СОВЕРШЕНСТВОВАНИЕ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ УЗБЕКИСТАНА: ЭВРИСТИЧЕСКИЕ МЕТОДЫ И ЗАРУБЕЖНЫЙ ОПЫТ

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

Аннотация. В данном исследовании анализируются теоретические и практические проблемы использования цифровых доказательств в уголовном процессе Республики Узбекистан в условиях интенсивной цифровизации. Особое внимание уделено правовым и организационным аспектам обращения с электронными данными, а также вопросам их допустимости, достоверности и идентификации. Рассмотрены тенденции развития цифровой криминалистики, включая нормативные нововведения и институциональные преобразования. Обоснована необходимость применения эвристических методов как интеллектуального инструмента анализа цифровых следов в случаях неполноты, искажения или утраты информации. Автором предложен комплекс рекомендаций, направленных на совершенствование уголовно-процессуальной практики, включая внедрение эвристических подходов, заимствование международного опыта ЕС и США, развитие специализированных программ и усиление межведомственного взаимодействия. Подчеркивается роль эвристики как механизма адаптации системы доказывания к реалиям цифровой эпохи.

Ключевые слова: уголовный процесс, эвристические методы, цифровая криминалистика, киберпреступность, кибербезопасность.

Abstract. This study analyzes the theoretical and practical problems of using digital evidence in the criminal process of the Republic of Uzbekistan in the context of intensive digitalization. Special attention is paid to the legal and organizational aspects of handling electronic data, as well as issues of their admissibility, reliability and identification. The trends in the development of digital forensics, including regulatory innovations and institutional transformations, are considered. The necessity of using heuristic methods as an intelligent tool for analyzing digital footprints in cases of incompleteness, distortion or loss of information is substantiated. The author offers a set of recommendations aimed at improving criminal procedure practice, including the introduction of heuristic approaches, borrowing international experience from the EU and the USA, the development of specialized programs and strengthening interagency cooperation. The role of heuristics as a mechanism for adapting the evidence system to the realities of the digital age is emphasized.

Keywords: criminal procedure, heuristic methods, digital forensics, cybercrime, cybersecurity.

Annotatsiya. Ushbu tadqiqot intensiv raqamlashtirish sharoitida O'zbekiston Respublikasi jinoyat protsessida raqamli dalillardan foydalanishning nazariy va amaliy muammolarini tahlil qiladi. Elektron ma'lumotlar bilan ishlashning huquqiy va tashkiliy jihatlariga, shuningdek ularning qabul qilinishi, ishonchliligi va identifikatsiyasi masalalariga alohida e'tibor qaratilmoqda. Raqamli sud ekspertizasining rivojlanish tendentsiyalari, shu jumladan me'yoriy yangiliklar va institutsional o'zgarishlar ko'rib chiqildi. Axborot to'liq bo'lmagan, buzilgan yoki yo'qolgan hollarda raqamli izlarni tahlil qilishning intellektual vositasi sifatida evristik usullardan foydalanish zarurati asoslanadi. Muallif jinoiy protsessual amaliyotni takomillashtirishga, shu jumladan evristik yondashuvlarni joriy etishga, Yevropa Ittifoqi va AQShning xalqaro tajribasini o'zlashtirishga, ixtisoslashtirilgan dasturlarni ishlab chiqishga va idoralararo hamkorlikni kuchaytirishga qaratilgan tavsiyalar to'plamini taklif qildi. Dalillar tizimini raqamli davr haqiqatlariga moslashtirish mexanizmi sifatida evristikaning roli ta'kidlangan.

Kalit so'zlar: jinoyat jarayoni, evristik usullar, raqamli sud ekspertizasi, kiberjinoyatchilik, kiberxavfsizlik.

В условиях стремительной цифровизации всех сфер жизни вопрос использования цифровых доказательств в уголовном процессе приобретает особую актуальность. Цифровые носители информации стали неотъемлемой частью современной преступной деятельности и, одновременно, важным источником доказательств. Однако, несмотря на это, использование цифровых доказательств сопряжено с рядом проблем, связанных с их идентификацией, извлечением, допустимостью и представлением в суде. В этой связи особое значение приобретают эвристические методы – подходы, основанные на практическом опыте, логических допущениях и методах поиска, – как инструменты решения данных задач.

