Uzbek Scholar Journal
Volume- 51, April- 2026
www.uzbekscholar.com

KIBERJINOYATLAR BO'YICHA TERGOV HARAKATLARIDA SUN'IY INTELLEKTNING QO'LLANILISHI

Komilov Diyorbek Zokir o‘g‘li
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi
“Kiberxavfsizlikni huquqiy ta’minlash” yo‘nalishi magistratura bosqichi tinglovchisi
E-mail: diyorbekkomilov2404@gmail.com

ANNOTATSIYA
Ushbu maqolada kiberjinoyatlar bo'yicha tergov harakatlarida sun'iy intellekt (SI) texnologiyalarining qo'llanilishi ilmiy jihatdan tahlil etiladi. Maqolada mavzuning dolzarbligi asoslanib, xalqaro va milliy statistik ma'lumotlar, olimlar va tadqiqotchilarning ilmiy xulosalari hamda amaliy tajriba natijalariga tayanilgan. Raqamli kriminalistika, anomaliyalarni aniqlash, shaxsni identifikatsiya qilish va prognozlash kabi tergov bosqichlarida SI ning samaradorligi ko'rib chiqiladi. Shuningdek, O'zbekiston sharoitidagi vaziyat tahlil qilinib, huquqiy, etik muammolar va tavsiyalar ilgari suriladi.

Kalit so'zlar: kiberjinoyat, sun'iy intellekt, tergov harakatlari, raqamli kriminalistika, mashinaviy o'rganish, anomaliyalarni aniqlash.

ABSTRACT
This article provides a scientific analysis of the application of artificial intelligence (AI) technologies in investigative actions related to cybercrimes. The relevance of the topic is substantiated, and the study is based on international and national statistical data, scientific conclusions of scholars and researchers, as well as the results of practical experience. The effectiveness of AI is examined at various stages of investigation, including digital forensics, anomaly detection, identification of individuals, and forecasting. In addition, the situation in Uzbekistan is analyzed, and legal and ethical issues, along with recommendations, are put forward.

Keywords: cybercrime, artificial intelligence, investigative actions, digital forensics, machine learning, anomaly detection.

АННОТАЦИЯ
В данной статье научно анализируется применение технологий искусственного интеллекта (ИИ) в следственных действиях по делам о киберпреступлениях. Обосновывается актуальность темы, при этом исследование опирается на международные и национальные статистические данные, научные выводы ученых и исследователей, а также результаты практического опыта. Рассматривается эффективность ИИ на различных этапах расследования, включая цифровую криминалистику, выявление аномалий, идентификацию личности и прогнозирование. Кроме того, анализируется ситуация в Узбекистане, а также выдвигаются правовые и этические проблемы и рекомендации.

Ключевые слова: киберпреступление, искусственный интеллект, следственные действия, цифровая криминалистика, машинное обучение, выявление аномалий.

KIRISH

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi insoniyatga ulkan imkoniyatlar ochish bilan birga, yangi turdagi jinoyatlarning — kiberjinoyatlarning paydo bo'lishi va keng yoyilishiga ham zamin hozirladi. Bugungi kunda kiberjinoyatlar global miqyosdagi eng jiddiy tahdidlardan biriga aylanib, nafaqat iqtisodiy, balki siyosiy va ijtimoiy barqarorlikka ham xavf solmoqda.

Kiberjinoyatlardan global miqyosdagi yillik zarar 2023-yilda 8 trillion AQSh dollariga yetdi, ya'ni har soniyada 250 000 dollardan ortiq yo'qotish ro'y berdi. Bu raqam 2025-yilga kelib 10,5 trillion dollarga yetishi prognoz qilinmoqda. USI Insurance Services

