ISSN:3030-332X
Impact factor: 9,493
International journal of scientific researchers

ОЧИҚ МАНБАЛАРДАН ОЛИНГАН РАҚАМЛИ МАЪЛУМОТЛАРНИ ДАЛИЛ СИФАТИДА МУСТАҲКАМЛАШ, ВЕРИФИКАЦИЯ ҚИЛИШ ВА ЖИНОЯТ-ПРОЦЕССУАЛ ЖИҲАТДАН МАҚБУЛЛИГИНИ ТАЪМИНЛАШ МУАММОЛАРИ

Жалолов Миркодир Мирхожиевич
Ҳуқуқни муҳофаза қилиш академияси
магистратура тингловсиси
https://doi.org/10.5281/zenodo.23080633

Аннотация. Мазкур мақолада трансчегаравий уюшган жиноятчилик ва кибержиноятларни тергов қилишда очиқ манбалардан маълумот тўплаш (OSINT) воситасида қўлга киритилган рақамли ахборотларни процессуал жиҳатдан мустаҳкамлаш, криминалистик верификация қилиш ҳамда уларнинг мақбуллигини (admissibility) таъминлаш муаммолари комплекс тадқиқ этилган.

Тадқиқотда рақамли маълумотларнинг ўта ўзгарувчанлиги (volatility), сунъий интеллект маҳсули бўлган дипфейк ва манипуляция қилинган контентлар хавфи шароитида EXIF метамаълумотлари таҳлили, хатоликлар даражаси, реверс-қидирув ва манба ишончлилигини баҳолаш механизмлари ёритиб берилган.

Калит сўзлар: рақамли далиллар, OSINT, далиллар мақбуллиги, Chain of Custody, SHA-256 хэш-қиймати, дипфейк, веб-архивлаш, Беркли протоколи, кўздан кечириш, ЖПК, ISO/IEC 27037.

Abstract (English version)

This article provides a comprehensive legal and forensic analysis of the challenges surrounding the procedural fixation, verification, and admissibility of digital data obtained from open sources (OSINT) within criminal proceedings, particularly in countering cross-border organized crime and cyber offenses.

The study examines the inherent volatility and vulnerability of open-source data, outlining methodologies for detecting deepfakes and digital manipulations via EXIF metadata analysis, Error Level Analysis (ELA), and reverse searches. It demonstrates the evidentiary inadequacy of basic screenshots and emphasizes the legal necessity of web archiving (e.g., Perma.cc), cryptographic hashing (SHA-256), strict Chain of Custody compliance, and blockchain timestamping.

Keywords: digital evidence, OSINT, admissibility of evidence, Chain of Custody, SHA-256 hash value, deepfake verification, web archiving, Berkeley Protocol, criminal procedure, ISO/IEC 27037.

КИРИШ

Трансчегаравий уюшган жиноятчилик ва кибержиноятларнинг жадал трансформацияси шароитида очиқ манбалардан маълумот тўплаш (OSINT) тергов ва суриштирув органлари учун муҳим оператив ва аналитик ресурсга айланди[1].

Очиқ интернет муҳитидан олинган рақамли маълумотларни оддий тезкор-қидирув материалидан жиноят-процессуал далил мақомига ўтказиш механизми ҳуқуқни муҳофаза қилиш амалиётининг фундаментал масалаларидан биридир[2].

Жиноят-процессуал кодекси (ЖПК) нормалари бўйича далилларнинг мақбуллиги (admissibility) мезонлари рақамли ахборотнинг манбаси ва олиниш тартиби қонунийлигини назарда тутади[3].

Ўзбекистон Республикаси Олий суди Пленумининг "Далиллар мақбуллигига оид жиноят-процессуал қонуни нормаларини қўллашнинг айрим масалалари тўғрисида"ги қарорига мувофиқ,

номаълум ёки процессуал текшириб бўлмайдиган манбадан олинган ахборот мақбул эмас деб топилади[4].

Дахлдорлик (relevance) мезони нуқтаи назаридан OSINT материаллари инобатга олинаётган жиноят иши бўйича исботланиши лозим бўлган ҳолатлар (ЖПК 82, 83-моддалари) билан тўғридан-тўғри ёки эришиладиган мантиқий алоқадорликка эга бўлиши зарур[5].

