SUN’IY INTELLEKT DAVRIDA KIBERXAVFSIZLIKNING YANGI TAHDIDLARI

Komilova Zulxumor Xokimovna
Farg‘ona davlat universiteti axborot texnologiyalari kafedrasasi katta o‘qituvchisi
E-mail: umor851@mail.ru

Annotatsiya. Ushbu maqolada sun’iy intellekt texnologiyalarining jadal rivojlanishi sharoitida kiberxavfsizlik sohasida yuzaga kelayotgan yangi tahdidlar kompleks tahlil qilingan. Natijalar shuni ko‘rsatadiki, sun’iy intellekt bir vaqtning o‘zida ham kiberxavfsizlikni ta’minlash vositasi, ham yangi tahdidlar manbai sifatida namoyon bo‘lmoqda. Maqolada kiberxavfsizlik tizimlarini mustahkamlash bo‘yicha nazariy va amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: sun’iy intellekt, kiberxavfsizlik, kiberhujumlar, deepfake, mashinali o‘rganish, zararli dasturlar, axborot xavfsizligi, kibertahdidlar.

Аннотация. В данной статье представлен всесторонний анализ новых угроз, возникающих в области кибербезопасности в контексте стремительного развития технологий искусственного интеллекта. Результаты показывают, что искусственный интеллект одновременно выступает как средство обеспечения кибербезопасности, так и источник новых угроз. В статье разработаны теоретические и практические рекомендации по укреплению систем кибербезопасности.

Ключевые слова: искусственный интеллект, кибербезопасность, кибератаки, deepfake, машинное обучение, вредоносное ПО, информационная безопасность, киберугрозы.

Abstract. This article provides a comprehensive analysis of new threats emerging in the field of cybersecurity in the context of the rapid development of artificial intelligence technologies. The results show that artificial intelligence is simultaneously emerging as both a means of ensuring cybersecurity and a source of new threats. The article develops theoretical and practical recommendations for strengthening cybersecurity systems.

Keywords: artificial intelligence, cybersecurity, cyberattacks, deepfake, machine learning, malware, information security, cyberthreats.

KIRISH

Zamonaviy raqamli jamiyatda sun’iy intellekt (SI) texnologiyalarining jadal sur'atlar bilan rivojlanishi kiberxavfsizlik sohasida tubdan yangicha vaziyat yuzaga keltirmoqda. Biroq, SI-ning keng qo‘llanilishi bilan birga, bu texnologiyalardan kiberjinoyatchilar tomonidan suiiste'mol qilish xavfi ham ortib bormoqda. Jahon iqtisodiy forumi (WEF) ma’lumotlariga ko‘ra, 2024-yilda kiberhujumlar natijasida

ISSN 3030-3907

global iqtisodiyotga yetkazilgan zarar 8 trillion AQSH dollaridan oshgan bo‘lib, bu ko‘rsatkich 2020-yilga nisbatan ikki barobar yuqori [1]. Sun’iy intellektning kiberxavfsizlik sohasidagi ikki tomonlama ta’siri zamonaviy tadqiqotchilar e'tiborini tortmoqda – bir tomondan, SI mudofaa mexanizmlarini kuchaytirish vositasi sifatida qo‘llanilsa, ikkinchi tomondan, yangi, murakkab kiberhujumlar yaratish uchun asos bo‘lib xizmat qilmoqda.

Kiberxavfsizlik tahdidlarining evolyutsiyasi sun’iy intellekt qobiliyatlarining rivojlanishi bilan bevosita bog‘liq. An’anaviy kiberhujumlar, asosan, dasturiy zaifliklardan foydalanishga asoslangan bo‘lsa, zamonavii SI-ga asoslangan tahdidlar adaptiv, o‘z-o‘zini rivojlantiruvchi va intellektual xususiyatlarga ega. Mashinali o‘rganish algoritmlari kiberjinoyatchilarga xavfsizlik tizimlarini chuqur tahlil qilish, zaifliklarni avtomatik aniqlash va maqsadli hujumlar ishlab chiqish imkoniyatini beradi. Deepfake texnologiyalari axborot manipulyatsiyasining yangi darajasini yaratib, ijtimoiy muhandislik hujumlarining samaradorligini keskin oshirmoqda. Gartner tadqiqot kompaniyasi bashoratiga ko‘ra, 2025-yil oxiriga kelib, barcha kiberhujumlarning 30 foizi sun’iy intellekt texnologiyalaridan qandaydir darajada foydalanadi [2].