O'zbekistonda ham vaziyat jiddiy tus olmoqda. IIV huzuridagi Kiberjinoyatlar markazi ma'lumotlariga ko'ra, so'nggi besh yil ichida mamlakatda kiberjinoyatlar soni 68 baravardan ortiq oshgan. 2019-yilda axborot texnologiyalari orqali 18 turdagi 863 ta jinoyat sodir etilgan bo'lsa, 2024-yilda bu ko'rsatkich 62 turdagi 58 800 ta jinoyatga yetgan. 2023-yilda kiberjinoyatlar umumiy jinoyatlar sonining 6,2 foizini tashkil etgan bo'lsa, 2024-yilda bu ko'rsatkich 44,4 foizga yetgan — ya'ni har ikkita jinoyatdan biri internet va axborot texnologiyalari orqali amalga oshirilgan. PinkodPinkod

An'anaviy tergov usullari kiberjinoyatlarning transchegaraviy tabiati, raqamli izlarni tez yo'q qilish imkoniyati va ma'lumotlarning ulkan hajmi oldida samarasiz bo'lib qolmoqda. Aynan shu muammoni hal etish uchun dunyo davlatlari tergov jarayonlarida sun'iy intellektdan foydalanishni jadal yo'lga qo'ymoqda.

Tadqiqotning maqsadi — kiberjinoyatlar bo'yicha tergov harakatlarida SI ning nazariy asoslarini, amaliy imkoniyatlarini, xalqaro tajribasini va O'zbekiston uchun istiqbollarini ilmiy-amaliy jihatdan tahlil etishdan iborat.

MATERIALLAR VA USULLAR

Tadqiqot jarayonida quyidagi ilmiy-metodologik usullardan foydalanildi: qiyosiy tahlil usuli (xalqaro va milliy tajribani solishtirish), tizimli tahlil usuli (SI texnologiyalarini tergov jarayoni tarkibida ko'rib chiqish), statistik tahlil usuli (miqdoriy ko'rsatkichlarni baholash) va huquqiy tahlil usuli (normativ-huquqiy bazani o'rganish).

Maqolaning ilmiy-empirik bazasini quyidagilar tashkil etadi:

Xalqaro hujjatlar va hisobotlar: Europol Internet Organised Crime Threat Assessment (IOCTA) 2024 hisoboti; Europol Innovation Lab'ning "Sun’iy intellekt va politsiya faoliyati" kuzatuv hisoboti (2024); FBI Internet Crime Report 2023; Sanna S.L., Regano L., Maiorca D., Giacinto G. tomonidan chop etilgan "Kiberjinoyatlarni aniqlash va raqamli kriminalistika tadqiqotlarini sun'iy intellekt yordamida takomillashtirish" nomli ilmiy maqola (2025).

Milliy statistik ma'lumotlar: O'zbekiston IIV Kiberjinoyatlar markazi press-anjumani materiallari (2025-yil,may); O'zbekiston Respublikasi Kiberxavfsizlik markazi (CSEC) 2023-yil hisoboti; O'zbekiston Markaziy bankining Kiberxavfsizlik markazi ma'lumotlari.

Ilmiy adabiyotlar: Goodfellow I., Bengio Y., Courville A. "Deep Learning" (MIT Press, 2016); Casey E. "Digital Evidence and Computer Crime" (Academic Press, 2011); TRM Labs tadqiqot hisoboti (2025) va boshqalar.

NATIJALAR VA ULARNI MUHOKAMA QILISH

SI texnologiyalari kiberjinoyatchilik sohasida ikki tomonlama ahamiyat kasb etadi: bir tomondan jinoyatchilar tomonidan yangi hujum vositalari sifatida, ikkinchi tomondan huquqni muhofaza qilish organlari tomonidan tergov quroli sifatida foydalanilmoqda.

