E CONF SERIES

International Conference on Scientific Research in Natural and Social Sciences
Hosted online from New York, USA
Website: econfseries.com 2nd November, 2025

ЦИФРОВАЯ КРИМИНАЛИСТИКА ПРОТИВ КИБЕРБЕЗОПАСНОСТИ: ЗНАЧИМОСТЬ ПРОЦЕССУАЛЬНОГО АСПЕКТА ПРАВОСУДИЯ В ЦИФРОВУЮ ЭПОХУ

Мелсова Камила Бахадыровна
E-mail: tkb3108666@gmail.com
Тел. +998970713666

Аннотация

В условиях современного акцента на превентивность в виде совершенствования кибербезопасности в Республике Узбекистан, представляется необходимым уделить внимание процессуальному аспекту, а именно, развитию цифровой криминалистики для обеспечения верховенства закона. Причина данного утверждения заключается в том, что именно данная отрасль гарантирует законность сбора, целостность хранения и допустимость использования цифровых и электронных доказательств в уголовном процессе, являясь, таким образом, незаменимым инструментом для реагирования на неизбежное совершение преступлений при помощи информационных технологий. Таким образом, в ныне разрабатываемых законодательных актах наблюдается дисбаланс в фокусе: доминирование превентивных мер (кибербезопасности) в государственной политики при недостаточном внимании к формированию надежной процессуальной базы для расследования уже совершенных преступлений с использованием цифровых технологий.

Ключевые слова: цифровая криминалистика, кибербезопасность, превентивность, расследование, уголовный процесс, раскрытие преступлений.

Abstract

In the context of the current focus on prevention in the form of improving cybersecurity in the Republic of Uzbekistan, it seems necessary to pay attention to the procedural aspect, namely, the development of digital forensics to ensure the rule of law. The reason for this statement is that it is this industry that guarantees the legality of the collection, integrity of storage and the permissibility of the use of

digital and electronic evidence in criminal proceedings, thus being an indispensable tool for responding to the inevitable commission of crimes using information technology. Thus, there is an imbalance in focus in the currently being developed legislative acts: the dominance of preventive measures (cybersecurity) in public policy with insufficient attention to the formation of a reliable procedural framework for investigating crimes already committed using digital technologies.

Keywords: digital forensics, cybersecurity, prevention, investigation, criminal process, crime detection.

Annotatsiya

O'zbekiston Respublikasida kiberxavfsizlikni takomillashtirish ko'rinishidagi preventivlikka zamonaviy e'tibor qaratgan holda, qonun ustuvorligini ta'minlash uchun protsessual jihatga, ya'ni raqamli sud ekspertizasini rivojlantirishga e'tibor qaratish lozim. Ushbu bayonotning sababi shundaki, aynan shu soha jinoiy jarayonda raqamli va elektron dalillarni to'plashning qonuniyligini, saqlashning yaxlitligini va ulardan foydalanishga yo'l qo'yilishini kafolatlaydi, shu bilan axborot texnologiyalari yordamida jinoyatlarning muqarrar sodir etilishiga javob berishning ajralmas vositasi hisoblanadi. O'z navbatida, hozirda ishlab chiqilayotgan qonun hujjatlarida diqqat markazida nomutanosiblik mavjud: davlat siyosatida profilaktika choralarining (kiberxavfsizlik) ustunligi, raqamli texnologiyalardan foydalangan holda allaqachon sodir etilgan jinoyatlarni tergov qilish uchun ishonchli protsessual bazani shakllantirishga yetarlicha e'tibor berilmagan.

Kalit so'zlar: raqamli sud ekspertizasi, kiberxavfsizlik, profilaktika, tergov, jinoiy sud jarayoni, jinoyatlarni ochish.

Современное общество переживает эпоху стремительной цифровизации, охватывающей все сферы жизни – от государственного управления и экономики до частных коммуникаций и повседневного быта граждан. Республика Узбекистан, следуя общемировым тенденциям, активно внедряет цифровые технологии, развивает систему электронного правительства,

расширяет доступ к интернет-услугам, стимулируя формирование информационного общества. Однако, процесс цифровизации одновременно порождает новые угрозы и вызовы, среди которых особое место отведено преступлениям с использованием ИКТ. Рост числа и разнообразия таких преступлений обуславливает необходимость совершенствования правовых и процессуальных механизмов их расследования.

Принимаемые государством меры в большинстве своем направлены на укрепление кибербезопасности, нежели на формирование эффективной процессуальной базы для расследования уже совершенных преступлений. В результате правоохранительные органы нередко сталкиваются с трудностями в сборе, фиксации и оценке цифровых доказательств, что снижает результативность уголовного преследования и препятствует достижению целей правосудия.

Цель данного исследования состоит в обосновании необходимости признания важности развития цифровой криминалистики как направления, обеспечивающего верховенство закона и осуществление правосудия.

