KIBERXAVFSIZLIKDA SUN'IY INTELLEKT: TAHDIDLARNI ANIQLASH VA OLDINI OLISH

Boymurzayeva Lobar Olimjon qizi
Toshkent Axborot Texnologiyalari Universiteti Samarqand filiali,
2-bosqich talabasi, boymirzayevalobar57@gmail.com
Rajabova Hulkaroy Zoir qizi
Toshkent Axborot Texnologiyalari Universiteti Samarqand filiali,
2-bosqich talabasi, rajabovahulkaroy800@gmail.com

Annotatsiya: *Ushbu maqolada raqamli muhitda kiberxavfsizlikni ta'minlashda sun'iy intellekt (SI) texnologiyalarining roli, afzalliklari va amaliy qo'llanilishi yoritiladi. Raqamli tizimlarning kengayib borishi bilan birga kiberhujumlar soni va murakkabligi ortib borayotgani sababli an'anaviy himoya mexanizmlari yetarli emas. Shu nuqtai nazardan mashinaviy o'qitish, chuqur o'qitish va neyron tarmoqlar kabi SI yondashuvlari tahdidlarni oldindan aniqlash, baholash va bartaraf etishda yuqori samaradorlikni ta'minlaydi. Maqolada sun'iy intellekt asosida malware, phishing va boshqa hujumlarni avtomatik tahlil qilish imkoniyatlari tahlil etilgan.*

Kalit so'zlar*: Sun'iy intellekt, kiberxavfsizlik, mashinaviy o'qitish, chuqur o'qitish, neyron tarmoqlar, Big Data, anomal faoliyat, avtomatlashtirilgan tahlil, zararli dasturlar, phishing, raqamli xavfsizlik, proaktiv himoya, ma'lumotlar xavfsizligi .*

KIRISH

So'nggi yillarda raqamli texnologiyalar misli ko'rilmagan darajada rivojlanib, inson hayotining barcha jabhalariga kirib bordi. Axborot almashinuvi, onlayn xizmatlar, elektron to'lov tizimlari va masofaviy ta'lim kabi jarayonlar zamonaviy jamiyatning ajralmas qismiga aylandi. Shu bilan birga, bu qulayliklar bilan bir qatorda, axborot xavfsizligiga tahdid soluvchi yangi xavf-xatarlar ham paydo bo'ldi. Har kuni dunyo miqyosida minglab kiberhujumlar sodir bo'lmoqda, ularning aksariyati davlat muassasalari, moliya tizimlari va foydalanuvchilarning shaxsiy ma'lumotlarini nishonga olmoqda [1]

ASOSIY QISM

Asosiy qism. Sun'iy intellekt (SI) texnologiyalari kiberxavfsizlik sohasida inqilobiy o'zgarishlar keltirib chiqardi. Dastlabki yillarda himoya tizimlari asosan reaktiv yondashuvga asoslangan edi, ya'ni hujum sodir bo'lgandan keyin unga javob choralari ko'rilardi. Hozirda esa sun'iy intellekt asosidagi tizimlar proaktiv himoya yondashuvini ta'minlab, tahdidlarni oldindan aniqlash, baholash va bartaraf etish imkonini yaratmoqda.

Sun'iy intellektning eng katta ustunligi — katta hajmdagi ma'lumotlarni (Big Data) tahlil qilish va undan o'z-o'zini o'rgatish orqali xulosa chiqarish qobiliyatidir [3]. Masalan, tarmoq trafigidagi millionlab ma'lumotlar paketlarini inson kuzatib chiqolmaydi, ammo AI algoritmlari ularni soniyalar ichida tahlil qilib, noodatiy xatti-harakatlarni (anomal activity) aniqlay oladi.

Shuningdek, mashinaviy o'qitish (Machine Learning) asosida yaratilgan tizimlar tarmoqdagi normal faoliyatni "o'rganib oladi" va undan chetga chiqqan har qanday harakatni

tahdid sifatida belgilaydi. Bu usul ayniqsa ransomware, malware, phishing va brute-force kabi murakkab hujumlarni aniqlashda samarali natijalar beradi.

2. Kiber tahdidlarni aniqlashda ishlatiladigan sun'iy intellekt usullari

Kiberxavfsizlikda qo'llaniladigan asosiy sun'iy intellekt usullari quyidagilardan iborat:

Mashinaviy o'qitish (Machine Learning) — tizim mavjud ma'lumotlar asosida o'z-o'zini o'rgatadi va yangi ma'lumotlarda tahdid belgilarini aniqlaydi.

Chuqur o'qitish (Deep Learning) — neyron tarmoqlar yordamida murakkab tarmoq tuzilmalarini tahlil qiladi, zero-day (yangi) hujumlarni ham aniqlashga qodir [2].

