ILMIY-AMALIY JURNAL

Impact Factor: 5.394

ISSN 2181-0958
DOI 10.26739/2181-0958

YURISPRUDENSIYA

ЮРИСПРУДЕНЦИЯ | JURISPRUDENCE

7 JILD, 1

2026

ISSN 2181-0958

Doi Journal 10.26739/2181-0958

YURISPRUDENSIYA

7 ЖИЛД, 1 СОН

ЮРИСПРУДЕНЦИЯ

ТОМ 7, НОМЕР 1

JURISPRUDENCE

VOLUME 7, ISSUE 1

ТОШКЕНТ-2026

YURISPRUDENSIYA | ЮРИСПРУДЕНЦИЯ | JURISPRUDENCE
№1 (2026)

Page Maker | Верстка | Sahifalovchi: Xurshid Mirzaxmedov

Editorial staff of the journals of www.tadqiqot.uz
Tadqiqot LLC The city of Tashkent,
Amir Temur Street pr.1, House 2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Phone: (+998-94) 404-0000

Контакт редакций журналов. www.tadqiqot.uz
ООО Tadqiqot город Ташкент,
улица Амира Темура пр.1, дом-2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Тел: (+998-94) 404-0000

МУНДАРИЖА | СОДЕРЖАНИЕ | CONTENT

KIBERJINOYATLARNING KRIMINALISTIK TAVSIFI VA ULARNI TERGOV QILISH USLUBIYATI.

http://dx.doi.org/10.5281/zenodo.20186574

Zaynabutdinov Said Axrorbek Ulug'bek ugli
Toshkent davlat yuridik universiteti
Mustaqil tadqiqotchi

Annotatsiya: Ushbu maqolada O‘zbekiston Respublikasida kiberjinoyatlarning kriminalistik tavsifi hamda ularni tergov qilishning metodologik asoslari raqamlashtirish sharoitida kompleks ilmiy tahlil qilinadi. So‘nggi yillarda kiberjinoyatchilik jinoyatchilikning eng tez o‘sayotgan yo‘nalishlaridan biriga aylangan bo‘lib, rasmiy statistik ma’lumotlarga ko‘ra, kiberfiribgarlik, fishing hujumlari, bank kartalari orqali sodir etiladigan jinoyatlar hamda zararli dasturlar yordamidagi hujumlar sezilarli darajada oshgan.

Tadqiqot doirasida kiberjinoyatlarning kriminalistik tasnifi ishlab chiqilib, axborot tizimlariga ruxsatsiz kirish, elektron to‘lov tizimlarida firibgarlik, shaxsiy ma’lumotlarni noqonuniy egallash, ransomware hujumlari hamda internet muhitida sodir etiladigan boshqa jinoyat turlari tahlil qilinadi. Shu bilan birga, ularni aniqlash va tergov qilishda qo‘llaniladigan zamonaviy kriminalistik usullar — raqamli dalillarni yig‘ish va tahlil qilish, tarmoq trafigini monitoring qilish, OSINT texnologiyalari, raqamli izlarni rekonstruksiya qilish hamda kompyuter va mobil kriminalistika vositalarining ahamiyati yoritiladi.

Metodologik jihatdan tadqiqot qiyosiy-huquqiy tahlil, empirik statistik ma’lumotlar hamda xalqaro kriminalistik tajribani milliy huquqiy tizimga tatbiq etish asosida amalga oshirilgan. Shuningdek, kiberjinoyatlarni tergov qilish jarayonida yuzaga kelayotgan asosiy muammolar — shifrlash texnologiyalarining murakkablashuvi, anonimlashtirish vositalaridan foydalanish, transchegaraviy jinoyatlar va yurisdiksiya muammolari hamda raqamli kriminalistika texnologiyalarining yetarli darajada joriy etilmaganligi tahlil qilingan.

Tadqiqot natijalari O‘zbekistonda kiberjinoyatlarga qarshi kurashish samaradorligini oshirish uchun raqamli kriminalistika infratuzilmasini rivojlantirish, tergov xodimlarining malakasini oshirish hamda yagona metodologik standartlarni ishlab chiqish zarurligini ko‘rsatadi.

Kalit so‘zlar: Kiberjinoyat; raqamli kriminalistika; kibertergov metodologiyasi; elektron dalillar; OSINT; kiberfiribgarlik; axborot xavfsizligi; raqamli izlar; jinoyat protsessi; kiberxavfsizlik tahdidlari; bank kartalari firibgarligi;

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ И МЕТОДИКА ИХ РАССЛЕДОВАНИЯ

Зайнабутдинов Саид Ахорбек Улугбек угли
Ташкентский государственный юридический университет
Независимый исследователь

