

**Ссылка для цитирования этой статьи:**

Амирова М.Г., Таилова А.Г. Криминалистические аспекты цифровых технологий // Human Progress. 2025. Том 11, Вып. 6. С. 27. URL: [http://progress-human.com/images/2025/Tom11\\_6/Tailova.pdf](http://progress-human.com/images/2025/Tom11_6/Tailova.pdf) DOI 10.46320/2073-4506-2025-6a-29.

## **КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ**

**Амирова Марьям Гатамовна**

кандидат экономических наук,  
старший преподаватель кафедры экономических и  
общеобразовательных дисциплин,  
Дагестанский государственный университет,  
г. Избербаш, Российская Федерация

**Таилова Айша Габибовна**

кандидат юридических наук,  
доцент кафедры юридических дисциплин,  
Дагестанский государственный университет,  
г. Избербаш, Российская Федерация

**Аннотация.** В статье рассматриваются современные криминалистические аспекты использования цифровых технологий в процессе раскрытия и расследования преступлений. Анализируется влияние цифровизации на трансформацию криминалистической науки и практики, исследуются новые возможности и вызовы, связанные с внедрением искусственного интеллекта, больших данных, блокчейн-технологий и других инновационных решений в деятельность правоохранительных органов. Особое внимание уделяется вопросам цифровой криминалистики, методикам работы с электронными доказательствами, проблемам их процессуального закрепления и оценки. Рассматриваются перспективные направления развития криминалистической техники и тактики в условиях цифровой трансформации общества. Автор приходит к выводу о необходимости комплексной модернизации криминалистического обеспечения правоохранительной деятельности с учетом современных технологических реалий, совершенствования нормативно-правовой базы и подготовки квалифицированных специалистов в области цифровой криминалистики.

**Ключевые слова:** цифровые технологии, криминалистика, электронные доказательства, цифровая криминалистика, искусственный интеллект, большие данные, блокчейн, киберпреступления, цифровые следы, информационная безопасность.

Стремительное развитие цифровых технологий оказывает существенное влияние на все сферы общественной жизни, включая криминальную среду и деятельность правоохранительных органов. Современная криминалистика сталкивается с принципиально новыми вызовами, связанными как с появлением новых видов преступлений в цифровой среде, так и с необходимостью адаптации традиционных криминалистических методов и средств к условиям цифровой реальности.

Актуальность исследования криминалистических аспектов цифровых технологий обусловлена несколькими факторами. Во-первых, наблюдается экспоненциальный рост киберпреступности и преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. По данным МВД России, количество таких преступлений в 2023 году превысило 600 тысяч, что составляет более четверти от общего числа зарегистрированных преступлений. Во-вторых, цифровые следы становятся ключевыми доказательствами не только при расследовании киберпреступлений, но и традиционных общеуголовных преступлений. В-третьих, правоохранительные органы получают в свое распоряжение новые высокотехнологичные инструменты для раскрытия и расследования преступлений, эффективное использование которых требует соответствующей теоретической и методической базы.

Цифровизация общества привела к фундаментальным изменениям в теории и практике криминалистики. Традиционное понимание криминалистики как науки о закономерностях механизма преступления, возникновения информации о преступлении и его участниках, закономерностях собирания, исследования, оценки и использования доказательств требует переосмысления с учетом особенностей цифровой среды.

В цифровом пространстве механизм следообразования приобретает специфические черты. Цифровые следы, в отличие от традиционных материальных следов, обладают рядом уникальных свойств: они могут существовать одновременно в нескольких местах, легко копируются без потери качества, могут быть изменены или уничтожены дистанционно, часто имеют временные метки и метаданные, позволяющие восстановить хронологию событий. При этом цифровые следы характеризуются высокой латентностью – пользователи цифровых устройств часто не осознают, какой объем информации о своих действиях они оставляют в информационных системах.

Современная криминалистическая техника активно обогащается цифровыми технологиями, которые существенно расширяют возможности обнаружения, фиксации, изъятия и исследования следов преступления. Рассмотрим основные направления применения цифровых технологий в этой сфере.

Искусственный интеллект и машинное обучение находят широкое применение в различных областях криминалистической техники. Системы распознавания лиц на основе нейронных сетей позволяют идентифицировать подозреваемых по записям камер видеонаблюдения даже при плохом качестве изображения или частичном закрытии лица. Алгоритмы машинного обучения успешно применяются для анализа почерка, идентификации авторства текстов, выявления поддельных документов. Особенно эффективны такие системы при работе с большими массивами данных, где человеческий анализ был бы слишком трудоемким или невозможным.

3D-сканирование и моделирование революционизировали процесс фиксации места происшествия. Современные лазерные сканеры позволяют создать точную трехмерную модель места происшествия за считанные минуты, сохранив все пространственные характеристики и взаимное расположение объектов. Такие модели могут использоваться для виртуальной реконструкции событий преступления, проведения следственных экспериментов, а также представления доказательств в суде. Технология фотограмметрии позволяет создавать 3D-модели на основе серии фотографий, что делает данный метод доступным даже при отсутствии специализированного оборудования.

