ILMIY YANGILIKLAR VA INTELLEKTUAL TADQIQOTLAR JURNALI
1-Jild. 4-Son. NOYABR. 2025-yil

SUN’IY INTELLEKT VA KIBERXAVFSIZLIK: IMKONIYATLAR VA XAVF-XATARLAR

Qurbonaliyev G’olibjon Alisher o’g’li
Ichki Ishlar Vazirligi Akademiyasi

Annotatsiya: Ushbu maqolada sun’iy intellekt (SI) texnologiyalarining kiberxavfsizlik sohasidagi roli, imkoniyatlari va yuzaga keladigan xavf-xatarlar tahlil qilinadi. SI yordamida kiberxavflarni aniqlash, oldini olish va ularga qarshi tezkor javob berish tizimlari samaradorligi oshirilmoqda. Biroq, ayni paytda SI texnologiyalarining noto‘g‘ri qo‘llanilishi yoki yomon niyatli subyektlar tomonidan suiiste’mol qilinishi yangi tahdidlarni keltirib chiqaradi. Maqolada SI asosida ishlovchi kiberxavfsizlik tizimlari, ularning afzalliklari va kamchiliklari, shuningdek, sun’iy intellektning kiberhujumlarda qo‘llanilishi bilan bog‘liq xavf-xatarlar muhokama qilinadi. Kiberxavfsizlikda SI texnologiyalarining xavfsiz va samarali qo‘llanilishi uchun tavsiyalar beriladi.

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, mashinani o‘rganish, tahdidlarni aniqlash, avtomatlashtirilgan xavfsizlik, kiberhujumlar, tahdidlarni prognozlash, SI xatarlar.

Sun’iy intellekt (SI) so‘nggi yillarda tez sur’atlar bilan rivojlanib, turli sohalarda, jumladan kiberxavfsizlikda ham muhim rol o‘ynay boshladi. Kiberxavfsizlik — axborot tizimlari, tarmoqlar va foydalanuvchilarni kiberhujumlar, zararli dasturlar va boshqa tahdidlardan himoya qilish jarayonidir. Ushbu jarayonda yuzaga keladigan murakkab va ko‘lamli tahdidlarni aniqlash va ularga qarshi tezkor javob berish uchun an’anaviy xavfsizlik vositalari yetarli bo‘lmasligi mumkin. Shu sababli, SI asosida ishlovchi texnologiyalar kiberxavfsizlik tizimlarini yangi darajaga olib chiqmoqda.

SI yordamida tahdidlarni avtomatik aniqlash, tahlil qilish va ularni oldini olish imkoniyatlari kengaymoqda. Mashinani o‘rganish algoritmlari asosida ishlovchi tizimlar tarmoq trafigini kuzatib borib, noan’anaviy harakatlarni aniqlay oladi, shu orqali kiberhujumlarni erta bosqichda aniqlash imkonini yaratadi. Bunga qo‘shimcha ravishda, SI texnologiyalari kiberxavfsizlikni boshqarish jarayonlarini avtomatlashtirish, resurslarni samarali taqsimlash va insonga bog‘liq xatolarni kamaytirishda yordam beradi.

Biroq, sun’iy intellekt kiberxavfsizlikda faqat imkoniyatlar emas, balki yangi xavf-xatarlarni ham yuzaga keltiradi. Yomon niyatli foydalanuvchilar SI texnologiyalaridan kiberhujumlar uchun foydalanishi, xususan, avtomatik xakerlik vositalarini yaratishi yoki tahdidlarni yashirish uchun ilg‘or texnikalarni qo‘llashi mumkin. Shuning uchun, SI texnologiyalarining xavfsiz va samarali qo‘llanilishi uchun ilmiy va amaliy tadqiqotlar olib borilishi, xavfsizlik standartlari ishlab chiqilishi muhim ahamiyat kasb etadi. Ushbu maqolada sun’iy intellektning kiberxavfsizlikdagi imkoniyatlari, mavjud xatarlar va ularning oldini olish yo‘llari haqida keng qamrovli tahlil beriladi hamda amaliy tavsiyalar taqdim etiladi.