Аннотация: В данной статье проводится комплексный научный анализ криминалистической характеристики киберпреступлений в Республике Узбекистан и методологических основ их расследования в условиях цифровизации. В последние годы киберпреступность стала одним из наиболее быстро растущих направлений преступности, и согласно официальным статистическим данным наблюдается значительный рост кибермошенничества, фишинговых атак, преступлений, совершаемых с использованием банковских карт, а также атак с применением вредоносного программного обеспечения.
В рамках исследования разработана криминалистическая классификация киберпреступлений, включающая несанкционированный доступ к информационным системам, мошенничество в электронных платёжных системах, незаконное завладение персональными данными, атаки типа ransomware, а также иные преступления, совершаемые в интернет-среде. Одновременно раскрывается значение современных криминалистических методов их выявления и расследования — сбора и анализа цифровых доказательств, мониторинга сетевого трафика, технологий OSINT, реконструкции цифровых следов, а также использования средств компьютерной и мобильной криминалистики.
С методологической точки зрения исследование основано на сравнительно-правовом анализе, эмпирических статистических данных, а также на адаптации международного криминалистического опыта к национальной правовой системе. Кроме того, проанализированы основные проблемы, возникающие в процессе расследования киберпреступлений, такие как усложнение технологий шифрования, использование средств анонимизации, трансграничный характер преступлений и проблемы юрисдикции, а также недостаточный уровень внедрения технологий цифровой криминалистики.
Результаты исследования свидетельствуют о необходимости развития инфраструктуры цифровой криминалистики в Узбекистане, повышения квалификации сотрудников следственных органов, а также разработки единых методологических стандартов для повышения эффективности противодействия киберпреступности.

Ключевые слова: Киберпреступление; цифровая криминалистика; методология киберрасследования; электронные доказательства; OSINT; кибермошенничество; информационная безопасность; цифровые следы; уголовный процесс; угрозы кибербезопасности; мошенничество с банковскими картами;

CRIMINALISTIC CHARACTERISTICS OF CYBERCRIME AND METHODOLOGY OF THEIR INVESTIGATION

Zaynabutdinov Said Axrorbek Ulug'bek ugli
Tashkent State University of Law
Independent Researcher

Abstract: This article provides a comprehensive scientific analysis of the criminalistic characteristics of cybercrime in the Republic of Uzbekistan and the methodological foundations of their investigation in the context of digitalization. In recent years, cybercrime has become one of the fastest-growing areas of criminal activity, and according to official statistical data, there has been a significant increase in cyber fraud, phishing attacks, crimes committed through bank cards, and attacks using malicious software.

Within the scope of the study, a criminalistic classification of cybercrimes has been developed, including unauthorized access to information systems, fraud in electronic payment systems, illegal acquisition of personal data, ransomware attacks, as well as other types of crimes committed in the online environment. At the same time, the importance of modern forensic methods used for their detection and investigation is highlighted, including the collection and analysis of digital evidence, network traffic monitoring, OSINT technologies, reconstruction of digital traces, and the use of computer and mobile forensic tools.

Methodologically, the study is based on comparative legal analysis, empirical statistical data, and the adaptation of international forensic experience to the national legal system. In addition, the main challenges arising in the process of investigating cybercrimes are analyzed, such as the increasing complexity of encryption technologies, the use of anonymization tools, transnational crime, jurisdictional issues, and the insufficient implementation of digital forensic technologies.

The results of the study indicate the need to develop digital forensic infrastructure in Uzbekistan, improve the qualifications of investigative personnel, and develop unified methodological standards to enhance the effectiveness of combating cybercrime.

Keywords: Cybercrime; digital forensics; cyber investigation methodology; electronic evidence; OSINT; cyber fraud; information security; digital traces; criminal procedure; cybersecurity threats; bank card fraud;

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi zamonaviy jamiyatning ijtimoiy-iqtisodiy tuzilmasini sezilarli darajada o‘zgartirib, raqamli xizmatlar, elektron tijorat va onlayn platformalarning kengayishiga olib keldi. Shu bilan birga, ushbu jarayonlar jinoyatchilikning yangi shakllari — xususan, kiberjinoyatchilikning paydo bo‘lishi va rivojlanishi uchun ham sharoit yaratdi. Bugungi kunda kiberjinoyatchilik milliy xavfsizlik va jamoat tartibiga jiddiy tahdid soluvchi eng murakkab va tez rivojlanayotgan jinoyat turlaridan biri sifatida e’tirof etilmoqda.[1]

O‘zbekiston Respublikasida raqamli transformatsiya jarayonlarining keng joriy etilishi, elektron hukumat tizimlarining rivojlanishi hamda moliyaviy texnologiyalarning ommalashuvi fonida kiberjinoyatlar sonining ortishi kuzatilmoqda. Amaliy statistik ma’lumotlarga ko‘ra, so‘nggi yillarda axborot tizimlariga ruxsatsiz kirish, onlayn to‘lov tizimlarida firibgarlik, fishing hujumlari, shaxsiy ma’lumotlarni noqonuniy egallash hamda zararli dasturlar orqali amalga oshiriladigan jinoyatlar

[1] UNODC. *Comprehensive Study on Cybercrime*. – New York: United Nations, 2013. – P. 15–29.

sezilarli darajada ko‘paygan.[1] Ushbu holat kiberjinoyatlarning nafaqat miqdoriy jihatdan, balki sifat jihatdan ham murakkablashib, transchegaraviy xususiyat kasb etayotganini ko‘rsatadi.