Технологии больших данных (Big Data) открывают новые возможности для выявления скрытых связей и закономерностей в расследовании преступлений. Анализ больших массивов данных из различных источников – социальных сетей, банковских транзакций, телефонных соединений, геолокационных данных – позволяет восстановить детальную картину действий подозреваемых, выявить сообщников, установить мотивы преступления. Предиктивная аналитика на основе исторических данных о преступлениях помогает прогнозировать вероятные места и время совершения преступлений, что позволяет более эффективно распределять ресурсы правоохранительных органов.

Блокчейн-технологии начинают применяться для обеспечения неизменности и прослеживаемости цифровых доказательств. Создание распределенного реестра всех действий с электронными доказательствами гарантирует их целостность и подлинность, что особенно важно при длительных расследованиях с участием множества субъектов. Некоторые страны уже экспериментируют с использованием блокчейна для хранения материалов уголовных дел и обеспечения цепочки поставки вещественных доказательств.

Электронные доказательства стали неотъемлемой частью современного уголовного процесса, что требует разработки специальных методик их обнаружения, изъятия, исследования и процессуального оформления. Специфика работы с электронными доказательствами заключается в их особой природе – они существуют в виде

электромагнитных сигналов и требуют специальных технических средств для восприятия человеком.

Процесс работы с электронными доказательствами начинается с их обнаружения и идентификации. На этом этапе критически важно определить все потенциальные источники цифровой информации: компьютеры, смартфоны, планшеты, умные часы, автомобильные системы, устройства "умного дома", облачные хранилища и т.д. Современный человек окружен множеством цифровых устройств, каждое из которых может содержать ценную криминалистически значимую информацию.

При изъятии электронных носителей информации необходимо соблюдать ряд специальных правил. Во-первых, следует обеспечить сохранность данных, предотвратив их изменение или уничтожение. Для этого используются специальные блокираторы записи, создаются побитовые копии носителей, применяется криминалистическое программное обеспечение, работающее в режиме "только чтение". Во-вторых, важно зафиксировать состояние устройства на момент изъятия – включено оно или выключено, какие программы запущены, какая информация отображается на экране. В-третьих, необходимо обеспечить непрерывность цепочки поставки доказательств, документируя все действия с электронными носителями.

Исследование электронных доказательств представляет собой сложный технический процесс, требующий специальных знаний и оборудования. Современные методы компьютерной криминалистики позволяют восстановить удаленные файлы, извлечь данные из поврежденных носителей, расшифровать зашифрованную информацию, проанализировать сетевой трафик, восстановить историю действий пользователя. При этом эксперт должен использовать только апробированные методики и сертифицированное программное обеспечение, чтобы результаты исследования были признаны допустимыми доказательствами.

Развитие цифровых технологий существенно влияет на тактику проведения следственных действий. Традиционные тактические приемы дополняются новыми, учитывающими особенности цифровой среды и поведения людей в ней [3, с. 47].

При проведении допроса в эпоху цифровых технологий следователь может использовать данные из социальных сетей, мессенджеров, геолокационную информацию для проверки показаний и выявления противоречий. Анализ цифровой активности допрашиваемого позволяет лучше понять его психологический профиль, круг общения, интересы, что помогает выбрать наиболее эффективную тактику допроса. Технологии

видеоконференцсвязи расширяют возможности проведения допросов с участием лиц, находящихся в других регионах или странах.

Обыск в цифровую эпоху требует особой подготовки и планирования. Помимо традиционных объектов поиска, следователь должен быть готов к обнаружению и изъятию различных цифровых устройств, включая скрытые камеры, устройства для майнинга криптовалют, аппаратные криптокошельки. Важно учитывать возможность удаленного уничтожения данных и принимать меры для предотвращения этого – отключение устройств от сети, использование экранирующих контейнеров для блокировки радиосигналов. При обыске все чаще применяются технические средства поиска – детекторы электронных устройств, тепловизоры для обнаружения работающей техники, специализированное ПО для быстрого анализа содержимого компьютеров [1, с. 58].

Следственный эксперимент с использованием цифровых технологий приобретает новые возможности. Виртуальная реконструкция события преступления на основе 3D-моделей места происшествия и данных о перемещении участников позволяет проверить различные версии произошедшего. Компьютерное моделирование может использоваться для проверки возможности совершения определенных действий в конкретных условиях, например, возможности произвести выстрел под определенным углом или увидеть что-либо с определенной точки.

Проблема квалификации кадров является одной из наиболее острых. Эффективное использование цифровых криминалистических методов требует от сотрудников правоохранительных органов не только традиционных юридических знаний, но и глубокого понимания информационных технологий. К сожалению, существующая система подготовки кадров не всегда успевает за стремительным развитием технологий. Необходима разработка специализированных образовательных программ, регулярное повышение квалификации действующих сотрудников, привлечение IT-специалистов к работе в правоохранительных органах., трансграничного обмена данными остаются недостаточно урегулированными. Законодательство часто не успевает адаптироваться к появлению новых типов киберпреступлений, таких как атаки с использованием искусственного интеллекта, преступления в метавселенных или манипулирование криптовалютными рынками. Это создаёт правовые лакуны, которыми пользуются преступники, и затрудняет привлечение их к ответственности.

