SUN'IY INTELLEKT YORDAMIDA KIBERXAVFSIZLIK: O'ZBEKISTON BANKLARI VA DAVLAT SAYTLARIDA PHISHING HAMDA DDoS HUJUMLARINI ZUDLIK BILAN ANIQLASH

Xakimov Muxammadzoxid Islomjon o'g'li

Turan International University talabasi

Doi: https://doi.org/10.5281/zenodo.20314695

Annotatsiya: Mazkur maqolada sun'iy intellekt texnologiyalarining zamonaviy kiberxavfsizlik tizimidagi o'rni, ayniqsa O'zbekiston bank sektori hamda davlat elektron platformalarini phishing va DDoS hujumlaridan himoya qilishdagi ahamiyati ilmiy jihatdan tahlil qilingan. Raqamli transformatsiya jarayonlarining jadallashuvi natijasida bank xizmatlari, elektron hukumat tizimlari, onlayn to'lov platformalari va masofaviy xizmatlarning kengayishi kiberjinoyatchilik xavfining ortishiga olib kelmoqda. Tadqiqot davomida sun'iy intellekt asosida ishlovchi monitoring tizimlari, trafikni real vaqt rejimida tahlil qilish algoritmlari, anomal xatti-harakatlarni aniqlash usullari hamda mashinaviy o'qitish texnologiyalarining amaliy samaradorligi yoritilgan. Maqolada phishing hujumlarining ijtimoiy muhandislik orqali amalga oshirilishi, DDoS hujumlarining server infratuzilmasiga ta'siri va ularga qarshi avtomatlashtirilgan himoya mexanizmlarining samaradorligi chuqur o'rganilgan. O'zbekiston sharoitida bank tizimi va davlat saytlarining axborot xavfsizligini mustahkamlashda sun'iy intellektning istiqbolli imkoniyatlari ilmiy asoslangan holda ochib berilgan. Tadqiqot natijalari raqamli iqtisodiyot sharoitida milliy kiberxavfsizlikni ta'minlash uchun innovatsion yondashuvlarni keng joriy etish zarurligini ko'rsatadi.

Kalit so'zlar: Sun'iy intellekt, kiberxavfsizlik, phishing, DDoS hujumlari, mashinaviy o'qitish, bank xavfsizligi, davlat saytlari, axborot xavfsizligi, kiberhujum, real vaqt monitoringi, neyron tarmoqlar, avtomatlashtirilgan himoya, raqamli transformatsiya, anomal trafik, elektron hukumat.

Abstract: This article scientifically analyzes the role of artificial intelligence technologies in modern cybersecurity systems, particularly their significance in protecting Uzbekistan's banking sector and government electronic platforms from phishing and DDoS attacks. As digital transformation processes accelerate, the expansion of banking services, e-government systems, online payment platforms, and remote services has increased the risk of cybercrime. The study highlights the practical effectiveness of AI-based monitoring systems, real-time traffic analysis algorithms, anomaly detection methods, and machine learning technologies. The article deeply examines the implementation of phishing attacks through social engineering methods, the impact of DDoS attacks on server infrastructure, and the effectiveness of automated protection mechanisms against such threats. The promising opportunities of artificial intelligence in strengthening information security within Uzbekistan's banking system and government websites are scientifically substantiated. The research findings demonstrate the necessity of widely implementing innovative approaches to ensure national cybersecurity in the context of the digital economy.

Keywords: Artificial intelligence, cybersecurity, phishing, DDoS attacks, machine learning, banking security, government websites, information security, cyberattack, real-time monitoring, neural networks, automated protection, digital transformation, anomalous traffic, e-government.

Аннотация: В данной статье научно проанализирована роль технологий искусственного интеллекта в современной системе кибербезопасности, особенно их

значение в защите банковского сектора Узбекистана и государственных электронных платформ от фишинговых и DDoS-атак. Ускорение процессов цифровой трансформации, расширение банковских услуг, систем электронного правительства, онлайн-платформ платежей и дистанционных сервисов приводят к росту угроз киберпреступности. В ходе исследования освещена практическая эффективность систем мониторинга на основе искусственного интеллекта, алгоритмов анализа трафика в режиме реального времени, методов выявления аномального поведения и технологий машинного обучения. В статье подробно изучены механизмы осуществления фишинговых атак с использованием методов социальной инженерии, влияние DDoS-атак на серверную инфраструктуру, а также эффективность автоматизированных механизмов защиты от подобных угроз. Научно обоснованы перспективные возможности искусственного интеллекта в укреплении информационной безопасности банковской системы и государственных сайтов Узбекистана. Результаты исследования показывают необходимость широкого внедрения инновационных подходов для обеспечения национальной кибербезопасности в условиях цифровой экономики.

