SUN'IY INTELLEKT ASOSIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH USULLARINI TAKOMILLASHTIRISH

UNIVERSITY OF BUSINESS AND SCIENCE
"aniq fanlar" kafedrasi
Katta o'qituvchisi ***Hayitov Nasim To'lqin o'g' li***
Nasimhayitov1996@gmail.com

Annotatsiya

Ushbu maqolada sun'iy intellekt texnologiyalaridan foydalangan holda kiberhujumlarni aniqlash va oldini olish usullarini takomillashtirish masalalari tahlil qilingan. Kiberxavfsizlik sohasida qo'llanilayotgan mashinaviy o'qitish va chuqur o'qitish algoritmlarining imkoniyatlari, ularning afzalliklari hamda cheklovlari ko'rib chiqilgan. Shuningdek, sun'iy intellekt asosida ishlovchi zamonaviy hujumlarni aniqlash tizimlari, ularning samaradorligini oshirish yo'llari va istiqbolli rivojlanish yo'nalishlari yoritilgan.

Kalit so'zlar: sun'iy intellekt, kiberxavfsizlik, kiberhujum, mashinaviy o'qitish, chuqur o'qitish, IDS, IPS, neyron tarmoqlar, tarmoq xavfsizligi.

Kirish

Raqamli transformatsiya jarayonlarining jadallashuvi natijasida axborot-kommunikatsiya texnologiyalari hayotning barcha jabhalariga keng joriy etilmoqda. Davlat boshqaruvi, bank tizimi, sog'liqni saqlash, ta'lim va sanoat korxonalarida axborot tizimlaridan foydalanishning ortishi kiberxavfsizlik masalasini dolzarb muammoga aylantirmoqda.

Kiberjinoyatchilar tomonidan amalga oshirilayotgan hujumlar soni va murakkabligining ortib borishi an'anaviy himoya vositalarining samaradorligini pasaytirmoqda. Signaturaga asoslangan himoya tizimlari yangi va ilgari uchramagan tahdidlarni aniqlashda qiyinchiliklarga duch keladi. Shu sababli sun'iy intellekt texnologiyalarini kiberxavfsizlik tizimlariga integratsiya qilish zarurati yuzaga kelmoqda.

Sun'iy intellekt katta hajmdagi ma'lumotlarni tezkor qayta ishlash, yashirin qonuniyatlarni aniqlash va kelajakdagi tahdidlarni bashorat qilish imkoniyatiga ega bo'lib, zamonaviy kiberxavfsizlik tizimlarining muhim tarkibiy qismiga aylanmoqda.

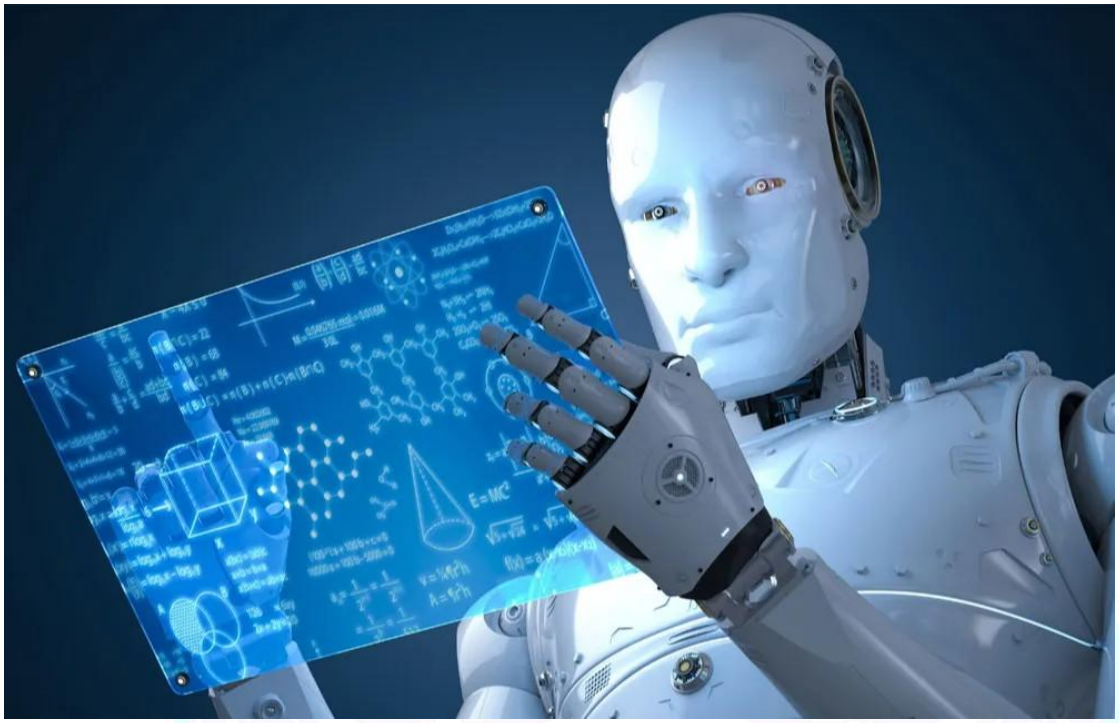
Sun'iy intellektning kiberxavfsizlikdagi o‘rni