Kriminalistik nuqtai nazardan kiberjinoyatlarni tergov qilish o‘ziga xos metodologik va amaliy murakkabliklarga ega. An’anaviy jinoyatlardan farqli ravishda, kiberjinoyatlar raqamli muhitda sodir etilib, ular asosan elektron izlar ko‘rinishida namoyon bo‘ladi. Ushbu izlar esa tez o‘zgaruvchan, oson yo‘q qilinadigan hamda ko‘pincha bir nechta davlat yurisdiksiyasiga taalluqli bo‘ladi. Shu sababli raqamli dalillarni yig‘ish va saqlash, tarmoq trafikini kriminalistik tahlil qilish, zararli dasturlarni o‘rganish hamda raqamli muhitda foydalanuvchi harakatlarini rekonstruksiya qilish kabi maxsus usullarni qo‘llash zarur bo‘ladi.[2]

O‘zbekistonda kiberjinoyatchilikka qarshi kurashish bo‘yicha normativ-huquqiy baza va institutsional tizimni takomillashtirish yo‘nalishida izchil islohotlar amalga oshirilmoqda. Biroq amaliyotda bir qator muammolar saqlanib qolmoqda. Jumladan, kiberjinoyatlarni tergov qilish metodologiyalarining yetarli darajada standartlashtirilmaganligi, zamonaviy raqamli kriminalistika vositalarining to‘liq joriy etilmaganligi, shuningdek, anonimlashtirish texnologiyalari va shifrlangan aloqa kanallari orqali sodir etilayotgan jinoyatlarning murakkablashuvi shular jumlasidandir.

Shu nuqtai nazardan, kiberjinoyatlarning kriminalistik xususiyatlarini chuqur o‘rganish hamda ularni tergov qilish metodologiyasini takomillashtirish dolzarb ilmiy-amaliy ahamiyat kasb etadi. Bu esa jinoyat ishlari bo‘yicha odil sudlov samaradorligini oshirish, raqamli xavfsizlikni ta’minlash hamda davlat, biznes va fuqarolarning axborot resurslarini ishonchli himoya qilishga xizmat qiladi.

ADABIYOTLAR TAHLILI

Kiberjinoyatlarni tergov qilish muammosi zamonaviy ilmiy adabiyotlarda kriminal huquq, axborot xavfsizligi, kompyuter fanlari va kriminalistika kesishmasida rivojlanayotgan ko‘p tarmoqli tadqiqot yo‘nalishi sifatida qaraladi. Xalqaro ilmiy manbalarda kiberjinoyatlarning tabiati, raqamli dalillar xususiyatlari hamda ularni tergov qilish metodologiyasi bo‘yicha keng nazariy va amaliy yondashuvlar shakllantirilgan.

Eoghan Casey raqamli dalillarni kriminalistik jihatdan tahlil qilishda ularning o‘zgaruvchanligi, nozikligi va to‘g‘ri yig‘ish hamda saqlash jarayonlariga bog‘liqligini asoslab bergan. Uning ishlari raqamli dalillarni protsessual jihatdan maqbul shaklda rasmiylashtirish va ularning sud jarayonida ishonchliligini ta’minlash bo‘yicha muhim ilmiy asos yaratgan.[3] Brian Carrier esa fayl tizimlarini kriminalistik tahlil qilish modelini ishlab chiqib, raqamli qurilmalarda foydalanuvchi harakatlarini tizimli rekonstruksiya qilish imkonini bergan.[4]

[1] O‘zbekiston Respublikasi Kiberxavfsizlik markazi. *Yillik tahliliy hisobot*. – Toshkent, 2024. – B. 8–14.
[2] Carrier B. *File System Forensic Analysis*. – Boston: Addison-Wesley, 2005. – P. 77–95.
[3] Casey E. *Digital Evidence and Computer Crime*. – London: Academic Press, 2011. – P. 112–140.
[4] Carrier B. *File System Forensic Analysis*. – Boston: Addison-Wesley, 2005. – P. 201–228.

G‘arb ilmiy maktabida kiberjinoyatchilik tadqiqotlari doirasida tarmoq kriminalistikasi, zararli dasturlar tahlili va virtual muhitda jinoyatchi xulq-atvorini o‘rganish muhim o‘rin tutadi. Richard A. Clarke va Thomas J. Holt kiberjinoyatchilikning tashkiliy shakllarini, jumladan moliyaviy motivga asoslangan jinoyatchilar, xaktivist guruhlar hamda transmilliy kiberjinoyat tarmoqlarini tahlil qilib, ushbu jinoyatlarning anonimlik va markazlashmaganlik xususiyatini asoslab bergan.[1]

Postsovet ilmiy makonida, xususan O‘zbekiston va qo‘shni davlatlarda olib borilgan tadqiqotlar asosan elektron dalillarni yig‘ish, mustahkamlash va protsessual rasmiylashtirish muammolariga qaratilgan. Biroq mavjud ilmiy adabiyotlarda sun’iy intellekt asosida tahdidlarni aniqlash, avtomatlashtirilgan log tahlili hamda platformalararo raqamli izlarni integratsiyalashgan tahlil qilish kabi zamonaviy metodlar yetarli darajada yoritilmagan.

So‘nggi tahliliy hisobotlar O‘zbekistonda, ayniqsa moliya va telekommunikatsiya sohalarida kiberjinoyatlar o‘sish tendensiyasini ko‘rsatadi. Jinoyatlarning asosiy qismi fishing hujumlari, bank tizimlariga noqonuniy kirish va ijtimoiy muhandislik usullari bilan bog‘liq ekani qayd etilgan.[2] Shu bilan birga, milliy ilmiy adabiyotlarda kiberjinoyatlarni kriminalistik rekonstruksiya qilish va tergov metodologiyasini takomillashtirishga oid empirik tadqiqotlar yetarli emas.