Ключевые слова: Искусственный интеллект, кибербезопасность, фишинг, DDoS-атаки, машинное обучение, банковская безопасность, государственные сайты, информационная безопасность, кибератака, мониторинг в реальном времени, нейронные сети, автоматизированная защита, цифровая трансформация, аномальный трафик, электронное правительство.

Kirish

Jahon miqyosida raqamli texnologiyalar taraqqiyoti insoniyat hayotining barcha sohalariga chuqur kirib bormoqda. Bank tizimi, davlat boshqaruvi, elektron savdo, sog‘liqni saqlash va ta’lim kabi strategik sohalarning raqamlashtirilishi katta hajmdagi axborot almashinuvi va elektron infratuzilmalarning shakllanishiga olib keldi. Shu bilan birga, global axborot makonida kiberjinoyatchilik ham murakkablashib bormoqda. Xususan, phishing va DDoS hujumlari bugungi kunda dunyo bo‘yicha eng xavfli kiberxavf turlaridan biri sifatida e’tirof etilmoqda. Ushbu hujumlar orqali foydalanuvchilarning shaxsiy ma’lumotlari o‘g‘irlanadi, bank hisoblari buziladi, davlat tizimlari faoliyati izdan chiqariladi hamda iqtisodiy zarar yetkaziladi.

O‘zbekiston Respublikasida ham raqamli iqtisodiyot va elektron hukumat tizimlarini rivojlantirish davlat siyosatining ustuvor yo‘nalishlaridan biri hisoblanadi. So‘nggi yillarda internet-bank xizmatlari, mobil ilovalar, davlat xizmatlari portallari va onlayn to‘lov tizimlarining jadal rivojlanishi aholining raqamli xizmatlardan foydalanish imkoniyatlarini kengaytirdi. Biroq ushbu jarayon kiberxavfsizlik masalasining dolzarbligini yanada oshirdi. Ayniqsa, bank tizimlari va davlat saytlariga nisbatan uyushtirilayotgan fishing va DDoS hujumlari milliy axborot xavfsizligiga jiddiy tahdid tug‘dirmoqda. An’anaviy kiberxavfsizlik vositalari zamonaviy kiberhujumlarning murakkab va tezkor xarakteriga qarshi har doim ham yetarli darajada samarali natija bera olmaydi. Chunki bugungi kunda kiberjinoyatchilar avtomatlashtirilgan botlar, yashirin tarmoqlar va sun’iy intellekt imkoniyatlaridan foydalanib hujumlarni murakkablashtirmoqda. Shu sababli kiberxavfsizlik sohasida sun’iy intellekt texnologiyalaridan foydalanish zarurati yuzaga kelmoqda. Sun’iy intellekt katta hajmdagi ma’lumotlarni qisqa vaqt ichida tahlil qilish, noodatiy holatlarni aniqlash, xavfli faoliyatni bashorat qilish va hujumlarni avtomatik ravishda bartaraf etish imkoniyatini beradi.

Bugungi kunda rivojlangan davlatlarda banklar va yirik davlat tashkilotlari sun’iy intellekt asosidagi xavfsizlik platformalarini keng joriy etmoqda. Mazkur tizimlar foydalanuvchilarning xatti-harakatlarini tahlil qilish, tarmoq trafigidagi g‘ayritabiiy o‘zgarishlarni aniqlash va ehtimoliy hujumlarni oldindan prognoz qilish imkonini bermoqda. O‘zbekiston sharoitida ham

sun’iy intellekt texnologiyalarini kiberxavfsizlikka integratsiya qilish strategik ahamiyat kasb etadi. Chunki mamlakatda raqamli xizmatlardan foydalanuvchilar sonining ortishi kiberhujumlar ehtimolini ham oshirmoqda. Mazkur maqolada sun’iy intellekt asosidagi kiberxavfsizlik tizimlarining nazariy va amaliy jihatlari, phishing hamda DDoS hujumlarini aniqlash mexanizmlari, O‘zbekiston banklari va davlat saytlarida ularni qo‘llash istiqbollari ilmiy tahlil qilinadi.

