Дата поступления рукописи в редакцию: 17.04.2026 г. DOI: 10.24412/2782-3830-2026-6-251-254
Дата принятия рукописи в печать: 02.07.2026 г.

МАКАЗИЕВА Зара Даутовна,
старший преподаватель кафедры
уголовного права, процесса и национальной безопасности
Чеченского государственного университета имени А. А. Кадырова,
e-mail: zara6756@mail.ru

ДАДАШОВ М.М.,
доцент кафедры информационного права и юриспруденции
Грозненский государственный нефтяной технический университет
имени М.Д. Миллионщикова, Грозный, Россия,
e-mail: musa_dadashov12.10.1988@mail.ru

ТЕОРЕТИЧЕСКИЕ И ПРАВОВЫЕ ОСНОВЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Аннотация. *Актуальность темы исследования обусловлена глобальной трансформацией преступности, которая в условиях четвертой промышленной революции приобретает ярко выраженный цифровой характер. Современное общество столкнулось с беспрецедентным ростом киберугроз, при которых традиционные методы криминалистики зачастую оказываются недостаточно эффективными. Использование злоумышленниками зашифрованных каналов связи, анонимайзеров и технологий блокчейна создает серьезные препятствия для правоохранительных органов. В связи с этим внедрение передовых компьютерных технологий в процесс раскрытия и расследования преступлений становится не просто вспомогательным инструментом, а жизненно необходимой мерой обеспечения национальной безопасности и правопорядка*

Ключевые слова: *киберпреступность, киберугроза, зашифрованные каналы, анонимайзеры, технологии блокчейна, расследование преступления, нациоанльная безопасность.*

MAKAZIEVA Zara Dautovna,
Senior Lecturer at the Department
of Criminal Law, Process and National Security
Chechen State University named after A. A. Kadyrov

DADASHOV M.M.,
Associate Professor,
Department of Information Law and Jurisprudence
Grozny State Petroleum Technological University
named after M.D. Millionshchikov, Grozny, Russia

THEORETICAL AND LEGAL FOUNDATIONS OF DIGITAL CRIMINOLOGY

Annotation. *The relevance of the research topic is due to the global transformation of crime, which has become highly digitalized in the context of the Fourth Industrial Revolution. Modern society is facing an unprecedented increase in cyber threats, where traditional forensic methods are often insufficient. The use of encrypted communication channels, anonymizers, and blockchain technologies by criminals poses significant challenges for law enforcement agencies. As a result, the integration of advanced computer technologies into the process of crime detection and investigation has become not just an auxiliary tool, but a vital measure for ensuring national security and law enforcement.*

Key words: *cybercrime, cyber threat, encrypted channels, anonymizers, blockchain technologies, crime investigation, national security.*

Современный этап развития криминалистической науки характеризуется глубокой интеграцией информационных достижений в практическую деятельность правоохранительных органов. Под компьютерными технологиями в контексте раскрытия преступлений следует понимать совокупность методов, программных и технических средств, предназначенных для сбора, фиксации, исследования и хранения цифровой информации, имеющей значение для уголовного дела. Данная категория охватывает не только аппаратное обеспечение, но и сложные алгоритмические системы, позволяющие оперировать виртуальными следами, которые по своей природе принципиально отличаются от материальных объектов традиционной криминалистики [2].

Классификация компьютерных технологий в следственной деятельности может быть проведена по нескольким основаниям. По функциональному назначению выделяют поисковые системы, средства фиксации цифровой информации, аналитические программные комплексы и системы защиты данных. Поисковые технологии направлены на обнаружение скрытых файлов, зашифрованных разделов дисков и следов сетевой активности. Средства фиксации обеспечивают создание точных побитовых копий носителей информации, что гарантирует неизменность исходных данных и соблюдение принципа процессуальной чистоты доказательств [1].

Важное место занимают аналитические технологии, включающие в себя инструменты для восстановления удаленных данных, дешифрования паролей и анализа структуры баз данных. В последние годы особое развитие получили технологии интеллектуального анализа, способные обрабатывать неструктурированные массивы информации. Возможность анализа данных позволяет следователю обнаруживать скрытые паттерны в действиях участников, воссоздавать последовательность инцидентов по метаданным и интегрировать сведения из разных цифровых платформ — смартфонов, облачных сервисов, систем видеонаблюдения [7]. Особое значение имеет градация по степени автоматизации: среди решений выделяются автоматизированные информационные комплексы, экспертные системы и независимые программные блоки. Применение подобных инструментов значительно снижает время на выполнение шаблонных задач, обеспечивая высвобождение ресурсов для аналитической работы, формулировки предположений и разработки следственных версий. Благодаря этому компьютерные технологии создают новую модель в криминалистике, в которой цифровое пространство превращается в полноценную среду для раскрытия дела и поиска достоверной информации. [3].

