



SUN'IY INTELLEKT DASTURLARIDA AXBOROT XAVFSIZLIGI
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРИЛОЖЕНИЯХ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
INFORMATION SECURITY IN ARTIFICIAL INTELLIGENCE
APPLICATIONS

Kuniso va Gulmira Urazxonovnaga

Navoiy davlat universiteti "Tillar" fakulteti tyutori

Кунисова Гулимира Уразхоновна

Преподаватель факультета языков Навоийского

государственного университета

Kuniso va Gulmira Urazxonovna

Tutor, Faculty of Languages, Navoi State University

Annotatsiya

Ushbu maqola sun'iy intellekt dasturlarining axborot xavfsizligidagi rolini, imkoniyatlari va xavf-xatarlarini ilmiy tahlil qiladi. Tadqiqot SI tizimlarining kiberxavfsizlikdagi qo'llanilishi, tahdidlarni aniqlash, prognoz qilish va javob choralarini avtomatlashtirish mexanizmlari konseptual va analitik yondashuvlar asosida o'rganildi. Natijalar sun'iy intellektning texnologik imkoniyatlari bilan cheklanmay, ijtimoiy, etik va normativ kontekstda ham muhim ekanligini ko'rsatadi. Maqola olimlarning tadqiqotlari bilan solishtirilgan va inson-mashina hamkorligi hamda etik mas'uliyat konsepsiyalarini tahlil qiladi.

Kalit so'zlar: Sun'iy intellekt, axborot xavfsizligi, kiberxavfsizlik, mashina o'rganish, generativ modellar, inson-mashina hamkorligi, etik mas'uliyat, normativ me'yorlar, tahdidlarni aniqlash, xavfsizlik strategiyalari.

АННОТАЦИЯ

В статье представлен научный анализ роли, возможностей и рисков применения искусственного интеллекта (ИИ) в области информационной безопасности. Исследование рассматривает использование ИИ в кибербезопасности, включая выявление угроз, прогнозирование и



автоматизированные меры реагирования, на основе концептуальных и аналитических подходов. Результаты показывают, что влияние ИИ выходит за рамки технологических возможностей и существенно зависит от социальных, этических и нормативных контекстов. Статья также сопоставляет эти результаты с существующими исследованиями и анализирует модели взаимодействия человека и машины, а также концепции этической ответственности.

Ключевые слова: Искусственный интеллект, информационная безопасность, кибербезопасность, машинное обучение, генеративные модели, взаимодействие человек–машина, этическая ответственность, нормативные стандарты, выявление угроз, стратегии безопасности.

Abstract

This article provides a scientific analysis of the role, opportunities, and risks of artificial intelligence (AI) applications in information security. The study examines the use of AI systems in cybersecurity, including threat detection, prediction, and automated response mechanisms, based on conceptual and analytical approaches. The results show that the impact of AI extends beyond technological capabilities and is significantly influenced by social, ethical, and regulatory contexts. The study also compares these findings with existing research and analyzes human–machine collaboration models and ethical responsibility frameworks.

Keywords: Artificial intelligence, information security, cybersecurity, machine learning, generative models, human–machine collaboration, ethical responsibility, regulatory standards, threat detection, security strategies.

KIRISH

So‘nggi o‘n yilliklarda sun‘iy intellekt (SI) texnologiyalari axborot xavfsizligi sohasida inqilobiy o‘zgarishlarni amalga oshirdi. Kiberxavfsizlik ilgari insonning tajribasiga va oddiy dasturiy vositalarga bog‘liq bo‘lsa, bugungi kunda SI algoritmlari murakkab tahdidlarni aniqlash, ularni prognoz qilish va javob choralarini avtomatlashtirish imkoniyatiga ega bo‘ldi. Sun‘iy intellekt dasturlari katta hajmdagi ma‘lumotlarni qayta ishlash, naqshlarni aniqlash va tarmoq trafigidagi g‘ayritabiiy



xatti-harakatlarni sezish orqali tizimlarning mustahkamligini oshiradi. Shu bilan birga, SI texnologiyalarining integratsiyasi yangi turdagi xavf-xatarlar, etik masalalar va normativ mas'uliyatni ham yuzaga keltirmoqda. Shu nuqtai nazardan, sun'iy intellektning axborot xavfsizligidagi roli ikki qirrali jarayon sifatida qaralishi lozim: u tizimlarni mustahkamlash bilan bir qatorda yangi xatarlarni ham yuzaga keltiradi.

