SUN'IY INTELLEKT TEXNOLOGIYALARINING AXBOROT XAVFSIZLIGIGA TA'SIRI

Turayeva Sabrina Kamoliddin qizi
Shahrisabz davlat pedagogika instituti
Pedagogika fakulteti Biologiya yo'nalishi 2-kurs talabasi
https://doi.org/10.5281/zenodo.15393727

Annotatsiya: Hozirgi kunda sun'iy intellekt (SI) texnologiyalari turli sohalarga jadal kirib kelmoqda. U axborot xavfsizligini ta'minlashda ham, unga tahdid solishda ham muhim rol o'ynamoqda. SI asosida ishlovchi tizimlar kiberxavfsizlikni mustahkamlash bilan birga, zararli hujumlarning ham yanada rivojlanishiga sabab bo'lishi mumkin. Ushbu maqolada sun'iy intellektning axborot xavfsizligiga ta'siri, uning ijobiy va salbiy jihatlari ko'rib chiqiladi.

Kalit so'zlar: Biometrik autentifikatsiya, Xavfsizlik devorlarini kuchaytirish, Avtomatlashtirilgan tahdid tahlili, kiberhujumlarni aniqlash, Kiberxavfsizlik monitoringi, Deepfake texnologiyasi, Adversarial Attacks, Zero Trust Security Model, Avtomatlashtirilgan xakerlik, Zararli dasturlarni aniqlash

Аннотация: В настоящее время технологии искусственного интеллекта (ИИ) стремительно проникают в различные области. Оно играет важную роль как в обеспечении информационной безопасности, так и в угрозе ей. Системы, работающие на основе СИ, усиливая кибербезопасность, могут стать причиной дальнейшего развития злонамеренных атак. В данной статье рассматривается влияние искусственного интеллекта на информационную безопасность, его положительные и отрицательные стороны.

Ключевые слова: биометрическая аутентификация, усиление межсетевых экранов, автоматический анализ угроз, обнаружение кибератак, мониторинг кибербезопасности, технология Deepfake, состязательные атаки, модель безопасности с нулевым доверием, автоматический взлом, обнаружение вредоносных программ.

Abstract: Currently, artificial intelligence (AI) technologies are rapidly entering various fields. It plays an important role both in ensuring information security and in threatening it. Systems operating on the basis of SI, while strengthening cyber security, can cause further development of malicious attacks. This article examines the impact of artificial intelligence on information security, its positive and negative aspects.

Keywords: Biometric Authentication, Strengthening Firewalls, Automated Threat Analysis, Cyber Attack Detection, Cyber Security Monitoring, Deepfake Technology, Adversarial Attacks, Zero Trust Security Model, Automated Hacking, Malware Detection

Kirish: Zamonaviy dunyoda raqamli texnologiyalar rivojlanishi bilan axborot xavfsizligi masalasi dolzarb muammolardan biriga aylandi. Sun'iy intellekt (SI) bu jarayonda muhim rol o'ynab, kiberxavfsizlikni ta'minlashda ham, uni buzishda ham samarali vositaga aylanyapti. SI algoritmlari tahdidlarni avtomatik aniqlash, xavflarni baholash, shuningdek, kiberjinoyatchilar tomonidan kiberhujumlarni takomillashtirish uchun ham qo'llanmoqda. Ushbu maqolada sun'iy intellektning axborot xavfsizligiga ta'siri, uning ijobiy va salbiy jihatlari, hamda bu texnologiyalarning kelajakdagi istiqbollari tahlil qilinadi.

