KIBERXAVFSIZLIKNI TA’MINLASHDA SUN’IY INTELLEKTDAN FOYDALANISHNING MAZMUN-MOHIYATI

TECHNOLOGICAL CHARACTERISTICS OF CYBERCRIME AND ITS SOCIAL, ECONOMIC, AND POLITICAL IMPACTS

ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ КИБЕРПРЕСТУПНОСТИ И ЕЁ СОЦИАЛЬНОЕ, ЭКОНОМИЧЕСКОЕ И ПОЛИТИЧЕСКОЕ ВЛИЯНИЕ

Yusupov Javohir O‘tkirjonovich
(O‘zbekiston Respublikasi IIV Akademiyasi kursanti)
Iminov Abdurasul Abdulatipovich
(O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i)

Annotatsiya: Ushbu maqolada global raqamli makonda xavfsizlikni ta’minlash, kiberhujumlarni barvaqt aniqlash va ularga tezkor javob qaytarishda sun’iy intellekt (SI) hamda mashinali o‘qitish (Machine Learning) texnologiyalaridan foydalanishning mazmun-mohiyati va huquqiy-texnik asoslari tahlil qilinadi. Muallif an’anaviy xavfsizlik tizimlarining zamonaviy kiber-tahdidlar oldidagi zaifligini ko‘rsatib, SI platformalarining proaktiv (oldindan ogohlantiruvchi) imkoniyatlarini yoritib beradi. Tadqiqot davomida kiber-mudofaada sun’iy intellektni qo‘llashning institutsional mexanizmlari, shuningdek, jinoyatchilar tomonidan SIdan zararli maqsadlarda (Adversarial AI) foydalanish xavflari o‘rganilib, milliy qonunchilik va amaliyotni takomillashtirish bo‘yicha ilmiy-huquqiy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, mashinali o‘qitish, proaktiv mudofaa, kiberhujum, raqamli xavfsizlik, algoritmlar, ijtimoiy muhandislik

Abstract: This article analyzes the essence, legal, and technical foundations of utilizing Artificial Intelligence (AI) and Machine Learning (ML) technologies in ensuring security, early detection of cyberattacks, and rapid incident response within the global digital space. The author highlights the vulnerabilities of traditional security systems against modern cyber threats and demonstrates the proactive capabilities of AI platforms. The research explores the institutional mechanisms of implementing AI in cyber-defense, as well as the risks of malicious AI exploitation (Adversarial AI) by cybercriminals, subsequently formulating scientific and legal recommendations to enhance national legislation and practices.

Keywords: Artificial Intelligence, cybersecurity, machine learning, proactive defense, cyberattack, digital security, algorithms, social engineering.

Аннотация: В данной статье анализируются суть, правовые и технические основы использования технологий искусственного интеллекта (ИИ) и машинного обучения (ML) в обеспечении безопасности, раннем обнаружении кибератак и оперативном реагировании на инциденты в глобальном цифровом пространстве. Автор указывает на уязвимость традиционных систем безопасности перед современными киберугрозами и раскрывает проактивные возможности ИИ-платформ. В ходе исследования изучаются институциональные механизмы применения ИИ в кибероборонe, а также риски использования ИИ злоумышленниками в преступных целях (Adversarial AI), и разрабатываются научно-правовые рекомендации по совершенствованию национального законодательства и практики.

Ключевые слова:Искусственный интеллект, кибербезопасность, машинное обучение, проактивная защита, кибератака, цифровая безопасность, алгоритмы, социальная инженерия.

Kirish

Axborot texnologiyalari va global tarmoq infratuzilmasining shiddatli rivojlanishi insoniyat hayotini butunlay raqamli ekotizimga ko‘chirdi. Davlat boshqaruvi, strategik infratuzilmalar (energetika, transport, harbiy majmua), bank-moliya sektori va shaxsiy ma’lumotlar to‘liq kompyuterlashtirilgan tizimlarga tayanmoqda. Biroq, bu taraqqiyot kiber-jinoyatchilikning ham misli ko‘rilmagan darajada o‘sishiga sabab bo‘ldi.