Очиқ манбалардан маълумот тўплашда инсон ҳуқуқлари, хусусан, шахсий ҳаёт дахлсизлиги ва шахсга доир маълумотларни ҳимоя қилиш тўғрисидаги қонунчилик талабларига риоя этилиши процессуал мақбулликнинг муҳим шарти ҳисобланади[6].

АСОСИЙ ҚИСМ

OSINT материалларини процессуал тан олишда уларни ЖПКнинг 204-моддасига кўра "ҳужжатлар" ёки 204-2-моддаси тартибида "рақамли далиллар" сифатида мақомини аниқ белгилаш ва ишга қўшиб қўйиш талаб этилади[7].

Очиқ интернет муҳитида рақамли маълумотларнинг ўта ўзгарувчанлиги (volatility) ва сохталаштиришга мойиллиги сабабли уларни верификация қилиш ва ҳақиқийлигини текшириш биринчи даражали криминалистик вазифа ҳисобланади[8].

Замонавий кибертаҳдидлар ва сунъий интеллект технологияларининг ривожланиши дипфейк (deepfake) аудио ва видеоматериаллар ҳамда манипуляция қилинган рақамли тасвирларнинг кенг тарқалишига олиб келди[9].

Рақамли сохталикларни аниқлашда метамаълумотларни (EXIF) криминалистик таҳлил қилиш, пикселлар тузилишидаги хатоликлар даражасини (ELA) ва спектрал шовқинларни экспертизадан ўтказиш усуллари қўлланилади[10].

Ижтимоий тармоқлар ва мессенжерлар (Telegram, Facebook, Instagram ва б.) томонидан юкланган файлларнинг EXIF метамаълумотлари автоматик ўчириб ташланиши сабабли мета-таҳлил имкониятлари чекланади[11].

Реверс-қидирув (reverse image/video search) усуллари тасвирларнинг интернетдаги илк пайдо бўлиш манбасини аниқлашга хизмат қилади, бироқ Deep Web ва Dark Web сегментларида уларнинг алгоритмик камчиликлари намоён бўлади[12].

Очиқ ахборот манбасининг ишончлилигини баҳолаш (source evaluation) учта фундаментал мезонга суянади: ishonchlilik (credibility), barqarorlik (reliability) ва aniqlik (accuracy)[13].

Рақамли изларнинг бутлигини (integrity) таъминлаш ва уларни криминалистик тадқиқ этиш жараёнида аслият нусхаларидан (bit-stream image) ва write-blocking ҳимоя воситаларидан фойдаланиш шарт ҳисобланади[14].

Онлайн муҳитдаги рақамли изларни процессуал мустаҳкамлаш (procedural fixation) терговчи томонидан ЖПК 135–140-моддалари бўйича интернет-ресурсни кўздан кечириш тергов ҳаракати орқали амалга оширилади[15].

Рақамли далиллар аслийлигини техник кафолатлашнинг марказий усули бу – криптографик хэш-қийматларни (SHA-256, MD5) олиш ва қайд этишдир[16].

O‘z DSt ISO/IEC 27037:2017 стандартига мувофиқ, интернетдан юклаб олинган ёки қайд этилган ҳар бир рақамли объектнинг хэш-қиймати шакллантирилган лаҳзадаёқ ҳисобланиши ва баённомада кўрсатилиши шарт[17].

Оддий онлайн-скриншотлар (screenshot) фақат визуал графикани акс эттиргани ва осон сохталаштирилиши мумкинлиги сабабли судда паст далилий кучга эга бўлади[18].

Веб-архивлаш хизматлари (Wayback Machine, Archive.today, Perma.cc) саҳифанинг пўлат кодини, HTML-структурасини, сервер сарлавҳаларини ва вақт тамғасини (timestamp) мустаҳкамлаб, юқори процессуал қиммат беради[19].

Веб-саҳифа ва ижтимоий тармоқ ахборотларини кўздан кечириш тергов ҳаракати URL ва IP-манзилни аниқлаш, архивлаш, хэш-пайдо қилиш ва мутахассис иштирокида баённома тузиш алгоритми асосида олиб борилади[20].

Далилларни сақлаш ва ҳаракатланиш занжири – Chain of Custody талаблари рақамли ахборотнинг тўпланганидан судда кўриб чиқилгунга қадар аслий ва ўзгармас сақланганини ҳужжатлаштиришни тақозо этади[21].