Sun'iy intellektning axborot xavfsizligida qo'llanilishi: Sun'iy intellekt texnologiyalari axborot xavfsizligini ta'minlashda quyidagi yo'nalishlarda qo'llaniladi. Kiberxavfsizlik monitoringi va tahdidlarni aniqlash: SI asosida ishlovchi tizimlar real vaqtda kiberhujumlarni

aniqlash va ularga qarshi chora ko‘rish imkoniyatiga ega. Masalan, Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS) SI yordamida kiberhujumlarni aniqlash va ularningoldini olish uchun ishlatiladi. Avtomatlashtirilgan tahdid tahlili: SI katta hajmdagi ma’lumotlarni tahlil qilish orqali kiberxavfsizlik tahdidlarini aniqlaydi va hujumlar ssenariylarini taxmin qilishga yordam beradi. Bu usul yordamida kompaniyalar o‘z himoyasini kuchaytirishi mumkin. Xavfsizlik devorlarini kuchaytirish: Sun’iy intellektdan foydalanilgan firewall va antivirus dasturlari tarmoq trafigini tahlil qilib, zararli harakatlarni avtomatik ravishda bloklaydi. Biometrik autentifikatsiya: SI yuzni tanish, ovoz identifikatsiyasi va barmoq izi orqali shaxsni aniqlash kabi xavfsizlik choralarini avtomatlashtirishda keng qo‘llaniladi.

Sun’iy intellektning axborot xavfsizligiga tahdidlari

Sun’iy intellekt texnologiyalarining rivojlanishi bilan birga, ular kiberjinoyatchilar tomonidan ham foydalanilishi mumkin. Quyida SI asosidagi asosiy xavflar keltirilgan. Deepfake va ijtimoiy manipulyatsiya: SI yordamida yaratilgan deepfake texnologiyalari soxta videolar va tovush yozuvlarini tayyorlash imkonini beradi. Bu esa firibgarlik va ijtimoiy manipulyatsiyaga olib kelishi mumkin. Avtomatlashtirilgan kiberhujumlar: SI asosida ishlaydigan zararli dasturlar (masalan, AI-powered malware) kiberhujumlarni avtomatlashtirish orqali an’anaviy xavfsizlik tizimlaridan osonroq o‘tib ketishi mumkin. Adversarial Attacks (raqib hujumlari): Hujumchilar sun’iy intellekt tizimlariga o‘rgatilgan ma’lumotlarni o‘zgartirish orqali noto‘g‘ri qaror chiqarishiga sabab bo‘lishi mumkin. Masalan, SI asosidagi yuz tanish tizimlari noto‘g‘ri ishlashi uchun maxsus manipulyatsiya qilingan tasvirlardan foydalaniladi.SI asosida phishing hujumlari: Sun’iy intellektning tabiiy tilni qayta ishlash imkoniyatlari phishing hujumlarini yanada ishonchli qilishga yordam beradi. Masalan, Chatbot phishing texnologiyasi foydalanuvchilar bilan real vaqt rejimida muloqot qilib, ularning shaxsiy ma’lumotlarini olishga urinishadi.

Sun’iy intellekt asosida axborot xavfsizligini mustahkamlash yo‘llari

Sun’iy intellektga qarshi sun’iy intellekt: Kiberxavfsizlik mutaxassislari hujumchilarning SI asosidagi hujumlariga qarshi himoya sifatida o‘z sun’iy intellekt tizimlarini ishlab chiqishmoqda. Ma’lumotlarning yaxlitligini ta’minlash: SI tizimlarini manipulyatsiyalardan himoya qilish uchun raqib hujumlariga qarshi tahlil va sinov jarayonlarini kuchaytirish zarur. Kiberxavfsizlik bo‘yicha xodimlarni tayyorlash: Sun’iy intellektning xavflaridan himoyalanish uchun kiberxavfsizlik mutaxassislari yangi tahdidlarga qarshi tayyorgarlik ko‘rishi kerak.