An’anaviy kiberxavfsizlik tizimlari (masalan, imzolarga asoslangan antiviruslar yoki oddiy tarmoq ekranlari — Firewall) faqatgina **“ilgari ma’lum bo‘lgan”** tahdidlarni qaytara oladi. Bugungi kunda har kuni millionlab yangi zararli dasturlar va “nolinchi kun” (Zero-day) zaifliklari yaratilayotgan bir davrda, inson-operatorlar va eski dasturlar tahdidlar tezligiga yetib ulgurmayapti. Aynan shu sababli, kiberxavfsizlik sohasida **Sun’iy Intellekt (SI)** texnologiyalarini joriy etish shunchaki innovatsiya emas, balki hayotiy zaruriyatga aylandi.

Kiberxavfsizlikda Sun’iy Intellektning Rolini Baholash (Tizimli tahlil)

Kiberxavfsizlikda SI o‘zining katta hajmdagi ma’lumotlarni (Big Data) soniyalar ichida qayta ishlash va mantiqiy qonuniyatlarni topish qobiliyati bilan ajralib turadi. Uning mazmun-mohiyatini uchta asosiy funksional yo‘nalishda ko‘rish mumkin:

Tahdidlarni Barvaqt Aniqlash va Anomaliyalarni Tahlil Qilish

SI tizimlari tarmoq trafigini va foydalanuvchilarning xatti-harakatlarini doimiy ravishda (24/7) monitoring qiladi. Mashinali o‘qitish modellari tizim uchun nima

“normal holat” ekanligini o‘rganadi. Agar tarmoqda kutilmagan, noodatiy ma’lumotlar oqimi yoki shubhali faollik (anomaliya) kuzatilsa, SI uni kiberhujum sifatida baholaydi va inson aralashuvisiz bloklaydi.

Avtomatlashtirilgan Kiber-mudofaa va Hodisalarga Javob Berish

Hujum sodir bo‘lganda vaqt eng muhim omil hisoblanadi. SI tizimlari (masalan, SOAR — Security Orchestration, Automation, and Response) hujumni aniqlagan zahoti tizimning zararlangan qismini lokalizatsiya qiladi, xavfli IP-manzillarni to‘sadi va zaxira nusxalarini (backup) xavfsiz joyga ko‘chiradi. Bu jarayon millisekundlar ichida sodir bo‘ladi.

Bashoratli (Predictive) Xavfsizlik

SI o‘tmishdagi global kiberhujumlar strategiyasini tahlil qilib, kelajakda xakerlar tizimning qaysi zaif nuqtalariga hujum qilishi mumkinligini bashorat qiladi. Bu esa xavfsizlik xizmatlariga passiv mudofaadan **proaktiv (hujumdan oldin choralarni ko‘rish)** mudofaaga o‘tish imkonini beradi.

Sun’iy Intellektning Kiber-tahdid Sifatidagi Salbiy Tomoni (Adversarial AI)

SIdan nafaqat himoyachilar, balki kiber-jinoyatchilar ham keng foydalanmoqda. Ushbu dualizm (ikki yoqlamalik) bugungi kunda kiber-urushlarning yangi bosqichini boshlab berdi:

Polimorf zararli dasturlar: Jinoyatchilar SI yordamida har safar antivirus tizimlariga tushganda o‘z kodini va tuzilishini o‘zgartiradigan, ammo zararli funksiyasini saqlab qoladigan viruslarni yaratmoqdalar.

Oliy darajadagi Fishing (Phishing): Generativ SI (ChatGPT va uning klonlari) orqali xakerlar hech qanday grammatik xatolarsiz, psixologik jihatdan mukammal ishlangan fishing xatlarini ommaviy ishlab chiqmoqdalar.

Deepfake firibgarligi: Korxona rahbarlarining ovozi va qiyofasini sun’iy intellekt yordamida soxtalashtirib, buxgalteriya xodimlariga yirik miqdorda pul o‘tkazish bo‘yicha buyruq berish holatlari ko‘paygan.

Huquqiy Normalar va Xalqaro Standartlar

Kiberxavfsizlikda SIdan foydalanish faqat texnik masala emas, u jiddiy huquqiy tartibga solishni talab etadi.

