SUN’IY INTELLEKT YORDAMIDA KIBERXAVFSIZLIK TIZIMLARINI AVTOMATLASHTIRISH

Madraximov Shuxratjon Shukurovich - Qo‘qon davlat universiteti

Raqamli texnologiyalar va sun’iy intellekt kafedrasi dotsent v.b.

Madraximova Maxfuza Axmedovna - Qo‘qon davlat universiteti

Raqamli texnologiyalar va sun’iy intellekt kafedrasi assistent o‘qituvchisi

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, avtomatlashtirish, anomaliya aniqlash, tahdidlarni prognozlash.

Annotatsiya: Ushbu maqolada sun’iy intellekt (SI) texnologiyalarining kiberxavfsizlik sohasida avtomatlashtirishdagi o‘rni va ahamiyati tahlil qilinadi. SI yordamida kiberxavfsizlik tizimlarining samaradorligi oshirilishi, tahdidlarni aniqlash va ularga javob berish jarayonlari avtomatlashtirilishi haqida batafsil ma’lumotlar keltiriladi. Shuningdek, avtomatlashtirish jarayonida yuzaga keladigan muammolar va ularning yechimlari ko‘rib chiqiladi.

OF CYBERSECURITY SYSTEMS USING ARTIFICIAL INTELLIGENCE

Madrakhimov Shukhratjon Shukurovich – Acting Associate Professor at the Department of Digital Technologies and AI, Kokand State University

Madrakhimova Makhfuza Akhmedovna – Assistant Teacher, Department of Digital Technologies and AI, Kokand State University

Keywords: Artificial intelligence, cybersecurity, automation, anomaly detection, threat forecasting.

Abstract: This article analyzes the role and significance of artificial intelligence (AI) technologies in automating the field of cybersecurity. It provides detailed insights into enhancing the efficiency of cybersecurity systems through AI, as well as the automation of threat detection and response processes.

Additionally, the challenges arising during the automation process and their potential solutions are examined.

Kirish

Bugungi kunda shiddat bilan rivojlanayotgan raqamli dunyoda kiberxavfsizlik har qanday tashkilot, korxona va davlat muassasalari uchun barqaror faoliyat yuritishning eng muhim va strategik omillaridan biri hisoblanadi. Global internet tarmog‘i va axborot texnologiyalarining keng joriy etilishi natijasida, kiberhujumlar soni va ularning murakkablik darajasi yil sayin eksponental ravishda oshib bormoqda. Zamonaviy xakerlik hujumlari an’anaviy himoya tizimlarini osongina aylanib o‘tishga qodir bo‘lgani sababli, kiberxavfsizlik tizimlarini tubdan isloh qilish va ularni to‘liq avtomatlashtirish davr talabiga aylanmoqda.

Aynan shu bosqichda sun’iy intellekt (SI) va mashinali o‘qitish (Machine Learning) texnologiyalari kiberxavfsizlik sohasida inqilobiy burilish yasamoqda. SI algoritmlari tarmoqdagi trillionlab ma'lumotlarni real vaqt rejimida tahlil qilish, shubhali faolliklarni soniyalarda aniqlash va inson omilidan kelib chiqadigan charchoq hamda e’tiborsizlik kabi xatolarni maksimal darajada kamaytirish uchun keng qo‘llanilmoqda. Ushbu maqolada sun’iy intellekt texnologiyalari yordamida kiberxavfsizlik tizimlarini avtomatlashtirishning asosiy usullari, ushbu jarayonning tizim samaradorligini oshirishdagi afzalliklari hamda SI texnologiyalarini joriy etishda yuzaga kelayotgan dolzarb muammolar va ularning yechimlari batafsil tahlil qilinadi.

Asosiy qism

Sun’iy intellekt (SI) - bu zamonaviy kompyuter tizimlari va algoritmlarining inson intellektiga xos bo‘lgan fikrlash, ma’lumotlardan xulosa chiqarib o‘rganish (adaptatsiya) va murakkab muammolarni mustaqil hal qilish qobiliyatiga ega bo‘lishidir. Axborot texnologiyalari shiddat bilan rivojlanayotgan bugungi davrda, kiberxavfsizlik sohasida SI texnologiyalarining o‘rni beqiyos darajada oshib bormoqda. An’anaviy xavfsizlik tizimlari faqatgina oldindan kiritilgan qoliplar

(pattern) asosida ishlagani sababli yangi turdagi tahdidlar qarshisida ojiz qolmoqda.

Aksincha, sun’iy intellektga asoslangan tizimlar tarmoq trafigini real vaqt rejimida uzluksiz monitoring qilib, undagi eng kichik anomal holatlar va shubhali xatti-harakatlarni ham soniyalar ichida aniqlash imkonini beradi. Mashinali o‘qitish va neyron tarmoqlari yordamida SI potentsial tahdidlarni nafaqat aniqlaydi, balki ularni oldindan prognoz qilib, tizimga zarar yetmasdan turib zaruriy mudofaa choralarini avtomatik tarzda ishga tushiradi. Bunday intellektual yondashuv kiberhujumlarga qarshi soniyaning ulushlarida, o‘ta samarali va tezkor javob qaytarishni ta’minlab, xavfsizlik xizmati xodimlarining ish yukini yengillatadi va ma’lumotlar daxlsizligini kafolatlaydi.

