

KIBERXAVFSIZLIKNI TA'MINLASHDA SUN'IY INTELLEKTDAN FOYDALANISH VA UNING AHAMIYATI

Shukurov Orziqul Pardayevich

Muhammad al-Xorazmiy nomidagi TATU, Axborot xavfsizligi kafedrasida katta o'qituvchisi

Annotatsiya. Sun'iy intellekt (SI) axborot xavfsizligini ta'minlashda yangi imkoniyatlar ochib bermoqda. Bugungi kunda kiberhujumlar murakkablashib, an'anaviy usullar bilan xavfsizlikni ta'minlash qiyinlashmoqda. Ushbu maqolada SI texnologiyalarining kiberxavfsizlik sohasidagi roli, ularning tahdidlarni aniqlash va oldini olishdagi samaradorligi, shuningdek mamlakatimizda yuzaga kelayotgan kiberjinoyatlar holati statistik ma'lumotlar asosida keltirilgan. SI yordamida xavfsizlikni ta'minlash va mavjud muammolarni bartaraf etish istiqbollari ko'rib chiqilgan.

Kalit so'zlar: sun'iy intellekt, kiberhujum, kiberjinoyat.

Raqamli taraqqiyot jamiyat hayotining barcha sohalariga kirib borgan sari axborot xavfsizligi dolzarb muammoga aylandi. Internet asosidagi tizimlar, bank xizmatlari, davlat onlayn xizmatlari va ijtimoiy tarmoqlarga bo'lgan talab ortgani sari kiberhujumlar soni ham keskin ortib bormoqda. Ayni paytda sun'iy intellekt(SI) texnologiyalarining kiberxavfsizlik sohasida qo'llanilishi xavfsizlikni ta'minlashda kalit omilga aylanmoqda. SI algoritmlari yordamida katta hajmdagi trafik tahlil qilinadi, anomal xatti-harakatlar aniqlanadi va tahdidlar real vaqt rejimida oldini olish imkoniyati yaratiladi[1].

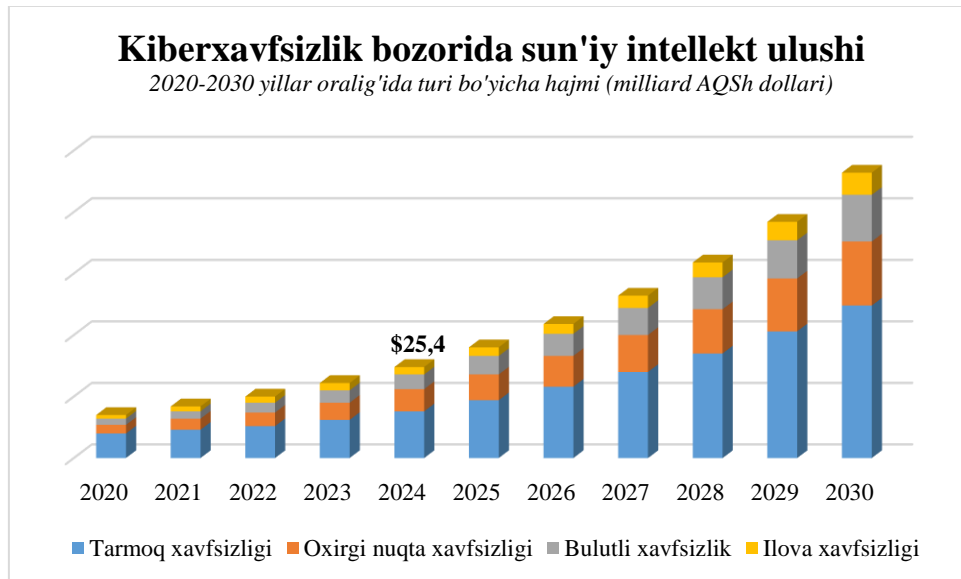
Kiberxavfsizlikni ta'minlashda SI texnologiyalarining asosiy imkoniyatlari quyidagi yo'nalishlar orqali namoyon bo'ladi:

Tahdidni aniqlash - SI yordamida anomaliyalarni aniqlash an'anaviy usullarga qaraganda sezilarli yuqori darajada amalga oshadi (70%+).

Xavfsizlikni avtomatlashtirish - SI tizimlari xavfsizlik jarayonlarini 80% gacha avtomatlashtiradi(1-rasm) [2].

Zero-day hujumlarga qarshi kurash - SI yordamida oldindan bashorat qilish va himoya qilish imkoniyati oshadi[3].

Foydalanuvchi xatti-harakatini tahlil qilish - Xulq-atvor tahlili yordamida ichki tahdidlarni 40% gacha aniqlash samaradorligi oshadi.



1-rasm. Kiberxavfsizlikni ta'minlashda SI dan foydalanish.

Statistik tadqiqotlarga ko'ra, global tashkilotlarning 57% SI texnologiyalarni anomaliyalarni aniqlash uchun qo'llamoqda, 50% esa zararli dasturlarni aniqlash uchun SIga tayanmoqda[4].

