KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI DALILLARNI ANIQLASHNING ZAMONAVIY USULLARI

Nematilloyev Baxrom Vaxobovich
O‘zbekiston Respublikasi IIV Akademiyasi mustaqil izlanuvchisi (PhD)
researchs2002@gmail.com
https://orcid.org/0009-0003-6392-0816

ANNOTATSIYA. Mazkur tezisda kiberjinoyatlarni tergov qilishda raqamli dalillarni aniqlashning zamonaviy usullari ilmiy-nazariy va amaliy jihatdan tahlil qilinadi. Raqamli texnologiyalar rivoji natijasida kompyuter, mobil qurilma, internet, ijtimoiy tarmoq va boshqa manbalardagi elektron izlarni o‘z vaqtida aniqlash muhim ahamiyat kasb etmoqda. Tadqiqotda elektron ma’lumot va raqamli dalil tushunchalari, shuningdek OSINT ochiq manbalar razvedkasi (keyingi o‘rinlarda OSINT) hamda sun’iy intellektdan foydalanish imkoniyatlari yoritiladi. Shuningdek, raqamli dalillarning haqiqiyligi, yaxlitligi va ishonchliligini ta’minlash, ularni aniqlashning bosqichma-bosqich algoritmi hamda O‘zbekiston Respublikasi jinoyat-protsessual qonunchiligidagi huquqiy asoslari ko‘rib chiqiladi.

Kalit so‘zlar: kiberjinoyat, raqamli dalil, elektron ma’lumot, raqamli iz, OSINT, sun’iy intellekt, mobil qurilma, internet, metadata, IP-manzil, elektron pochta, messenjer, raqamli kriminalistika.

ANNOTATION. This thesis provides a scientific and theoretical-applied analysis of modern methods for identifying digital evidence in the investigation of cybercrimes. As digital technologies continue to develop, the timely identification of electronic traces found on computers, mobile devices, the Internet, social networks, and other sources is becoming increasingly important. The study examines the concepts of electronic information and digital evidence, as well as the possibilities of

using OSINT and artificial intelligence. It also addresses ensuring the authenticity, integrity, and reliability of digital evidence, a step-by-step identification algorithm, and the legal framework for identifying digital evidence under the criminal procedural legislation of the Republic of Uzbekistan.

Keywords: cybercrime, digital evidence, electronic information, digital trace, OSINT, artificial intelligence, mobile device, Internet, metadata, IP address, electronic mail, messenger, digital forensics.

Аннотация. В настоящих тезисах на научно-теоретическом и прикладном уровне анализируются современные методы выявления цифровых доказательств при расследовании киберпреступлений. В условиях развития цифровых технологий особое значение приобретает своевременное выявление электронных следов, содержащихся в компьютерах, мобильных устройствах, сети Интернет, социальных сетях и других источниках. В исследовании рассматриваются понятия электронной информации и цифровых доказательств, а также возможности использования OSINT и искусственного интеллекта. Кроме того, рассматриваются вопросы обеспечения подлинности, целостности и достоверности цифровых доказательств, поэтапный алгоритм их выявления, а также правовые основы данной деятельности в уголовно-процессуальном законодательстве Республики Узбекистан.

Ключевые слова: киберпреступность, цифровые доказательства, электронная информация, цифровой след, OSINT, искусственный интеллект, мобильное устройство, Интернет, метаданные, IP-адрес, электронная почта, мессенджер, цифровая криминалистика.

KIRISH. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi kompyuter, smartfon, internet, ijtimoiy tarmoqlar va messenjerlardan jinoyat sodir etishda foydalanish holatlarining ko‘payishiga olib kelmoqda, natijada ishning

mohiyatini ochuvchi muhim ma’lumotlar endilikda moddiy predmetlarda emas, balki elektron muhitda saqlanadigan bo‘lib qolmoqda. Elektron xabarlar, internet sahifalari, server jurnallari va mobil qurilmalardagi ma’lumotlar tez o‘zgarishi yoki o‘chirilishi mumkinligi sababli, ularning kelib chiqishini, mazmunini, vaqt belgisini va jinoyat bilan aloqadorligini o‘z vaqtida belgilash zamonaviy tergov faoliyatining ustuvor vazifalaridan biriga aylanmoqda [1]. O‘zbekiston Respublikasida 2024-yil 21-noyabrdagi O‘RQ-1003-son Qonun bilan raqamli dalillar bilan bog‘liq huquqiy normalarning takomillashtirilishi ushbu yo‘nalishni ilmiy va amaliy jihatdan tadqiq etish dolzarbligini yanada oshirdi [2].

