KIBERXAVFSIZLIKDA SUN'IY INTELLEKTNING ROLI

Toshboltayev Faxriddin O'rinboyevich
FarDU, Axborot texnologiyalari kafedrasi katta o'qituvchisi (Phd)
Tojiddinova Diyoraxon Sanjarbek qizi
FarDU, 24.110 guruh talabasi

Annotatsiya: Ushbu maqolada kiberxavfsizlikda sun'iy intellektning roli tahlil qilingan. Avvalo, sun'iy intellektning asosiy imkoniyatlari – anomaliyalarni aniqlash, tahdidlarni real vaqt rejimida tahlil qilish va avtomatik qarorlar qabul qilish kabi afzalliklar taqdim etilgan. Shu bilan birga, sun'iy intellekt tizimlarining cheklovlari va xavflari, jumladan, noto'g'ri o'rgatish, adversarial hujumlar va avtomatik qarorlar qabul qilishdagi inson omilining yetishmasligi ham ko'rib chiqilgan. Maqolada kiberxavfsizlik tizimlarida sun'iy intellektning samaradorligini oshirish uchun zarur bo'lgan ehtiyot choralari va tavsiyalar ham berilgan.

Kalit so'zlar: Kiberxavfsizlik, sun'iy intellekt, mashinaviy o'rganish, chuqur o'rganish, adversarial hujumlar, kiberhujumlar, avtomatik qarorlar, xavfsizlik tizimlari.

Annotation: This article analyzes the role of artificial intelligence in cybersecurity. First, the main capabilities of artificial intelligence are presented, such as anomaly detection, real-time threat analysis, and automated decision-making. At the same time, the limitations and risks of AI systems, including improper training, adversarial attacks, and the lack of human factors in automated decision-making, are also discussed. The article provides necessary precautions and recommendations to improve the effectiveness of AI in cybersecurity systems.

Keywords: Cybersecurity, artificial intelligence, machine learning, deep learning, adversarial attacks, cyberattacks, automated decision-making, security systems.

Аннотация: В данной статье анализируется роль искусственного интеллекта в кибербезопасности. В первую очередь представлены основные возможности искусственного интеллекта, такие как обнаружение аномалий, анализ угроз в реальном времени и принятие автоматических решений. Также рассмотрены ограничения и риски систем искусственного интеллекта, включая неправильное

обучение, адверсариальные атаки и недостаток человеческого фактора в принятии автоматических решений. В статье также даны рекомендации и меры предосторожности, необходимые для повышения эффективности искусственного интеллекта в системах кибербезопасности.

Ключевые слова: Кибербезопасность, искусственный интеллект, машинное обучение, глубокое обучение, адверсариальные атаки, кибератаки, автоматические решения, системы безопасности.

Kiberxavfsizlik sohasida sun’iy intellekt (SI) texnologiyalarining qo‘llanilishi hozirgi kunda juda muhim rol o‘ynamoqda. Xavfsizlik tizimlarining samaradorligini oshirishda, SI imkoniyatlari alohida o‘ringa ega. Masalan, mashinaviy o‘rganish va chuqur o‘rganish algoritmlari yordamida kiberhujumlarni aniqlash va ularga javob berish jarayoni sezilarli darajada tezlashdi. Sun’iy intellektning asosiy afzalliklaridan biri – u o‘zini o‘rgatish va ma'lumotlarni tahlil qilish orqali yangilangan xavf-xatarlarni aniqlashda an’anaviy tizimlarga qaraganda ancha samarali ishlay oladi.

Biroq, sun’iy intellektning kiberxavfsizlikdagi rolini yanada chuqurroq tushunish uchun uning imkoniyatlarini aniqlash va xatoliklarni kamaytirish uchun tizimlarni doimiy ravishda yangilab borish zarur. Bu masalada tizimning real vaqt rejimida tahdidlarni aniqlash va ularga samarali javob berish qobiliyati muhim rol o‘ynaydi. Sun’iy intellekt tomonidan yaratilgan avtomatlashtirilgan xavfsizlik tahlillari tez va to‘liq javob berish imkoniyatini yaratadi, bu esa insonga bo‘lgan ehtiyojni kamaytiradi va xatoliklar sonini qisqartiradi.