Sun'iy intellekt asosidagi tizimlar tarmoq trafigini uzluksiz monitoring qilish, foydalanuvchilarning xatti-harakatlarini tahlil qilish hamda zararli faoliyat belgilarini aniqlash imkonini beradi.

Kiberxavfsizlikda sun'iy intellekt quyidagi vazifalarni bajaradi:

- tarmoqdagi anomaliyalarni aniqlash;
- zararli dasturlarni tasniflash;
- fishing hujumlarini aniqlash;
- foydalanuvchi xatti-harakatlarini tahlil qilish;
- tahdidlarni prognozlash;
- avtomatik javob choralarini ishlab chiqish.

An'anaviy xavfsizlik vositalaridan farqli ravishda, sun'iy intellekt tizimlari yangi tahdidlarga moslasha oladi va o‘z faoliyatini doimiy ravishda takomillashtirib boradi.



Mashinaviy o‘qitish algoritmlaridan foydalanish

Mashinaviy o‘qitish sun'iy intellektning muhim yo‘nalishlaridan biri bo‘lib, kiberhujumlarni aniqlashda keng qo‘llaniladi.

Nazorat ostida o‘qitish (Supervised Learning)

Mazkur yondashuvda tizim oldindan belgilangan ma'lumotlar asosida o‘qitiladi.

Eng ko‘p qo‘llaniladigan algoritmlar:

- Decision Tree;
- Random Forest;
- Support Vector Machine (SVM);
- Logistic Regression;
- Naive Bayes.

Ushbu algoritmlar normal va zararli trafikni tasniflashda yuqori aniqlikni namoyon etadi.

Nazoratsiz o‘qitish (Unsupervised Learning)

Nazoratsiz o‘qitish usullari belgilangan ma'lumotlar mavjud bo‘lmaganda qo‘llaniladi.

Asosiy algoritmlar:

- K-Means;
- DBSCAN;
- Principal Component Analysis (PCA).

Mazkur usullar ilgari noma'lum bo‘lgan tahdidlarni aniqlash imkonini beradi.

Chuqur o‘qitish texnologiyalarining qo‘llanilishi

Chuqur o‘qitish murakkab tarmoq hujumlarini aniqlashda samarali hisoblanadi.

Konvolyutsion neyron tarmoqlar (CNN)

CNN algoritmlari tarmoq trafigidagi murakkab bog‘liqliklarni aniqlash imkonini beradi. Ular ayniqsa zararli dasturlarni aniqlashda samarali qo‘llaniladi.

Rekurrent neyron tarmoqlar (RNN)

RNN va LSTM modellaridan vaqt qatorlari ko‘rinishidagi ma'lumotlarni tahlil qilishda foydalaniladi.

Ularning afzalliklari:

- ketma-ket hodisalarni tahlil qilish;
- DDoS hujumlarini aniqlash;
- uzoq muddatli bog‘liqliklarni aniqlash.

Autoencoder modellari

Autoencoderlar anomaliyalarni aniqlashda keng qo‘llaniladi. Ular normal trafik modelini o‘rganib, undan chetlanishlarni tahdid sifatida belgilaydi.

IDS va IPS tizimlarini takomillashtirish

IDS (Intrusion Detection System)

IDS tizimlari tarmoq faoliyatini monitoring qilib, shubhali harakatlar haqida xabar beradi.

Sun'iy intellekt asosidagi IDS tizimlarining afzalliklari:

- real vaqt rejimida tahlil;
- yuqori aniqlik;
- yangi tahdidlarni aniqlash imkoniyati;
- avtomatik o‘rganish.