Umuman olganda, adabiyotlar tahlili shuni ko‘rsatadiki, xalqaro darajada raqamli kriminalistika sezilarli darajada rivojlangan bo‘lsa-da, O‘zbekiston sharoitiga moslashtirilgan kompleks metodologik yondashuvlarni ishlab chiqish zarurati mavjud.

METODOLOGIYA

Ushbu tadqiqotning metodologik asosini kiberjinoyatlarning kriminalistik xususiyatlarini o‘rganish hamda ularni tergov qilish jarayonlarini takomillashtirishga qaratilgan umumilmiy, huquqiy-dogmatik va maxsus kriminalistik usullar tizimi tashkil etadi.[3]

Birinchidan, **dialektik usul** O‘zbekistonda raqamli transformatsiya jarayonlari va kiberjinoyatchilik o‘rtasidagi o‘zaro bog‘liqlikni o‘rganishda qo‘llanilib, texnologik rivojlanish va jinoyatchilik evolyutsiyasi o‘rtasidagi sababiy aloqalarni aniqlash imkonini beradi.[4]

Ikkinchidan, **qiyosiy-huquqiy tahlil usuli** Yevropa Ittifoqi, AQSh va MDH davlatlarining kiberjinoyatlarni tergov qilish tajribasini o‘rganish va milliy huquqiy tizimga moslashtirilishi mumkin bo‘lgan samarali modellarning aniqlanishi uchun qo‘llaniladi.[5]

Uchinchidan, **statistik tahlil usuli** huquqni muhofaza qiluvchi organlar va kiberxavfsizlik bo‘yicha rasmiy hisobotlar asosida kiberjinoyatlar dinamikasini

[1] Holt T.J. *Cybercrime Through an Interdisciplinary Lens*. – New York: Routledge, 2016. – P. 55–83.
[2] O‘zbekiston Respublikasi IIV. *Kiberjinoyatlar statistik tahlili*. – Toshkent, 2025. – B. 20–31.
[3] Casey, E. *Digital Evidence and Computer Crime*. – Academic Press, 2011. – 35–48-betlar.
[4] UNODC. *Comprehensive Study on Cybercrime*. – Vienna, 2013. – 120–135-betlar.
[5] Clarke, R. A., Holt, T. J. *Cybercrime and Cyberwarfare*. – 2010. – 75–90-betlar.

o‘rganish, ularni tasniflash hamda asosiy hujum yo‘nalishlarini aniqlash imkonini beradi.[1]

To‘rtinchidan, **kriminalistik modellashtirish va rekonstruksiya usullari** raqamli izlar, log fayllar, metadata va tarmoq trafigi asosida kiberhodisa jarayonlarini qayta tiklashga xizmat qiladi. Ushbu yondashuv jinoyatchi harakatlarining ketma-ketligini aniqlashda muhim ahamiyatga ega.[2]

Beshinchidan, **OSINT (ochiq manbalar razvedkasi)** va elektron kontent tahlili usullari internetdagi ochiq ma’lumotlar asosida jinoyatchi infratuzilmasi, kommunikatsiya kanallari va raqamli izlarni aniqlashga imkon beradi.[3]

Oxirida, tadqiqot **tizimli yondashuv** asosida amalga oshiriladi, bunda kiberjinoyatlarni tergov qilish texnik, protsessual va huquqiy komponentlarni o‘z ichiga olgan yaxlit tizim sifatida ko‘rib chiqiladi. Bu yondashuv O‘zbekiston sharoitida kriminalistik samaradorlikni oshirishga qaratilgan ilmiy asoslangan takliflarni ishlab chiqishga xizmat qiladi.[4]

NATIJALAR

O‘tkazilgan tadqiqot O‘zbekiston Respublikasida kiberjinoyatchilikka xos bo‘lgan bir qator muhim kriminalistik qonuniyatlarni hamda ularni tergov qilish samaradorligiga ta’sir etuvchi metodologik muammolarni aniqladi.

Birinchidan, empirik tahlillar so‘nggi yillarda kiberjinoyatlar sonining barqaror o‘sish tendensiyasiga ega ekanligini tasdiqlaydi. Qayd etilgan jinoyatlarning asosiy qismi moliyaviy texnologiyalar sohasi — elektron to‘lov tizimlari, onlayn bank xizmatlari va mobil platformalar bilan bog‘liq. Eng ko‘p uchraydigan jinoyat shakllari sifatida fishing hujumlari, bank hisoblariga ruxsatsiz kirish, ijtimoiy muhandislik asosidagi firibgarlik hamda zararli dasturlar yordamida ma’lumotlarni o‘g‘irlash holatlari aniqlangan.[5] Bu esa kiberjinoyatlarning tobora iqtisodiy manfaatga yo‘naltirilgan va murakkab raqamli sxemalarga asoslanayotganini ko‘rsatadi.

