SUN’IY INTELLEKT VA KIBERXAVFSIZLIK: IMKONIYATLAR VA XAVFLAR

Akbutayev Shoxro‘zbek Xusniddin o‘g‘li
Ichki Ishlar Vazirligi Akademiyasi 2-bosqich kursanti
Sultonboyev Otabek Dilshodbek o‘g‘li
Ichki Ishlar Vazirligi Akademiyasi 2-bosqich kursanti

Annotatsiya: *Ushbu maqolada sun’iy intellektning kiberxavfsizlik sohasidagi o‘rni, uning imkoniyatlari va yuzaga kelayotgan xavflari tahlil qilinadi. Sun’iy intellekt yordamida tahdidlarni aniqlash, avtomatlashtirilgan himoya tizimlarini yaratish va zaifliklarni oldindan aniqlash imkoniyatlari yoritilgan. Shu bilan birga, SI asosidagi kiberhujumlar, zararli dasturlar va ma’lumotlar xavfsizligi bilan bog‘liq muammolar ham ko‘rib chiqiladi. Maqolada, shuningdek, sun’iy intellektdan samarali va xavfsiz foydalanish bo‘yicha tavsiyalar berilgan.*

Kalit so‘zlar: *sun’iy intellekt, kiberxavfsizlik, kiberhujum, phishing, zararli dastur, ma’lumotlar xavfsizligi, avtomatlashtirish, raqamli tahdidlar*

Аннотация: *В данной статье рассматривается роль искусственного интеллекта в сфере кибербезопасности, его возможности и возникающие угрозы. Освещаются вопросы обнаружения угроз в реальном времени, автоматизации защитных механизмов и выявления уязвимостей. Наряду с этим анализируются риски, связанные с использованием ИИ, включая кибератаки, вредоносное программное обеспечение и проблемы защиты данных. Также предлагаются рекомендации по безопасному и эффективному применению искусственного интеллекта.*

Ключевые слова: *искусственный интеллект, кибербезопасность, кибератака, фишинг, вредоносное ПО, защита данных, автоматизация, цифровые угрозы*

Abstract: *This article examines the role of artificial intelligence in cybersecurity, highlighting its opportunities and emerging risks. It discusses the use of AI in real-time threat detection, automated defense mechanisms, and proactive vulnerability identification. At the same time, it analyzes the risks associated with AI, including advanced cyberattacks, malware, and data security issues. The article also provides recommendations for the safe and effective use of artificial intelligence in cybersecurity.*

Keywords: *artificial intelligence, cybersecurity, cyberattack, phishing, malware, data security, automation, digital threats*

Kirish

Bugungi kunda raqamli texnologiyalar jadal rivojlanib borayotgan bir davrda kiberxavfsizlik masalasi global muammolardan biriga aylanib bormoqda. Internet tarmoqlarining kengayishi, bulutli texnologiyalar, IoT qurilmalarining ko‘payishi axborot

xavfsizligiga bo‘lgan talabni yanada oshirdi. Shu jarayonda sun’iy intellekt (SI) texnologiyalarining keng joriy etilishi kiberxavfsizlik sohasida tub burilish yasamoqda.

Sun’iy intellekt bir tomondan kiberxavfsizlik tizimlarini kuchaytirish, tahdidlarni tezkor aniqlash va oldini olish imkonini bersa, ikkinchi tomondan kiberjinoyatchilar uchun yangi va murakkab hujum usullarini yaratish imkonini ham bermoqda. Shu bois, sun’iy intellekt va kiberxavfsizlik o‘rtasidagi o‘zaro bog‘liqlikni chuqur o‘rganish dolzarb ahamiyat kasb etadi.

Asosiy qism

1. Sun’iy intellektning kiberxavfsizlikdagi imkoniyatlari

Sun’iy intellekt kiberxavfsizlik tizimlarini yanada samarali, tezkor va moslashuvchan qilish imkonini beradi.

Birinchidan, SI real vaqt rejimida tahdidlarni aniqlash imkoniga ega. U katta hajmdagi ma’lumotlarni tahlil qilib, noodatiy xatti-harakatlarni aniqlaydi va ehtimoliy hujumlarni erta bosqichda fosh etadi. Bu esa zarar yetkazilishining oldini olishda muhim ahamiyatga ega.

Ikkinchidan, SI avtomatlashtirilgan javob mexanizmlarini ta’minlaydi. Masalan, tizim zararli faoliyatni aniqlagan zahoti avtomatik tarzda foydalanuvchini bloklashi, zararli fayllarni o‘chirishi yoki tarmoqdan ajratishi mumkin.

Uchinchidan, SI proaktiv himoyani ta’minlaydi. Ya’ni, u nafaqat hujumlarni aniqlaydi, balki tizimdagi zaifliklarni oldindan topib, ularni bartaraf etishga yordam beradi.