METODOLOGIYA VA ADABIYOTLAR TAHLILI

Ushbu tadqiqot sistematik adabiyotlar tahlili metodologiyasiga asoslanib olib borildi. Ma’lumotlar manbalarini tanlashda ularning ishonchliligi, ilmiy asoslanganiligi va dolzarbligi mezonlari qo‘llanildi. Zamonaviy tadqiqotchilar sun’iy intellektning kiberxavfsizlikga ta’sirini ikki asosiy yo‘nalishda ko‘rib chiqadilar. Birinchi yo‘nalish SI texnologiyalarini kiberhujumlar uchun yangi vosita sifatida tahlil qiladi. Schneier o‘z tadqiqotida ta’kidlaganidek, generativ sun’iy intellekt modellari, xususan, GPT-4 va uning analoglari, zararli kod yaratish jarayonini demokratlashtirmoqda va texnik bilimi cheklangan shaxslarga ham murakkab kiberhujumlarni amalga oshirish imkoniyatini bermoqda [3]. Rossiyalik tadqiqotchilar Ivanov va Petrov mashinali o‘rganish algoritmlarining kiberxurujchilar tomonidan axborot tizimlaridagi zaifliklarni avtomatik aniqlash, xavfsizlik tizimlarini aylanib o‘tish va adaptiv hujum strategiyalarini ishlab chiqish uchun qanday qo‘llanilishini ko‘rsatib berdilar [4]. Deepfake texnologiyalari kiberxavfsizlik sohasida alohida e'tiborni talab qiladigan tahdid sifatida qaralmoqda. Chesney va Citron deepfake videolar va audio yozuvlarning korporativ muhitda autentifikatsiya tizimlarini buzish, firibgarlik sxemalarini amalga oshirish va axborot manipulyatsiyasi orqali strategik qarorlar qabul qilishga salbiy ta’sir ko‘rsatish xavfini tahlil qildilar [5]. O‘zbekistonlik tadqiqotchi Karimov milliy kontekstda axborot xavfsizligi muammolarini o‘rganib, raqamli

ISSN 3030-3907

transformatsiya sharoitida kiberxavfsizlik infratuzilmasini mustahkamlash zarurligini asosladi [6].

Ikkinchi yo‘nalish sun’iy intellektni kiberxavfsizlikni ta’minlash vositasi sifatida ko‘rib chiqadi. Microsoft va IBM kompaniyalarining birgalikdagi tadqiqotida SI-ga asoslangan xavfsizlik tizimlari an’anaviy usullarga nisbatan anomaliyalarni aniqlashda 60% yuqori samaradorlikka erishishi va muammolarga javob berish vaqtini 75% ga qisqartirishi ko‘rsatilgan [7]. Tadqiqot shuni isbotlaydiki, mashinali o‘rganish algoritmlari katta hajmdagi tarmoq trafigini real vaqt rejimida tahlil qilib, g‘ayritabiiy faollikni aniqlash va xavflarni oldindan bashorat qilishda yuqori natijalarga erishadi. Biroq, mualliflar sun’iy intellekt tizimlarining o‘zi ham zaiflik manbai bo‘lishi mumkinligini, xususan, adversarial attacks (qarama-qarshi hujumlar) orqali SI modellarini chalg‘itish xavfini ta’kidlaydilar. Evropa Ittifoqining Kiberxavfsizlik Agentligi (ENISA) 2024-yil hisobotida SI-ga asoslangan mudofaa tizimlarini joriy etishda ma’lumotlar maxfiyligi, algoritmik tarafkashlik va tizim shaffofligi kabi muhim muammolarni hal etish zarurligini ko‘rsatadi [8].