SI asosidagi kiberxavfsizlik usullari

1. Anomaliya aniqlash (Anomaly Detection): SI tizimlari tarmoq trafigidagi odatdagidan farq qiluvchi holatlarni aniqlaydi, bu esa yangi turdagi hujumlarni vaqtida aniqlashga yordam beradi.

2. Xavfsizlik voqealarini boshqarish (Security Information and Event Management -SIEM) SIEM tizimlarida SI yordami bilan katta hajmdagi ma'lumotlar tahlil qilinadi va xavf-xatarlarni avtomatik ravishda aniqlash imkoniyati yaratiladi.

3. Avtomatik javob berish (Automated Response) - SI tizimlari kiberhujum aniqlanganda avtomatik tarzda tizimni himoya qilish choralarini ko‘rishi mumkin, masalan, tarmoq ulanishini cheklash yoki hujumchi qurilmani bloklash.

4. Tahdidlarni prognozlash (Threat Intelligence) - SI yordamida kelajakdagi hujumlar va tahdidlar oldindan bashorat qilinadi, bu esa xavfsizlikni oldindan rejalashtirishga yordam beradi.

Kiberxavfsizlik tizimlarini avtomatlashtirishning afzalliklari

a) Tezlik va samaradorlik - SI tizimlari insonga nisbatan juda tez va keng ko‘lamda ma’lumotlarni tahlil qilishi mumkin.

b) Doimiy monitoring - 24/7 asosida tizimlarni nazorat qilish va tahdidlarni darhol aniqlash.

c) Inson omilini kamaytirish - Xatolar va ko‘ngilsizlik holatlarining oldini olish.

Avtomatlashtirish jarayonidagi muammolar va cheklovlar

Ma’lumotlarning sifati - SI tizimlari sifatli va yetarli miqdorda ma’lumotlarga bog‘liq, noto‘g‘ri ma’lumotlar tizimning ishlash sifatini pasaytirishi mumkin.

Yuqori hisoblash resurslari talabi - Katta ma’lumotlar bazasini tahlil qilish uchun kuchli hisoblash imkoniyatlari zarur.

Falsifikatsiya va qarshi hujumlar - Kiberjinoyatchilar SI tizimlarini aldagan holda chalg‘itish imkoniyatiga ega.

Maxfiylik va etik masalalar - Ma’lumotlarni yig‘ish va tahlil qilishda maxfiylikni ta’minlash va etik tamoyillarni buzmaslik zarur.

Xulosa

Sun’iy intellekt texnologiyalari yordamida kiberxavfsizlik tizimlarini avtomatlashtirish bugungi kunda shunchaki qo‘shimcha imkoniyat emas, balki zamonaviy va barqaror kiberxavfsizlik strategiyalarining eng markaziy va uzviy qismiga aylanib ulgurdi. Mazkur intellektual yondashuv axborot tizimlarini himoya qilish mexanizmlarini har qachongidan ham samaraliroq, tezkorroq va ishonchliroq qilish imkonini beradi. Biroq, SI tizimlarini amaliyotga keng joriy etish jarayonida bir qator jiddiy muammolarni ham chetlab o‘tib bo‘lmaydi. Algoritmlarni o‘qitish uchun foydalaniladigan ma’lumotlarning yuqori sifatda bo‘lishi, o‘ta katta hajmdagi hisoblash resurslariga (hardware) bo‘lgan ehtiyoj hamda kiber-makonda SI qarorlari bilan bog‘liq etik masalalar va qonuniy javobgarlik kabi omillarni chuqur hisobga olish lozim. Shunga qaramay, kelajakda sun’iy intellekt va kiberxavfsizlik sohalarining integratsiyasi yanada chuqurlashishi muqarrar. Bu esa yaqin yillarda kibertahdidlarga mutlaqo yangicha,

proaktiv (oldindan ko‘ra biladigan) tarzda javob beruvchi innovatsion yechimlar va to‘liq mustaqil himoya platformalarining paydo bo‘lishiga zamin yaratadi.

Foydalanilgan adabiyotlar:

1. Alimov R. H., Karimov S. S. Kiberxavfsizlik tizimlarida intellektual monitoring texnologiyalarini qo‘llash istiqbollari. Axborot texnologiyalari va xavfsizlik, 2023, № 2(3), 45–53 b.

2. Bazarova Sh. A. Tarmoq xavfsizligida anomaliyalarni aniqlashning intellektual usullari va algoritmlari. O‘zbekiston zamonaviy axborot tizimlari va texnologiyalari jurnali, 2024, № 5(2), 78–85 b.

3. Gulyamov S. S. Kiberxavfsizlikning huquqiy va institutsional asoslarida sun’iy intellekt texnologiyalarini qo‘llash istiqbollari. Axborot texnologiyalari va xavfsizlik, 2023, № 1(4), 112–119 b.

4. Xalilov M. M., Tojiyev J. R. Katta ma’lumotlar (Big Data) muhitida kiberhujumlarni neyron tarmoqlari yordamida prognozlash. Oliy ta’limda raqamli texnologiyalar jurnali, 2024, № 3(1), 18–29 b.