SUN’IY INTELLEKT YORDAMIDA KIBERXAVFLARNI ANIQLASH USULLARI

Muallif: *Palvaniyazova Dilbar Ametjanovna*

Kirish

Raqamli texnologiyalar jamiyat hayotining barcha sohalariga chuqur kirib borgani sari axborot xavfsizligi muammolari tobora dolzarb bo‘lib bormoqda. Kiberhujumlar, ma’lumotlarning o‘g‘irlanishi, fishing va zararli dasturlar soni har yili ortib bormoqda.

An’anaviy himoya vositalari — antiviruslar, parol tizimlari va fayrvolllar — zamonaviy tahdidlarga qarshi yetarli darajada samarali emas. Shu bois, bugungi kunda **sun’iy intellekt (AI)** texnologiyalarini kiberxavflarni aniqlash va ularning oldini olishda qo‘llash dolzarb yo‘nalishlardan biri hisoblanadi.

Asosiy qism

Sun’iy intellekt inson tafakkuriga xos tahlil va qaror qabul qilish jarayonlarini avtomatlashtirish imkonini beradi. Kiberxavfsizlik sohasida AI texnologiyalari yordamida xavf-xatarlarni **oldindan aniqlash**, **xatti-harakatlarni tahlil qilish** va **tezkor javob choralarini ishlab chiqish** imkoniyati paydo bo‘ldi.

1. Mashinali o‘rganish asosidagi xavfsizlik tizimlari

Mashinali o‘rganish (Machine Learning) algoritmlari tarmoqdagi millionlab ma’lumotlar oqimini kuzatib, odatiy xatti-harakatlar modelini shakllantiradi. Agar tizim odatdagidan farqli faoliyatni aniqlasa, bu holatni kiberxavf sifatida belgilaydi. Masalan, bank tizimlarida foydalanuvchining noodatiy pul o‘tkazmalari yoki yangi qurilmadan kirish holatlari avtomatik tarzda xavfli deb baholanadi va tizim darhol ogohlantirish beradi.

2. Neyron tarmoqlar va tahdidlarni prognozlash

Sun’iy neyron tarmoqlar (Artificial Neural Networks) katta hajmdagi ma’lumotlardan o‘rganib, ilgari noma’lum bo‘lgan kiberxavf turlarini aniqlay oladi. Bu tizimlar viruslar, fishing havolalar, zararli fayllarni aniqlashda yuqori aniqlikka

ega.

Masalan, Google va Microsoft kompaniyalari o‘z serverlarida AI asosida tahdidlarni prognozlovchi modellarni joriy etgan. Bu esa xakerlik urinishlarini ular sodir bo‘lishidan avval aniqlash imkonini bermoqda.

3. Blokcheyn va sun’iy intellekt integratsiyasi

Blokcheyn texnologiyasi ma’lumotlar butligini ta’minlasa, sun’iy intellekt ularni tahlil qiladi. Ularning integratsiyasi orqali tizimdagi har qanday o‘zgarish nazorat ostida bo‘ladi. Bu usul bank, sug‘urta, elektron hukumat va ta’lim tizimlarida ishonchli axborot muhitini yaratishga xizmat qilmoqda.

4. Real vaqt rejimida xavfsizlik monitoringi

AI asosidagi tizimlar foydalanuvchi faoliyatini doimiy kuzatib boradi, tarmoqdagi har bir kirish va chiqish jarayonini baholaydi. Natijada, tahdidlar aniq vaqtida aniqlanib, avtomatik ravishda bartaraf etiladi. Bu inson omilini kamaytiradi va himoya darajasini oshiradi.

Xulosa

Sun’iy intellekt texnologiyalarining kiberxavfsizlik sohasiga kirib kelishi — axborot tizimlarini himoyalashda sifat jihatdan yangi bosqichni boshlab berdi. AI yordamida kiberhujumlarni tezda aniqlash, ularning oqibatlarini kamaytirish va foydalanuvchi ma’lumotlarini ishonchli himoya qilish imkoniyati yaratildi. Kelgusida mashinali o‘rganish, chuqur o‘rganish (Deep Learning) va blokcheyn asosidagi AI modellarini yanada rivojlantirish orqali global axborot xavfsizligini ta’minlashda yuqori natijalarga erishish mumkin.

- European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2025: AI Reshapes Cyber Attacks, from Phishing to Supply Chain Abuse.* 2025. Security Affairs+1
- Kaspersky. “Kaspersky Achieves 25% Increase in APT Detection with Machine Learning in H1 2024”. Press release, 2024. Касперский+1
- Alisher Ismailovich Kadirov. “Blockchain Technology and Information Security in Uzbekistan’s Digital Economy”. *International Journal of Asian Economic Light (JAEL)*, Vol.12 Issue 3, May 2024. eprajournals.com

- Andrey Rodionov. “The Potential of Blockchain Technology to Enhance Security, Privacy, and Standardization in the Internet of Things”. *Uzbek Journal of Law and Digital Policy*, Vol.1 No.3, 2024. irshadjournals.com
- Kuvonchbek Rakhimberdiev. “Application of Blockchain Technologies in Ensuring the Security of Lending Transactions in the Digital Economy”. *Economics and Innovative Technologies*, Vol.11 Issue 2, 2024.