SUN'IY INTELLEKT VA AXBOROT XAVFSIZLIGI: YANGI TAHDIDLAR VA IMKONIYATLAR

Akramova Munisa A'zamjon qizi
Farg'ona Davlat Universiteti Chet tillari fakulteti, Filologiya va tillarni o'qitish:ingliz tli yo'nalishi 1-bosqich talabasi
Ilmiy Rahbar: **Toshboltayev Faxriddin O'rinboyevich**

Annotatsiya: *Maqolada sun'iy intellekt (SI) texnologiyalarining jadal rivojlanishi va ularning axborot xavfsizligiga bo'lgan ta'siri atroflicha tahlil qilinadi. SI texnologiyalarining axborotni himoya qilishdagi imkoniyatlari bilan bir qatorda, yangi tahdidlar, xususan kiberhujumlar, ma'lumotlarni soxtalashtirish, avtomatlashtirilgan hujumlar kabi xavf omillari yoritiladi. Shuningdek, maqolada sun'iy intellekt yordamida xavfsizlik tizimlarini takomillashtirish imkoniyatlari, huquqiy va axloqiy muammolar, xalqaro tajriba ham ko'rib chiqilgan. Tahlillar asosida SI sohasida axborot xavfsizligini ta'minlash bo'yicha taklif va tavsiyalar ilgari suriladi.*

Kalit so'zlar: *Sun'iy intellekt, axborot xavfsizligi, kiberxavfsizlik, raqamli tahdidlar, ma'lumotlarni himoya qilish, avtomatlashtirilgan tizimlar, kiberhujumlar.*

Abstract: *The article provides an in-depth analysis of the rapid development of artificial intelligence (AI) technologies and their impact on information security. Along with the opportunities AI offers for protecting information, the article highlights new threats, including cyberattacks, data falsification, and automated attacks. It also examines the possibilities for improving security systems through AI, as well as the legal and ethical issues involved, and reviews international experiences. Based on the analysis, the article proposes suggestions and recommendations for ensuring information security in the field of AI.*

Keywords: *Artificial intelligence, information security, cybersecurity, digital threats, data protection, automated systems, cyberattacks.*

Raqamli transformatsiya jarayonlari globallashgan dunyoda axborot texnologiyalarining hayotimizdagi o'rni keskin ortib bormoqda. Sun'iy intellekt (SI) esa bu jarayonning muhim tarkibiy qismiga aylangan bo'lgan. U nafaqat iqtisodiyot, tibbiyot, ta'lim yoki sanoatda, balki axborot xavfsizligi sohasida ham

tub o‘zgarishlarga sabab bo‘lmoqda. Axborot xavfsizligi bugungi kunda har bir davlat, tashkilot va shaxs uchun strategik muammo sifatida ko‘rilmoqda. Zero, raqamli dunyodagi har bir ma’lumot — bu boylik, qudrat va hukmronlik vositasi. Sun’iy intellektning imkoniyatlari kengaygani sari u bilan bog‘liq xavflar ham ortib bormoqda. Zamonaviy kiberxavflar tobora murakkablashmoqda. Sun’iy intellekt yordamida amalga oshiriladigan avtomatlashtirilgan hujumlar, “deep fake” texnologiyalari orqali soxta axborotlar yaratish, kiberjosuslik kabi xavfli holatlar axborot xavfsizligi sohasidagi mavjud yondashuvlarni qayta ko‘rib chiqishga majbur qilmoqda. Shu bilan birga, SI xavfsizlikni ta’minlashda yangi imkoniyatlar — anomaliyalarni aniqlash, tahdidlarni oldindan bashorat qilish, real vaqt rejimida monitoring olib borish kabi yechimlarni ham taklif qilmoqda.

So‘nggi yillarda sun’iy intellekt texnologiyalari informatsion texnologiyalar sohasida inqilobiy o‘zgarishlarga sabab bo‘ldi. Dastlabki oddiy algoritmlar va ekspert tizimlardan boshlab, bugungi kunda chuqur o‘rganish (deep learning), tabiiy tilni qayta ishlash (natural language processing), mashinali o‘rganish (machine learning) kabi ilg‘or yondashuvlar ishlab chiqildi va keng qo‘llanilmoqda. Sun’iy intellekt — bu kompyuter tizimlariga inson aqliga xos funksiyalarni, ya’ni o‘rganish, mantiqiy xulosa chiqarish, rejalashtirish, tilni tushunish, muammoni hal qilish, va qaror qabul qilish kabi imkoniyatlarni beruvchi texnologiyalar majmuasidir. SI quyidagi asosiy turlarga bo‘linadi:

Daraxt ko‘rinishidagi qaror qabul qilish tizimlari (Decision Trees)

Mashinali o‘rganish tizimlari (Machine Learning)

Chuqur o‘rganish tizimlari (Deep Learning)

Ekspert tizimlar (Expert Systems)

Neyron tarmoqlar (Neural Networks)

Har bir tur axborotni qayta ishlash, tahlil qilish va xavfsizlikka taalluqli qarorlar chiqarishda o‘ziga xos ahamiyatga ega. Bugungi kunda SI quyidagi sohalarda keng qo‘llanilmoqda:

Tibbiyot: diagnostika, dorilarni ishlab chiqish, genetik tahlil.

Iqtisodiyot: fond bozorlarini tahlil qilish, moliyaviy firibgarlikni aniqlash.

Transport: avtonom avtomobillar, yo‘l harakati oqimini boshqarish.

Axborot xavfsizligi: tahdidlarni aniqlash, hujumlarni bashorat qilish, xavfsizlik monitoringi.

Demak, SI texnologiyalari nafaqat axborotni qayta ishlashni avtomatlashtiradi, balki uni himoyalash, potentsial tahdidlarni aniqlash va bartaraf etish vositasi sifatida ham xizmat qiladi. Sun’iy intellektning rivojlanishi nafaqat imkoniyatlar, balki qator xavf-xatarlarni ham yuzaga keltirmoqda. SI texnologiyalarining noto‘g‘ri yoki yovuz niyatlarda qo‘llanilishi axborot xavfsizligiga bevosita tahdid

soladi. Bu tahdidlar turli shakllarda namoyon bo‘ladi va tobora murakkab tus olmoqda. SI yordamida amalga oshiriladigan avtomatlashtirilgan kiberhujumlar hozirgi davrning eng jiddiy tahdidlaridan biridir. Masalan, mashinali o‘rganish asosida yaratilgan dasturlar tarmoqlarda zaifliklarni aniqlab, ular orqali tezkor tarzda hujum uyushtirishi mumkin. An’anaviy hujumlardan farqli ravishda, bu kabi hujumlar real vaqt rejimida o‘zgaruvchan strategiyalar asosida harakat qiladi.

Tabiiy tilni qayta ishlash va tasvirni tahrirlashda SI texnologiyalari yutuqlari orqali “deepfake” texnologiyalari paydo bo‘ldi. Bu orqali haqiqiyga o‘xshagan, ammo soxta video yoki audiodan foydalanib, shaxsiy obro‘ga putur yetkazish, ijtimoiy g‘alayonlar keltirib chiqarish yoki siyosiy manipulyatsiya qilish mumkin bo‘lmoqda. SI asosidagi tizimlar foydalanuvchilar haqidagi katta hajmdagi axborotni to‘playdi, tahlil qiladi va undan foydalanadi. Bu jarayonlar axborot maxfiyligi va shaxsiy hayot daxlsizligiga tahdid soladi. Ayniqsa, reklamachilar, IT kompaniyalar va hukumatlar tomonidan kuzatuv tizimlari orqali shaxsiy ma’lumotlar nazoratsiz yig‘ilishi xavflidir. Ba’zi davlatlar tomonidan ishlab chiqilayotgan sun’iy intellekt asosidagi avtonom qurollar, jumladan axborot urushlarida foydalanilayotgan avtomatik botlar, tarmoq manipulyatorlari — global axborot xavfsizligiga jiddiy xavf tug‘dirmoqda. Bunday tizimlar sun’iy aql asosida mustaqil hujum yoki zarar yetkazuvchi qarorlar qabul qilishi mumkin. Mashinali o‘rganish texnologiyasi yordamida ishlab chiqilgan zararli dasturlar (self-learning malware) o‘z faoliyatini muhitga moslab o‘zgartirishi, aniqlanishdan qochishi va murakkab tarmoqlarda yashirincha harakat qilishi mumkin. Bu esa an’anaviy antivirus dasturlarining zaiflashuviga olib keladi.