Europol'ning IOCTA 2024 hisobotida ta'kidlanishicha, SI vositalari texnik bilimga ega bo'lmagan shaxslarga ham murakkab kiberjinoyatlar uyushtirish imkonini bermoqda, bu esa kiberjinoyatchilik sohasiga kirishning «to'sig'ini» sezilarli pasaytirmoqda. Cointelegraph

Deepfake hujumlari 2024-yilda 50-60 foizga o'sib, jahon bo'yicha 140 000 dan 150 000 gacha voqea ro'y bergani taxmin qilinmoqda. Deloitte prognozlariga ko'ra, ushbu va shunga o'xshash hujumlardan yillik yo'qotishlar 2027-yilga kelib 40 milliard dollarga yetishi kutilmoqda. Cobalt

2025-yilning birinchi choragi davomida yolg'iz shu uch oyda 179 ta deepfake hodisasi qayd etildi — bu 2024-yilning to'liq yillik ko'rsatkichidan 19 foizga ko'pdir. Deepfake hujumlarining barcha firibgarlik hujumlaridagi ulushi 6,5 foizni tashkil etib, 2022-yildan beri 2 137 foizga oshdi. Programs

Biroq ayni shu SI texnologiyalari tergov amaliyotida ham kuchli vosita bo'lib xizmat qilmoqda.

Raqamli kriminalistika va ma'lumotlarni tahlil qilish.

Europol hisobotiga ko'ra, kiberjinoyatlarga qarshi kurashda avtomatlashtirilgan tarmoq va zararli dasturlar tahlili muhim ahamiyat kasb etadi. Raqamli kriminalistika usullari raqamli qurilmalardan olingan ma'lumotlarni qayta ishlash orqali jinoyatchilar haqida ma'lumot olish imkonini beradi, bu esa o'z navbatida yangi kiberjinoyatlarni aniqlash tizimlarini takomillashtirishga xizmat qiladi. arxiv

Europol va Eurojust'ning qayd etishicha, tergov ishlarida tahlil qilinishi lozim bo'lgan ma'lumotlar hajmi tobora ortib bormoqda. Masalan, bolalarga nisbatan jinsiy zo'ravonlik bilan bog'liq standart tergov ishida 1 dan 3 terabaytgacha ma'lumot, jumladan 1 dan 10 milliongacha rasm va minglab soatlik video tahlil qilinishi zarur bo'lmoqda. EncroChat ishida esa tashkiliy jinoyat guruhlari o'rtasidagi 115 million dan ortiq suhbat ushlanib olingan; mashinaviy o'rganish usullaridan foydalangan holda Europol va huquqni muhofaza qilish organlari naqshlar, bog'liqliklar va harakatlanish markazlarini aniqlagan hamda 6 558 shubhali shaxs qamoqqa olingan.

Ushbu misol SI ning ulkan hajmdagi ma'lumotlarni tahlil qilishdagi amaliy imkoniyatlarini yaqqol ko'rsatib beradi.

Anomaliyalarni aniqlash va zararli dasturlarni tasniflashtirish.

Kiberinsidentlarni tergov qilishda mashinaviy o'rganish vositalari tarqalgan tarmoqlar bo'yicha keng qamrovli naqsh tahlilini amalga oshirish imkonini beradi. SI asosidagi tizimlar xavfsizlik ogohlantirishlarini taqdim etish va kiberincidentlarni ustuvorlik bo'yicha tartiblash, xatti-harakat tahlili, monitoring hamda anomaliyalarni aniqlash kabi vazifalarni bajaradi.

Tabiiy tilni qayta ishlash (NLP) usullari kiberjinoyatchilar tomonidan yozilgan fishing xatlari, forum postlari va boshqa matnlarni stilometrik tahlil qilish orqali muallifni aniqlashga (authorship attribution) imkon beradi. Bu usul ayniqsa anonim kiberjinoyatchilarni identifikatsiya qilishda muhim ahamiyat kasb etadi.

Yuz tanish va biometrik identifikatsiya.

AQShda FBI tarkibidagi Next Generation Identification – Interstate Photo System (NGI-IPS) 17 ta shtat va 2 ta federal idoraning ma'lumotlarini birlashtiradi hamda 67 million dan ortiq hibsga olinganlar

fotosuratini o'z ichiga oladi. Yuz tanish texnologiyasi tergov chegarasida ruxsat etilgan jinoyat qidiruvlarida jabrdiydalar, shubhalilar va guvohlarni aniqlash uchun qo'llaniladi. Biroq shuni ta'kidlash lozimki, FBI siyosatiga ko'ra, yuz tanish texnologiyasi natijalari yolg'iz o'zi shaxsni isbotlash uchun etarli asos sifatida tan olinmaydi — shaxsning kimligini boshqa tahlil va tergov usullari orqali ham tasdiqlash talab etiladi.