Sun’iy intellekt tizimlarining kiberxavfsizlikdagi imkoniyatlari juda keng bo‘lsa-da, ularda ayrim cheklovlar va xavflar ham mavjud. Biri, bu tizimlar noto‘g‘ri o‘rgatilgan bo‘lsa, noto‘g‘ri qarorlar qabul qilishi mumkin. Aniqroq aytganda, mashina o‘rganish algoritmlari tahdidlarni noto‘g‘ri baholash va xavfsiz tizimga zarar yetkazish mumkin. Bundan tashqari, sun’iy intellekt tizimlari uchun mavjud bo‘lgan “adversarial attacks” (qarama-qarshi hujumlar) kabi tahdidlar xavfsizlikni zaiflashtirishi mumkin. Bunday hujumlar sun’iy intellekt tizimlarini noto‘g‘ri yo‘nalishda o‘rgatib, xavfsizlikni buzish imkoniyatini yaratadi.

Shu bilan birga, sun’iy intellekt tizimlarining avtomatik ravishda qarorlar qabul qilishi, ba’zan inson muhokamasining yetishmasligi va noto‘g‘ri qarorlar qabul qilishiga olib kelishi mumkin. Tizimlar avtomatik javoblar ishlab chiqarsa ham, bunday javoblar har doim to‘liq va optimal bo‘lmasligi mumkin. Avtomatik tizimlarning ishlashi faqatgina o‘z-o‘zini o‘rganish va takomillashtirish jarayonlarining muvaffaqiyatiga bog‘liq bo‘lib, agar tizimning o‘rganish jarayoni yetarli bo‘lmasa, tahdidlarni aniqlashda zaifliklar yuzaga kelishi mumkin.

Sun’iy intellekt (SI) texnologiyalarining kiberxavfsizlik tizimlaridagi amaliy qo‘llanilishi ko‘plab sohalarda o‘zining samaradorligini isbotladi. Masalan, ma'lumotlarni himoya qilish, xakerlik hujumlarini aniqlash va zararlangan tizimlarga tezkor javob berish kabi vazifalar sun’iy intellektning eng keng tarqalgan foydalanish sohalaridan biridir. Buning uchun SI tizimlari katta hajmdagi ma'lumotlarni tez va samarali tahlil qilib, noxush hodisalarni, xususan, kiberhujumlarni aniqlashda ishlatiladi. Bu jarayonda mashinaviy o‘rganish algoritmlari kiberhujumlarni aniqlash va ularga qarshi kurashishda samarali rol o‘ynaydi. Tizim o‘z-o‘zini o‘rgatib, yangi tahdidlar haqida ma'lumot to‘playdi va ularni oldini olish uchun avtomatik javoblarni ishlab chiqadi.

Masalan, Intrusion Detection Systems (IDS) yoki Intrusion Prevention Systems (IPS) kabi tizimlar, SI yordamida avtomatik ravishda tarmoqqa kiruvchi noma'lum tahdidlarni aniqlash va zararlangan tizimlarni himoya qilish imkonini beradi. Ushbu tizimlar sun’iy intellekt algoritmlari yordamida tarmoqlardagi odatiy va odatdagidan tashqari faoliyatni tahlil qiladi, bu esa ular uchun yangi tahdidlarni tezda aniqlashga imkon beradi. Shu bilan birga, "behavioral analysis" (xulq-atvor tahlili) orqali zararli faoliyatni aniqlashda sun’iy intellektdan foydalanish kiberhujumlarning yangi va ilg‘or usullarini oldini olish imkoniyatini yaratadi.

Bundan tashqari, sun’iy intellekt kiberxavfsizlikni mustahkamlashda maxsus algoritmlar, masalan, "anomaly detection" (anomaliyani aniqlash) va "pattern recognition" (na'muna tanib olish) kabi texnikalar orqali ishlaydi. Ushbu algoritmlar yordamida tizimlar odatiy xatti-harakatlarga asoslanib tahdidlarni bashorat qiladi. Tizimda yuzaga kelgan har qanday oddiy yoki noxush xatti-harakat sun’iy intellekt tomonidan avtomatik aniqlanadi va xavfsizlikni ta'minlash uchun zarur choralar ko‘riladi.

Sun’iy intellektning kiberxavfsizlik sohasida rivojlanishi kelajakda yanada kengayib borishi kutilmoqda. Hozirgi kunda sun’iy intellekt texnologiyalari, ayniqsa, mashinaviy o‘rganish va chuqur o‘rganish algoritmlari yordamida xavfsizlikni ta'minlashda juda katta muvaffaqiyatlarga erishgan. Biroq, sun’iy intellekt tizimlarining kiberxavfsizlikdagi roli yana ham kengayishi mumkin, chunki texnologiya rivojlanishda davom etmoqda. Kelajakda sun’iy intellektning kiberhujumlarga qarshi kurashishda o‘rni yanada muhimlashadi.