Ikkinchidan, tadqiqot natijalari kiberjinoyatlarning kriminalistik tuzilmasi ko‘p qatlamli raqamli izlar tizimidan iborat ekanligini ko‘rsatadi. Jinoyat faoliyati odatda bir nechta darajada iz qoldiradi: qurilma darajasida (brauzer tarixi, kesh, reyestr yozuvlari), tarmoq darajasida (IP manzillar, trafik loglari, server so‘rovlari) hamda bulutli muhitda (sinxronizatsiya qilingan hisoblar va masofaviy zaxira ma’lumotlari). Biroq ushbu izlarning tez o‘zgaruvchanligi va yo‘q qilinishi ularni to‘liq kriminalistik rekonstruksiya qilishni murakkablashtiradi.[6]

Uchinchidan, kiberjinoyatchilar tomonidan anonimlashtirish texnologiyalaridan keng foydalanilishi aniqlangan. VPN xizmatlari, proksi zanjirlari, shifrlangan kommunikatsiya vositalari hamda darknet infratuzilmasi jinoyatchini identifikatsiya qilish jarayonini sezilarli darajada qiyinlashtirmoqda. Natijada an’anaviy tergov

[1] O‘zbekiston Respublikasi IIV. *Raqamli jinoyatlar statistikasi*. – Toshkent, 2025. – 15–22-betlar.
[2] Carrier, B. *File System Forensic Analysis*. – Addison-Wesley, 2005. – 110–128-betlar.
[3] INTERPOL. *Global Cybercrime Report*. – Lyon, 2023. – 28–36-betlar.
[4] OECD. *Cybersecurity Policy Framework*. – Paris, 2021. – 44–58-betlar.
[5] O‘zbekiston Respublikasi IIV. *Kiberjinoyatchilik statistikasi*. – Toshkent, 2025. – B. 17–42.
[6] Carrier B. *File System Forensic Analysis*. – Boston: Addison-Wesley, 2005. – P. 241–267.

usullari yetarli bo‘lmay qolib, ilg‘or raqamli kriminalistik vositalar va transchegaraviy hamkorlik mexanizmlarini qo‘llash zarurati ortmoqda.[1]

To‘rtinchidan, amaliy tergov jarayonlari tahlili shuni ko‘rsatadiki, kiberjinoyatlarni aniqlash samaradorligi tergovchilarning texnik tayyorgarligi va raqamli kriminalistika vositalaridan foydalanish darajasiga bevosita bog‘liq. Ayrim holatlarda raqamli dalillarni yig‘ishdagi kechikishlar, standartlashtirilgan protsessual protokollarning yetishmasligi hamda avtomatlashtirilgan tahlil tizimlarining to‘liq joriy etilmaganligi muhim ma’lumotlarning yo‘qolishiga olib kelmoqda. Bu esa yagona kriminalistik standartlarni ishlab chiqish zarurligini ko‘rsatadi.[2]

Beshinchidan, natijalar interdisiplinar yondashuv kiberjinoyatlarni tergov qilish samaradorligini sezilarli oshirishini tasdiqlaydi. Tarmoq kriminalistikasi, OSINT usullari va xulq-atvor tahlilini birgalikda qo‘llash jinoyat hodisalarini to‘liqroq rekonstruksiya qilish imkonini beradi. Turli manbalardan olingan metadata ma’lumotlarini korrelyatsiya qilish esa takroriy jinoyat sxemalarini aniqlashga yordam beradi.

Nihoyat, tadqiqot O‘zbekistonda kiberjinoyatlarga qarshi kurashish tizimi bosqichma-bosqich raqamli transformatsiyaga moslashayotganini ko‘rsatdi. Shu bilan birga, sun’iy intellekt asosidagi tahlil tizimlari, real vaqt monitoring vositalari hamda avtomatlashtirilgan dalillarni korrelyatsiya qilish platformalarining yetarli darajada integratsiya qilinmaganligi mavjud. Bu esa tergov jarayonining tezligi va aniqligini cheklovchi asosiy omillardan biri hisoblanadi.[3]

Umuman olganda, olingan natijalar kiberjinoyatlarni tergov qilish tizimi tobora texnologik jihatdan murakkab va interdisiplinar modelga o‘tib borayotganini tasdiqlaydi. Ushbu jarayonda huquqiy asoslar, raqamli kriminalistika vositalari va xalqaro hamkorlik mexanizmlarining uyg‘unligi hal qiluvchi ahamiyatga ega.

MUNOZARA

Olingan natijalar O‘zbekistonda kiberjinoyatchilik endilikda yordamchi yoki ikkilamchi jinoyat turi emas, balki zamonaviy jinoyatchilik tizimining asosiy tarkibiy elementi sifatida shakllanib, moliyaviy, axborot va ijtimoiy infratuzilmalar bilan chuqur integratsiyalashganini ko‘rsatadi. Ushbu tendensiya global kiberjinoyatchilik rivojlanish yo‘nalishlari bilan uyg‘un bo‘lib, raqamli muhitning bir vaqtning o‘zida ham jinoyat vositasi, ham jinoyat obyekti sifatida namoyon bo‘layotganini tasdiqlaydi.[4]

Tadqiqotda aniqlangan asosiy muammolardan biri kiberjinoyatlarni aniq shaxs yoki jinoyatchi guruhga bog‘lash (atributsiya qilish) jarayonining murakkablashuvidir. Anonimlashtirish texnologiyalari, shifrlangan kommunikatsiya kanallari va geografik jihatdan tarqoq raqamli infratuzilma jinoyatchi va jinoyat o‘rtasidagi bevosita sababiy bog‘liqlikni aniqlashni sezilarli darajada qiyinlashtirmoqda. Natijada kriminalistik identifikatsiyaning an’anaviy tamoyillari virtual muhitda to‘liq samarali ishlamay