Asosiy qism

Kiberxavfsizlik va sun’iy intellekt masalalari xalqaro ilmiy hamjamiyat tomonidan keng tadqiq qilinayotgan dolzarb yo‘nalishlardan biri hisoblanadi. Xorijiy tadqiqotchilar tomonidan olib borilgan ilmiy ishlarda sun’iy intellektning axborot xavfsizligini ta’minlashdagi samaradorligi yuqori baholanadi. Xususan, Stuart Russell va Peter Norvig sun’iy intellektning ma’lumotlarni qayta ishlash tezligi hamda avtomatik qaror qabul qilish imkoniyatlari zamonaviy xavfsizlik tizimlarining asosiy komponentiga aylanayotganini ta’kidlaydi. Tadqiqotchilar fikricha, neyron tarmoqlar va chuqur o‘qitish algoritmlari kiberhujumlarni aniqlash aniqligini sezilarli darajada oshiradi. Klaus Schwab raqamli inqilob sharoitida sun’iy intellekt insoniyat oldida yangi imkoniyatlar bilan bir qatorda xavfsizlikka oid jiddiy tahdidlarni ham yuzaga keltirayotganini qayd etadi. Uning tadqiqotlarida moliyaviy texnologiyalar va elektron hukumat tizimlarining himoyasi strategik masala sifatida talqin qilinadi. Shuningdek, IBM Security, Cisco va Kaspersky kabi xalqaro kompaniyalar hisobotlarida phishing hujumlarining asosiy maqsadi inson omili ekani, DDoS hujumlari esa server resurslarini izdan chiqarishga qaratilganligi ilmiy-statistik ma’lumotlar bilan asoslangan.

Mashinaviy o‘qitish algoritmlaridan foydalanish orqali fishing xabarlarini aniqlash bo‘yicha ko‘plab ilmiy tadqiqotlar olib borilgan. Tadqiqotlarda elektron pochta matnlari, URL manzillar, foydalanuvchi harakati va trafik oqimlarini tahlil qilish orqali xavfli faoliyatni aniqlash samaradorligi yuqori ekanligi ko‘rsatilgan. Ayrim ishlarda sun’iy intellekt tizimlari an’anaviy filtratsiya usullariga nisbatan ancha yuqori aniqlik ko‘rsatgani qayd etilgan.

O‘zbekiston olimlari tomonidan ham axborot xavfsizligi va raqamli texnologiyalar sohasida ilmiy izlanishlar olib borilmoqda. Mahalliy tadqiqotlarda elektron hukumat tizimlari, bank infratuzilmalari va milliy axborot resurslarini himoya qilish masalalariga alohida e’tibor qaratilgan. Shu bilan birga, sun’iy intellekt asosida phishing va DDoS hujumlarini aniqlash masalasi hali yetarlicha chuqur tadqiq qilinmagan yo‘nalishlardan biri hisoblanadi. Mavjud ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, zamonaviy kiberxavfsizlikni ta’minlashda sun’iy intellekt texnologiyalari nafaqat yordamchi vosita, balki strategik himoya mexanizmi sifatida ham muhim o‘rin tutmoqda. Ayniqsa, real vaqt rejimida ishlovchi monitoring tizimlari, avtomatik tahlil platformalari va xatti-harakatlarni bashorat qilish modellarining rivojlanishi kiberxavfsizlik sohasida yangi bosqichni boshlab bermoqda. Mazkur tadqiqotda ilmiy bilishning zamonaviy usullaridan kompleks ravishda foydalanildi. Tadqiqot jarayonida tizimli tahlil, qiyosiy solishtirish, statistik kuzatuv, analitik baholash va ilmiy umumlashtirish metodlari qo‘llanildi. O‘zbekiston banklari va davlat saytlarining faoliyatiga oid ochiq statistik ma’lumotlar, xalqaro tashkilotlar hisobotlari, ilmiy maqolalar hamda kiberxavfsizlik platformalari tahlil qilindi.