Kiberxavfsizlikda sun’iy intellektning asosiy istiqbollaridan biri – bu "predictive analytics" (bashoratli tahlil) vositalarining yanada rivojlanishi. Bu vositalar yordamida sun’iy intellekt tizimlari tahdidlarni oldindan bashorat qilish imkoniyatiga ega bo‘ladi. Masalan, xavfsizlikni ta'minlashda sun’iy intellekt tizimlari foydalanuvchi faoliyatini tahlil qilish orqali kelajakdagi xavf-xatarlarni aniqlash va ularga qarshi choralar ko‘rish imkonini beradi. Shuningdek, sun’iy intellekt tomonidan yaratilgan boshqaruv tizimlari yirik korporatsiyalar va davlatlar uchun xavfsizlikni ta'minlashda zarur vositalarga aylanishi mumkin.

Shu bilan birga, sun’iy intellektning kiberxavfsizlikdagi yanada rivojlanishi, “ethical AI” (axloqiy sun’iy intellekt) masalalarini ham dolzarb qilmoqda. Kelajakda sun’iy intellektni kiberxavfsizlikda samarali va adolatli tarzda ishlatish uchun axloqiy tamoyillar va qonunchilikni ishlab chiqish zaruriyatining oshishi kutilmoqda. Bu jarayonda quyidagi omillarni inobatga olish muhim: sun’iy intellekt tizimlarining shaffofligi, boshqarilishi va inson xavfsizligini ta'minlashdagi o‘rni.

Kiberxavfsizlikda sun’iy intellektning kelajagi juda yuqori darajada va tez rivojlanayotgan soha bo‘lib, uning yangi imkoniyatlari, texnologiyalari va yondashuvlari kiberxavfsizlikni sezilarli darajada kuchaytiradi. Sun’iy intellektning kiberxavfsizlik tizimlaridagi amaliy qo‘llanilishi endi faqatgina hujumlarni aniqlash va ularni oldini olish bilan cheklanmaydi, balki u xavfsizlikni optimallashtirish va avtomatlashtirish jarayonlariga ham kirib bormoqda.

Kelajakda sun’iy intellekt tizimlarining yirik va murakkab tarmoq infratuzilmalarini boshqarish imkoniyatlari yanada kuchayadi. Misol uchun, tarmoq xavfsizligini ta'minlashda "self-healing networks" (o‘zini davolash tarmoqlari) kabi texnologiyalar

sun’iy intellekt orqali rivojlanishi mumkin. Bunday tizimlar avtomatik ravishda xatoliklarni aniqlab, ularni o‘z vaqtida bartaraf etadi, shu bilan birga foydalanuvchilarning xavfsizligini ta'minlashda sun’iy intellektning roli oshadi.

Sun’iy intellektning rivojlanish istiqbollaridan yana biri bu "predictive maintenance" (bashoratli texnik xizmat) texnologiyasining kiberxavfsizlikka tatbiqidir. Bu texnologiya orqali xavfsizlik tizimlari kelajakdagi tizim ishdan chiqishlarini yoki hujumlarni oldindan aniqlab, ularga qarshi zarur choralar ko‘rish imkonini beradi. Sun’iy intellektning yordamida tarmoqlardagi barcha ma'lumotlar avtomatik ravishda tahlil qilinadi va potentsial xavflar belgilanishi bilan tizimlar o‘zini himoya qilish choralarini ko‘rishi mumkin.

Bundan tashqari, sun’iy intellektning yirik korporatsiyalar va davlatlar darajasida qo‘llanishi kiberxavfsizlikni global miqyosda samarali boshqarish imkoniyatini yaratadi. Kelajakda sun’iy intellektni jahon miqyosidagi kiberhujumlarga qarshi kurashish uchun yagona tizim sifatida ishlatish mumkin. Shu bilan birga, sun’iy intellektdan foydalangan holda kiberxavfsizlikka aloqador bo‘lgan hamkorliklarni kuchaytirish, global tarmoqlarda xavfsizlikni ta'minlashda xalqaro hamjihatlikni rivojlantirish uchun yangi imkoniyatlar ochiladi.