Sun’iy intellektning axborot xavfsizligidagi ijobiy ta’siri

Kiberxavfsizlik monitoring tizimlarini rivojlantirish: An’anaviy kiberxavfsizlik tizimlari odatda statik qoidalarga asoslangan bo‘lsa, sun’iy intellekt o‘z-o‘zini o‘rganish (self-learning) algoritmlari yordamida yanada moslashuvchan va samarali ishlaydi. SI asosidagi tahdidlarni aniqlash tizimlari (Threat Detection Systems) real vaqt rejimida tarmoq trafikini kuzatib, noan’anaviy harakatlarni aniqlash va oldini olishga yordam beradi. Zararli dasturlarni aniqlash: SI asosidagi Machine Learning (ML) va Deep Learning (DL) texnologiyalari zararli dasturlarni (malware) an’anaviy antivirus dasturlaridan ancha tez aniqlashi mumkin. Masalan, Google’s Chronicle Backstory SI yordamida zararli dasturiy ta’minotlarni avtomatik ravishda skanerlash va bloklash imkoniyatiga ega. Avtomatlashtirilgan xakerlik hujumlarini aniqlash: SI asosida ishlaydigan Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS) tizimlari tarmoqda o‘zini g‘ayritabiiy tutayotgan foydalanuvchilar yoki

dasturlarni aniqlash va ularni to‘xtatish uchun ishlatiladi. SI asosida ishlaydigan autentifikatsiya va identifikatsiya: Biometrik autentifikatsiya tizimlari (yuzni aniqlash, ovoz identifikatsiyasi, barmoq izi skaneri) kiberxavfsizlikni mustahkamlashga yordam beradi. Sun’iy intellektning Behavioral Authentication (foydalanuvchining odatlariga asoslangan identifikatsiya) usuli ham shaxsiy ma’lumotlarni himoya qilishda qo‘llanilmoqda.Zero Trust Security Model (Ishonchsiz xavfsizlik modeli): SI asosida ishlovchi Zero Trust xavfsizlik modeli har bir so‘rovni oldindan tekshiradi va hatto ishonchli foydalanuvchilarning ham harakatlarini doimiy kuzatib boradi. Bu, ayniqsa, katta tashkilotlar uchun muhim.

Sun’iy intellekt asosidagi tahdidlar va xavflar

Sun’iy intellekt texnologiyalari kiberjinoyatchilar tomonidan ham ishlatilishi mumkin. Quyida ushbu tahdidlarning asosiy turlari keltirilgan.Sun’iy intellekt yordamida avtomatlashtirilgan kiberhujumlar: Hujumchilar sun’iy intellekt vositasida avtomatlashtirilgan virus va zararli kodlarni yaratib, ularni ommaviy hujumlarda qo‘llashi mumkin. AI-powered Malware (sun’iy intellekt orqali yaratilgan zararli dasturlar) an’anaviy himoya vositalaridan yashirina oladi va doimiy ravishda yangilanadi. Adversarial Attacks (raqib hujumlari): Sun’iy intellekt tizimlariga hujum qilishning eng xavfli usullaridan biri adversarial attacks hisoblanadi. Bu usulda hujumchilar SI tizimini chalg‘itish uchun maxsus manipulyatsiya qilingan ma’lumotlardan foydalanadilar. Masalan, yuzni aniqlash tizimlarini chalg‘itish uchun manipulyatsiya qilingan suratlar ishlatilishi mumkin. Deepfake texnologiyasi: Deepfake texnologiyasi yordamida hujumchilar soxta videolar va tovush yozuvlarini yaratib, odamlarni firibgarlik yoki ijtimoiy manipulyatsiyaga uchratishlari mumkin. Masalan, kiberjinoyatchilar deepfake yordamida rahbarlarning ovozini yaratib, xodimlardan maxfiy ma’lumotlar so‘rashi mumkin.