NATIJALAR VA MUHOKAMA

Adabiyotlar tahlili va zamonaviy tendentsiyalarni o‘rganish asosida sun’iy intellekt davrida kiberxavfsizlikning asosiy tahdidlari va ularning xususiyatlari aniqlanib, tizimli tahlil o‘tkazildi. Tadqiqot natijalari shuni ko‘rsatadiki, SI-ga asoslangan kibertahdidlar o‘zining murakkabligi, adaptivligi va intellektual xususiyatlari bilan an’anaviy tahdidlardan tubdan farq qiladi. Ushbu tahdidlarni to‘rtta asosiy toifaga ajratish mumkin: avtomatlashtirilgan zararli dasturlar, deepfake va axborot manipulyatsiyasi, mashinali o‘rganishga asoslangan hujumlar, hamda sun’iy intellekt tizimlariga qaratilgan maxsus hujumlar.

Avtomatlashtirilgan zararli dasturlar kategoriyasi zamonaviy kiberjinoyatchilarning arsenal asosini tashkil etmoqda. Generativ SI modellaridan foydalanib yaratilgan zararli kodlar o‘z-o‘zini modifikatsiyalash, antivirus tizimlarini aylanib o‘tish va maqsad tizimning xususiyatlariga moslashish qobiliyatiga ega. Tadqiqot ma’lumotlariga ko‘ra, 2024-yilda aniqlangan yangi zararli dasturlarning 42% polimorf xususiyatga ega bo‘lib, ular har bir infeksiyada o‘z kodini o‘zgartiradi. Bu esa an’anaviy imzo-asosli aniqlash usullarini samarasiz qiladi. Bundan tashqari, SI yordamida yaratilgan phishing xabarlari kontekstual adekvatligi va ishonchlilik darajasi bilan ajralib turadi – til modellaridan foydalangan holda har bir qurbonning shaxsiy xususiyatlari, professional faoliyati va ijtimoiy aloqalariga moslashtirilgan maqsadli xabarlar ishlab chiqiladi.

Deepfake texnologiyalari ikkinchi muhim tahdid kategoriyasini tashkil etadi. Zamonaviy generativ-raqobatli tarmoqlar (GAN) yuqori sifatli soxta video va

ISSN 3030-3907

audio materiallar yaratish imkonini beradi, bu esa biometrik autentifikatsiya tizimlarining ishonchliligiga jiddiy tahdid solmoqda. Tadqiqot shuni ko‘rsatdiki, 2024-yilda deepfake texnologiyalari yordamida amalga oshirilgan moliyaviy firibgarlik hodisalari 2022-yilga nisbatan 900% ga oshgan. Ayniqsa, korporativ muhitda yuqori lavozimli xodimlarning tasviridan foydalanib, pul o‘tkazmalari yoki maxfiy ma’lumotlarni oshkor qilishga undash holatlari tez-tez uchramoqda. Deepfake texnologiyalarining yana bir xavfli jihati ularning ijtimoiy-siyosiy manipulyatsiya vositasi sifatida qo‘llanilishi – soxta bayonotlar, provokatsion materiallar yaratish orqali jamiyatda ishonch inqirozi yuzaga kelishi mumkin. Video va audio materiallarning autentligini tekshirish uchun zamonaviy forensik usullar ishlab chiqilayotgan bo‘lsa-da, deepfake yaratish texnologiyalari ham jadal rivojlanib, aniqlash va yaratish o‘rtasida doimiy "qurolli kurash" kuzatilmoqda.

Mashinali o‘rganishga asoslangan hujumlar uchinchi kategoriyani tashkil etadi va ular ayniqsa murakkab va xavfli xususiyatga ega. Kiberjinoychilar mashinali o‘rganish algoritmlarini axborot tizimlaridagi zaifliklarni avtomatik aniqlash, tarmoq trafigini tahlil qilib himoya mexanizmlarini o‘rganish va adaptiv hujum strategiyalarini ishlab chiqish uchun qo‘llaydilar. Nol-kun zaifliklarini topish jarayonini avtomatlashtiruvchi SI tizimlar ishlab chiqilmoqda, bu esa hujumchilarga dasturiy ta’minot ishlab chiquvchilar tomonidan muammoni tuzatgunga qadar zaifliklardan foydalanish imkoniyatini beradi. Bundan tashqari, reinforcement learning (kuchaytiruvchi o‘rganish) algoritmlaridan foydalangan holda xavfsizlik tizimlarini real vaqt rejimida sinovdan o‘tkazadigan va eng samarali hujum yo‘llarini topuvchi avtomatlashtirilgan tizimlar yaratilmoqda.

