УГОЛОВНО-ПРАВОВЫЕ НАУКИ

CRIMINAL LAW SCIENCES

Научная статья
УДК 343.14
DOI 10.33184/pravgos-2026.1.24

Original article

ЖАНДРОВ Владимир Юрьевич
Московский университет МВД России имени В.Я. Кикотя,
Москва, Россия,
vaisvladimir74@gmail.com,
https://orcid.org/0000-0002-1353-2837

ZHANDROV Vladimir Yuryevich
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia,
Moscow, Russia

ОБЕСПЕЧЕНИЕ ДОКАЗАТЕЛЬСТВЕННОГО ЗНАЧЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

ENSURING THE EVIDENTIAL VALUE OF DIGITAL INFORMATION OBTAINED DURING OPERATIVE INVESTIGATIVE ACTIVITIES

Аннотация. *Бурное развитие цифровых технологий кардинально изменило условия получения и использования в уголовном процессе доказательственной информации. Распространение мессенджеров, социальных сетей, облачных сервисов и анонимных коммуникационных платформ позволяет преступникам скрывать следы своей противоправной деятельности, что обусловливает особую актуальность вопросов извлечения, фиксации и верификации цифровых данных, получаемых в ходе оперативно-розыскных мероприятий. Цель исследования заключается в формировании комплексного подхода к обеспечению доказательственного значения цифровой информации, который сочетает правовые гарантии допустимости и технические требования к сохранности и воспроизводимости данных. Методологическую основу исследования составили: диалектический метод познания, позволивший рассмотреть обеспечение доказательственного значения цифровой информации как развивающееся правовое явление; системный метод, применявшийся для анализа условий допустимости цифровых доказательств и разработки алгоритма их получения и фиксации; сравнительно-правовой метод, использованный при сопоставлении законодательства и правоприменительной практики, а также логический и экспертно-аналитический методы, обеспечившие формулирование выводов и обобщение практики обращения с цифровыми дан-*

Abstract. *The rapid development of digital technologies has radically changed the conditions for obtaining and using evidentiary information in criminal proceedings. The widespread use of messengers, social networks, cloud services, and anonymous communication platforms enables criminals to hide their tracks, making the extraction, fixation, and verification of digital data obtained during operative investigative activities particularly relevant. The purpose of this study is to develop a comprehensive approach to ensuring the evidentiary value of digital information, combining legal guarantees of admissibility with technical requirements for data preservation and reproducibility. The methodological basis of the research comprises the dialectical method of cognition, which allows for consideration of the evidentiary value of digital information as an evolving legal phenomenon; the systemic method, used to analyze the admissibility conditions of digital evidence and develop an algorithm for its acquisition and fixation; the comparative legal method, employed to compare legislation and law enforcement practice; as well as the logical and expert-analytical methods, which ensure the formulation of conclusions and the generalization of the practice of handling digital data. Results: The article identifies the main risks of losing the evidentiary value of digital information: lack of*

ными. Результаты: определены основные риски утраты доказательственного значения цифровой информации: отсутствие судебного разрешения на доступ к данным, нарушение «цепочки сохранности», использование несертифицированных программно-аппаратных средств, недостаточная фиксация технических параметров и вмешательство в системные файлы без процессуальных оснований. Предложен алгоритм минимизации данных рисков, включающий пять этапов: подготовительный, технический, документирование, хранение и передача цифровых данных, подготовка к судебному исследованию. Обоснована необходимость стандартизации участия специалистов и внедрения ведомственных инструкций, а также разработки судебных стандартов допустимости цифровых доказательств. Предложенные алгоритм и комплекс процессуальных и технических мер могут служить основой для совершенствования ведомственных регламентов и выработки единой судебной практики по оценке цифровых доказательств, обеспечивая их эффективное использование в уголовном судопроизводстве.

Ключевые слова: *цифровая информация, цифровые доказательства, оперативно-розыскная деятельность, допустимость доказательств, «цепочка сохранности», мессенджеры и социальные сети, инициативная аналитика, уголовное судопроизводство*

Для цитирования: Жандров В.Ю. Обеспечение доказательственного значения цифровой информации, получаемой при проведении оперативно-розыскных мероприятий / В.Ю. Жандров. – DOI 10.33184/pravgos-2026.1.24 // Правовое государство: теория и практика. – 2026. – № 1. – С. 233–246.

judicial authorization to access data, breach of the "chain of custody", use of uncertified software and hardware, insufficient recording of technical parameters, and interference with system files without procedural grounds. The article proposes an algorithm for minimizing these risks, comprising five stages: preparatory, technical, documentation, storage and transfer of digital data, and preparation for forensic examination. Additionally, the article substantiates the need for standardizing specialist participation and implementing departmental instructions, as well as developing judicial standards for the admissibility of digital evidence. The proposed algorithm and the set of procedural and technical measures can serve as a basis for improving departmental regulations and developing a unified judicial practice for evaluating digital evidence, ensuring its effective use in criminal proceedings.