Sun’iy intellekt (SI) texnologiyalari so‘nggi yillarda kiberxavfsizlik sohasida inqilobiy o‘zgarishlarni olib keldi. An’anaviy xavfsizlik vositalari va usullari ko‘pincha murakkab va tezkor rivojlanayotgan kiberhujumlarga javob berishda yetarli bo‘lmaydi. Shu bois, SI yordamida yaratilgan tizimlar tahdidlarni aniqlash, oldini olish va ularga tezkor javob qaytarishda yuqori samaradorlik ko‘rsatmoqda. SI asosidagi yondashuvlar ko‘plab sohalarda — tarmoqlarni monitoring qilish, zararli dasturlarni aniqlash, foydalanuvchi xatti-harakatlarini tahlil qilish va hujumlarni prognozlashda qo‘llanilmoqda.

Mashinani o‘rganish (machine learning) algoritmlari yordamida qurilgan kiberxavfsizlik tizimlari noan’anaviy va ilg‘or kiberhujumlarni aniqlashda samaradorligini namoyish etmoqda. Masalan, anomal trafikni kuzatib borish orqali tizim kutilmagan xatti-harakatlarni aniqlaydi va ularga tezkor javob beradi. Bu esa phishing, DDoS, ransomware kabi hujumlarni boshlanish bosqichida aniqlash imkonini beradi. Shuningdek, SI yordamida foydalanuvchi profillarini yaratish va normal holatdan chetga chiqishni aniqlash — kiberhujumlarni oldini olishda muhim vosita hisoblanadi.

SI texnologiyalarining yana bir afzalligi — xavfsizlik tizimlarini avtomatlashtirishdir. Inson omili kiberxavfsizlikdagi eng zaif bog‘ bo‘lib, xodimlarning kamchiliklari, noto‘g‘ri qarorlari ko‘plab hujumlarga sabab bo‘ladi. SI yordamida avtomatik tarzda tahdidlarni aniqlash va ularni bartaraf etish jarayonlari joriy etilib, inson xatolarini kamaytirish mumkin. Shu bilan birga, SI tizimlari xodimlarga yordamchi vosita sifatida faoliyat yuritib, katta hajmdagi ma’lumotlarni tez va samarali tahlil qiladi.

Biroq, sun’iy intellektning kiberxavfsizlik sohasidagi qo‘llanilishi bilan bog‘liq xavf-xatarlar ham mavjud. Eng asosiy xavf — bu SI texnologiyalaridan yomon niyatli subyektlar tomonidan foydalanishdir. Masalan, avtomatik xakerlik vositalari, zararli dasturlarni yaratish yoki tahdidlarni yashirish uchun SI algoritmlari qo‘llanilishi mumkin. Shu sababli, kiberhujumlarning yanada murakkablashishi va avtomatlashtirilishi ehtimoli ortmoqda. Bundan tashqari, SI tizimlari ham hujumga uchrashi mumkin, ya’ni hujumchilar mashinani o‘rganish modellarini aldash yoki noto‘g‘ri qaror qabul qilishga majbur qilish usullarini ishlab chiqmoqda (adversarial attacks).

SI asosidagi tizimlarning zaifliklari, shu jumladan ma’lumotlar sifati va miqdoriga bog‘liq muammolar, modellarni noto‘g‘ri o‘rgatish, va algoritmik xatolar ham kiberxavfsizlikda salbiy ta’sir ko‘rsatishi mumkin. Masalan, noto‘g‘ri o‘rgatilgan model aniq tahdidlarni aniqlay olmasligi yoki noto‘g‘ri ogohlantirishlar berishi mumkin. Bu esa tizim ishonchliligini pasaytiradi va xavfsizlikni ta’minlashdagi muammolarni keltirib chiqaradi.

Kiberxavfsizlikda sun’iy intellektdan samarali foydalanish uchun bir qator muhim yondashuvlar mavjud. Avvalo, SI tizimlarini qurishda ma’lumotlarning sifati va ishonchliligiga e’tibor qaratish zarur. Shuningdek, mashinani o‘rganish modellarini doimiy yangilash va monitoring qilish orqali ularning samaradorligini saqlash mumkin. Bundan tashqari, SI texnologiyalaridan foydalanish jarayonida inson nazorati va aralashuvi ham muhimdir — avtomatik tizimlar xatolarni yuzaga keltirishi mumkinligi sababli, inson ekspertlari tizim ish faoliyatini doimiy kuzatib borishi zarur.