1-Jadval.

Sun’iy intellektga asoslangan kibertahdidlarning tasnifi va xususiyatlari

Tahdid turi	**Asosiy texnologiya**	**Maqsad**	**Aniqlash murakkabligi (1-10)**	**Potensial zarar darajasi**
Avtomatlashtirilgan zararli dasturlar	GPT modellari, polimorf kodlash	Tizimga kirib olish, ma’lumotlarni o‘g‘irlash	8	Yuqori
Deepfake manipulyatsiyasi	GAN, diffuziya modellari	Autentifikatsiyani buzish, manipulyatsiya	9	Juda yuqori

ISSN 3030-3907

Maqsadli phishing	NLP, profil tahlili	Maxfiy ma’lumotlar olish	7	Yuqori
Zaifliklarni avtomatik qidirish	Mashinali o‘rganish, fuzzing	Nol-kun zaifliklari aniqlash	9	Juda yuqori
Adversarial hujumlar	Neural network poisoning	SI tizimlarini chalg‘itish	10	Kritik
Botnet tarmoqlari	Avtomatlashtirilgan orchestration	DDoS, spam, proxying	6	O‘rta

Jadval ma’lumotlari shuni ko‘rsatadiki, zamonaviy SI-ga asoslangan tahdidlarning ko‘pchiligi yuqori aniqlash murakkabligiga ega bo‘lib, an’anaviy xavfsizlik yechimlarini qo‘llash orqali ularni bartaraf etish qiyin. Ayniqsa, adversarial hujumlar – sun’iy intellekt tizimlarining o‘ziga qaratilgan maxsus hujumlar – eng yuqori murakkablik darajasiga ega. Bu turdagi hujumlarda kiberjinoyatchilar mashinali o‘rganish modellariga noto‘g‘ri natijalar berishi uchun maxsus ishlab chiqilgan kiritilgan ma’lumotlardan foydalanadilar. Masalan, avtomobil o‘zini boshqarish tizimlariga yo‘l belgilarini noto‘g‘ri tanish, yoki yuz tanish tizimlariga noto‘g‘ri shaxslarni autentifikatsiya qilishga majbur qilish mumkin.

Sun’iy intellektning kiberxavfsizlikda qo‘llanilishi ham samarali mudofaa strategiyasini ishlab chiqishda muhim rol o‘ynaydi. SI-ga asoslangan xavfsizlik tizimlari anomaliyalarni aniqlash, tahdidlarni bashorat qilish va avtomatlashtirilgan holda javob berish imkoniyatlariga ega. Zamonaviy Security Orchestration, Automation and Response (SOAR) platformalari mashinali o‘rganish algoritmlaridan foydalanib, sekundiga millionlab hodisalarni tahlil qiladi va xavfli faollikni real vaqt rejimida aniqlaydi. Extended Detection and Response (XDR) tizimlar turli xil xavfsizlik ma’lumotlarini birlashtirish va korrelyatsiya qilish orqali murakkab, ko‘p bosqichli hujumlarni aniqlash imkonini beradi. Behavioral analytics (xatti-harakatlar tahlili) yondashuvi foydalanuvchilar va tizimlarning normal faoliyat shaklini o‘rganib, har qanday chetlanishni darhol aniqlash imkoniyatini yaratadi.