O‘zbekiston Respublikasi Jinoyat-protsessual kodeksining 204^1 va 204^2-moddalariga ko‘ra, elektron ma’lumotlar — elektron qurilmalar va axborot tizimlarida yaratiladigan, saqlanadigan yoki qayta ishlanadigan ma’lumotlarni, raqamli dalillar esa ish uchun ahamiyatli holatlar to‘g‘risidagi elektron ma’lumotlarni anglatadi [1; 2]. Ushbu ikki tushunchani farqlash muhim ahamiyatga ega: har qanday elektron ma’lumot avtomatik ravishda raqamli dalil hisoblanmaydi, chunki uning ishga aloqadorligi, haqiqiyligi, kelib chiqishi va ishonchliligi alohida tekshirilishi zarur. Raqamli dalillarni aniqlash va ularga dastlabki ishlov berish jarayonida ISO/IEC 27037 standarti identifikatsiya, yig‘ish va saqlash bosqichlariga [10], ISO/IEC 27041 qo‘llanilgan uslub va vositalarning yaroqliligini asoslashga [11], ISO/IEC 27042 esa tahlil natijalarini talqin qilish tartibiga [12] metodik asos bo‘lib xizmat qiladi; bu yondashuvlar kriminalistik jarayonni yig‘ish, tekshirish, tahlil va hisobot bosqichlariga ajratuvchi NIST qo‘llanmasi bilan ham uyg‘unlashadi [13].

Raqamli dalillar kompyuter, mobil qurilma, elektron pochta, messenjer, ijtimoiy tarmoq, internet-sayt, server, bulutli xizmat, log fayllar, IP-manzil, GPS ma’lumotlari, fayllar, audio-video yozuvlar va metadata kabi turli manbalarda mavjud bo‘lishi mumkin. UNODC tomonidan o‘tkazilgan keng qamrovli tadqiqotda ta’kidlanganidek,

bunday manbalarning aksariyati bir nechta yurisdiksiyada va xususiy xizmat ko‘rsatuvchilar infratuzilmasida joylashgani ularni o‘z vaqtida aniqlash va olishni murakkablashtiradi [16]. Shu sababli aniqlash jarayonida ma’lumotning haqiqiyligi, yaxlitligi, ishonchliligi va kelib chiqish zanjirini izchil ta’minlash zarur. Raqamli ma’lumotlarni aniqlashning zamonaviy usullaridan biri — OSINT (Open Source Intelligence) bo‘lib, u ochiq internet-saytlari, ijtimoiy tarmoqlar, forumlar, ma’lumotlar bazalari va internet-arxivlardan axborot izlash hamda ular o‘rtasidagi bog‘liqliklarni aniqlash imkonini beradi [22]. Biroq OSINT orqali topilgan ma’lumotni avtomatik ravishda raqamli dalil deb baholab bo‘lmaydi, chunki uning soxtalashtirilgan, eskirgan yoki manipulyatsiya qilingan bo‘lishi ehtimoli mavjud, shu bois manbasi, texnik belgilari va mazmuni qo‘shimcha tekshirilishi shart. Berkeley Protocol ochiq manbalardan olingan ma’lumotlarni to‘plash, tekshirish va hujjatlashtirish jarayonlariga alohida talablar qo‘yadi [14], bu esa yig‘ilgan ma’lumotning shaxsga doir ma’lumotlarni himoya qilish talablariga muvofiqligini ham nazorat qilishni taqozo etadi [5].

Raqamli ma’lumotlarning hajmi kattaligi sababli ularni qo‘lda to‘liq tahlil qilish qiyin bo‘lib, sun’iy intellekt (AI) ushbu ma’lumotlarni dastlabki saralash va tahlil qilishda samarali analitik vosita bo‘lishi mumkin [19; 21]. AI yordamida katta hajmdagi fayllarni saralash, matn va audio yozuvlarni tahlil qilish, tasvir va videolardan muhim ma’lumotlarni ajratish, metadata hamda yozishmalardagi zarur axborotni aniqlash mumkin; so‘nggi yillarda esa vazifani bosqichlarga mustaqil ajratib, ko‘p bosqichli qidiruv va tahlilni avtonom bajaradigan AI-agentlar ham istiqbolli yo‘nalish sifatida shakllanmoqda [23]. Shu bilan birga, sun’iy intellekt tomonidan yaratilgan natija raqamli dalilning o‘zi emas, balki asl manbaning algoritmik talqini hisoblanadi, shu sababli uning natijalari asl ma’lumot bilan albatta solishtirilishi lozim [17]. ChatGPT kabi generativ modellarning raqamli kriminalistikadagi imkoniyatlarini o‘rgangan eksperimental tadqiqot ham ularning artefaktlarni tushuntirishda foydali

bo‘lishi bilan birga, noto‘g‘ri taxmin va xatolarga yo‘l qo‘yishi mumkinligini ko‘rsatdi [18]. Shu sababli AI natijalarining tushuntirilishi (explainability) talabiga alohida e’tibor qaratiladi: qarorning qanday asosda qabul qilinganini izohlab bera olmaydigan tizim natijasi sud tekshiruvidan o‘ta olmaydi [20; 24]. Demak, sun’iy intellekt raqamli dalillarni tez va samarali aniqlashga yordam beruvchi analitik vosita sifatida qo‘llanilishi, yakuniy baholash esa asl manba va boshqa ishonchli ma’lumotlar asosida amalga oshirilishi kerak.