Организационные проблемы проявляются в недостаточной координации между различными правоохранительными органами и ведомствами. Киберпреступления часто носят межведомственный характер, требуя взаимодействия полиции, служб безопасности,

финансовых регуляторов, но механизмы такого взаимодействия не всегда эффективны. Бюрократические процедуры замедляют реагирование на инциденты, в то время как киберпреступники действуют оперативно и слаженно.

Международное сотрудничество представляет особую сложность. Киберпреступники легко пересекают государственные границы в цифровом пространстве, используют серверы в разных юрисдикциях, применяют методы анонимизации. При этом международные механизмы расследования и экстрадиции работают медленно, существуют политические барьеры, различия в правовых системах. Отсутствие единых международных стандартов в области кибербезопасности и борьбы с киберпреступностью серьёзно осложняет глобальное противодействие этой угрозе.

Проблема доказательств в киберпреступлениях имеет свою специфику. Электронные следы легко уничтожить или модифицировать, что затрудняет их использование в суде. Вопросы аутентификации цифровых доказательств, обеспечения их целостности, соблюдения процессуальных требований при их сборе требуют особых подходов и экспертизы. Традиционные методы криминалистики часто оказываются неприменимыми в цифровой среде.

Финансовые ограничения также играют важную роль. Создание и поддержание современной инфраструктуры кибербезопасности требует значительных инвестиций. Необходимо постоянное обновление оборудования и программного обеспечения, оплата высококвалифицированных специалистов, проведение исследований. Государственное финансирование часто отстаёт от реальных потребностей, особенно в развивающихся странах [2, с. 47].

Психологические и социальные аспекты борьбы с киберпреступностью также важны. Низкая осведомлённость населения о киберугрозах делает людей лёгкими жертвами мошенников. Необходимы масштабные просветительские кампании, формирование культуры цифровой безопасности. Важно преодолеть стереотип о том, что киберпреступления менее серьёзны, чем традиционные преступления, хотя их последствия могут быть катастрофическими.

Этические дилеммы возникают при использовании современных технологий в правоохранительной деятельности. Вопросы о допустимых пределах слежки, использовании искусственного интеллекта для профилирования потенциальных преступников, применении взлома для получения доказательств требуют тщательного рассмотрения. Необходимо найти баланс между эффективностью борьбы с преступностью и защитой гражданских прав и свобод.

Решение этих проблем требует комплексного подхода, включающего модернизацию законодательства, увеличение финансирования, подготовку квалифицированных кадров, развитие международного сотрудничества, повышение осведомлённости общества. Только системные усилия на всех уровнях позволят эффективно противостоять растущей угрозе киберпреступности в современном цифровом мире.

### Список литературы

1. Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 2021. 342 с.
2. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2020. 428 с.
3. Гаврилин Ю.В., Сотов А.И. Расследование преступлений в сфере компьютерной информации: учебное пособие. М.: Юрлитинформ, 2022. 256 с.

## FORENSIC ASPECTS OF DIGITAL TECHNOLOGIES

**Amirova Maryam Gatamovna**

Candidate of Economic Sciences,  
Senior Lecturer, Department of Economic and General Educational Disciplines,  
Dagestan State University,  
Izberbash, Russian Federation

**Tailova Aisha Gabibovna**

Candidate of Law,  
Associate Professor, Department of Legal Disciplines,  
Dagestan State University,  
Izberbash, Russian Federation

**Annotation.** The article examines modern criminalistic aspects of the use of digital technologies in the process of crime detection and investigation. The impact of digitalization on the transformation of forensic science and practice is analyzed, new opportunities and challenges associated with the introduction of artificial intelligence, big data, blockchain technologies and other innovative solutions into the activities of law enforcement agencies are explored. Special attention is paid to the issues of digital forensics, methods of working with electronic evidence, problems of their procedural consolidation and evaluation. Promising areas of development of forensic technology and tactics in the context of digital transformation of society are considered. The author comes to the conclusion that it is necessary to comprehensively modernize the forensic support of law enforcement activities, taking into account modern technological realities, improve the regulatory framework and train qualified specialists in the field of digital forensics.

**Keywords:** digital technologies, forensics, electronic evidence, digital forensics, artificial intelligence, big data, blockchain, cybercrime, digital footprints, information security.

### References

1. Baturin, Yu. M., Problems of Computer Law. Moscow: Legal Literature, 2021. 342 p.

2. Vekhov, V. B., Fundamentals of Forensic Science on the Study and Use of Computer Information and Means of Its Processing: Monograph. Volgograd: VA MVD of Russia, 2020. 428 p.
3. Gavrilin, Yu. V., Sotov, A. I., Investigation of Computer Crimes: A Study Guide. Moscow: Yurlitinform, 2022. 256 p.