Kiberxavfsizlik siyosatini ishlab chiqishda SI texnologiyalarining imkoniyatlari va xavf-xatarlarini hisobga olish kerak. Bu nafaqat texnologik choralar, balki xodimlarni o‘qitish, yangi tahdidlar haqida muntazam xabardor qilish va kiberxavfsizlik madaniyatini shakllantirishni ham o‘z ichiga oladi. Tashkilotlar sun’iy intellektga asoslangan xavfsizlik yechimlarini tanlashda ehtiyotkor bo‘lishlari va ularni mavjud infratuzilma bilan uyg‘unlashtirishlari lozim.

Yana bir muhim jihat — xalqaro hamkorlik va qonunchilik sohasida SI texnologiyalarining kiberxavfsizlikda xavfsiz qo‘llanilishini ta’minlash. Bu, ayniqsa, sun’iy intellektning tahdidlarga qarshi kurashda salbiy foydalanilishi holatlarini kamaytirish uchun zarur. Xalqaro standartlar va tartibga solish mexanizmlari ishlab

chiqilishi, tajriba almashinuvi va birgalikdagi tadqiqotlar kiberxavfsizlik sohasida SI imkoniyatlarini to‘liq ochishga xizmat qiladi.

Kelajakda sun’iy intellektning kiberxavfsizlikda roli yanada kuchayishi kutilmoqda. Zamonaviy texnologiyalar, xususan, chuqur o‘rganish (deep learning), tabiiy tilni qayta ishlash (NLP) va avtomatlashtirilgan qaror qabul qilish tizimlari kiberxavfsizlikning yangi darajasini yaratadi. Shu bilan birga, yangi kiberxavfsizlik yondashuvlari va strategiyalarini ishlab chiqish, doimiy ravishda tahdidlarni aniqlash va ularga qarshi kurashish imkoniyatlarini kengaytirish uchun ilmiy tadqiqotlar va amaliy ishlar davom ettirilishi lozim.

Xulosa qilib aytganda, sun’iy intellekt kiberxavfsizlikda yangi imkoniyatlar ochmoqda va tizimlarni samarali himoya qilishga yordam bermoqda. Biroq, ushbu texnologiyaning yomon niyatli qo‘llanilishi va texnologik zaifliklar yangi xavf-xatarlarni yuzaga keltiradi. Shuning uchun, SI asosidagi xavfsizlik tizimlarini yaratishda, qo‘llashda va rivojlantirishda ehtiyotkorlik, doimiy monitoring va xalqaro hamkorlik talab etiladi. Faqat shu yo‘l bilan kiberxavfsizlik sohasida sun’iy intellektning afzalliklaridan to‘liq foydalanish mumkin bo‘ladi.

Foydalanilgan adabiyotlar

1. Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
3. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, 305–316.
4. Bostrom, N. (2017). *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press.
5. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011). Adversarial Machine Learning. *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, 43–58.
6. Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The Security of Machine Learning. *Machine Learning*, 81(2), 121–148.

7. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.

8. Sommer, R. (2017). Machine Learning and Security: The Future. *IEEE Security & Privacy*, 15(4), 14–16.

9. Kaspersky Lab. (2023). *Artificial Intelligence in Cybersecurity: Opportunities and Threats*.

10. FireEye. (2022). *M-Trends Report: Cyber Threat Landscape and AI*.

11. National Institute of Standards and Technology (NIST). (2020). *Special Publication 800-207: Zero Trust Architecture*.

12. Chio, C., & Freeman, D. (2018). *Machine Learning and Security: Protecting Systems with Data and Algorithms*. O'Reilly Media.

13. Zhang, C., & Chen, H. (2019). Artificial Intelligence in Cybersecurity: The State of the Art. *Computers & Security*, 85, 1–15.

14. Bower, D. J., & Butt, S. (2021). AI and Cybersecurity: Understanding Risks and Benefits. *Journal of Cybersecurity Technology*, 5(3), 148–163.

15. Ng, A. (2018). *Machine Learning Yearning*. [Online] Available at: https://www.mlyearning.org/