Prognozlash va darknet monitoringi.

INTERPOL hujjatlari shuni ko'rsatadiki, SI agentlari maqsadli xabarlarni avtomatlashtirish va zaif aholi qatlamlarini nishonga olish uchun allaqachon qo'llanilmoqda. Darknet forumlarida esa 2024-yilning iyul oyida faqat bitta forumda 3 500 dan ortiq SI tomonidan yaratilgan jinoyatchilik tasviri aniqlanib, bu ular sonining doimiy o'sib borayotganini ko'rsatdi.

Xalqaro amaliyot: natijalari va samaradorligi.

Europol'ning Innovatsion laboratoriyasi birinchi marta "Sun'iy intellekt va politsiya faoliyati" mavzusida kuzatuv hisoboti nashr etdi. Hisobot huquqni muhofaza qilish organlarida SI'ni joriy etish bilan bog'liq imkoniyatlar va muammolarni yoritib, SI'ning samaradorlik, effektivlik hamda qonuniy va etik standartlarni saqlagan holda ish ko'rsatkichlarini oshirishdagi hissasini ko'rsatib berdi. Hisobotda ma'lumotlarni tahlil qilish, raqamli kriminalistika, kompyuter ko'rishi va biometrika, shuningdek generativ SI kabi qo'llanilish sohalari ko'rib chiqildi.

Yevropa Kiberxavfsizlik Markazi (EC3) 2013-yildan buyon kiberjinoyatlarga qarshi kurashda a'zo davlatlarni qo'llab-quvvatlash, tergov ishlarini muvofiqlashtirish va texnik ekspertiza ko'rsatish vazifalarini bajarib kelmoqda. So'nggi hisobotda SI'dan kiberhujumlarni aniqlash va raqamli kriminalistika tahlilida qo'shimcha vosita sifatida unumliroq foydalanish zaruriyati ta'kidlandi.

Yevropa davlat prokuraturaasi (EPPO) ma'lumotlariga ko'ra, 2024-yil oxirida Yevropada kiberjinoyatlar soni 38 foizga oshib, yetkazilgan zarar 24,8 milliard yevroni tashkil etdi.

O’zbekistondagi vaziyat: dolzarb muammolar.

O'zbekistonda kiberjinoyatchilik keskin sur'atlar bilan o'smoqda. IIV Kiberjinoyatlar markazi ma'lumotlariga ko'ra, 2021-2024-yillarda kiberjinoyatlar oqibatida fuqarolarning 1 trillion 909 milliard so'mdan ortiq mablag'i talon-taroj qilingan. 2024-yilning o'zida esa zarar 603 milliard so'mni tashkil etgan. Shu bilan birga, 2024-yilda kiberjinoyatlar soni 2023-yilga nisbatan 9,1 baravar oshgan.

2024-yil may oyida O'zbekistonning «uz» domen veb-saytlariga 6,6 milliondan ortiq kiberhujumlar amalga oshirildi. 2024-yilda umumiy jinoyatlarning 44,4 foizi kiberjinoyatlar hissasiga to'g'ri kelgan. Chuqurroq tahlil qilinsa, mashhurlar qiyofasidan foydalangan holda jinoyat sodir etish — deepfake ham tobora ommalashib borayotgani qayd etildi.

O'zbekiston IIV akademiyasida «Raqamli texnologiyalar sohasida jinoyatlarga qarshi kurashish faoliyati» yo'nalishi bo'yicha kadrlar tayyorlash yo'lga qo'yilib, 2025-yildan boshlab 100 nafar kursant qo'shimcha tayyorlanmoqda

Biroq tergov amaliyotida SI texnologiyalaridan tizimli foydalanish hali to'liq yo'lga qo'yilmagan. Bugungi kunda O'zbekistonda 50 ga yaqin to'lov tizimi mavjud bo'lib, ularning hammasi ham kiberxavfsizlik talablariga javob bermasligi qayd etilgan.