Агар рақамли далилни сақлаш занжирида узилиш бўлса ёки хэш-қийматлар мос келмаса, ЖПКнинг 95-1-моддасига асосан далил мақбул эмас деб топилади[22].

Блокчейн (Blockchain) ва децентраллашган реестрлар технологиясини қўллаш рақамли далилларнинг хэш-қийматлари ва вақт тамғаларини орқага қараб ўзгартириб бўлмайдиган тарзда мустаҳкамлаш имконини беради[23].

Халқаро жиноий суд (ICC) амалиётида Prosecutor v. Al-Werfalli ва Prosecutor v. Katanga ишлари бўйича OSINT ва ижтимоий тармоқ рақамли далилларини тан олиш тажрибаси шаклланган[24].

ICC томонидан видео ва фотоматериалларни мақбул далил сифатида қабул қилишда манбанинг келиб чиқиши, метамаълумотлар ва геолокация/хронолокация экспертизалари асосий мезон деб топилган[25].

БМТ Инсон ҳуқуқлари бўйича Олий комиссари бошқармаси томонидан ишлаб чиқилган "Беркли протоколи" (The Berkeley Protocol) рақамли очиқ манбаларни суриштирув қилиш ва далиллаштиришнинг глобал стандартидир[26].

Беркли протоколи верификациянинг уч босқичли моделини белгилайди: манба таҳлили (source analysis), техник таҳлил (technical analysis) ва мазмуний таҳлил (content analysis)[27].

АҚШ судотлиги тажрибасида Федерал далиллар қоидаларининг (FRE 902(13)/(14)) 902-моддаси электрон ёзувлар ва рақамли маълумотларни хэш-кодлар орқали ўз-ўзини аутентификация қилиш механизмини назарда тутади[28].

Европа Иттифоқида E-Evidence пакети (Regulation (EU) 2023/1543) ва Кибержиноятчилик тўғрисидаги конвенциянинг Иккинчи қўшимча протоколи трансчегаравий электрон далилларни тезкор олиш режимини жорий этди[29].

Халқаро ва қиёсий тажрибани умумлаштириш миллий жиноят-процессуал қонунчилигида рақамли далилларни мустаҳкамлаш ва верификация қилиш нормаларини унификация қилиш зарурлигини кўрсатади[30].

ХУЛОСА

Ўзбекистон Республикаси амалдаги ЖПКда очиқ манбалардан олинган рақамли маълумотларни мустаҳкамлаш, хэш-фиксация ва веб-архивлашнинг махсус процессуал нормалари мавжуд эмаслиги бўшлиқ яратмоқда[31].

Қонунчиликни такомиллаштириш бўйича биринчи таклиф – ЖПК 87-моддасига "Рақамли далиллар" тушунчасини ва OSINT материалларининг процессуал мақомини аниқ киритишдан иборат[32].

Иккинчи таклиф – ЖПКни **"Рақамли далиллар ва очиқ интернет манбаларини кўздан кечириш хусусиятлари"** номли 140-1-модда билан тўлдириб, унда SHA-256 хэш-қийматини қайд этиш ва веб-архивлаш тартибини мустаҳкамлаш[33].

Учинчи таклиф – ЖПК 95-1-моддасига хэш-қиймати қайд этилмаган ёки Chain of Custody (далилларни сақлаш занжири) бузилган рақамли маълумотларни номақбул далил деб топиш нормасини киритиш[34].

Тўртинчи таклиф – Беркли протоколи ва ISO/IEC 27037:2017 стандартлари асосида ҳуқуқни муҳофаза қилувчи органлар учун "Очиқ манбалардан олинган рақамли далилларни верификация қилиш ва процессуал расмийлаштириш бўйича ягона миллий методик йўриқнома" тасдиқлаш[35].