Bugungi kunda dunyoda har soniyada taxminan 2200 ta kiberhujum sodir bo'ladi[5]. SI yordamida yaratilgan fishing hujumlar soni so'nggi yillarda sezilarli darajada oshgan, bu esa an'anaviy xavfsizlik tizimlariga katta bosim ko'rsatmoqda.

O'zbekiston sharoitida ham kiber jinoyatlar soni oshib bormoqda. Mahalliy statistikaga ko'ra:

Ko'rsatkich	2024 yil 1-yarim yillik
Ekspertiza o'tkazilgan saytlar	79 ta
“.UZ” domenida aniqlangan xavfsizlik hodisalari	63 ta
Davlat tashkilotlarida aniqlangan holatlar	22 ta

Bundan tashqari, norasmiy statistik ma'lumotlarga ko'ra, oxirgi besh yil ichida O'zbekistonda kiber jinoyatlar soni 68 barobar ko'paygani va 2024 yilda 12 million yaqin kiberhujum sodir bo'lgani qayd etilgan (noaniq, lekin trendni ko'rsatadi)[6]. 2025-yilning birinchi 11 oyi davomida kiberjinoyatlar oqibatida fuqarolarga yetkazilgan moddiy zarar miqdori qariyb 1,9 trillion so'mni (aniqrog'i 1 trillion 890 milliard so'm) tashkil etdi.

Ushbu sohadagi asosiy ko'rsatkichlar:

- *Zararning o'sishi:* So'nggi 5 yil (2021–2025) ichida jami zarar miqdori 3,73 trillion so'mga yetgan bo'lib, uning qariyb yarmi aynan 2025-yil hisobiga to'g'ri kelmoqda.
- *Jinoyatlar soni:* Kiberjinoyatlar soni oxirgi 5 yilda 11 baravardan ziyod ko'payib, 4 865 tadan 62 440 taga oshgan.
- *Asosiy yo'nalish:* Kiberjinoyatlarning 98 foizi bank kartalari bilan bog'liq o'g'rilik va firibgarliklardir.

Bu holatlar O'zbekiston raqamli infratuzilmasida SI texnologiyalarini keng ko'lamda joriy etish zaruratini yana bir bor ko'rsatmoqda.

Kiberjinoyatlarni aniqlashda sun'iy intellektni qo'llash quyidagi imkoniyatlarni beradi: *Tahdidlarni aniqlash va oldini olish.* SI modellar tarmoq trafikini real vaqt rejimida tahlil qilib, anomaliyalarga asoslangan xujumlarni tezda aniqlaydi. Anomaliyalarni aniqlash darajasi an'anaviy usullarga qaraganda sezilarli darajada yuqoriroq hisoblanadi.

Xavfsizlikni avtomatlashtirish. Aksariyat tashkilotlar SI yordamida hodisalarga avtomatik javob berish tizimlarini yaratmoqda, bu esa xodimlar ish yuklamasini kamaytiradi va vaqtni tejaydi.

Murakkabliklar va cheklovlar. Sun'iy intellektdan foydalanish quyidagi murakkabliklarni ham olib keladi:

- SI tizimlarini noto'g'ri o'rgatish xavfi va noto'g'ri huquqiy qarorlar qabul qilish xavfi[7].
- SI asosidagi tizimlarning ham hujumga uchrashi ehtimoli (masalan, adversarial attack)[8].
- Ma'lumotlar maxfiyligi va etik masalalar.

Bugungi axborot xavfsizligi sohasi murakkablashib borar ekan, sun'iy intellekt texnologiyalari xavfsizlikni ta'minlashda strategik ahamiyat kasb etadi. SI asosidagi tizimlar tahdidlarni tezda aniqlash, avtomatlashtirilgan javob berish, hamda oldini olish choralarini kuchaytiradi. O'zbekiston sharoitida kiberjinoyatlar sonining ortishi milliy xavfsizlik tizimlarini modernizatsiya qilish va SI yechimlarini keng joriy etishni talab qiladi. Shu bois, SIni kiberxavfsizlik tizimlariga integratsiya qilish ham xalqaro standartlarga rioya etish, ham tizim samaradorligini oshirish uchun muhimdir.

Foydalanilgan adabiyotlar

1. <https://litslink.com/blog/ai-in-cybersecurity-statistics>
2. <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-cybersecurity-market-report>
3. <https://zerothreat.ai/blog/impact-of-ai-in-cybersecurity>

4. <https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#statistic2>
5. SamCyber.uz — Kiber xavfsizlik statistikasi (O‘zbekiston).
6. <https://medium.com/@city.paul/uzbekistans-cybercrime-crisis-52673478190f>
7. "SUN'YIY INTELLEKT XAVFSIZLIGI VA AXLOQIY MUAMMOLARI". (2025). *Modern Education and Development*, 20(3), 336-341.
8. https://deloitte.wsj.com/riskandcompliance/cisos-guide-using-ai-for-cyber-defense-d6e06cfc?reflink=desktopwebshare_permalink