[1] INTERPOL. *Cyber Threat Assessment Report*. – Lyon, 2024. – P. 61–80.
[2] O‘zbekiston Respublikasi Kiberxavfsizlik markazi. *Analitik hisobot*. – Toshkent, 2024. – B. 44–57.
[3] INTERPOL. *Global Cybercrime Trend Report*. – Lyon: INTERPOL Global Complex for Innovation, 2024. – B 61–80.
[4] UNODC. *Cybercrime and Digital Transformation*. – 2022. – 55–63-betlar.

qolmoqda, chunki raqamli dalillar fragmentatsiyalashgan, dinamik va tez yo‘qoluvchan xususiyatga ega.[1]

Metodologik nuqtai nazardan, natijalar kiberjinoyatlarni tergov qilishda chiziqli yondashuvdan ko‘ra ko‘p o‘lchovli kriminalistik rekonstruksiya tizimlariga o‘tish zarurligini tasdiqlaydi. Bunday tizimlarda raqamli izlar alohida obyekt sifatida emas, balki qurilmalar, tarmoqlar va bulutli infratuzilmalar o‘rtasidagi o‘zaro bog‘liq ma’lumot klasterlari sifatida tahlil qilinishi lozim. Ushbu yondashuv xalqaro kriminalistika amaliyotiga mos kelib, jinoyatchi xulq-atvorini korrelyatsion tahlil qilish va profilaktik modellashtirish imkonini kengaytiradi.[2]

Tadqiqot, shuningdek, kiberjinoyatchilik usullarining tez rivojlanishi va tergov metodologiyalarining moslashuv tezligi o‘rtasida doimiy nomutanosiblik mavjudligini ko‘rsatadi. Jinoyatchilar sun’iy intellekt asosidagi fishing sxemalari, deepfake texnologiyalari va avtomatlashtirilgan hujum skriptlaridan faol foydalanayotgan bir sharoitda, tergov amaliyotida ayrim holatlarda hanuzgacha qisman qo‘lda tahlil usullari qo‘llanilmoqda. Bu esa kriminalistik javob reaksiyasi tezligini pasaytiradi hamda muhim raqamli dalillar yo‘qolishi xavfini oshiradi.[3]

Muhokama etiladigan muhim jihatlardan yana biri O‘zbekistondagi kriminalistik va huquqni muhofaza qiluvchi organlarning institutsional va texnik tayyorgarligi masalasidir. So‘nggi yillarda raqamli infratuzilma va huquqiy asoslarni rivojlantirish bo‘yicha sezilarli yutuqlarga erishilgan bo‘lsa-da, kiberkriminalistika sohasida ixtisoslashgan kadrlar tayyorlash darajasini oshirish zarurati saqlanib qolmoqda. Zamonaviy kiberjinoyatlarni kompleks tahlil qilish uchun huquqiy bilimlar bilan bir qatorda kompyuter fanlari, tarmoq arxitekturasi va ma’lumotlar tahlili bo‘yicha chuqur texnik kompetensiyalar ham talab etiladi.[4]

Bundan tashqari, tadqiqot kiberjinoyatlarni tergov qilishda xalqaro hamkorlikning hal qiluvchi ahamiyatga ega ekanligini tasdiqlaydi. Raqamli jinoyatlarning transchegaraviy xususiyati tezkor axborot almashinuvi, o‘zaro huquqiy yordam va muvofiqlashtirilgan kriminalistik operatsiyalarni talab qiladi. Bu ayniqsa global moliyaviy firibgarliklar va taqsimlangan kiberhujum tarmoqlariga qarshi kurashda muhim ahamiyat kasb etadi.[5]

Shu bilan birga, sun’iy intellekt, mashinaviy o‘rganish va avtomatlashtirilgan kriminalistik tizimlar kabi texnologiyalarni joriy etish ikki tomonlama ta’sirga ega. Ular ma’lumotlarni tahlil qilish tezligini oshirishi va kriminalistik naqshlarni aniqlash samaradorligini kuchaytirishi bilan birga, algoritmik shaffoflik, dalillarning ishonchliligi hamda sud jarayonida maqbulligi bilan bog‘liq yangi huquqiy va metodologik muammolarni ham yuzaga keltiradi. Shu sababli ularni joriy etish qat’iy normativ va protsessual kafolatlar asosida amalga oshirilishi lozim.[6]

Xulosa qilib aytganda, O‘zbekistonda kiberjinoyatlarni samarali tergov qilish kriminalistik metodologiyaning kompleks transformatsiyasini talab etadi. Bu jarayon

[1] Casey, E. *Digital Evidence and Computer Crime*. – 2011. – 200–215-betlar.
[2] Carrier, B. *File System Forensic Analysis*. – 2005. – 300–315-betlar.
[3] Holt, T. J. *Cybercrime*. – 2016. – 120–134-betlar.
[4] O‘zbekiston Respublikasi Kiberxavfsizlik markazi. *Yillik hisobot*. – Toshkent, 2024. – 14–19-betlar.
[5] INTERPOL. *Cybercrime Cooperation Report*. – 2023. – 60–72-betlar.
[6] OECD. *AI in Criminal Justice*. – 2021. – 90–104-betlar.

texnologik modernizatsiya, institutsional salohiyatni kuchaytirish hamda xalqaro standartlar bilan uyg‘unlashtirishni o‘z ichiga olishi zarur. Faqat integratsiyalashgan yondashuv asosida tobora murakkablashib borayotgan kiberxavflarga samarali javob berish mumkin bo‘ladi.