TADQIQOD METODLARI

intellektning axborot xavfsizligidagi qo'llanilishi va uning ijtimoiy hamda texnologik ta'sirlarini chuqur o'rganishga imkon berdi. Tadqiqot jarayonida zamonaviy ilmiy adabiyotlar, xalqaro nashrlar, kitoblar va maqolalardagi tadqiqot natijalari tizimli tarzda tahlil qilindi. Shu orqali sun'iy intellektning kiberxavfsizlik sohasidagi imkoniyatlari va xavf-xatarlarini keng qamrovli baholash imkoniyati yaratilgan.

Metodologik yondashuv uch asosiy bosqichdan iborat bo'ldi. Birinchidan, nazariy tahlil amalga oshirildi. Bu bosqichda sun'iy intellekt va kiberxavfsizlik sohasidagi fundamental konseptlar, paradigmalar va ilgari olib borilgan tadqiqotlar o'rganilib, tizimli sharh berildi. Shu jarayon orqali SI texnologiyalarining asosiy printsiplari, ishlash mexanizmlari va xavfsizlikka ta'sir ko'rsatish usullari aniqlangan [4].

Ikkinchidan, komparativ tahlil o'tkazildi. Turli ilmiy manbalar orqali sun'iy intellekt tizimlarining xavfsizlikka ta'siri solishtirilib, ularning samaradorligi, tahdidlarni aniqlash qobiliyati va mavjud zaifliklari tahlil qilindi. Bu bosqich SI texnologiyalarining turli kontekstlarda qanday ishlashi va qaysi sharoitlarda samarali ekanligini aniqlash imkonini berdi.

Uchinchidan, konseptual model yaratish bosqichi amalga oshirildi. Bu bosqichda SI tizimlarining tahdidlarni aniqlash, prognoz qilish va javob choralarini avtomatlashtirish jarayonidagi o'zaro bog'liqliklar va mexanizmlar aniqlanib, tizimli yondashuv shakllantirildi. Ushbu yondashuv maqolaga ilmiy izchillik, aniqlik va metodologik asos berdi hamda sun'iy intellektning axborot xavfsizligidagi murakkab rolini tushuntirishga imkon yaratdi. Shu tarzda, maqola nafaqat nazariy jihatdan asoslangan, balki amaliy konseptual ramka orqali SI tizimlarining xavfsizlikdagi samaradorligini va muammolarini tizimli ko'rsatishga erishdi.

NATIJALAR



Tahlil natijalari shuni ko'rsatadiki, sun'iy intellekt dasturlari axborot xavfsizligi tizimlarida bir nechta asosiy funksiyani bajaradi. Birinchidan, SI tizimlari anomaliya aniqlash va tahdidlarni prognoz qilishda yuqori aniqlikka ega. Mashinaviy o'rganish va chuqur o'rganish algoritmlari tarmoq trafigidagi g'ayritabiiy naqshlarni aniqlab, xavf-xatarlarni real vaqt rejimida qayd etadi. Tadqiqot shuni ko'rsatdiki, tarixiy ma'lumotlar asosida o'rgatilgan SI tizimlari kiberhujumlarning ehtimolini oldindan baholash imkoniyatiga ega, bu esa inson resurslariga bo'lgan bog'liqlikni kamaytiradi. Ikkinchidan, SI tizimlari javob choralarini avtomatlashtirish imkoniyatiga ega. Tarmoqdagi noma'lum faoliyat aniqlanganda tizimlar avtomatik ravishda reaksiya qiladi, bu esa xodimlar ish yukini kamaytiradi va tezkor choralarni ta'minlaydi. Uchinchidan, SI tizimlari doimiy optimallashtirish va moslashuvchanlik orqali yangi hujum turlariga moslashadi. Shu orqali ular an'anaviy xavfsizlik vositalaridan ustunroq bo'ladi va murakkab kiberhujumlarni samarali bartaraf etadi [10].

Biroq natijalar shuni ham ko'rsatadiki, sun'iy intellektning axborot xavfsizligidagi qo'llanilishi bilan birga yangi turdagi tahdidlar yuzaga keladi. Generativ modellar va katta ma'lumotlar bilan ishlaydigan tizimlar xakerlar tomonidan noto'g'ri qo'llanishi mumkin, bu esa avtomatlashtirilgan hujumlar va yanada murakkab kiberhujumlarni yuzaga keltiradi. Shuningdek, noto'g'ri yoki cheklangan ma'lumotlar asosida o'rgatilgan tizimlar xavf-xatarlarni noto'g'ri baholashi yoki umuman e'tiborsiz qoldirishi mumkin. Shu jihatlar SI tizimlarini joriy etishda ehtiyotkorlikni talab qiladi.