Цифровая криминалистика (ЦК) или Digital Forensics (DF), иногда называемая также «кибер-криминалистикой», представляет собой процесс выявления, сохранения, сбора и анализа цифровых улик, таких как текстовые сообщения, электронные письма, история посещения различного рода браузеров, записи в социальных сетях и многое другое. Цифровые доказательства также чаще всего ассоциируются с судебными разбирательствами, однако они могут использоваться и в другом контексте, например, в расследовании административных правонарушений. Интерпол[1] и NIST (Национальный институт стандартов и технологий США)[2] подчеркивают, что такие доказательства присутствуют практически во всех видах преступной деятельности, их сбор и анализ имеют исключительное значение для правоохранительных органов.

[1] https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Electronic%20evidence%20can%20be%20collected,systems%2C%20shipborne%20equipment%2C%20and%20more

[2] https://www.nist.gov/itl/ssd/digital-forensics#:~:text=Digital%20evidence%20includes%20data%20on,software%20applications%20that%20is%20an

Кибербезопасность же, в свою очередь, является упреждающим подходом к защите цифровой информации, различных сетей, компьютеров и других видов технологий от кибератак и других угроз их безопасности. Официальная формулировка звучит следующим образом: «кибербезопасность – состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве»[3]. На сегодняшний день она включает в себя защиту всего – от компьютеров и ноутбуков до мобильных телефонов, планшетов, электронной почти, кредитных карт, критически важных объектов инфраструктуры, банковских счетов в Интернете и медицинских карт – всего, что может содержать ценные данные и информацию.

Согласно данным МВД Республики Узбекистан, за последние пять лет количество преступлений в сфере киберпространства возросло в несколько десятков раз и был понесен материальный ущерб практически в 2 млрд сумов[4]. При этом, основные силы правоохранительных органов направлены на предотвращение преступлений, что подчеркивается созданием таких профилактических мер, как «Месяц повышения киберкультуры» или создание «антифрод-системы», указанных в ПП №153 от 30 апреля 2025 года. Возникла необходимость создания отдельной структуры или структурного подразделения, которое должно заниматься как подготовкой специализированных кадров, так и исследовательской работой в области цифровой криминалистики. Такой институт был образован в 2024 году в структуре Правоохранительной академии Республики Узбекистан[5]. Тем не менее, как показывает практика, никакие превентивные меры не смогут полностью предотвратить преступления, поскольку их развитие не способно угнаться за темпами роста новых способов их совершения. Следовательно, при реформировании системы, присутствует необходимость перехода от «если» к «когда»: от попытки предотвращения к способам расследования и обеспечению правосудия.

[3] https://lex.uz/ru/docs/5960609
[4] https://gov.uz/ru/iiv/news/view/57775
[5] https://lex.uz/uz/docs/6977762

Строгие криминалистические процедуры гарантируют, что доказательство будет принято судом, а соблюдение принципов криминалистических тактик обеспечивают неизменность и надежность доказательств, поскольку цифровые доказательства довольно нестабильны: они легко поддаются изменению, уничтожению или фальсификации. Одной из тактик по их сохранению является использование стандартных процедур фиксации hash-сумм для соблюдения условий неприкосновенности оригинала.

Практическая ценность цифровой криминалистики проявляется также в её способности обеспечивать выявление не только непосредственных исполнителей противоправных действий, но и их организаторов и заказчиков. Применение методов ЦК позволяет анализировать пути перемещения похищенной информации, отслеживать финансовые потоки и транзакции, формирующиеся в результате кибермошенничества, а также устанавливать структуру и характер взаимодействия между участниками преступных сетей. Так, например, в делах, связанных с фишингом и несанкционированным доступом к банковским аккаунтам, результаты цифровой экспертизы нередко становятся решающим фактором при выявлении связей между подозреваемыми и транснациональными преступными группировками.

Кроме того, цифровая криминалистика играет ключевую роль в развитии противодействия киберпреступности как в Республике Узбекистан, так и в рамках международного сотрудничества, поскольку формирует правоприменительную практику. В рамках транснациональных расследований, предполагающих получение доступа к цифровым данным, размещенным на серверах за пределами национальной юрисдикции, результаты криминалистического анализа зачастую служат основанием для направления международных запросов и оказания правовой помощи.

В Европейском союзе с 2023 года разработана специальная регламентация цифровых доказательств (e-evidence)[6], которая предусматривает создание:

- единого ордера на предоставление электронной информации (European Production Order) для государств-членов ЕС;

[6] https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en#:~:text=,will%20allow%20a%20judicial%20authority

- децентрализованной ИТ-системы, посредством которой все взаимодействия между органами власти и поставщиками услуг может осуществляться безопасным способом;
- документ, предусматривающий сохранность данных (European Preservation Order), что позволяет государствам-членам направлять запрос на предоставление сохраненных данных, необходимых для расследования.