Sun’iy intellekt yordamida axborotni himoyalash imkoniyatlari: Sun’iy intellekt texnologiyalari axborot xavfsizligi sohasida nafaqat xavf, balki ilg‘or himoya choralarini ishlab chiqish imkoniyatini ham taqdim etadi. Bugungi kunda SI yordamida ishlab chiqilgan ilg‘or xavfsizlik tizimlari kiberhujumlarni aniqlash, real vaqt rejimida monitoring olib borish, xatti-harakatlarni bashorat qilish va avtomatik qaror qabul qilish imkonini bermoqda. Mashinali o‘rganish algoritmlari odatdagi tarmoq faoliyati asosida normal xatti-harakatni “o‘rganadi” va undan og‘ishlarni aniqlash orqali kiberxavflarni aniqlashga yordam beradi. Bu yondashuv odatiy hujumlarni emas, balki ilgari kuzatilmagan yangi tahdidlarni ham aniqlay oladi. SI yordamida ishlovchi xavfsizlik tizimlari real vaqt rejimida axborot oqimini tahlil qilib, xavfni aniqlagan zahoti avtomatik choralar ko‘rishi mumkin. Masalan, kiruvchi trafikni to‘xtatish, foydalanuvchi kirishini vaqtincha bloklash yoki administratorga xabarnoma yuborish kabi amallar bajariladi. SI algoritmlari tarixiy kiberhujumlar, foydalanuvchi xatti-harakatlari va tizimdagi o‘zgarishlar asosida tahdidlarni oldindan prognozlash imkonini beradi. Bu yondashuv orqali

korxonalar xavflarni yuzaga kelishidan oldin oldini olish choralarini ko‘rishi mumkin bo‘ladi. Yuzni tanish, ovozni aniqlash, barmoq izi yoki iris orqali autentifikatsiya qilishda SI algoritmlari ancha yuqori aniqlikka ega. Bu esa an’anaviy parollar asosidagi tizimlarga qaraganda ishonchliroq xavfsizlikni ta’minlaydi. Axborot tizimlarida foydalanuvchilarning xulq-atvorini SI orqali kuzatish orqali “insayder” tahdidlarini aniqlash mumkin. Masalan, odatiy vaqtdan tashqari tizimga kirish, nomaqbul fayllarga murojaat qilish yoki ma’lumotlarni ko‘chirib olish harakatlari aniqlanib, xavf signalizatsiyasi ishga tushiriladi. Bugungi kunda ko‘plab yirik korxonalar va davlat idoralari sun’iy intellektni o‘z xavfsizlik strategiyalariga integratsiyalamoqdalar. IBM Watson, Darktrace, CrowdStrike kabi platformalar SI asosida ishlovchi xavfsizlik yechimlarini taqdim etmoqda. Ular tahdidlarni doimiy tahlil qilib, qarorlarni avtomatik ravishda qabul qilish imkonini beradi.

Sun’iy intellekt va axborot xavfsizligi zamonaviy raqamli dunyoning ajralmas qismlariga aylangan. SI texnologiyalari, bir tomondan, axborotni himoya qilish, tahdidlarni aniqlash va oldini olish uchun ilg‘or imkoniyatlarni yaratmoqda, boshqa tomondan esa, yangi va murakkab xavf-xatarlarni yuzaga keltirmoqda. Avtomatlashtirilgan kiberhujumlar, soxta axborot tarqatish, maxfiylikning buzilishi, o‘zini o‘rganuvchi zararli dasturlar kabi tahdidlar SI orqali kuchaymoqda. Shu bilan birga, SI asosida ishlovchi anomaliya aniqlash, real vaqt rejimida monitoring, xavflarni prognozlash va biometrik autentifikatsiya kabi imkoniyatlar axborot xavfsizligi sohasida inqilobiy o‘zgarishlarni ta’minlamoqda. Sun’iy intellekt sohasining rivojlanishi huquqiy va axloqiy regulyatsiyani ham talab etmoqda. Xalqaro va milliy darajada SI bilan bog‘liq qonunlarni takomillashtirish, shaffoflik va hisobdorlikni ta’minlash, shaxsiy hayotni himoya qilish asosiy vazifalardan biri bo‘lib qolmoqda. Kelgusida sun’iy intellekt va axborot xavfsizligi sohasida o‘zaro uyg‘unlikni mustahkamlash, tahdidlar va imkoniyatlarni mutanosib tarzda boshqarish, texnologik innovatsiyalarni inson huquqlari va jamiyat manfaatlariga mos ravishda rivojlantirish eng muhim ustuvorliklardan biri bo‘ladi.

Foydalanilgan adabiyotlar

1. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. Pearson Education.

2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

3. Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review.

4. Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.

5. European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act).

6. Marr, B. (2019). Artificial Intelligence in Practice: How 50 Successful Companies Used AI and Machine Learning to Solve Problems. Wiley.

7. Darktrace. (2022). AI-powered Cyber Defense Overview. [Online] Mavjud: www.darktrace.com

8. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston – 2030” strategiyasi to‘g‘risidagi Farmoni.