ФОЙДАЛАНИЛГАН МАНБАЛАР РЎЙХАТИ

1. Böhm R., Lolagar S. Defining OSINT in the Criminal Investigation Context // Balkan Journal of Interdisciplinary Research. – 2026. – Vol. 12, No. 1. – P. 15–28.
2. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь (амалдаги таҳрири) // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.
3. Ibid.
4. Ўзбекистон Республикаси Олий суди Пленумининг "Далиллар мақбуллигига оид жиноят-процессуал қонуни нормаларини қўллашнинг айрим масалалари тўғрисида"ги Қарори, 2018 йил 24 август, 24-сон // lex.uz.
5. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь // lex.uz.
6. Ўзбекистон Республикасининг "Шахсга доир маълумотлар тўғрисида"ги Қонуни, 2019 йил 2 июль, ЎРҚ-547-сон // lex.uz.
7. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь // lex.uz.
8. Stoykova R. A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings // Computer Law & Security Review. – 2024. – Vol. 55. – Art. 106040.
9. Groh M., Epstein Z., Firestone C., Picard R. Deepfake detection by human crowds, machines, and machine-informed crowds // Proceedings of the National Academy of Sciences. – 2022. – Vol. 119, No. 1. – P. e2110013119.
10. Farid H. Digital forensics // Annual Review of Statistics and Its Application. – 2018. – Vol. 5. – P. 79–97.
11. Bazzell M. Open Source Intelligence Techniques: A Practical Guide to Online Intelligence. – 9th ed. – AuthorHouse, 2023. – 670 p.
12. Mirsky Y., Lee W. The creation and detection of deepfakes: A survey // ACM Computing Surveys. – 2021. – Vol. 54, No. 1. – P. 1–41.
13. Wardle C., Derakhshan H. Information disorder: Toward an interdisciplinary framework for research and policy making // Council of Europe Report. – Strasbourg: Council of Europe, 2017. – 108 p.
14. Stoykova R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence // Computer Law & Security Review. – 2021. – Vol. 42. – Art. 105575.
15. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь // lex.uz.
16. O‘z DSt ISO/IEC 27037:2017. Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Рақамли исботларни идентификация қилиш, йиғиш, олиш ва сақлаш. – Тошкент: Ўзстандарт агентлиги, 2017. – 65 б.
17. Ibid.
18. Godbole S. Chronolocation: Applying temporal analysis to open source investigations // International Journal of Digital Evidence. – 2019. – Vol. 18, No. 2. – P. 44–59.
19. Ismail I., Akram Zainol Ariffin K. The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance // PLoS ONE. – 2025. – Vol. 20, No. 9. – Art. e0331683.
20. Mason S., Seng D. Electronic Evidence and Electronic Signatures. – 5th ed. – London: Institute of Advanced Legal Studies, 2021. – 540 p.
21. Ibid.

22. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь // lex.uz.
23. Patil A., Malik S., Sharma R. Blockchain for Digital Evidence Preservation and Chain of Custody // Journal of Asia Entrepreneurship and Sustainability. – 2024. – Vol. 22, No. 5s. – P. 112–128.
24. International Criminal Court. Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli (Warrant of Arrest). Case No. ICC-01/11-01/17. 15 August 2017. – The Hague: ICC, 2017. – 15 p.
25. International Criminal Court. Prosecutor v. Germain Katanga. Decision on the Admission of Evidence. Case No. ICC-01/04-01/07. 2015. – The Hague: ICC, 2015. – 32 p.
26. Office of the United Nations High Commissioner for Human Rights (OHCHR) & UC Berkeley Human Rights Center. Berkeley Protocol on Digital Open Source Investigations. – New York and Geneva: United Nations, 2022. – 108 p.
27. Koenig A. Digital Investigations of Systematic and Conflict-Related Sexual Violence // Chicago Journal of International Law. – 2025. – Vol. 26, No. 1. – P. 185–204.
28. Federal Rules of Evidence. Rule 902. Evidence That Is Self-Authenticating // Legal Information Institute, Cornell Law School. – 2023.
29. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 November 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings // Official Journal of the European Union. – 2023. – L 191. – P. 1–38.
30. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). – Strasbourg: Council of Europe, 2022. – 28 p.
31. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь // lex.uz.
32. Gillett M., Fan W. Expert evidence and digital open source information: Bringing online evidence to the courtroom // Journal of International Criminal Justice. – 2023. – Vol. 21, No. 4. – P. 661–693.
33. Ibid.
34. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь // lex.uz.
35. Office of the United Nations High Commissioner for Human Rights (OHCHR) & UC Berkeley Human Rights Center. Berkeley Protocol on Digital Open Source Investigations. – New York and Geneva: United Nations, 2022. – 108 p.