между пространственно-временными и морфологическими характеристиками артефактов.

В связи с этим возникает необходимость разработки автоматизированных математических и интеллектуальных систем, способных решать задачи таксономии (многомерной классификации и кластеризации) и выделения ключевых признаков (особенностей) исторических объектов. Особую сложность представляет динамическая природа исторических данных: по мере пополнения цифровых баз данных и появления новых археологических открытий критерии оценки и сходства объектов должны гибко перестраиваться. Это обуславливает востребованность **адаптивных алгоритмов вычисления оценок** (ААВО), способных подстраивать параметры метрических пространств под специфику конкретной предметной области в режиме реального времени.

Современным и наиболее перспективным математическим аппаратом для реализации таких адаптивных систем являются методы искусственного интеллекта (ИИ), основанные на теории графов, а именно **графовые нейронные сети (Graph Neural Networks, GNN)**, алгоритмы интеллектуального анализа сетевых структур (Network Science) и графы знаний (Knowledge Graphs). В отличие от классических векторных представлений, графовые модели позволяют естественным образом закодировать не только индивидуальные свойства исторического объекта (атрибуты из базы данных), так и сложную топологию его связей: контекстуальные, хронологические,