Разработка данных мер показывает, что европейские государства признают приоритет получения цифровых доказательств для расследования преступлений и, как следствие, приоритет процессуального аспекта. В то же время, принятый в Республике Узбекистан Закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами», не только не упрощает работу с таковыми, но и вносит юридические и процедурные неясности. Так, например, принцип работы с e-evidence описывается таким же образом, как и с традиционными видами, однако первые обладают совершенно иной природой: они нематериальны, требуют специальных технических средств и компетенций для получения и фиксации, их содержимое легко копируется, изменяется, удаляется или фальсифицируется.

Цифровая криминалистика является ключевым элементом современного уголовного судопроизводства, обеспечивающим адаптацию правоприменительной практики к условиям стремительной цифровизации. Ее развитие позволяет эффективно выявлять, фиксировать и анализировать цифровые доказательства, без чего невозможна результативная борьба и предотвращение преступлений, совершаемых с помощью информационных технологий.

Анализ зарубежного опыта показывает, что акцент на процессуальных аспектах обращения с цифровыми доказательствами существенно повышает эффективность расследований и международного сотрудничества. В то же время, национальное законодательство Республики Узбекистан остаётся на этапе становления и пока не учитывает в полной мере специфическую природу цифровых доказательств.

Следовательно, развитие цифровой криминалистики должно рассматриваться как приоритетное направление государственной политики в сфере правосудия и кибербезопасности. Ее институциональное укрепление, нормативное регулирование и кадровое обеспечение станут основой также для формирования эффективной системы противодействия преступности в цифровом пространстве.

Список использованных источников

1. Закон Республики Узбекистан от 15 апреля 2022 года №ЗРУ-764 «О кибербезопасности». https://lex.uz/ru/docs/5960609.
2. Закон Республики Узбекистан от 21 ноября 2024 года №ЗРУ-1003 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами». https://lex.uz/ru/docs/7228823.
3. Постановление Президента Республики Узбекистан от 30 апреля 2025 года №ПП-153 «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий». https://www.lex.uz/uz/docs/7511168.
4. Постановление Президента Республики Узбекистан от 21 июня 2024 года №ПП-229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики». https://lex.uz/uz/docs/6977762.
5. Gourav Kumar Sharma, Importance and Advantages of Digital Forensics for Law Enforcement and Corporations // International Journal of Advanced Research and Multidisciplinary Trends (IJARMT). — Volume 1 Issue 1 July. — September 2024. — P. 1–6.
6. Б.У.Умаров. Procedural aspects of ensuring the preservation of electronic evidence in criminal proceedings // European Journal of Economics, Finance and Business Development. — Volume 2, Issue 10. — October 2024. — P. 26–40.
7. Русанова Д.Ю. Цифровая криминалистика: возможности и перспективы развития // Международный журнал гуманитарных и естественных наук. — 2019. — №12-4 (39). — С. 142–145.

8. Cory Wolff. From Reactive to Proactive: The Value of Offensive Security. https://risk3sixty.com/blog/from-reactive-to-proactive-the-value-of-offensive-security.
9. Tolulope Michael. Cybersecurity Vs Cyber Forensics: A Comprehensive Analysis. https://tolumichael.com/cybersecurity-vs-cyber-forensics/.
10. Matt Aubin. Digital Forensics vs Cyber Security. https://srecon.com/digital-forensics-vs-cyber-security/.
11. Для представителей средств массовой информации и общественности организован пресс-тур, посвященный деятельности Центра кибербезопасности Оперативно-розыскного департамента Министерства внутренних дел Республики Узбекистан. https://gov.uz/ru/iiv/news/view/57775.
12. Узбекистан усилит борьбу с киберпреступлениями. https://www.gazeta.uz/ru/2025/05/06/cybercrime/.
13. В Узбекистане число киберпреступлений за последние пять лет выросло в 68 раз. https://yuz.uz/ru/news/v-uzbekistane-chislo-kiberprestupleniy-za-poslednie-pyat-let-vroslo-v-68-raz.
14. International standard ISO/IEC 27037:2012. https://cdn.standards.iteh.ai/samples/44381/4002941492f247deac2a7bca1bc69e5b/ISO-IEC-27037-2012.pdf.
15. Cybersecurity and Digital Forensics – What's the Difference?. https://www.marshall.edu/blog/cyber-forensics-and-cybersecurity/#:~:text=What%20Is%20Digital%20Forensics%3F.
16. Importance of Digital Forensics In Cybersecurity. https://virtualcyberlabs.com/importance-of-digital-forensics/#:~:text=Importance%20of%20digital%20forensics%20in,nature%20and%20scope%20of%20attacks.
17. Digital forensics. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Electronic%20evidence%20can%20be%20collected,systems%2C%20shipborne%20equipment%2C%20and%20more.
18. Software and Systems Division: Digital forensics. https://www.nist.gov/itl/ssd/digital-forensics#:~:text=Digital%20evidence%20includes%20data%20on,software%20applications%20that%20is%20an.