Kiberjinoyatlarni tergov qilishda raqamli dalillarni aniqlash jarayoni quyidagi bosqichlardan iborat bo‘lishi mumkin: tergov vazifasini belgilash, potensial raqamli manbalarni aniqlash, ma’lumotlarning o‘zgaruvchanlik darajasini baholash, OSINT va sun’iy intellekt yordamida izlash hamda saralash, aniqlangan ma’lumotlarni qayd etish va ularning o‘zaro bog‘liqligini tekshirish. Keyingi bosqichda ma’lumotning manbasi va haqiqiyligi verifikatsiya qilinib, OSINT yoki AI orqali olingan natijaning asl raqamli manbasi aniqlanadi hamda tegishli protsessual tartibda mustahkamlanadi [2]. O‘RQ-1003-son Qonun bilan raqamli dalillarga oid normalarning Jinoyat-protsessual kodeksida takomillashtirilishi ularni aniqlash, olish, saqlash va ishga qo‘shish uchun muhim huquqiy asos yaratdi [1; 2], sud ekspertizasi sohasida esa tekshirish obyektlari qatoriga raqamli dalillar va elektron ma’lumotlar mavjud bo‘lgan elektron jismlar kiritildi [3]. Dalillarning maqbulligi masalasida Oliy sud Plenumining 2018-yildagi tushuntirishlari [6] O‘RQ-1003-son Qonun qabul qilinishi munosabati bilan 2025-yil 23-iyundagi qarori bilan yangilandi [7]. Kiberxavfsizlikni ta’minlash [4] va shaxsga doir ma’lumotlarni himoya qilish [5] talablariga rioya etish, shuningdek sun’iy intellekt sohasidagi milliy strategiyada belgilangan yo‘nalishlar [8] ham raqamli dalillar bilan ishlash tizimining ajralmas qismi hisoblanadi.

Xalqaro tajribada Yevropa Kengashining Kiberjinoyatchilik to‘g‘risidagi konvensiyasi transchegaraviy elektron dalillar bilan ishlash mexanizmlarini belgilaydi

[9], INTERPOLning raqamli kriminalistika laboratoriyalari uchun global qo‘llanmasi esa laboratoriya jarayonlarini standartlashtirish talablarini o‘rnatadi [15]. Ushbu xalqaro-huquqiy va uslubiy manbalar milliy qonunchilikni takomillashtirishda qiyosiy-huquqiy asos sifatida xizmat qilishi mumkin.

Raqamli dalillarni aniqlash amaliyotida ma’lumotlarning tez o‘zgarishi yoki yo‘qolishi, ularning haqiqiyligi va birlamchi manbasini aniqlashdagi murakkablik, ma’lumotlar hajmining kattaligi, sun’iy intellekt natijalarining xatolik ehtimoli hamda shaxsga doir ma’lumotlarni himoya qilish bilan bog‘liq muammolar mavjud. Mazkur muammolarni bartaraf etish uchun kiberjinoyatlarni tergov qilishda raqamli dalillarni aniqlashning yagona uslubiy algoritmini ishlab chiqish va amaliyotga joriy etish, OSINT orqali olingan ma’lumotlarni texnik, manbaviy va mazmuniy jihatdan kompleks verifikatsiya qilish maqsadga muvofiq. Sun’iy intellektdan foydalanishda uning natijalarini asl raqamli manba bilan majburiy taqqoslash, aniqlangan ma’lumotlarning kelib chiqishi va ishonchliligini tekshirish, shuningdek tergovchi va mutaxassislarning raqamli kriminalistika bo‘yicha amaliy kompetensiyalarini muntazam oshirish zarur.

XULOSA. Kiberjinoyatlarni tergov qilishda raqamli dalillarni o‘z vaqtida va to‘g‘ri aniqlash zamonaviy tergov faoliyatining muhim yo‘nalishi bo‘lib, buning uchun tergovchidan raqamli texnologiyalar bilan ishlash bo‘yicha zarur bilim va ko‘nikmalar talab etiladi. Raqamli dalillar kompyuter, mobil qurilma, internet, ijtimoiy tarmoqlar, messenjerlar, elektron pochta, serverlar, log fayllar va boshqa raqamli manbalarda mavjud bo‘lishi mumkin. OSINT ochiq manbalardan dastlabki ma’lumotlarni aniqlash, sun’iy intellekt esa katta hajmdagi ma’lumotlarni saralash va tahlil qilish imkonini beradi, biroq ularning natijalari albatta verifikatsiya qilinishi lozim. Shu bois raqamli dalillarni aniqlashda «manbani aniqlash — OSINT orqali izlash — AI yordamida saralash — verifikatsiya — asl manbani aniqlash — protsessual mustahkamlash» ketma-ketligidan foydalanish maqsadga muvofiqdir.