В последние годы в Узбекистане наблюдается положительная динамика в сфере цифровизации уголовного судопроизводства:

- в Уголовно-процессуальный кодекс РУз внедрены понятия «цифровые доказательства» (ст. 204²) и «электронные данные» (ст. 204¹);

- приняты НПА, регулирующие обращение с электронной информацией: №ПП-4818 «О мерах по цифровизации деятельности органов судебной власти», №ЗРУ-1003, направленный на совершенствование системы работы с цифровыми доказательствами, №ПП-229, направленный на организацию научно-исследовательской деятельности в сфере цифровой криминалистики и др.;

- в августе 2022 года в структуре ГУВД Ташкента создан специализированный отдел по борьбе с преступностью в сфере информационных технологий, а также ГУП «Центр технического содействия» был передан в систему СГБ РУз и переименован в «Центр кибербезопасности» в соответствии с №ПП-4452 от 14 сентября 2019 года;

- в учебных программах некоторых факультетов ВУЗов появились дисциплины, посвящённые цифровой криминалистике (ТУИТ, Академия МВД и др.).

Тем не менее, данные меры ещё не полностью решают существующие проблемы и требуют дополнения со стороны научных методов исследования и практических решений.

Количество киберпреступлений в Узбекистане значительно выросло с развитием технологии искусственного интеллекта. В 2024 году было зарегистрировано более 130 тысяч киберпреступлений, при этом, больше половины из них – несовершеннолетними, а ущерб от киберпреступлений за последние годы составляет почти 2 трлн сумов.

В 2024 году в службу омбудсмана поступило свыше 6 000 обращений, касающихся экономических прав граждан, из которых свыше 150 были связаны с мошенничеством и оформлением онлайн-кредитов посредством кражи личных данных.

Основные проблемы, связанные с цифровыми доказательствами в уголовном процессе, включают:

- трудности идентификации источников информации и их уязвимость к фальсификации: цифровые данные легко подделать, стереть или зашифровать;

- недостаток правовой регламентации: в национальном законодательстве Республики Узбекистан отсутствует чёткое определение допустимости и процедуры сбора цифровых доказательств (несмотря на то, что в УПК РУз ст.205 и ст.208 изложенных в новой редакции №ЗРУ-1003 от 21 ноября 2024 года, содержится такое понятие, как «цифровые доказательства», они не отвечают необходимым требованиям, предъявляемым к таковым);

- техническая неподготовленность следственных органов: нехватка необходимого оборудования и специалистов по цифровой криминалистике;

- ограниченность межведомственного и международного сотрудничества в сфере обмена цифровыми доказательствами.

Несмотря на использование технологии хэширования файлов, существует проблема, когда дознаватели, следователи или прокуроры попросту не предоставляют «hash-файлы» (уникальная строка символов, сгенерированная специальным алгоритмом, которая используется для проверки целостности и

подлинности данных) защитнику или суду, либо, зачастую, файлы, находящиеся у последних, оказываются не идентичны предоставленным.

Эвристические методы позволяют в условиях неопределённости использовать адаптивные подходы для анализа цифровой информации – в частности, при восстановлении удалённых данных, анализе сетевой активности, профилировании поведения подозреваемого и установлении подлинности информации, поскольку нацелены на достижение эффективности несмотря на неполноту исходной информации.

Современная цифровая криминалистика представляет собой сложный синтез технических и правовых подходов, где исследователь нередко сталкивается с неполными, поврежденными или противоречивыми данными. В таких условиях классические методы анализа оказываются недостаточными. Именно здесь проявляется значение эвристических методов – гибких способов поиска решения, основанных не только на строгих алгоритмах, но и на логике, интуиции и профессиональном опыте эксперта.