Xulosa

O‘tkazilgan tadqiqot natijalariga ko‘ra, O‘zbekiston Respublikasida kiberjinoyatchilik murakkab, yuqori darajada strukturaviylashgan va texnologik jihatdan rivojlangan jinoyat turi sifatida shakllanib, milliy axborot xavfsizligi, moliyaviy barqarorlik hamda raqamli infratuzilma yaxlitligiga jiddiy tahdid solmoqda.[1] Kriminalistik tahlillar zamonaviy kiberjinoyatlar yuqori darajadagi anonimlik, transchegaraviy amalga oshirilish va ilg‘or yashirish texnologiyalaridan foydalanish bilan tavsiflanishini ko‘rsatadi. Bu esa an’anaviy tergov usullarining samaradorligini sezilarli darajada cheklaydi.

Aniqlanishicha, kiberjinoyatlarning daliliy bazasi asosan raqamli xarakterga ega bo‘lib, u tez o‘zgaruvchan, fragmentatsiyalashgan va turli axborot tizimlari bo‘ylab tarqalgan ma’lumotlardan iborat. Bu holat klassik kriminalistik yondashuvlardan farqli ravishda ko‘p manbali korrelyatsiya, tezkor dalillarni saqlash va ilg‘or raqamli rekonstruksiya metodlariga asoslangan kompleks yondashuvni talab etadi.[2]

Tadqiqot, shuningdek, O‘zbekistonda kiberjinoyatchilikka qarshi kurashish bo‘yicha huquqiy va institutsional tizimni takomillashtirish yo‘nalishida ijobiy o‘zgarishlar amalga oshirilganini, biroq kriminalistik metodologiyalarni modernizatsiya qilish zarurati saqlanib qolayotganini ko‘rsatdi. Xususan, raqamli dalillar bilan ishlash jarayonlarini standartlashtirish, ilg‘or tahliliy texnologiyalarni joriy etish hamda mutaxassislar tayyorgarligini kuchaytirish bo‘yicha institutsional bo‘shliqlar mavjud.[3]

Umuman olganda, tadqiqot kiberjinoyatlarga qarshi samarali kurashish faqat huquqiy baza, kriminalistik metodologiya va texnologik infratuzilmaning yagona integratsiyalashgan tizimda rivojlanishi orqali ta’minlanishini tasdiqlaydi.

Takliflar

Tadqiqot natijalaridan kelib chiqib, quyidagi ilmiy-amaliy tavsiyalar ilgari suriladi:

1. Yagona raqamli kriminalistik standartlarni ishlab chiqish
Elektron dalillarni yig‘ish, saqlash, tahlil qilish va sud jarayonida taqdim etish bo‘yicha milliy yagona standart va protokollarni ishlab chiqish hamda joriy etish zarur.

2. Kriminalistik infratuzilmani modernizatsiya qilish
Tergov va ekspertiza organlarini tarmoq kriminalistikasi, zararli dasturlar tahlili, xotira kriminalistikasi hamda avtomatlashtirilgan log tahlili vositalari bilan ta’minlash lozim.

3. Sun’iy intellekt asosidagi tahlil tizimlarini joriy etish
Kiberxavflarni aniqlash, anomal holatlarni monitoring qilish va prognozlash uchun

[1] UNODC. *Cybercrime Report*. – 2022. – 70–78-betlar.
[2] Casey, E. *Digital Evidence and Computer Crime*. – 2011. – 250–265-betlar.
[3] O‘zbekiston Respublikasi Kiberxavfsizlik markazi. *Tahliliy hisobot*. – 2024. – 22–28-betlar.

mashinaviy o‘rganish va sun’iy intellekt texnologiyalaridan foydalanish tavsiya etiladi.[1]

4. Kadrlar tayyorlash va malaka oshirish tizimini takomillashtirish Tergovchilar uchun kiberkriminalistika, raqamli dalillar tahlili va axborot xavfsizligi bo‘yicha uzluksiz o‘quv dasturlarini joriy etish zarur.

5. Idoralararo va xalqaro hamkorlikni kengaytirish Huquqni muhofaza qiluvchi organlar, moliyaviy institutlar, internet provayderlar hamda INTERPOL va Europol kabi xalqaro tashkilotlar bilan hamkorlikni kuchaytirish lozim.[2]

6. Kiberjinoyatchilik bo‘yicha huquqiy bazani takomillashtirish Sun’iy intellekt, deepfake texnologiyalari va markazlashmagan raqamli platformalar bilan bog‘liq yangi jinoyat tarkiblarini qonunchilikka kiritish zarur.

7. Markazlashtirilgan raqamli dalillar bazasini yaratish Kiberjinoyatlarga oid raqamli dalillarni saqlash va tahlil qilish uchun yagona integratsiyalashgan ma’lumotlar bazasini shakllantirish tergov samaradorligini oshiradi.