MUHOKAMA

Ushbu tadqiqot natijalari sun'iy intellekt dasturlarining kelajakdagi rivojlanishi texnologik yutuqlar bilan cheklanib qolmasdan, chuqur ijtimoiy va etik oqibatlarga ega ekanligini ko'rsatadi. Olingan xulosalar bir qator zamonaviy tadqiqotlar bilan uyg'unlik kasb etadi. Xususan, Brynjolfsson va McAfee sun'iy intellektni iqtisodiy va ijtimoiy transformatsiyaning asosiy drayveri sifatida baholab, uning mehnat bozori va qaror qabul qilish jarayonlariga kuchli ta'sir ko'rsatishini ta'kidlaydi. Mazkur tadqiqot natijalari ham sun'iy intellektning inson faoliyatini to'liq siqib chiqarmasdan, balki uni qayta konfiguratsiyalashini tasdiqlaydi [2].



Shu bilan birga, ushbu maqolada ilgari surilgan inson–mashina hamkorligi modeli ba’zi texno-deterministik yondashuvlardan farq qiladi. Masalan, Bostrom sun’iy intellektning yuqori avtonomiyasi kelajakda inson nazoratidan chiqish xavfini keltirib chiqarishini qayd etadi. Bizning natijalar esa sun’iy intellekt avtonomiyasi oshgan sari insonning strategik va normativ nazorat roli ham kuchayib borayotganini ko’rsatadi [1]. Bu holat sun’iy intellekt rivojlanishini nol-summa jarayon emas, balki hamkorlikka asoslangan dinamik tizim sifatida talqin qilish imkonini beradi.

Etik mas’uliyat masalasida Floridi tomonidan ilgari surilgan “etik jihatdan moslashtirilgan sun’iy intellekt” konsepsiyasi bilan muayyan uyg’unlik kuzatiladi. Tadqiqot natijalari shuni ko’rsatadiki, sun’iy intellektning ijtimoiy ta’siri uning texnik imkoniyatlaridan ko’ra, ko’proq normativ va institutsional mexanizmlarga bog’liqdir [3]. Shu jihatdan, mazkur tadqiqot sun’iy intellektni tartibga solish masalasida texnologik yondashuv bilan bir qatorda ijtimoiy va falsafiy yondashuv zarurligini asoslaydi. Ushbu muhokama sun’iy intellektni faqat texnik innovatsiya sifatida emas, balki ijtimoiy mas’uliyatga ega intellektual tizim sifatida baholash zarurligini ilmiy jihatdan tasdiqlaydi.

XULOSA

Sun’iy intellekt dasturlari axborot xavfsizligi sohasida yangi imkoniyatlar yaratadi. Ular tahdidlarni aniqlash, ularni prognoz qilish, javob choralarini avtomatlashtirish va tizimlarni optimallashtirish orqali an’anaviy vositalardan yuqori samaradorlikka ega bo’ladi. Shu bilan birga, sun’iy intellektning noto’g’ri qo’llanilishi yoki nazoratsiz rivojlanishi yangi turdagi xavf-xatarlarni yuzaga keltiradi. Shu sababli axborot xavfsizligida SI tizimlarini joriy etishda strategik yondashuv, sifatli ma’lumotlar, inson nazorati va etik tamoyillar hisobga olinishi lozim. Kelajakda sun’iy intellektning axborot xavfsizligidagi roli yanada oshadi, lekin uning samarali va xavfsiz qo’llanilishi texnologik imkoniyatlar bilan bir qatorda, ijtimoiy, normativ va etik yondashuvga ham bog’liq bo’ladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Bostrom, Nick. Superintelligence: Paths, Dangers, Strategies. Oxford University Press, 2014.
2. Brynjolfsson, Erik, and Andrew McAfee. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company, 2014.
3. Floridi, Luciano. The Ethics of Artificial Intelligence. Oxford University Press, 2019.
4. Russell, Stuart, and Peter Norvig. Artificial Intelligence: A Modern Approach. 4th ed., Prentice Hall, 2020.
5. Tegmark, Max. Life 3.0: Being Human in the Age of Artificial Intelligence. Knopf, 2017.
6. Stone, Peter, et al. Artificial Intelligence and Life in 2030: The One Hundred Year Study on Artificial Intelligence (AI100). Stanford University, 2016.
7. Vaswani, Ashish, et al. "Attention Is All You Need." NeurIPS, 2017, pp. 5998–6008.
8. Schmidhuber, Jürgen. "Annotated History of Modern AI and Deep Learning." preprint, 2015.
9. Clune, Jeff. "AI-GAs: AI-Generating Algorithms, an Alternate Paradigm for Producing General Artificial Intelligence." 2019.
10. Abbosov, M. M. Sun'iy Intellekt Texnologiyalarini Tartibga Solishning Dolzarbligi. Tashkent University Press, 2022.