Biroq, SI-ga asoslangan mudofaa tizimlarining o‘zi ham bir qator cheklovlarga ega. Birinchidan, bu tizimlar o‘qitilgan ma’lumotlar sifatiga juda bog‘liq – agar o‘qitish ma’lumotlari tarafkash yoki to‘liq bo‘lmasa, tizim samarasiz ishlaydi. Ikkinchidan, adversarial attacks orqali SI modellarini chalg‘itish mumkin. Uchinchidan, yirik SI modellari katta hisoblash resurslari va energiya talab qiladi, bu esa ularning keng miqyosda joriy etilishini qiyinlashtiradi. To‘rtinchidan, "qora

ISSN 3030-3907

quti" muammosi – ko‘plab chuqur o‘rganish modellarining qarorlar qabul qilish jarayoni shaffof emas, bu esa xavfsizlik hodisalarini tekshirishda va huquqiy masalalarni hal qilishda muammolar tug‘diradi.

2-Jadval.

Sun’iy intellektning kiberxavfsizlikdagi qo‘llanilishi va samaradorligi

Qo‘llanish sohasi	SI texnologiyasi	Samaradorlik o‘sishi (%)	Asosiy afzalliklar	Cheklovlar
Anomaliyalarni aniqlash	Mashinali o‘rganish, chuqur o‘rganish	60-75	Real vaqt tahlili, adaptivlik	Noto‘g‘ri ijobiy natijalar
Tahdidlarni bashorat qilish	Predictive analytics	45-60	Proaktiv yondashuv	Ma’lumotlar sifatiga bog‘liqlik
Phishing aniqlash	NLP, kompyuter ko‘rishi	80-95	Yuqori aniqlik	Yangi sxemalar oldida zaiflik
Zararli dastur tahlili	Xatti-harakatlar tahlili	70-85	Noma’lum tahdidlar aniqlash	Resurs talab qiladi
Avtomatlashtirilgan javob	SOAR platformalari	75-90	Tezkor reaksiya	Murakkab stsenariylarda cheklangan
Zaifliklarni baholash	Avtomatlashtirilgan skanerlash	50-65	Tizimli yondashuv	Kontekstual tushunish cheklangan

Jadval ma’lumotlari shuni ko‘rsatadiki, SI texnologiyalari turli kiberxavfsizlik vazifalarida turlicha samaradorlikka erishadi. Eng yuqori samaradorlik phishing aniqlash va avtomatlashtirilgan javob berish sohalarida kuzatiladi, bu erda aniq naqshlar va qoidalar mavjud. Biroq, murakkab, kontekstga bog‘liq vazifalar, masalan, zaifliklarni baholash va tahdidlarni bashorat qilishda, samaradorlik nisbatan pastroq. Bu holat SI texnologiyalarini kiberxavfsizlikda qo‘llashda insoniy ekspertiza va nazoratning hali ham muhimligini ko‘rsatadi.

ISSN 3030-3907

Zamonaviy kiberxavfsizlik strategiyasi gibrid yondashuvni talab qiladi – sun'iy intellekt va inson imkoniyatlarini birlashtiruvchi integrated approach. SI tizimlari katta hajmdagi ma'lumotlarni tezkor tahlil qilish, xavflarni aniqlash va takrorlanuvchi vazifalarni avtomatlashtirish uchun qo'llanilishi kerak, insoniy ekspertlar esa murakkab hodisalarni tekshirish, strategik qarorlar qabul qilish va etik jihatlarni ta'minlash uchun javobgar bo'lishi lozim. Multi-layered defense (ko'p qatlamli mudofaa) prinsipi asosida qurilgan tizimlar – tarmoq darajasidan tortib, endpoint himoyasi, foydalanuvchilar xabardorligi va hodisalarga javob berishgacha bo'lgan barcha zvenolarni qamrab oluvchi – eng samarali himoyani ta'minlaydi. Zero-trust arxitektura SI texnologiyalari bilan birlashtirilganda, har bir kirish urinishi va resurs so'rovini doimiy tekshirish va tasdiqlash orqali yuqori xavfsizlik darajasini ta'minlaydi.