В цифровой криминалистике эвристика применяется при идентификации цифровых следов, реконструкции событий, восстановлении удаленной информации и оценке ее достоверности. Так, например, когда часть файлов утрачена, а хронология действий пользователя нарушена, то специалист использует именно эвристический анализ, который проявляется в виде построения вероятных версий, выявлении закономерности по фрагментарным данным и проверке гипотез о построенных версиях и сценариях совершенного преступления. Такой подход позволяет восполнить пробелы, возникающие из-за технических ограничений или преднамеренного уничтожения цифровых следов.

Кроме того, эвристические методы тесно связаны с правовой оценкой цифровых доказательств. В реальной практике нередко возникают ситуации, когда цифровые данные формально не удовлетворяют всем процессуальным требованиям (например, отсутствует хэш-сумма, метаданные частично повреждены или не подтверждён источник). В подобных случаях эвристический анализ помогает экспертам и следователям обосновать допустимость и достоверность информации, исходя из совокупности косвенных признаков. Это способствует более справедливой оценке доказательств и минимизирует риск исключения значимых материалов из процесса.

Таким образом, эвристика выступает интеллектуальным мостом между техническим анализом и юридической оценкой цифровых доказательств. Она не заменяет процессуальные нормы, но дополняет их, позволяя адаптировать правоприменительную практику к реалиям стремительно развивающихся технологий. Внедрение эвристических подходов в систему подготовки

следователей и экспертов может существенно повысить эффективность расследования преступлений в цифровой среде.

Для повышения эффективности использования цифровых доказательств в уголовном процессе автором предлагается следующее:

1) Нормативно-правовое совершенствование – разработать и внедрить единый закон о цифровых доказательствах, с учётом международных стандартов (например, Конвенция о киберпреступности, Будапешт, 2001 г.); установить чёткие процедуры сбора, хранения, анализа и представления цифровых доказательств в суде, либо доработать и принять Цифровой кодекс, проект которого был представлен в 2022 году, с учетом именно уголовно-процессуальной основы.

2) Использование зарубежного опыта – внедрить практику Digital Forensics Units (США, Германия, Южная Корея) при органах внутренних дел; перенять методы осмотрительных алгоритмов и эвристического анализа, применяемые в системе Europol и Interpol, поскольку, несмотря создание НИИ цифровой криминалистики, согласно №ПП-229 от 21 июня 2024 года, он занимается исследовательской деятельностью и находится лишь в структуре Правоохранительной академии Республики Узбекистан, не выступая в роли конкретного подразделения каждого из правоохранительных органов.

Также необходимо создать единую платформу обмена цифровыми уликами между правоохранительными органами и провайдерами, на примере Европейского союза и их системы e-Evidence Digital Exchange System, созданной на основе Заключения Совета Европейского союза от 9 июня 2016 года, призванной повысить эффективность использования процедур взаимопомощи для получения электронных доказательств.

В Европейском союзе также активно применяется Руководство ENFSI по цифровой криминалистике (ENFSI Guidelines for Forensic Examination of Digital Technology, 2020), где отдельное внимание уделяется методам вероятностного анализа и эвристическим подходам при оценке цифровых следов.

Данная платформа также позволит сохранить подлинность доказательств, сохраняя первоначальный вид с помощью «hash-суммы» хэшированных файлов.

3) Повышение квалификации кадров – обязательное обучение дознавателей, следователей и прокуроров методам цифрового анализа путём создания специализированных магистерских программ по цифровой криминалистике, что на данный момент реализуется только в Правоохранительной академии Республики Узбекистан.

4) Международное сотрудничество – подписание двусторонних соглашений об обмене цифровыми доказательствами и взаимодействии в области

кибербезопасности; участие в международных инициативах по борьбе с киберпреступностью.

5) Внедрение эвристических методов в практику цифровой криминалистики.