To‘rtinchidan, SI katta hajmdagi infratuzilmani boshqarishda samaradorlikni oshiradi. Minglab qurilmalar va foydalanuvchilarni bir vaqtning o‘zida monitoring qilish imkoniyati inson omiliga bo‘lgan ehtiyojni kamaytiradi va xatolik ehtimolini pasaytiradi.

2. Sun’iy intellekt bilan bog‘liq kiberxavfsizlik xavflari

Shu bilan birga, sun’iy intellekt kiberjinoyatchilar uchun ham yangi imkoniyatlar yaratmoqda.

Birinchidan, SI yordamida yanada murakkab va ishonchli phishing hujumlari amalga oshirilmoqda. Bunday xabarlar inson yozgan matndan deyarli farq qilmaydi va foydalanuvchini aldash ehtimoli yuqori bo‘ladi.

Ikkinchidan, avtomatlashtirilgan zararli dasturlar (AI-based malware) yaratilmoqda. Bu dasturlar o‘zini doimiy ravishda yangilab, an’anaviy antivirus tizimlarini chetlab o‘tishi mumkin.

Uchinchidan, “adversarial attack” hujumlari mavjud bo‘lib, bunda hujumchilar sun’iy intellekt tizimlarini chalg‘itadi va noto‘g‘ri qaror qabul qilishga majbur qiladi.

To‘rtinchidan, ma’lumotlar xavfsizligi muammosi yanada keskinlashmoqda. SI tizimlari katta hajmdagi shaxsiy va korporativ ma’lumotlar bilan ishlaydi, bu esa maxfiylikka jiddiy tahdid tug‘diradi.

Bundan tashqari, zamonaviy texnologiyalar rivojlanishi natijasida sun’iy intellekt asosidagi tizimlar ba’zi hollarda inson aralashuvisiz ham hujumlarni amalga oshirish darajasiga yetib bormoqda. Bu esa kiberxavfsizlikni yanada murakkablashtiradi.

3. Sun’iy intellektdan foydalanishdagi muammolar

Sun’iy intellektni kiberxavfsizlikda qo‘llash bir qator muammolarni keltirib chiqaradi:

Noto‘g‘ri signal (false positive) – xavfsiz faoliyat ham tahdid sifatida baholanishi mumkin

Shaffoflik muammosi – SI qarorlarini tushuntirish qiyin

Mutaxassislar yetishmasligi – malakali kadrlar kam

Haddan tashqari ishonch – inson nazoratining kamayishi xavf tug‘diradi

Shuningdek, ayrim tashkilotlar SI texnologiyalarini yetarli sinovsiz joriy etishi natijasida ma’lumotlar sizib chiqishi holatlari ham kuzatilmoqda.

4. Kelajak istiqbollari va yechimlar

Kelajakda sun’iy intellekt kiberxavfsizlikning ajralmas qismiga aylanadi. Shu sababli quyidagi choralarni amalga oshirish muhim:

SI tizimlari ustidan inson nazoratini saqlash

Kiberxavfsizlik siyosatini takomillashtirish

Ma’lumotlarni himoya qilish bo‘yicha qat’iy qonunchilikni rivojlantirish

SI tizimlarini muntazam test va auditdan o‘tkazish

Malakali mutaxassislar tayyorlash

Mutaxassislarning fikriga ko‘ra, hozirgi kunda SI va kiberxavfsizlik o‘rtasida o‘ziga xos “qurollanish poygasi” mavjud bo‘lib, himoya va hujum texnologiyalari bir vaqtda rivojlanmoqda.

Xulosa

Xulosa qilib aytganda, sun’iy intellekt kiberxavfsizlik sohasida ulkan imkoniyatlar yaratmoqda. U tahdidlarni tez aniqlash, hujumlarning oldini olish va tizimlarni samarali boshqarishda muhim vosita hisoblanadi. Biroq, u bilan bog‘liq xavf va muammolarni ham inkor etib bo‘lmaydi.

Shu sababli, sun’iy intellektdan foydalanishda ehtiyotkorlik, muvozanat va doimiy nazorat zarur. Faqatgina texnologiya va inson omilini uyg‘unlashtirish orqali xavfsiz va barqaror raqamli muhitni ta’minlash mumkin.

Foydalanilgan adabiyotlar:

1. Russell, S., Norvig, P. — Artificial Intelligence: A Modern Approach. Pearson, 2021.
2. Goodfellow, I., Bengio, Y., Courville, A. — Deep Learning. MIT Press, 2016.
3. Stallings, W. — Network Security Essentials. Pearson, 2020.
4. Bishop, M. — Computer Security: Art and Science. Addison-Wesley, 2019.
5. ENISA (European Union Agency for Cybersecurity) — AI and Cybersecurity Report, 2023.
6. IBM Security — Cost of a Data Breach Report, 2024.
7. NIST — AI Risk Management Framework, 2023.
8. McKinsey & Company — The State of AI, 2023.
9. World Economic Forum — Global Cybersecurity Outlook, 2024.

10. Kaspersky Lab — Cyberthreat Landscape Report, 2023.