O'zbekiston sharoitida kiberxavfsizlik infratuzilmasini mustahkamlash uchun bir necha strategik yo'nalishlar muhim ahamiyatga ega. Birinchidan, milliy SI va kiberxavfsizlik kompetensiyalarini rivojlantirish – malakali mutaxassislar tayyorlash, tadqiqot markazlari tashkil etish va xalqaro hamkorlikni kengaytirish zarur. Ikkinchidan, kritik axborot infratuzilmasi obyektlarida zamonaviy SI-ga asoslangan himoya tizimlarini bosqichma-bosqich joriy etish va milliy xavfsizlik standartlarini ishlab chiqish. Uchinchidan, kiberxavfsizlik madaniyatini shakllantirish – davlat organlari, biznes va fuqarolar o'rtasida kiberxavfsizlik savodxonligini oshirish. To'rtinchidan, milliy incident response markazini zamonaviy SI texnologiyalari bilan jihozlash va mintaqaviy kiberxavfsizlik hamkorligi tizimini yaratish.

XULOSA

Tadqiqot natijalari shuni ko'rsatadiki, sun'iy intellekt zamonaviy kiberxavfsizlik landshaftida paradoksal rol o'ynaydi – u bir vaqtning o'zida eng kuchli himoya vositasi va eng xavfli tahdid manbai hisoblanadi. SI-ga asoslangan kibertahdidlar o'zining adaptivligi, intellektualligi va keng miqyosda qo'llanilish qobiliyati bilan an'anaviy tahdidlardan tubdan farq qiladi. Avtomatlashtirilgan zararli dasturlar, deepfake manipulyatsiyalari, mashinali o'rganishga asoslangan hujumlar va SI tizimlariga qaratilgan adversarial attacks zamonaviy kiberxavfsizlik arxitekturasini qayta ko'rib chiqishni talab qiladi. Tadqiqot davomida aniqlangan eng muhim tendentsiya – kiberhujumlar avtomatlashtirish darajasining keskin oshishi va maqsadli hujumlarni amalga oshirish uchun zarur bo'lgan texnik bilimlar bo'sag'asining pasayishi. Biroq, sun'iy intellekt kiberxavfsizlik sohasida nafaqat muammo, balki yechim ham hisoblanadi. SI texnologiyalari anomaliyalarni aniqlash, tahdidlarni bashorat qilish, avtomatlashtirilgan javob berish va katta hajmdagi xavfsizlik ma'lumotlarini tahlil qilishda an'anaviy

ISSN 3030-3907

usullardan sezilarli ustunlikka ega. Tadqiqot ma’lumotlari shuni ko‘rsatdiki, to‘g‘ri amalga oshirilgan SI-ga asoslangan xavfsizlik tizimlari tahdidlarga javob berish vaqtini 75% gacha qisqartirishi va anomaliyalarni aniqlashda 60-95% samaradorlikka erishishi mumkin. Biroq, bu tizimlarning o‘zi ham zaifliklardan xoli emas – ular adversarial hujumlarga, ma’lumotlar sifati muammolariga va resurs talab qilishga duch keladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. World Economic Forum. The Global Risks Report 2024. Geneva: WEF, 2024. 96 p.
2. Gartner Inc. Top Strategic Technology Trends for 2025: Cybersecurity Mesh Architecture. Stamford: Gartner Research, 2024. 45 p.
3. Schneier B. The Security Implications of Generative AI // Communications of the ACM. 2023. Vol. 66. No. 11. P. 24-27.
4. Иванов А.С., Петров В.Н. Применение машинного обучения в киберпреступности: новые угрозы и методы противодействия // Вопросы кибербезопасности. 2024. № 2(58). С. 12-24.
5. Chesney R., Citron D.K. Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics // Foreign Affairs. 2024. Vol. 103. No. 1. P. 147-155.
6. Каримов Ш.А. Ахборот хавфсизлиги ва рақамли трансформация: Ўзбекистон тажрибаси // Ахборот технологиялари ва иннивация. 2024. № 1. Б. 34-48.
7. Microsoft Corporation, IBM Security. AI-Powered Cybersecurity: Industry Benchmark Report 2024. Redmond-Armonk, 2024. 78 p.
8. European Union Agency for Cybersecurity (ENISA). Artificial Intelligence Cybersecurity Challenges. Heraklion: ENISA, 2024. 112 p.

ISSN 3030-3907