AIning axborot xavfsizligiga ijobiy ta'siri

AI tomonidan boshqariladigan tahdidlarni aniqlash va oldini olish: Sun’iy intellektga asoslangan kiberxavfsizlik yechimlari real vaqtda tarmoq trafigini tahlil qilishi, anomaliyalarni aniqlashi va potentsial tahdidlarni an’anaviy tizimlarga qaraganda tezroq aniqlashi mumkin. AI tomonidan boshqariladigan tajovuzni aniqlash tizimlari (IDS) va hujumni oldini olish tizimlari (IPS) doimiy ravishda faoliyatni kuzatib boradi va kiberhujumlardan faol himoya qiladi. Zararli dasturlar va to'lov dasturlarini aniqlash: AI va Machine Learning (ML) algoritmlari zararli koddagi naqshlarni tanib olishi va zararli dasturlar va to'lov dasturlarining yangi turlarini zarar yetkazishdan oldin aniqlashi mumkin. Misol uchun, Google Chronicle Backstory yirik tashkilotlardagi zararli dasturlar hujumlarini aniqlash va oldini olish uchun AIdan foydalanadi. Avtomatlashtirilgan xavfsizlik hodisasiga javob: Sun'iy intellekt kiber tahdidlarga javoblarni avtomatlashtirish orqali xavfsizlik ma'lumotlari va hodisalarni boshqarish (SIEM) tizimlarini yaxshilaydi. Sun'iy intellektga asoslangan xavfsizlikni tartibga solish, avtomatlashtirish va javob berish (SOAR) platformalari hodisalarni real vaqt rejimida tahlil qiladi va ularga javob beradi, inson aralashuvini minimallashtiradi va javob vaqtini qisqartiradi. AI quvvatli autentifikatsiya va identifikatsiyani tekshirish: AI biometrik autentifikatsiya usullarini, masalan, yuzni aniqlash, barmoq izini skanerlash va xulq-atvor biometriklarini takomillashtirmoqda. Sun'iy intellektga asoslangan doimiy autentifikatsiya tizimlari ruxsatsiz kirish urinishlarini dinamik ravishda aniqlash uchun foydalanuvchi xatti-harakatlarini kuzatib boradi. AI-Driven Zero Trust xavfsizlik modeli: AI tomonidan quvvatlangan Zero Trust modeli har bir so'rov hatto ishonchli

foydalanuvchilardan ham doimiy ravishda tekshirilishini ta'minlaydi. AI kirish modellarini tahlil qilish va buzilishni ko'rsatishi mumkin bo'lgan anomaliyalarni aniqlash orqali ushbu modelni yaxshilaydi.

AIning axborot xavfsizligiga salbiy ta'siri

O'zining afzalliklariga qaramay, AI kiberjinoyatchilar tomonidan qo'llanilganda ham katta xavf tug'diradi. AI tomonidan boshqariladigan kiberhujumlar: Xakerlar ilg'or zararli dasturlarni yaratish va keng ko'lamli kiberhujumlarni avtomatlashtirish uchun sun'iy intellektdan foydalanmoqda. AI tomonidan boshqariladigan zararli dasturlar va botnetlar xavfsizlik himoyasiga moslasha oladi, bu ularni aniqlashni qiyinlashtiradi. AI modellariga qarama-qarshi hujumlar: Kiberjinoyatchilar qarama-qarshi ma'lumotlarni kiritish orqali AI modellarini manipulyatsiya qilishlari mumkin, bu esa tizimni noto'g'ri qarorlar qabul qilishiga olib keladi. Qarama-qarshi mashinalarni o'rganish usullari yuzni aniqlash tizimlarini aldashi yoki AI tomonidan boshqariladigan xavfsizlik boshqaruvlarini chetlab o'tishi mumkin. Deepfake texnologiyasi va ijtimoiy muhandislik: Deepfake AI juda real soxta videolar va audio yozuvlarni yaratishi mumkin, bu esa identifikatsiya firibgarligi, noto'g'ri ma'lumotlar va ijtimoiy muhandislik hujumlariga imkon beradi. Kiberjinoyatchilar rahbarlarni taqlid qilish va maxfiy ma'lumotlarni oshkor qilish uchun xodimlarni manipulyatsiya qilish uchun deepfakesdan foydalanadilar. AI tomonidan kengaytirilgan fishing hujumlari: Sun'iy intellektga asoslangan fishing hujumlari yanada murakkablashmoqda. AI tomonidan yaratilgan elektron pochta va chatbotlar odamlarning o'zaro ta'siriga taqlid qilishi mumkin, bu esa fishing urinishlarini yanada ishonchli qiladi va muvaffaqiyat ehtimolini oshiradi. AI-quvvatlovchi Ransomware : AI tomonidan yaxshilangan to'lov dasturi jabrlanuvchining tarmog'ini aqlli tahlil qilishi va shifrlash uchun eng qimmatli ma'lumotlarga ustunlik berishi mumkin. Bu ransomware hujumlarini yanada samarali va halokatli qiladi.