IPS (Intrusion Prevention System)

IPS tizimlari nafaqat hujumlarni aniqlaydi, balki ularni oldini olish choralarini ham ko‘radi.

Sun'iy intellekt bilan integratsiyalashgan IPS tizimlari:

- zararli trafikni bloklaydi;
- foydalanuvchi sessiyalarini cheklaydi;
- xavf darajasini baholaydi;
- avtomatik javob mexanizmlarini ishga tushiradi.

Sun'iy intellekt asosidagi yondashuvlarning afzalliklari

Afzalliklar	Tavsifi
Yuqori aniqlik	Murakkab tahdidlarni aniqlash imkonini beradi
Moslashuvchanlik	Yangi hujum turlariga moslasha oladi
Tezkorlik	Katta hajmdagi ma'lumotlarni qisqa vaqtda qayta ishlaydi
Avtomatlashtirish	Inson omilini kamaytiradi
Bashorat qilish	Potensial tahdidlarni oldindan aniqlaydi

Mavjud muammolar

Sun'iy intellektning kiberxavfsizlikda qo‘llanilishiga qaramasdan, bir qator muammolar saqlanib qolmoqda:

- sifatli o‘quv ma'lumotlarining yetishmasligi;
- noto‘g‘ri ijobiy natijalar (False Positive);
- modelning tushuntiriluvchanligi pastligi;
- hisoblash resurslariga yuqori talab;
- sun'iy intellekt tizimlarining o‘ziga qaratilgan hujumlar.

Mazkur muammolarni bartaraf etish ilmiy tadqiqotlarning asosiy yo‘nalishlaridan biri hisoblanadi.

Takomillashtirish yo‘nalishlari

Kiberhujumlarni aniqlash va oldini olish tizimlarini yanada rivojlantirish uchun quyidagi yo‘nalishlar tavsiya etiladi:

1. Gibrid mashinaviy o‘qitish modellarini ishlab chiqish;
2. Federativ o‘qitish texnologiyalaridan foydalanish;
3. Izohlanadigan sun'iy intellekt (Explainable AI) modellarini joriy etish;
4. Real vaqt rejimida ishlovchi tizimlarni takomillashtirish;
5. Sun'iy intellekt va blokcheyn texnologiyalarini integratsiyalash;
6. Kiberxavfsizlik bo‘yicha milliy ma'lumotlar bazalarini shakllantirish.

Xulosa

Sun'iy intellekt asosida kiberhujumlarni aniqlash va oldini olish usullarini takomillashtirish zamonaviy kiberxavfsizlikning ustuvor yo‘nalishlaridan biri hisoblanadi. Mashinaviy o‘qitish va chuqur o‘qitish algoritmlari an'anaviy himoya vositalariga nisbatan yuqori samaradorlikni ta'minlaydi hamda yangi tahdidlarni aniqlash imkonini beradi.

Kelgusida sun'iy intellektning izohlanadigan modellari, federativ o‘qitish va gibrid himoya mexanizmlarini ishlab chiqish kiberxavfsizlik tizimlarining ishonchliligini yanada oshirishi kutilmoqda. Shu bois sun'iy intellektni kiberxavfsizlik sohasiga joriy etish bo‘yicha ilmiy tadqiqotlarni kengaytirish muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. Pearson Education, 2021.
2. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.
3. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 2016.
4. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, 2010.

5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2007.
6. Stallings W. *Network Security Essentials*. Pearson, 2017.
7. Shone N. et al. A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018.
8. Kim G., Lee S., Kim S. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection. *Expert Systems with Applications*, 2014.
9. Alzahrani A. Artificial Intelligence in Cybersecurity: A Comprehensive Review. *Journal of Information Security*, 2022.
10. Sutton R.S., Barto A.G. *Reinforcement Learning: An Introduction*. MIT Press, 2018.
11. NIST Cybersecurity Framework 2.0, 2024.
12. ENISA Threat Landscape Report, 2024.
13. IBM X-Force Threat Intelligence Index, 2025.
14. Microsoft Digital Defense Report, 2025.
15. Cisco Cybersecurity Readiness Index, 2025.
16. Palo Alto Networks Unit 42 Threat Report, 2025.
17. Kaspersky Security Bulletin, 2025.
18. Darktrace Annual Threat Report, 2025.
19. Ng A. *Machine Learning Yearning*. DeepLearning.AI, 2018.
20. O‘zbekiston Respublikasining kiberxavfsizlikni rivojlantirishga oid normativ-huquqiy hujjatlari.