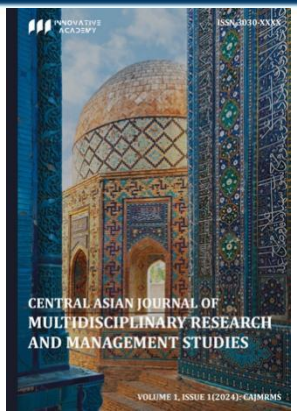

KIBERJINOYATLARGA QARSHI KURASHISHDA ZAMONAVIY TEXNOLOGIYALARNING ROLI: SUN'IY INTELLEKT VA BLOKCHEYN TEXNOLOGIYALARI

Yuldashev Kudrat Abduvaxatovich

O'zbekiston Respublikasi IIV Malaka oshirish instituti Maxsus-kasbiy fanlar kafedrasi dotsenti, siyosiy fanlar bo'yicha falsafa doktori, (PhD) podpolkovnik

https://doi.org/10.5281/zenodo.19511885

ARTICLE INFO

Received: 4th April 2026
Accepted: 5th April 2026
Published: 11th April 2026

KEYWORDS

ABSTRACT

Bugungi kunda axborot texnologiyalari tez sur'atlarda rivojlanib borayotgani bilan birga, kiberjinoyatlar ham global xavf sifatida tobora ko'payib bormoqda. Internet tarmoqlari va raqamli xizmatlarning kengayishi kiberxavfsizlik muammolarini yanada murakkablashtiradi, natijada zararli dasturlar, firibgarlik, ma'lumotlarni o'g'irlash kabi jinoyatlar ko'paymoqda. Shu sababli kiberjinoyatlarga qarshi samarali kurashish uchun yangi va ilg'or texnologiyalarni qo'llash zarurati yuzaga kelmoqda.

Sun'iy intellekt (SI) va blokcheyn texnologiyalari zamonaviy kiberxavfsizlik sohasida innovatsion vositalar sifatida katta ahamiyat kasb etmoqda. Sun'iy intellekt yordamida kiberxurujlarni aniqlash va oldini olish, avtomatlashtirilgan xavfsizlik tizimlarini yaratish imkoniyati kengaymoqda. Shu bilan birga, blokcheyn texnologiyasi ma'lumotlar xavfsizligi, ularning o'zgartirilmasligi va shaffofligini ta'minlashda yangi imkoniyatlar yaratmoqda.

Ushbu maqolada kiberjinoyatlarga qarshi kurashishda sun'iy intellekt va blokcheyn texnologiyalarining roli tahlil qilinib, ularning samaradorligi hamda amaliy qo'llanilish yo'llari ko'rib chiqiladi.

Sun'iy intellekt kiberxavfsizlik sohasida xavf-xatarlarni aniqlash, ularga javob berish va oldini olishda samarali vosita sifatida keng qo'llanilmoqda. Bugungi kunda kiberhujumlar murakkab va tezkor tarzda amalga oshirilayotgani sababli, sun'iy intellekt kiberxavfsizlikni ta'minlashda juda muhim rol o'ynaydi. Quyida sun'iy intellekt texnologiyasining kiberxavfsizlikdagi asosiy qo'llanilish yo'nalishlari ko'rib chiqiladi:

1. Xavfni aniqlash va tahlil qilish. Sun'iy intellekt tizimlari kiberxavfsizlikda eng samarali xavf-xatarlarni aniqlash va tahlil qilish vositalaridan biridir. Sun'iy intellekt algoritmlari, foydalanuvchi faoliyatini va tarmoqdagi trafikni doimiy ravishda kuzatib boradi va odatiy holatlardan og'ishlarni tezda aniqlaydi. Bu tizimlar yirik ma'lumotlar bazalaridan foydalanib, zararli harakatlarni yoki tahdidlarni erta bosqichda sezadi, bu esa kiberhujumlarga qarshi tezkor choralar ko'rish imkonini beradi. Masalan, AQShdagi moliyaviy kompaniyada sun'iy intellekt real vaqt rejimida kiberhujumni aniqlab, uni dastlabki bosqichdayoq to'xtatishga yordam bergan. Bugungi kunda Darktrace kabi tizimlar 110 dan ortiq mamlakatda minglab tashkilotlarni xuddi shunday real vaqt rejimida himoya qilmoqda.