Юридическое регулирование использования цифровых технологий служит основой, гарантирующей законность и обоснованность результатов, представленных в судебном заседании. Центральным нормативным документом, задающим принципы обращения с информацией, является Федеральный закон «Об информации, информационных технологиях и о защите информации», в котором закреплены ключевые термины — электронное сообщение и документированная информация [5]. Тем не менее, особенности уголовного процесса предполагают необходимость детализации процедур изъятия и анализа электронных носителей, что нашло своё отражение в положениях Уголовно-процессуального кодекса.

Статус электронных доказательств в процессе долгое время вызывал споры среди юристов. Сегодня под такими доказательствами понимаются данные, записанные на электронных носителях в формате, пригодном для интерпретации как людьми, так и техническими системами. Критерием приемлемости таких материалов являются их связь с делом, надежность и соответствие требованиям допустимости. Чтобы обеспечить последнюю, законодатель установил строгие процедуры обыска и изъятия, обязывающие привлекать экспертов и использовать средства копирования, исключающие произвольные изменения информации [7].

Особую значимость имеет защита прав сторон процесса на личную жизнь и конфиденциальность переписки при анализе цифровых устройств. Надзор со стороны суда за порядком получения доступа к данным, хранящимся на мобильных телефонах и персональных компьютерах, играет роль гарантии соблюдения конституционных свобод. Параллельно складывается правовой подход к работе с информацией, размещённой в «облачных» хранилищах, расположенных за пределами страны, что порождает потребность в развитии международного правового сотрудничества [8].

Несмотря на существующую нормативную базу, остаётся острая необходимость в стандартизации требований к выводам экспертов в сфере компьютерно-технических исследований. Законодательство должно не только отражать актуальное состояние информационных технологий, но и демонстрировать достаточную адаптивность, позволяющую учитывать новые формы цифровой информации без частой замены основополагающих правовых актов. Такое решение возможно за счёт совершенствования внутренних руководящих документов и методических указаний, содержащих чёткие алгоритмы использования специализированного программного обеспечения в процессе расследования дел [6].

Быстрое развитие цифровых решений формирует ситуацию, когда правовые рамки оказываются запаздывающими перед возникновением новых форм преступной деятельности. Особую сложность представляет отсутствие однозначного юридического определения ключевых категорий — «криптографические валюты», «виртуальные ценности» и «системы искусственного интеллекта» — в рамках уголовного законодательства. Из-за этого затрудняется правильная квалификация действий, связанных с хищением цифровых ресурсов либо применением нейросетей для производства ложных доказательств (например, дипфейков) [4].

Кроме того, высокая степень межгосударственной распространённости цифровых следов создаёт серьёзные препятствия для эффективного реагирования на киберпреступления. Серверы, где хранятся данные, могут находиться в разных юрисдикциях, что приводит к задержкам в получении информации через классические каналы международной правовой помощи. За время ожидания ответа данные уже могут быть стёрты или защищены шифрованием. Решение этой проблемы предполагает внедрение новых глобальных стандартов и механизмов быстрой электронной кооперации между правоохранительными органами, обеспечивающих оперативный доступ к информации без компрометации национального суверенитета [10].

Острый характер носит вопрос о признании данных, сгенерированных алгоритмами искусственного интеллекта, в качестве надежных доказательств. Текущее законодательство строится на основе человеческой оценки и экспертного суждения, однако скрытая природа сложных нейросетей — так называемого «черного ящика» — затрудняет проверку логики принятия решений. Юридическая система сталкивается с необходимостью выработать стандарты подтверждения достоверности таких решений, чтобы они могли быть приняты судом как допустимые доказательства[8].

В заключение, важным аспектом остаётся обеспечение достаточного уровня цифровой компетентности у участников правоохранительного процесса. Растущая сложность норм, регулирующих фиксацию электронных следов, требует от следователей высокой степени технической осведомлённости. Расхождение между уровнем подготовки сотрудников и усложнившимися правовыми нормами приводит к процессуальным нарушениям, зачастую ведущим к отказу в приёме доказательств. Поэтому модернизация правовой базы должна осуществляться одновременно с совершенствованием образовательных программ и обновлением технической инфраструктуры следственных и дознавательных органов [9].