Mazkur yondashuv zamonaviy texnologiyalardan samarali foydalanish bilan birga, raqamli dalillarning ishonchliligi va protsessual qonuniyligini ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. 1994-yil 22-sentabr. URL: https://lex.uz/docs/-111460

2. O‘zbekiston Respublikasining 2024-yil 21-noyabrdagi O‘RQ-1003-son «O‘zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida»gi Qonuni. URL: https://lex.uz/docs/-7228758

3. O‘zbekiston Respublikasining 2010-yil 1-iyundagi O‘RQ-249-son «Sud ekspertizasi to‘g‘risida»gi Qonuni. URL: https://lex.uz/docs/-1633102

4. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son «Kiberxavfsizlik to‘g‘risida»gi Qonuni. URL: https://lex.uz/docs/-5960604

5. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. URL: https://lex.uz/docs/-4396419

6. O‘zbekiston Respublikasi Oliy sudi Plenumining 2018-yil 24-avgustdagi 24-son «Dalillar maqbulligiga oid jinoyat-protsessual qonuni normalarini qo‘llashning ayrim masalalari to‘g‘risida»gi qarori. URL: https://lex.uz/docs/-3895986

7. O‘zbekiston Respublikasi Oliy sudi Plenumining 2025-yil 23-iyundagi 14-son qarori (2018-yil 24-avgustdagi 24-son qarorga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida).
URL: https://lex.uz/docs/-7613615

8. O‘zbekiston Respublikasi Prezidentining 2024-yil 14-oktabrdagi PQ-358-son «Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida»gi qarori. URL: https://lex.uz/docs/-7158604

9. Council of Europe. Convention on Cybercrime (ETS No. 185). Budapest, 23.XI.2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

10. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

11. ISO/IEC 27041:2015. Guidance on assuring suitability and adequacy of incident investigative method. Geneva: ISO, 2015.

12. ISO/IEC 27042:2015. Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO, 2015.

13. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86. Gaithersburg: NIST, 2006. DOI: 10.6028/NIST.SP.800-86.

14. Berkeley Protocol on Digital Open Source Investigations. New York; Geneva: United Nations (OHCHR) and Human Rights Center, UC Berkeley School of Law, 2022.

15. INTERPOL. Global Guidelines for Digital Forensics Laboratories. Lyon: INTERPOL Global Complex for Innovation, 2019.

16. UNODC. Comprehensive Study on Cybercrime. Vienna: United Nations Office on Drugs and Crime, 2013.

17. Stoykova R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence // Computer Law & Security Review. 2021. Vol. 42. Art. 105575. DOI: 10.1016/j.clsr.2021.105575.

18. Scanlon M., Breitinger F., Hargreaves C., Hilgert J.-N., Sheppard J. ChatGPT for digital forensic investigation: The good, the bad, and the unknown // Forensic Science International: Digital Investigation. 2023. Vol. 46. Art. 301609. DOI: 10.1016/j.fsidi.2023.301609.

19. Jarrett A., Choo K.-K. R. The impact of automation and artificial intelligence on digital forensics // WIREs Forensic Science. 2021. Vol. 3, No. 6. Art. e1418. DOI: 10.1002/wfs2.1418.

20. Hall S. W., Sakzad A., Choo K.-K. R. Explainable artificial intelligence for digital forensics // WIREs Forensic Science. 2022. Vol. 4, No. 2. Art. e1434. DOI: 10.1002/wfs2.1434.

21. Sikos L. F. AI in digital forensics: Ontology engineering for cybercrime investigations // WIREs Forensic Science. 2021. Vol. 3, No. 3. Art. e1394. DOI: 10.1002/wfs2.1394.

22. Pastor-Galindo J., Nespoli P., Gómez Mármol F., Martínez Pérez G. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends // IEEE Access. 2020. Vol. 8. P. 10282–10304. DOI: 10.1109/ACCESS.2020.2965257.

23. Wang L., Ma C., Feng X. et al. A Survey on Large Language Model Based Autonomous Agents // Frontiers of Computer Science. 2024. Vol. 18, No. 6. Art. 186345. DOI: 10.1007/s11704-024-40231-1.

24. Khalid Z., Iqbal F., Fung B. C. M. Towards a unified XAI-based framework for digital forensic investigations // Forensic Science International: Digital Investigation. 2024. Vol. 50. Art. 301806.