2. Zararli dasturlarni aniqlash. Sun'iy intellekt zararli dasturlarni aniqlashda keng qo'llaniladi. Traditsion antivirus dasturlari faqat ma'lum bir zararli dasturlarni aniqlay oladi, lekin sun'iy intellekt tizimlari yangi va ilgari noma'lum zararli dasturlarni o'z-o'zini o'rgatish asosida aniqlash imkoniyatiga ega. Sun'iy intellekt yordamida, zararli dasturlar tizimga kirish usulini va uning qanday faoliyat yuritishini o'rganadi, bu esa unga mutatsiyalangan yoki yangi turdagi

zararli dasturlarni oldindan aniqlash imkonini beradi. Sun'iy intellektning o'rganish qobiliyati tizimni doimiy ravishda yangilab boradi va tahdidlarni yangi shakllariga moslashishga yordam beradi. Sun'iy intellekt asosidagi Cylance kabi tizimlar WannaCry kabi global tahdidlarni tahlil qilib, yangi mutatsiyalangan versiyalarini oldindan aniqlash imkonini bergan. Tadqiqotlarga ko'ra, sun'iy intellekt asosidagi antiviruslar an'anaviy antiviruslarga qaraganda 60% ko'proq yangi tahdidlarni erta aniqlaydi[1].

3. Phishing hujumlarini oldini olish. Phishing hujumlari kiberjinoyatchilar tomonidan foydalanuvchilarni aldanishga undash uchun ishlatiladi. Sun'iy intellekt tizimlari foydalanuvchi xatti-harakatlarini tahlil qilish va shubhali xabarlar yoki havolalarni avtomatik tarzda aniqlash imkoniyatiga ega. Shuningdek, phishing hujumlariga oid ilg'or usullarni (masalan, soxta veb-saytlar yoki manipulyatsiya qilingan email xabarlar) avtomatik tarzda identifikatsiya qilishda sun'iy intellekt tizimlarining o'z-o'zini o'rgatish funksiyasi yordam beradi. Bunda sun'iy intellekt foydalanuvchini ogohlantirishi yoki xabarni avtomatik tarzda bloklashi mumkin. Shu bilan birga, Google sun'iy intellekti 2021-yilda Gmail orqali yuborilgan 100 milliondan ortiq phishing xabarlarini avtomatik ravishda bloklagan. Bugungi kunda Gmail AI tizimi phishing hujumlarini 99,9% aniqlik bilan aniqlay oladi.

4. Avtomatik javob va reaksiya. Kiberxavfsizlikni ta'minlashda sun'iy intellektning asosiy afzalliklaridan biri uning avtomatik javob berish imkoniyatidir. Kiberhujumlar aniqlangach, Sun'iy intellekt tizimlari avtomatik tarzda zarur choralarni ko'rishga o'rgatilgan. Masalan, tizimga kirish urinishlarini bloklash, zararli dasturlarni o'chirish yoki zarar ko'rgan tizimni izolyatsiya qilish kabi chora-tadbirlar Sun'iy intellekt tomonidan tezkor amalga oshiriladi. Inson aralashuvisiz amalga oshiriladigan bu jarayonlar, kiberhujumlarni oldini olishda samarali bo'lib, tizimning uzluksiz ishlashini ta'minlaydi. Bunday avtomatik javoblar nafaqat vaqtni tejaydi, balki kiberxavfsizlikning yanada samarali boshqarilishini ta'minlaydi[2].