Etik va huquqiy muammolar

Olimlar va tadqiqotchilar SI'ning tergov jarayonida qo'llanilishi bir qator huquqiy va etik muammolarni keltirib chiqarishini ta'kidlaydilar.

Yuz tanish texnologiyasi noto'g'ri qo'llanilsa, fuqarolik erkinliklarini cheklashi mumkin. Masalan, bu texnologiya faqat qonuniy asosda amalga oshirilayotgan jamoat aksiyalari yoki e'tiroz namoyishlarida ishtirok etayotgan kishilarni identifikatsiya qilish uchun suiste'mol qilinishi xavfi mavjud.

Xavfsizlik mutaxassislarining 60 foizi o'z tashkilotlari SI tomonidan yaratiladigan tahdidlarga qarshi turish uchun yetarlicha tayyorgarlik ko'rmagan deb hisoblaydi.

Algoritmik tarafkashlik muammosi ham jiddiy tadqiqot talab etadi. SI tizimlari o'qitilgan ma'lumotlar to'plamidagi tizimli xatolarni takrorlab, aybsiz shaxslar shubha ostiga olinishiga olib kelishi mumkin. Bu holat, ayniqsa, kiberjinoyat ishlarida raqamli dalillar sud tomonidan qabul qilinishi masalasida insonning oxirgi qaror qabul qiluvchi bo'lib qolishini zaruriy qiladi.

TAKLIF VA TAVSIYALAR

Tadqiqot natijalari asosida quyidagi taklif va tavsiyalar ilgari suriladi:

1. Qonunchilikni takomillashtirish. O'zbekiston Respublikasi Jinoyat-protsessual kodeksiga SI yordamida olingan raqamli dalillarning huquqiy maqomini tartibga soluvchi maxsus normalar kiritilishi va raqamli kriminalistika bo'yicha yagona milliy standart ishlab chiqilishi lozim.
2. Ixtisoslashgan kadrlar tayyorlash. Huquqni muhofaza qilish organlari xodimlarini raqamli kriminalistika va SI texnologiyalari bo'yicha muntazam malaka oshirish tizimini joriy etish hamda IIV akademiyasida bu yo'nalishni kengaytirish zarur.
3. Texnik infratuzilmani rivojlantirish. Kiberjinoyatlarni tergov qilish uchun milliy SI asosidagi platforma yaratish, tarmoq monitoringi tizimlarini zamonaviylashtirishni davom ettirish va "O'zbektelekom" AK qoshidagi UzSOC markazining texnik salohiyatini oshirish maqsadga muvofiq.
4. Xalqaro hamkorlikni kuchaytirish. Kiberjinoyatlar bo'yicha Budapesht konventsiyasiga qo'shilish masalasini ko'rib chiqish, Europol va INTERPOL bilan axborot almashish mexanizmlarini institutlashtirish hamda mintaqaviy hamkorlikni rivojlantirish zarur.
5. Etik nazorat mexanizmini yaratish. SI tizimlarining tergov jarayonida qo'llanilishini nazorat qiluvchi mustaqil ekspert kengashi tuzilsin va fuqarolik nazorati ta'minlansin; hech qanday SI tizimi inson nazoratisiz yakuniy qaror qabul qilmasligi kafolatlansin.
6. Raqamli savodxonlikni oshirish. Aholi o'rtasida kiberhavfsizlik bo'yicha targ'ibot-tashviqot ishlarini kuchaytirish va moliyaviy savodxonlikni oshirish kiberjinoyatlarga qarshi kurashning eng samarali profilaktik vositalaridan biri hisoblanadi.