Xulosa:

Sun’iy intellekt texnologiyalari axborot xavfsizligini mustahkamlashga katta hissa qo‘shmoqda. Biroq, ular kiberjinoyatchilar tomonidan zararli maqsadlarda ham ishlatilishi mumkin. Shu sababli, sun’iy intellekt asosida xavfsizlik tizimlarini rivojlantirish va raqib hujumlariga qarshi choralar ko‘rish muhim ahamiyatga ega.Zamonaviy raqamli dunyoda sun'iy intellekt (AI) turli sohalarda, jumladan kiberxavfsizlikda inqilob qilmoqda. Axborot xavfsizligida sun'iy intellekt ikki tomonlama rol o'ynaydi: u kiberxavfsizlik choralarini kuchaytiradi va shu bilan birga yangi zaifliklarni kiritadi. Sun'iy intellektga asoslangan tizimlar tahdidlarni aniqlashi, katta ma'lumotlar to'plamini tahlil qilishi va javoblarni avtomatlashtirishi mumkin, biroq ayni paytda kiberjinoyatchilar yanada murakkab hujumlarni ishlab chiqish uchun AIdan foydalanmoqda. Ushbu maqola AIning axborot xavfsizligiga ta'sirini o'rganadi, uning afzalliklari, xavflari va kelajakdagi oqibatlarini ta'kidlaydi.

References:
Используемая литература:
Foydalanilgan adabiyotlar:

1. Qodirov, Farrux, and Sabrina Turayeva. "ELEKTRON TIJORAT PLATFORMALARINING EKOLOGIK TOZA QISHLOQ MAHSULOTLARI BOZORIGA TA’SIRI." *Наука и технология в современном мире* 4.7 (2025): 37-44.