Shuningdek, Microsoftning Azure Sentinel tizimi sun'iy intellekt yordamida hujumlarni aniqlagandan so'ng, zararli trafikni bloklash, shubhali qurilmalarni ajratish va xavf darajasini baholash kabi chora-tadbirlarni avtomatik ravishda amalga oshiradi. Shunday tizimlar kiberhujumlarga javob berish samaradorligini 70% ga oshirgan. So'nggi yillarda sun'iy intellekt texnologiyalari kiberxavfsizlik sohasida samarali vosita sifatida faol qo'llanilmoqda. Xususan, turli mamlakatlarda sun'iy intellekt asosida kiberjinoyatchilikka qarshi kurashish bo'yicha aniq natijalarga erishilmoqda. 2024-yilga oid quyidagi tahliliy ma'lumotlar sun'iy intellekt texnologiyalarining kiberxavfsizlikda tutgan o'rnini yaqqol namoyon etadi[3].

Blokcheyn texnologiyasi kiberxavfsizlikni ta'minlashda samarali vosita sifatida qabul qilinmoqda. Uning asosiy afzalliklari, ya'ni ma'lumotlarni o'zgartirishning imkonsizligi, shaffoflik va ishonchlilik, kiberxavfsizlikni mustahkamlashda katta rol o'ynaydi. Blokcheyn texnologiyasi ma'lumotlarning xavfsizligini ta'minlashda bir qator imkoniyatlar yaratadi. Quyida blokcheynning kiberxavfsizlikda qo'llanilishining asosiy yo'nalishlari ko'rib chiqiladi:

1. Ma'lumotlar integritetini ta'minlash. Blokcheyn texnologiyasining asosiy afzalligi uning o'zgartirilmasligi hisoblanadi. Har bir blok o'zaro kriptografik bog'lanishlar bilan ulanib, tizimdagi ma'lumotlar ishonchliligini ta'minlaydi. Blokcheyn orqali ma'lumotlarni soxtalashtirish yoki o'zgartirish deyarli imkonsiz bo'ladi, bu esa kiberxavfsizlikni kuchaytiradi. Misol uchun, Walmart o'zining ta'minot zanjirini boshqarishda blokcheyn texnologiyasidan foydalanadi. Har bir mahsulotning kelib chiqishi va yetkazib berish jarayonidagi har bir

[1] Mirzayev Sh. R. (2024). Kiberxavfsizlik sohasida sun'iy intellekt va blokcheyn texnologiyalarini qo'llash imkoniyatlari. Science and innovation, 3(Special Issue 42), 179-185.

[2] Giyazova, N.B. (2024). Zamonaviy raqamli iqtisodiyotdagi muammolar va chora-tadbirlar. Science and innovation, 3(Special Issue 42), 482-489

[3] 4 Shukhratovna, U. M., & Bayazovna, G. N. (2025). Foreign experience in the development of mobile internet. innovation in the modern education system, 6(49), 250-256.

qadam blokcheynga yoziladi. Agar mahsulot sifati bo‘yicha muammo chiqsa, Walmart bir necha soniya ichida uning manbasini aniqlay oladi[4].

2. Decentralizatsiya va xavfsizlik. Blokcheynning markazlashtirilmagan tuzilishi tizimni yanada xavfsiz qiladi. Ma’lumotlar bir nechta joyda saqlanadi, bu esa tizimga kirish va ma’lumotlarni o‘g‘irlashni qiyinlashtiradi. Markazlashtirilgan tizimlarga nisbatan blokcheynning decentralizatsiya qilingan strukturasida biror qismning buzilishi butun tizimga zarar yetkazmaydi. Blokcheyn tarmoqlariga hujum qilish uchun kiberjinoyatchilar tarmoq quvvatining kamida 51% ini egallashi kerak. Bu esa katta energiya va resurs talab qiladi, shuning uchun blokcheyn tizimlariga bo‘lgan muvaffaqiyatli hujumlar darajasi an’anaviy markazlashgan tizimlarga nisbatan 90% kam.