Tadqiqot davomida phishing va DDoS hujumlarining ishlash mexanizmlari texnik jihatdan o‘rganildi. Shuningdek, sun’iy intellekt asosidagi xavfsizlik tizimlarining real vaqt rejimida ishlash samaradorligi ilmiy manbalar asosida tahlil qilindi. Mashinaviy o‘qitish algoritmlarining tahdidlarni aniqlashdagi aniqlik darajasi, xatolik ko‘rsatkichlari va avtomatlashtirish imkoniyatlari qiyosiy baholandi. Bundan tashqari, O‘zbekistonning raqamli infratuzilmasi, elektron hukumat tizimlari va bank sektoridagi raqamlashtirish jarayonlari kiberxavfsizlik nuqtai nazaridan tahlil qilindi. Tadqiqotda milliy axborot makonining himoyasi, foydalanuvchilarning

raqamli savodxonligi va sun’iy intellekt texnologiyalarini joriy etish imkoniyatlari alohida e’tiborga olindi. Tadqiqot natijalari shuni ko‘rsatadiki, phishing hujumlari bugungi kunda O‘zbekiston bank tizimi va davlat platformalari uchun eng xavfli tahdidlardan biri bo‘lib qolmoqda. Kiberjinoyatchilar foydalanuvchilarning ishonchidan foydalanib, soxta havolalar, qalbaki bank saytlar va firibgar elektron xabarlar orqali maxfiy ma’lumotlarni qo‘lga kiritishga urinmoqda. Ayniqsa, mobil bank xizmatlarining keng ommalashuvi phishing xavfini yanada kuchaytirmoqda. Chunki foydalanuvchilarning aksariyati mobil qurilmalarda xavfsizlik belgilariga yetarli darajada e’tibor bermaydi.

Sun’iy intellekt texnologiyalari phishing hujumlarini aniqlashda yuqori samaradorlikni namoyon etmoqda. Mashinaviy o‘qitish algoritmlari foydalanuvchi odatlarini tahlil qilib, noodatiy faoliyatni tezkor aniqlash imkonini beradi. Masalan, foydalanuvchi odatda bir hududdan tizimga kiradigan bo‘lsa, boshqa geografik nuqtadan amalga oshirilgan shubhali kirish tizim tomonidan avtomatik ravishda xavf sifatida baholanadi. Shuningdek, sun’iy intellekt elektron pochta matnlarini lingvistik tahlil qilish orqali fishing xabarlarini aniqlash imkoniga ega. DDoS hujumlari esa asosan serverlarga ortiqcha trafik yuborish orqali xizmatlarni ishdan chiqarishga qaratiladi. O‘zbekiston davlat xizmatlari portallari va bank saytlarining uzluksiz ishlashi iqtisodiy va ijtimoiy barqarorlik uchun muhim ahamiyatga ega. Shu sababli DDoS hujumlarini erta aniqlash strategik vazifa hisoblanadi. Sun’iy intellekt asosidagi monitoring tizimlari tarmoq trafigidagi anomal o‘zgarishlarni soniyalar ichida aniqlash imkonini beradi. Bu esa hujum boshlanishidan oldin himoya choralarini ishga tushirish imkoniyatini yaratadi.

Tahlillar shuni ko‘rsatdiki, an’anaviy xavfsizlik tizimlari ko‘pincha oldindan belgilangan qoidalarga asoslanadi. Sun’iy intellekt esa o‘z-o‘zini o‘rganish xususiyati orqali yangi tahdidlarni ham aniqlash imkoniyatiga ega. Ayniqsa, chuqur o‘qitish algoritmlari murakkab trafik oqimlarini tahlil qilishda yuqori samaradorlik ko‘rsatmoqda. Bu texnologiyalar katta hajmdagi ma’lumotlar ichidan xavfli xatti-harakatlarni aniqlab, administratorlarga tezkor signal yuboradi. O‘zbekiston banklarida sun’iy intellekt asosidagi xavfsizlik tizimlarini joriy etish moliyaviy yo‘qotishlarni kamaytirishga xizmat qiladi. Tadqiqot davomida aniqlanishicha, avtomatlashtirilgan monitoring tizimlari kiberhujumlarni inson omiliga nisbatan ancha tez aniqlaydi. Chunki inson operatorlari katta hajmdagi trafikni uzluksiz nazorat qila olmaydi. Sun’iy intellekt esa millionlab ma’lumotlarni bir vaqtning o‘zida qayta ishlash imkoniyatiga ega.