Список литературы:

[1] Криминалистика : учебник / под ред. А. Н. Колесниченко. — 3-е изд., перераб. и доп. — М. : Юрайт, 2020. — 541 с.

[2] Цифровая криминалистика : учеб. пособие / В. Ю. Флегонтов. — 3-е изд. — М. : РИТВУС, 2022. — 256 с.

[3] О соотношении традиционной криминалистики и цифровой криминалистики // Бюллетень Белгородского университета кооперации, экономики и права. — 2023. — № 2. — С. 45-52. — URL: https://brj-bguep.ru/reader/article.aspx?id=27156 (дата обращения: 20.01.2026).

[4] Угрюмов А. Ю. Криминалистическая характеристика киберпреступлений в системах электронных платежей // Вестник экономической безопасности. — 2023. — № 1. — С. 78-89. — URL: http://e-notabene.ru/view_article.php?id_article=78140 (дата обращения: 10.02.2026).

[5] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.03.2026).

[6] Криминалистика: место цифровой криминалистики в науке и перспективы развития // Информационно-правовые проблемы современной виртуальной среды. — 2023. — № 2. — С. 112-120. — URL: https://www.ippsvfu.ru/jour/article/view/223 (дата обращения: 18.02.2026).

[7] Полозов К. А. Цифровая криминалистика: проблемы и перспективы // Юрист. — 2024. — № 3. — С. 34-41. — URL: https://cyberleninka.ru/article/n/tsifrovoe-sostoyanie-kriminalisticheskoy-nauki-aktualnye-i-perspektivnye-razrabotki-i-ih-prakticheskoe-voploschenie (дата обращения: 12.03.2026).

[8] Reedy P. Interpol Review of Digital Forensics // Forensic Science International. — 2015. — Vol. 249. — P. 1-10.

[9] Garfinkel S. L. Digital Forensics Research: The Next 10 Years // Digital Investigation. — 2010. — Vol. 7, suppl. 1. — P. S64-S73.

[10] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021 [Electronic resource]. — URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-2021 (accessed: 15.02.2026).

References:

[1] Forensics: textbook/ed. A.N. Kolesnichenko. - 3rd ed., Revised and add. - M.: Yurayt, 2020. - 541 p.

[2] Digital forensics: tutory. manual/V. Yu. Flegontov. - 3rd ed. - M.: RITVUS, 2022. - 256 s.

[3] On the relationship between traditional forensics and digital forensics//Bulletin of the Belgorod University of Cooperation, Economics and Law. — 2023. — № 2. - S. 45-52. - URL: https://brj-bguep.ru/reader/article.aspx?id=27156 (access date: 20.01.2026).

[4] Ugryumov A. Yu. Forensic characteristics of cybercrimes in electronic payment systems//Bulletin of Economic Security. — 2023. — № 1. - S. 78-89. - URL: http://e-notabene.ru/view_article.php?id_article=78140 (access date: 10.02.2026).

[5] Federal Law No. 149-FZ of July 27, 2006 “On Information, Information Technology and Information Protection” [Electronic Resource]. - URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (access date: 05.03.2026).

[6] Forensics: the place of digital forensics in science and development prospects//Information and legal problems of the modern virtual environment. — 2023. — № 2. - S. 112-120. - URL: https://www.ippsvfu.ru/jour/article/view/223 (access date: 18.02.2026).

[7] Polozov K. A. Digital forensics: problems and prospects//Lawyer. — 2024. — № 3. - S. 34-41. — URL: https://cyberleninka.ru/article/n/tsifrovoe-sostoyanie-kriminalisticheskoy-nauki-aktualnye-i-perspektivnye-razrabotki-i-ih-prakticheskoe-voploschenie (дата обращения: 12.03.2026).

[8] Reedy P. Interpol Review of Digital Forensics // Forensic Science International. — 2015. — Vol. 249. — P. 1-10.

[9] Garfinkel S. L. Digital Forensics Research: The Next 10 Years // Digital Investigation. — 2010. — Vol. 7, suppl. 1. — P. S64-S73.

[10] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021 [Electronic resource]. — URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-2021 (accessed: 15.02.2026).