3. Xavfsiz autentifikatsiya va identifikatsiya. Blokcheyn foydalanuvchi identifikatsiyasini xavfsiz va ishonchli tarzda amalga oshirish imkonini beradi. Kriptografik kalitlar yordamida foydalanuvchilarni tasdiqlash jarayoni an’anaviy tizimlarga nisbatan yanada xavfsizdir, bu esa "account takeover" kabi hujumlarga qarshi samarali himoya yaratadi. Bunga qo‘shimcha, Microsoft o‘zining Azure Active Directory (Azure AD) tizimiga blokcheyn asosida Decentralized Identity funksiyasini qo‘shgan. Bu funksiyada foydalanuvchilar o‘z shaxsiy ma’lumotlarini blokcheynga joylashtirib, nazoratni o‘z qo‘lida saqlaydi[5].

4. Smart kontraktlar va avtomatik shartnomalar. Blokcheyn asosidagi smart kontraktlar taraflar o‘rtasidagi shartnomalarni avtomatik tarzda bajarilishini kafolatlaydi. Shartnomalar blokcheynda xavfsiz tarzda saqlanadi va barcha harakatlar tasdiqlanishi kerak, bu esa shaffoflikni ta’minlab, soxtalashtirish va manipulyatsiya qilish imkoniyatlarini kamaytiradi. Shuningdek, Siemens smart kontraktlar orqali logistika va yuk tashish jarayonlarini avtomatlashtirishda blokcheyn texnologiyasidan foydalanilmoqda. Yuk jo‘natish va qabul qilish shartlari to‘liq bajarilgandagina to‘lov amalga oshiriladi, bu ishonchli va xavfsiz hamkorlik uchun zamin yaratadi. Smart kontraktlar asosidagi tizimlar 2023-yilda xalqaro savdoda hujjatlarni soxtalashtirish holatlarini 70% ga kamaytirgan. Blockcheyn hamyon foydalanuvchilari sonining keskin o‘sishi (2016 yilda 10 mln.dan 2021 yilda 80 mln.ga) kiberxavfsizlik tahdidlarini oshirdi. Bu phishing hujumlari, kalitlarni o‘g‘irlash va firibgarlik kabi xatarlarning ko‘payishiga olib keldi. Foydalanuvchilarni himoya qilish uchun ikki bosqichli autentifikatsiya, apparat hamyonlari va xavfsizlik bo‘yicha xabardorlikni talab qiladi. Blockcheyn tizimining kengayishi bilan xavfsizlikni ta’minlash ustuvor vazifa bo‘lib qolyapti.

Xulosa qilib aytganda, bugungi globallashgan dunyoda raqamli texnologiyalarning keng qo‘llanilishi yangi imkoniyatlar yaratish bilan birga, turli xavf-xatarlarni ham yuzaga keltirmoqda. Kiberxavfsizlik nafaqat texnologik, balki strategik ahamiyatga ega bo‘lib, uning to‘g‘ri boshqarilishi iqtisodiyot barqarorligi va rivojlanishi uchun muhimdir. Sun’iy intellekt va blokcheyn texnologiyalari kabi ilg‘or texnologiyalar kiberxavfsizlik sohasida yangi ufqlarni ochmoqda. Sun’iy intellekt xavf-xatarlarni aniqlash va ularga tezkor javob berishda samarali vosita bo‘lib, zararli dasturlarni aniqlash va phishing hujumlarini oldini olish kabi yo‘nalishlarda muvaffaqiyatli qo‘llanilmoqda. Blokcheyn texnologiyasi esa ma’lumotlarning yaxlitligi va ishonchliligini ta’minlash, decentralizatsiya orqali tizimlarni mustahkamlash hamda xavfsiz autentifikatsiya kabi muhim imkoniyatlarni taqdim etadi.

[4] Rustam o‘g‘li, R. J., & Bayazovna, G. N. (2025). Mobil to ‘lovlar va ularning iqtisodiyotdagi ahamiyati. The theory of recent scientific research in the field of pedagogy, 3(30), 193-197.

[5] Sayfullayeva, M. (2023). Establishment Of Agritourism Clusters In Uzbekistan Based On The Principles Of Sustainable Tourism. Центр научных публикаций (Buxdu. Uz), 35(35).