2. Qodirov, Farrux, and Sabrina Turayeva. "BULUTLI HISOBLASH TEXNOLOGIYALARI VA AI ASOSIDA QISHLOQ XO ‘JALIGIDA PROGNOZLASH TIZIMLARI." *Наука и технология в современном мире* 4.7 (2025): 45-52.
3. Qodirov, Farrux, and Sabrina Turayeva. "AQLLI SHAHAR (SMART CITY) TIZIMLARI ORQALI EKOLOGIK MONITORING VA RESURSLARNI TEJASH." *Наука и технология в современном мире* 4.7 (2025): 21-28.
4. Qodirov, Farrux, and Sabrina Turayeva. "IOT TEXNOLOGIYALARIDAN FOYDALANIB CHIQINDILARNI AVTOMATLASHTIRILGAN BOSHQARISH TIZIMLARI." *Наука и инновация* 3.10 (2025): 68-75.
5. Qodirov, Farrux, and Sabrina Turayeva. "MOBIL ILOVALAR VA RAQAMLI PLATFORMALAR ORQALI EKOLOGIK ONGLILIKNI OSHIRISH." *Наука и инновация* 3.10 (2025): 85-92.
6. Qodirov, Farrux, and Sabrina Turayeva. "BULUT TEXNOLOGIYALARI VA KATTA MA’LUMOTLAR (BIG DATA) ORQALI TABIIY RESURSLARNI BOSHQARISH." *Инновационные исследования в современном мире: теория и практика* 4.10 (2025): 77-84.
7. Qodirov, Farrux, and Sabrina Turayeva. "SUN’IY INTELLEKT YORDAMIDA TABIIY RESURSLARDAN SAMARALI FOYDALANISH STRATEGIYALARI." *Инновационные исследования в современном мире: теория и практика* 4.10 (2025): 92-98.
8. Qodirov, Farrux, and Sabrina Turayeva. "BLOKCHEYN TEXNOLOGIYALARI VA TABIIY RESURSLARNI BOSHQARISHDA SHAFFOFLIKNI TA’MINLASH." *Инновационные исследования в современном мире: теория и практика* 4.10 (2025): 69-76.
9. Qodirov, Farrux, and Sabrina Turayeva. "DRONLAR YORDAMIDA QISHLOQ XO ‘JALIGINI RAQAMLASHTIRISH VA MONITORING QILISH." *Наука и технология в современном мире* 4.7 (2025): 29-36.
10. Qodirov, Farrux, and Sabrina Turayeva. "YASHIL ENERGETIKA VA AQLLI TARMOQLARNI BOSHQARISHDA SUN’IY INTELLEKT ROLI." *Общественные науки в современном мире: теоретические и практические исследования* 4.7 (2025): 57-66.
11. Qodirov, Farrux, and Sabrina Turayeva. "BLOKCHEYN TEXNOLOGIYALARI ORQALI QAYTA TIKLANADIGAN ENERGIYA SAVDOSINI AVTOMATLASHTIRISH." *Общественные науки в современном мире: теоретические и практические исследования* 4.7 (2025): 47-56.
12. Qodirov, Farrux, and Sabrina Turayeva. "AQLLI DEHQONCHILIK DASTURIY TA’MINOT VA SENSORLAR YORDAMIDA HOSILDORLIKNI OSHIRISH." *Общественные науки в современном мире: теоретические и практические исследования* 4.7 (2025): 67-74.
13. Qodirov, Farrux, and Sevinch Ne’matova. "WIRELESS (WI-FI) TEXNOLOGIYASINING RIVOJLANISHI VA TURLARI." *Прикладные науки в современном мире: проблемы и решения* 4.3 (2025): 116-121.
14. Qodirov, Farrux, and Sarvinoz Tursunova. "KIBERJINOYATLAR VA ULARNING OLDINI OLISH YOLLARI." *Наука и инновация* 3.7 (2025): 151-157.
15. Qodirov, Farrux, and Sevinch Ne’matova. "MOBIL ILOVALAR ISHLAB CHIQISHNING ASOSLARI." *Наука и технология в современном мире* 4.6 (2025): 8-14.
16. Qodirov, Farrux, and Sarvinoz Tursunova. "INTERNET ORQALI OVOZLI QONGIROQLAR (VOIP) TEXNOLOGIYASI." *Наука и инновация* 3.7 (2025): 40-44.

17. Qodirov, Farrux, Mehriniso Cho'lliyeva, and Sevinch Negmatova. "RAQAM TEXNOLOGIYALARNING QO'LLANISH SOHALARI." *Инновационные исследования в современном мире: теория и практика* 4.9 (2025): 4-9.
18. Qodirov, Farrux, Baxtiniso Boqiyeva, and Sevinch Negmatova. "ELEKTRON KARMON." *Инновационные исследования в современном мире: теория и практика* 4.9 (2025): 14-18. Qodirov, Farrux, Yulduz Ahmedova, and Sevinch Negmatova. "ELEKTRON TO'LOV VOSITALARI." *Инновационные исследования в современном мире: теория и практика* 4.9 (2025): 19-21.
19. Qodirov, Farrux, Jasmina Murodulloyeva, and Sevinch Negmatova. "SMART TEXNOLOGIYALARNI QO'LLASH VOSITALARI." *Естественные науки в современном мире: теоретические и практические исследования* 4.3 (2025): 63-67.
20. Qodirov, Farrux, Sevinch Nomozova, and Sevinch Negmatova. "BUYUMLAR INTERNETIDAN FOYDALANISH." *Молодые ученые* 3.7 (2025): 73-77.
21. Qodirov, Farrux, Sevinchoy Norboboyeva, and Sevinch Negmatova. "BLOKCHEYN TEXNOLOGIYASI HAQIDA TUSHUNCHA." *Молодые ученые* 3.7 (2025): 69-72.
22. Qodirov, Farrux, and Ozoda Maxsadova. "BULUTLI TEXNOLOGIYALARNING XUSUSIYATLARI, AFZALLIKLARI VA KAMCHILIKLARI." *Инновационные исследования в современном мире: теория и практика* 3.15 (2024): 111-115.

INNOVATIVE ACADEMY