Sun’iy intellektning kiberxavfsizlik tizimlarida qo‘llanishi bilan birga, bu jarayonni axloqiy va huquqiy nuqtai nazardan ko‘rib chiqish muhim ahamiyatga ega. Sun’iy intellekt tizimlarining kiberxavfsizlikda qo‘llanishi ko‘plab axloqiy va huquqiy masalalarni keltirib chiqaradi. Eng avvalo, sun’iy intellektni qo‘llash jarayonida ma'lumotlarning maxfiyligi va shaxsiy hayotga daxldor bo‘lgan masalalar ko‘tariladi. Kiberxavfsizlikni ta'minlash uchun tizimlarga o‘rnatilgan sun’iy intellektning ma'lumotlarga kirish huquqi cheklanishi va tegishli qonunchilikka muvofiq tartibga solinishi kerak.

Bundan tashqari, sun’iy intellekt tizimlarining qaror qabul qilishda inson omilini o‘rni ham muhim masaladir. Biroq, sun’iy intellekt tomonidan qabul qilingan qarorlar inson xatosi yoki xatoliklariga nisbatan ko‘proq ishonchli bo‘lishi mumkin, lekin har doim ham tizimning qarorlari to‘g‘ri yoki adolatli bo‘lmasligi mumkin. Shu sababli, sun’iy intellektni kiberxavfsizlikda ishlatishda uning axloqiy tamoyillariga va insonga qarshi qarorlar qabul qilmasligi uchun shaffoflik va axloqiy qoidalar ishlab chiqilishi zarur.

Axloqiy va huquqiy masalalar bilan bir qatorda, sun’iy intellektning kiberxavfsizlik sohasida muvaffaqiyatli qo‘llanilishi uchun doimiy ravishda tizimlarni yangilab borish va insonning yordamini ta'minlash muhimdir. Sun’iy intellektning avtomatik xavfsizlik choralarini amalga oshirish qobiliyati muhim bo‘lsa-da, uning qarorlari inson tomonidan nazorat qilinishi va tahlil qilinishi kerak.

Xulosa. Kiberxavfsizlikda sun’iy intellektning roli hozirgi va kelajakda yanada muhim bo‘lib boradi. Sun’iy intellekt texnologiyalarining kiberxavfsizlik sohasida qo‘llanilishi mavjud tahdidlarga samarali va tezkor javob berish imkoniyatini yaratadi. Dastlab, sun’iy intellekt yordamida xavfsizlik tizimlari avtomatik ravishda potentsial hujumlarni aniqlab, ularga qarshi choralar ko‘rish imkoniyatiga ega bo‘lishi mumkin. Shu bilan birga, sun’iy intellekt tizimlarining joriy etilishi bilan bog‘liq axloqiy va huquqiy masalalar ham e'tiborga olinishi zarur.

Sun’iy intellektning rivojlanishi kiberxavfsizlikni nafaqat optimallashtirish, balki global miqyosda xavfsizlikni ta'minlashda ham yangi imkoniyatlar yaratadi. Garchi sun’iy intellekt tizimlarining tezkorligi va samaradorligi yuqori bo‘lsa-da, ular ma'lumotlarning maxfiyligi va shaxsiy hayotni himoya qilish nuqtai nazaridan ehtiyotkorlik bilan joriy etilishi kerak.

Kelajakda sun’iy intellektning kiberxavfsizlikda yana bir keng tarqalgan qo‘llanilishi o‘zini davolash tarmoqlari va bashoratli texnik xizmatlar bilan bog‘liq bo‘ladi. Bu texnologiyalar tarmoqlardagi xavfsizlik tizimlarini yanada ishonchli va mustahkam qiladi. Shuningdek, sun’iy intellektni xalqaro darajada kiberxavfsizlikni ta'minlashda qo‘llash muhim bo‘ladi, bu esa jahon miqyosida hamkorlikni rivojlantirishga yordam beradi.

Foydalanilgan adabiyotlar

1. Cholakov, A. (2023). *AI in cybersecurity: A survey of current and future trends*. International Journal of Cybersecurity, 15(2), 142-153.
2. Smith, J., & Brown, D. (2022). *The ethics of AI in cybersecurity*. Journal of Information Security, 13(4), 225-237.
3. Williams, L. (2021). *Artificial intelligence in cybersecurity: A critical review*. International Journal of Information Technology, 19(3), 68-82.

4. Kaur, S. (2020). *AI-driven cybersecurity solutions: Opportunities and challenges*. Journal of Cybersecurity Research, 10(1), 99-112.
5. Anderson, R., & Taylor, P. (2019). *AI and its role in the future of cybersecurity*. Cybersecurity Innovations, 5(1), 45-58.