Davlat saytlarida sun’iy intellekt asosidagi himoya platformalarini joriy qilish fuqarolarning davlat xizmatlariga bo‘lgan ishonchini oshiradi. Elektron hukumat tizimlarining barqaror ishlashi davlat boshqaruvi samaradorligini ta’minlovchi asosiy omillardan biri hisoblanadi. Shu sababli kiberxavfsizlikni sun’iy intellekt bilan integratsiyalash davlat siyosatining muhim yo‘nalishiga aylanishi lozim. Shuningdek, tadqiqot davomida foydalanuvchilarning raqamli savodxonligi masalasi ham muhim omil sifatida qayd etildi. Chunki eng zamonaviy sun’iy intellekt tizimlari ham insonning ehtiyotsizligi tufayli yuzaga keladigan xavflarni to‘liq bartaraf eta olmaydi. Shu sababli aholining kiberxavfsizlik madaniyatini oshirish, phishing xabarlarini tanish ko‘nikmalarini rivojlantirish va xavfsiz internet foydalanish qoidalarini targ‘ib qilish muhim ahamiyat kasb etadi.

Xulosa

Zamonaviy raqamli transformatsiya sharoitida kiberxavfsizlik masalasi davlat va jamiyat xavfsizligining ajralmas qismiga aylanmoqda. Ayniqsa, bank tizimi va davlat elektron platformalarining keng rivojlanishi phishing hamda DDoS hujumlari xavfini keskin oshirmoqda. Mazkur tahdidlar iqtisodiy barqarorlikka, fuqarolarning shaxsiy ma’lumotlariga va davlat axborot infratuzilmasiga jiddiy zarar yetkazishi mumkin. Tadqiqot natijalari sun’iy intellekt texnologiyalarining kiberxavfsizlikni ta’minlashdagi samaradorligi yuqori ekanligini ko‘rsatdi.

Mashinaviy o‘qitish, neyron tarmoqlar va avtomatlashtirilgan monitoring tizimlari phishing hamda DDoS hujumlarini real vaqt rejimida aniqlash imkoniyatini yaratadi. Bu esa tahdidlarning oldini olish, xavfsizlik tizimlarini optimallashtirish va inson omiliga bog‘liq xatolarni kamaytirishga xizmat qiladi.

O‘zbekiston sharoitida sun’iy intellekt asosidagi kiberxavfsizlik tizimlarini joriy etish milliy axborot xavfsizligini mustahkamlashning muhim omillaridan biri hisoblanadi. Banklar, davlat tashkilotlari va elektron platformalarda zamonaviy himoya texnologiyalarini keng qo‘llash orqali kiberhujumlarga qarshi barqaror mudofaa tizimini shakllantirish mumkin. Shu bilan birga, foydalanuvchilarning raqamli savodxonligini oshirish va kiberxavfsizlik madaniyatini rivojlantirish ham dolzarb vazifalardan biri bo‘lib qoladi. Kelajakda sun’iy intellekt texnologiyalarining yanada rivojlanishi kiberxavfsizlik tizimlarining avtomatlashtirilish darajasini oshiradi. Bu esa O‘zbekistonning raqamli iqtisodiyoti va elektron hukumat tizimlari xavfsizligini ta’minlashda muhim strategik asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – New Jersey: Pearson Education, 2021.

2. Schwab K. The Fourth Industrial Revolution. – Geneva: World Economic Forum, 2016.

3. Stallings W. Network Security Essentials: Applications and Standards. – Boston: Pearson, 2020.

4. Bishop M. Computer Security: Art and Science. – Boston: Addison-Wesley, 2019.

5. Kaspersky Security Bulletin 2024. Global Cybersecurity Report. – Moscow, 2024.

6. IBM Security Report. Artificial Intelligence in Cybersecurity. – New York, 2023.

7. Cisco Annual Cybersecurity Report. – California, 2024.

8. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. – Toshkent, 2022.

9. O‘zbekiston Respublikasi Prezidentining raqamli iqtisodiyotni rivojlantirishga oid farmon va qarorlari. – Toshkent, 2020–2025.

10. Nazirov Sh., Axmedov B. Axborot xavfsizligi va kiberxavfsizlik asoslari. – Toshkent: Fan, 2021.

11. Abduqodirov A. Raqamli texnologiyalar va axborot xavfsizligi. – Toshkent: Innovatsiya, 2022.

12. Alimuhamedov J. Sun’iy intellekt va zamonaviy axborot tizimlari. – Toshkent: Universitet, 2023.

13. Symantec Internet Security Threat Report. – California, 2023.

14. ENISA Threat Landscape Report. European Union Agency for Cybersecurity. – Brussels, 2024.

15. McAfee Labs Threats Report. – Texas, 2024.