Tabiiy tilni qayta ishlash (NLP) — foydalanuvchi xabarlarini, elektron pochta matnlarini tahlil qilib, phishing yoki zararli kontentni aniqlashda qo'llaniladi.

Ma'lumotlarni tahlil qilish (Data Analytics) — foydalanuvchi faoliyatini kuzatib, g'ayritabiiy kirishlar yoki shubhali tranzaksiyalarni aniqlaydi.

Masalan, IBM Security QRadar, Darktrace, Cylance, CrowdStrike Falcon kabi platformalar sun'iy intellekt va mashinaviy o'qitish texnologiyalarini integratsiya qilib, tarmoqlarda avtomatik kuzatuv va himoya tizimlarini yaratgan [3]. Ular real vaqt rejimida tarmoq faoliyatini tahlil qilib, tahdidlarni millisekundlar ichida aniqlaydi.

3. Tahdidlarni oldini olishda AI asosidagi yondashuvlar

Sun'iy intellekt tahdidni aniqlash bilan cheklanib qolmaydi — u bashorat qilish (prediction) imkoniyatiga ham ega [4]. Masalan, tizim ilgari sodir bo'lgan hujumlar haqidagi ma'lumotlar asosida keyingi ehtimoliy hujumni oldindan aniqlay oladi.

AI asosidagi himoya tizimlari quyidagi bosqichlarda ishlaydi:

1. Ma'lumotlarni yig'ish
2. Tahlil qilish
3. Baholash — tahdid darajasini aniqlash
4. Avtomatik javob — zarur bo'lsa tizim tahdid manbasini bloklaydi

Bu jarayonlar inson aralashuvisiz amalga oshadi.

4. Amaliy natijalar va samaradorlik

Tadqiqotlar shuni ko'rsatadiki, sun'iy intellekt asosidagi tizimlar tahdidlarni aniqlashda 90–95% aniqlik darajasiga ega (Kumar & Patel, 2023). Bu an'anaviy tizimlarga nisbatan deyarli ikki baravar yuqori natijadir [3]. Masalan, AI asosida ishlovchi Darktrace tizimi tarmoqlardagi anomaliyalarni aniqlashda inson kuzatuvchisiga qaraganda 60 baravar tez ishlaydi.

Masalani yeshish usullari. Zamonaviy axborot-kommunikatsiya tizimlarida kiberxavfsizlikni ta'minlash eng muhim ustuvor yo'nalishlardan biri hisoblanadi. Bugungi kunda kiberxavfsizlik sohasida uchrayotgan asosiy muammolardan biri — tahdidlarning tezkor rivojlanishi, ularning murakkab turlarga ega bo'lishi hamda inson tomonidan real vaqt rejimida aniqlashning qiyinligidir. Ushbu muammolarni bartaraf etish uchun sun'iy intellekt texnologiyalarini keng miqyosda joriy etish, avtomatlashtirilgan himoya tizimlarini yaratish zaruriyati yuzaga kelmoqda.

Tizimning moslashuvchanligini oshirish

Kiberxavfsizlikdagi tahdidlar doimo o'zgarib turadi, shuning uchun himoya tizimlari moslashuvchan bo'lishi zarur. Bu muammoni hal etish uchun reinforcement learning texnologiyasiga asoslangan o'z-o'zini o'rganuvchi sun'iy intellekt tizimlari joriy etilmoqda.

Ular yangi hujumlardan o‘rganib, kelajakda o‘xshash holatlarda avtomatik himoya choralarini qo‘llaydi. Bunday tizimlar mustaqil ravishda o‘sadi, moslashadi va o‘z samaradorligini uzluksiz oshirib boradi.

XULOSA VA TAKLIFLAR

Bugungi raqamli asrda axborot xavfsizligini ta’minlash har qanday tashkilot, korxona va davlat uchun strategik ahamiyat kasb etadi . Internet tarmoqlari kengayib borar ekan, u bilan birga kiberhujumlar ham son va murakkablik jihatidan ortib bormoqda. Shu nuqtai nazardan, kiberxavfsizlik tizimlarini zamonaviy texnologiyalar — xususan sun’iy intellekt (AI) bilan uyg‘unlashtirish zaruratga aylanmoqda.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson Education.

2. Goodfellow, I., Bengio, Y., & Courville, A. (2022). Deep Learning. MIT Press.

3. Chio, C., & Freeman, D. (2020). Machine Learning and Security: Protecting Systems with Data and Algorithms. O’Reilly Media.

4. Sommer, R., & Paxson, V. (2023). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. ACM TISSEC, 26(2), 45–59.