Shaxsiy Ma’lumotlar va Konfidentsialli

SI modellari samarali ishlashi uchun juda ko‘p ma’lumotlarni yutishi va tahlil qilishi kerak. Bu jarayonda fuqarolarning shaxsiy hayot daxlsizligi huquqi buzilishi xavfi tug‘iladi. Yevropa Ittifoqining **GDPR (General Data Protection Regulation)** va **EU AI Act (2024)** hujjatlari sun’iy intellekt tizimlaridan foydalanishda inson huquqlari va shaffoflikni (Ethical AI) birinchi o‘ringa qo‘yadi.

O‘zbekiston Respublikasining Huquqiy Strategiyasi

Davlatimizda ham bu borada dadil qadamlar tashlanmoqda. O‘zbekiston Respublikasi Prezidentining 2021-yildagi “Sun’iy intellekt texnologiyalarini joriy etish

bo‘yicha shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida”gi PQ-4996-sonli qarori hamda “Kiberxavfsizlik to‘g‘risida”gi Qonun raqamli makonda xavfsizlikni huquqiy tartibga solishning asosi bo‘lib xizmat qiladi. Biroq, kiber-mudofaada SI algoritmlarining huquqiy javobgarligi va standartlari hali to‘liq shakllanmagan.

Tizimni Takomillashtirish Bo‘yicha Taklif va Tavsiyalar

O‘zbekiston kiber-hududini samarali himoya qilish va bu jarayonga sun’iy intellektni xavfsiz joriy etish uchun quyidagi chora-tadbirlar taklif etiladi:

Milliy Kiber-antivirus platformasini yaratish

Markazlashgan Milliy kiberxavfsizlik markazi qoshida davlat va strategik ahamiyatga ega obyektlar (aeroportlar, AES, banklar) tarmoqlarini himoya qiluvchi, o‘zbek tili va milliy kontent xususiyatlarini inobatga oladigan milliy SI-antifraud va kiber-mudofaa tizimini loyihalashtirish lozim.

Qonunchilikka “Aqlli texnologiyalar yordamida sodir etilgan jinoyat” tushunchasini kiritish

Jinoyat kodeksiga kiberjinoyat sodir etishda neyrotarmoqlar va sun’iy intellekt dasturlaridan foydalanishni javobgarlikni og‘irlashtiruvchi holat sifatida kiritish zarur.

“Ethical AI” (Etik Sun’iy Intellekt) standartlarini ishlab chiqish

SIdan foydalanganda fuqarolarning ma’lumotlari sizib chiqmasligi yoki algoritmlarning noto‘g‘ri qarorlari (false positives) tufayli inson huquqlari kamsitilishining oldini oluvchi milliy huquqiy etika kodeksini qabul qilish.

Xulosa

Sun’iy intellekt kiberxavfsizlik sohasida ham "qalqon", ham "qilich" vazifasini o‘tamoqda. Undan unumli foydalanish davlatlarning texnologik suverenitetini belgilab beradi. Biz faqatgina eski texnologiyalarga tayanib kiberxavfsizlikni ta’minlay olmaymiz; kelajakda kiber-tahdidlarni faqat texnologik jihatdan mukammal, o‘z-o‘zini o‘qituvchi intellektual tizimlar yordamida jilovlash mumkin. Buning uchun texnik innovatsiyalar bilan bir qatorda mustahkam huquqiy baza yaratilishi shart.

Foydalanilgan Adabiyotlar Ro‘yxati

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 05.04.2022 yildagi O‘RQ-764-son.
2. O‘zbekiston Respublikasi Prezidentining “Sun’iy intellekt texnologiyalarini joriy etishni jadallashtirish chora-tadbirlari to‘g‘risida”gi 17.02.2021 yildagi PQ-4996-son qarori.
3. European Parliament. (2024). *The European Union Artificial Intelligence Act (EU AI Act)*. Brussels.
4. National Institute of Standards and Technology (NIST). (2024). *Artificial Intelligence Risk Management Framework (AI RMF)*. U.S. Department of Commerce.

5. G‘ulomov S.S. va boshqalar. Raqamli iqtisodiyotda axborot xavfsizligi. – Toshkent: Fan, 2022.
6. Sodiqov, A. X. (2024). Kiberhududda huquqiy munosabatlarni tartibga solishning dolzarb muammolari. *O‘zbekiston qonunchiligi tahlili*, 4(2), 45-52.