Следует разработать методические рекомендации по применению эвристических подходов при анализе цифровых доказательств, особенно в условиях неполноты, противоречивости или искажения данных. Для этого необходимо включить соответствующие модули в программы повышения квалификации следователей, прокуроров и судебных экспертов, а также разработать национальный стандарт или методику эвристического анализа цифровых доказательств, аналогичную тем, что применяются в экспертных центрах ЕС и США. В руководстве ENFSI по судебной экспертизе цифровых технологий прописаны принципы гибкого анализа цифровых следов, допущения и обоснование выводов, что близко к эвристическому подходу, а в США группа SWGDE разрабатывает руководства и стандарты по цифровым доказательствам, предусматривая процедуры верификации, документооборота и оценки экспертных суждений. Также, в исследовании «Enabling forensics by proposing heuristics…» показано, что предложенные эвристики помогают разрешать противоречия в экспертном анализе, облегчая принятие решений при условиях неопределённости.

Интеграция таких методов обеспечит гибкость и научную обоснованность цифровых расследований, повысит качество интерпретации электронных следов и сократит риск ошибочной оценки доказательств.

В заключении, следует указать, что эвристические методы в условиях цифровизации играют ключевую роль в адаптации уголовного процесса к новым реалиям. Внедрение таких подходов, наряду с правовыми и техническими мерами, позволит обеспечить надлежащее использование цифровых доказательств в Республике Узбекистан. Синтез научных решений и международного опыта – путь к формированию эффективной правоприменительной практики, способной противостоять современным вызовам преступности. Интеграция эвристических методов в уголовно-процессуальную деятельность требует не только технического, но и методологического переосмысления процессуальных стандартов доказывания.

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 21 июня 2024 года №ПП-229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики». https://lex.uz/uz/docs/6977762.

4. Постановление Президента Республики Узбекистан от 14 сентября 2019 года №ПП-4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты». https://www.lex.uz/docs/4665551.

5. Постановление Президента Республики Узбекистан от 03 сентября 2020 года №ПП-4818 «О мерах по цифровизации деятельности органов судебной власти». https://lex.uz/docs/4979899.

6. OSAC Task Group on Digital/Multimedia Science, «A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence». https://www.nist.gov/system/files/documents/2018/01/10/osac_ts_0002.pdf.

7. Council conclusions on improving criminal justice in cyberspace, Luxembourg, 9 June 2016. https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.

8. Uche Mbanaso, Emmanuel S. Dandaura. The Cyberspace: Redefining A New World, June 2015. https://www.researchgate.net/publication/280101879_The_Cyberspace_Redefining_A_New_World.

9. E4J University Module Series: Cybercrime, Module 4: Introduction to Digital Forensics. https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html.

10. Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01, Ver.01, November 2015. https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

11. Алимова Р.Р. Борьба с киберпреступностью в Республике Узбекистан. Киберпреступность как вид мошенничества. // Central Asian Research Journal for Interdisciplinary Studies (CARJIS). — 2022. — №2. — С. 208-213.

12. Фазилов Ф.М., Аманжолова Б.А. Искусственный интеллект и уголовное право в Узбекистане и Казахстане. // Universum: экономика и юриспруденция. — 2025. — №10 (132). — С. 33-39.

13. Гаджиев Х., Худойбердиев А. Некоторые аспекты исследования мобильных устройств: опыт Узбекистана. // Общество и инновации. — 2020. — №2/S. — С. 437-448.

14. Иванов Д.Д. Применение цифровой криминалистики в современных расследованиях и анализе данных. // Вестник науки. — 2024. — №12 (81). — С. 672-677.

15. Цифра: сколько денег у жителей Узбекистана украли киберпреступники. https://www.spot.uz/ru/2025/05/30/cyber-crime/.

16. Crime rate in Uzbekistan: MIA reports nearly 200 offenses per 100,000 people for 2024. https://kun.uz/en/news/2025/02/27/crime-rate-in-uzbekistan-mia-reports-nearly-200-offenses-per-100000-people-for-2024.

17. В Узбекистане в 2024 году на 42 % выросло число обращений к омбудсману по кредитному мошенничеству. https://aktualno.uz/ru/a/14752-v-uzbekistane-v-2024-godu-na-42-vyroslo-cislo-obrashhenii-k-ombudsmanu-po-kreditnomu-mosennicestvu.