XULOSA

O'tkazilgan tadqiqot shuni ko'rsatadiki, kiberjinoyatlar bo'yicha tergov harakatlarida sun'iy intellektdan foydalanish bugungi kunda nafaqat imkoniyat, balki zaruriyatga aylangan. Raqamli ma'lumotlarning ulkan hajmi, kiberjinoyatlarning tez o'zgaruvchan tabiati va an'anaviy tergov usullarining cheklovlari — bularning barchasi SI texnologiyalarini tergov amaliyotiga jadal joriy etishni taqozo etmoqda.

Sanna, Regano, Maiorca va Giacinto (2025) kabi tadqiqotchilarning xulosalari, Europol va FBI amaliyoti hamda O'zbekiston IIV Kiberjinoyatlar markazining statistik ma'lumotlari ushbu xulosa to'g'riligini ilmiy va amaliy jihatdan tasdiqlaydi.

Biroq SI tergov amaliyotida vosita sifatida qo'llanganda inson nazorati, shaxsiy ma'lumotlarni himoya qilish va algoritmik adolat tamoyillariga rioya etilishi shart. O'zbekiston uchun esa qonunchilik bazasini takomillashtirish, ixtisoslashgan kadrlar tayyorlash va xalqaro hamkorlikni kuchaytirish ustuvor yo'nalishlar bo'lib qolmoqda. Ushbu masalalarni kechiktirmasdan hal etish mamlakatning raqamli xavfsizligini ta'minlashdagi strategik zaruriyatdir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasining «Axborot xavfsizligi to'g'risida»gi Qonuni. — Toshkent, 2022.
2. O'zbekiston Respublikasi Jinoyat kodeksi, 278–280-moddalar. — Toshkent, 2024 (so'nggi tahrir).
3. O'zbekiston Respublikasi Prezidentining «Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida»gi PQ-153-son Qarori. — Toshkent, 2025.
4. Sanna S.L., Regano L., Maiorca D., Giacinto G. Improving Cybercrime Detection and Digital Forensics Investigations with Artificial Intelligence // arXiv preprint. — 2025. — arXiv:2510.14638.
5. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. — Gaaga: Europol, 2024.
6. Europol Innovation Lab. Observatory Report on AI and Policing. — Gaaga: Europol, 2024.
7. FBI. Internet Crime Report 2023. — Vashington: Federal Bureau of Investigation, 2024.
8. Goodfellow I., Bengio Y., Courville A. Deep Learning. — Cambridge: MIT Press, 2016. — 800 b.
9. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. — Academic Press, 2011. — 840 b.
10. TRM Labs. The Rise of AI-Enabled Crime: Exploring the Evolution, Risks, and Responses to AI-Powered Criminal Enterprises. — San-Fransisko: TRM Labs, 2025.
11. Cobalt. Top 40 AI Cybersecurity Statistics. — 2025. URL: https://www.cobalt.io/blog/top-40-ai-cybersecurity-statistics
12. Darktrace. State of AI Cybersecurity Report. — Kembrij: Darktrace, 2024.
13. O'zbekiston IIV Kiberjinoyatlar markazi. Press-tur materiallari, 2025-yil 29-may. — Toshkent, 2025.
14. O'zbekiston Respublikasi Kiberxavfsizlik markazi (CSEC). 2023-yil yakuni bo'yicha hisobot. — Toshkent, 2024.
15. EUR-Lex. Roadmap for Lawful and Effective Access to Data for Law Enforcement. — Bryussel: Yevropa Komissiyasi, 2025.
16. Gazeta.uz. O'zbekistonda 2021–2024-yillarda banklar va fuqarolar kiberjinoyatlardan 1,9 trln so'm zarar ko'rdi. — Toshkent, 2025-yil 29-may.
17. Daryo.uz. O'zbekistonda kiberxavfsizlik muammosi: hujumlar soni 25 baravarga oshdi. — Toshkent, 2024-yil 27-avgust.
18. Cybersecurity Ventures. 2024 Official Cybercrime Report. — Northport: Cybersecurity Ventures, 2024.