Yakuniy xulosa

Umuman olganda, O‘zbekistonda kiberxavfsizlikni ta’minlash va kiberjinoyatlarga qarshi kurashish samaradorligini oshirish uchun ilg‘or kriminalistik texnologiyalar, huquqiy mexanizmlar va institutsional salohiyatning uyg‘un rivojlanishi zarur. Ushbu takliflarning amaliyotga tatbiq etilishi milliy raqamli xavfsizlik barqarorligini mustahkamlash va jinoyat odil sudlov tizimi samaradorligini oshirishga xizmat qiladi.

[1] OECD. *Artificial Intelligence Policy*. – 2021. – 110–118-betlar.
[2] INTERPOL. *Global Cybercrime Cooperation*. – 2023. – 80–92-betlar.

O‘ZBEK ADABIYOTLARI VA MANBALAR RO‘YXATI (GOST 7.1–2003 TALABLARI ASOSIDA)

1. Normativ-huquqiy hujjatlar

1. O‘zbekiston Respublikasi. Jinoyat kodeksi. – Toshkent: Adliya vazirligi rasmiy nashri, 2023. – 320 b.

2. O‘zbekiston Respublikasi. Jinoyat-protsessual kodeksi. – Toshkent: Adliya vazirligi rasmiy nashri, 2023. – 410 b.

3. O‘zbekiston Respublikasi Qonuni. “Axborotlashtirish to‘g‘risida”. – Toshkent, 2020-yil 11-dekabr. – Qonun hujjatlari to‘plami.

4. O‘zbekiston Respublikasi Qonuni. “Kiberxavfsizlik to‘g‘risida”. – Toshkent, 2022-yil. – Qonun hujjatlari to‘plami.

5. O‘zbekiston Respublikasi Qonuni. “Shaxsiy ma’lumotlar to‘g‘risida”. – Toshkent, 2019-yil. – Qonun hujjatlari to‘plami.

2. Davlat organlari rasmiy materiallari

6. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Kiberjinoyatchilik holati bo‘yicha statistik tahliliy hisobot (2021–2025 yillar). – Toshkent: IIV Axborot-tahlil markazi, 2025.

7. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Raqamli iqtisodiyot va kiberxavfsizlikni rivojlantirish bo‘yicha yillik hisobot. – Toshkent, 2024.

8. O‘zbekiston Respublikasi Kiberxavfsizlik markazi (CERT.uz). Kiber tahdidlar bo‘yicha axborot byulletenlari (2023–2025). – Toshkent, 2025.

3. Sud va huquqni qo‘llash amaliyoti materiallari

9. O‘zbekiston Respublikasi Oliy sudi. Axborot texnologiyalari bilan bog‘liq jinoyatlar bo‘yicha sud amaliyoti sharhi. – Toshkent, 2023.

10. O‘zbekiston Respublikasi Bosh prokuraturasi. Raqamli dalillarni yig‘ish, saqlash va baholash bo‘yicha uslubiy qo‘llanma. – Toshkent, 2022.

4. Uslubiy va tahliliy manbalar

11. O‘zbekiston Respublikasi Adliya vazirligi. Elektron dalillar bilan ishlash bo‘yicha metodik tavsiyalar. – Toshkent, 2023.

12. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. Raqamli transformatsiya sharoitida axborot xavfsizligi bo‘yicha tahliliy materiallar. – Toshkent, 2024.

5. Xorijiy adabiyotlar

13. Casey E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. – 3rd ed. – London: Academic Press,

14. Carrier B. *File System Forensic Analysis*. – Boston: Addison-Wesley, 2005.

15. Clarke R. A., Knake R. K. *Cyber War: The Next Threat to National Security and What to Do About It*. – New York: Ecco, 2010.

16. Holt T. J. *Cybercrime Through an Interdisciplinary Lens*. – New York: Routledge, 2016.

17. Wall D. S. *Cybercrime: The Transformation of Crime in the Information Age*. – Cambridge: Polity Press, 2007.

18. Yar M. *Cybercrime and Society*. – London: SAGE Publications, 2013.

19. Brenner S. W. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. – Boston: Northeastern University Press, 2012.
20. UNODC. *Comprehensive Study on Cybercrime*. – Vienna: United Nations Office on Drugs and Crime, 2013.
21. INTERPOL. *Global Cybercrime Report*. – Lyon: INTERPOL, 2023.
22. OECD. *Enhancing the Digital Security of Citizens*. – Paris: OECD Publishing, 2021.
23. Choo K. K. R. *Cybercrime: Risks and Responses*. – Melbourne: University of Melbourne Press, 2011.
24. Smith R. G. *Cybercrime: The Basics*. – New York: Routledge, 2017.

ISSN 2181-0958

Doi Journal 10.26739/2181-0958

YURISPRUDENSIYA

7 ЖИЛД, 1 СОН

ЮРИСПРУДЕНЦИЯ

ТОМ 7, НОМЕР 1

JURISPRUDENCE

VOLUME 7, ISSUE 1

Editorial staff of the journals of www.tadqiqot.uz
Tadqiqot LLC The city of Tashkent,
Amir Temur Street pr.1, House 2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Phone: (+998-94) 404-0000

Контакт редакций журналов. www.tadqiqot.uz
ООО Tadqiqot город Ташкент,
улица Амира Темура пр.1, дом-2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Тел: (+998-94) 404-0000