Keywords: *digital information, digital evidence, operative investigative activities, admissibility of evidence, chain of custody, messengers and social networks, proactive analytics, criminal proceedings*

For citation: Zhandrov V.Yu. Ensuring the Evidential Value of Digital Information Obtained During Operative Investigative Activities. *The Rule-of-Law State: Theory and Practice*, 2026, no. 1, pp. 233–246. (In Russian). DOI 10.33184/pravgos-2026.1.24.

Введение

Цифровая трансформация в XXI в. стала определяющим фактором развития социума и государства. Стремительное распространение интернет-сервисов, мессенджеров и социальных сетей не только изменило привычные формы коммуникации, но и сформировало новые модели экономической, профессиональной и досуговой активности. Сегодня информационное пространство превратилось в ключевую среду человеческого взаимодействия и оказывает влияние на все уровни общественных отношений. Однако вместе с новыми возможностями цифровизация создала и дополнительные риски: киберпространство стало ареной для совершения преступлений, а традиционные формы противоправной деятельности получили новые возможности для маскировки, координации и легализации доходов.

В этой связи особую значимость приобретает проблема обращения с цифровыми доказательствами в уголовном судопроизводстве. Их нематериальная природа, подверженность изменениям даже при минимальном вмешательстве, зависимость от программно-технических средств и специфические условия доступа требуют иных подходов, чем при работе с традиционными вещественными доказательствами. От корректности извлечения, фиксации и верификации цифровой информации напрямую зависит возможность установления истины по делу, а следовательно, и обеспечение принципов справедливости и законности в уголовном процессе.

На этом фоне значительно возрастает актуальность проблемы обеспечения доказательственного значения цифровой информации, получаемой при проведении оперативно-розыскных мероприятий (далее – ОРМ), что подтверждается целым рядом обстоятельств.

Во-первых, наблюдается устойчивый рост киберпреступлений, использования цифровых технологий в качестве вспомогательного инструмента при совершении преступлений общеуголовного характера. Кроме того, значительная часть уголовных дел последних лет имеет цифровые следы – переписку в мессенджерах, электронные письма, сведения из социальных сетей, данные о геолокации, электронные платежи. От корректности извлечения и закрепления таких следов зависит возможность установления истины по делу.

Во-вторых, судебная практика свидетельствует о том, что значительная доля цифровых доказательств не приобщается к материалам уголовных дел по процессуальным основаниям. Наиболее распространенными причинами являются:

1) проведение ОРМ, требующих судебного разрешения (например, снятие информации с технических каналов связи), без его получения либо с нарушением установленной процедуры получения разрешения (ст. 8, 9 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», далее – Закон «Об ОРД»). Например, отсутствие судебного разрешения при доступе к данным, защищенным тайной переписки или находящимся на удаленных серверах;

2) оформление результатов ОРМ без соблюдения требований к акту (неуказание даты, времени, места, примененных технических средств), отсутствие в акте/протоколе сведений о примененных средствах, версиях программ, методах извлечения;

3) невозможность установить, что именно сотрудники, уполномоченные на проведение ОРМ, имели доступ к данным (размытость «цепочки сохранности»);

4) вмешательство в системные файлы устройства без надлежащей фиксации и без процессуальных оснований, несоблюдение «цепочки сохранности», когда невозможно установить, кто, когда и с какой целью получил доступ к цифровым данным;

5) использование несертифицированного программного обеспечения без возможности проверки алгоритма его работы, использование не прошедших сертификацию или не включенных в установленный перечень технических средств, что ставит под сомнение достоверность полученной информации;

6) выход оперативных сотрудников за пределы санкционированного объема вмешательства (например, фиксация данных, не относящихся к предмету проверки или к конкретному лицу).

В результате следствие и суд лишаются возможности использовать ценные сведения, а справедливость судебного разбирательства оказывается под угрозой.

В-третьих, действующее законодательство Российской Федерации не содержит единой и четкой системы регулирования вопросов допустимости цифровых доказательств. В УПК РФ и Законе «Об ОРД» закреплены лишь общие положения, тогда как многие конкретные вопросы остаются на усмотрение правоприменителя. Это порождает неоднородность практики, противоречия в судебных решениях и снижает доверие к результатам уголовного судопроизводства.

Таким образом, актуальность исследования обусловлена необходимостью выработки теоретических и прикладных подходов к обеспечению сохранности и допустимости цифровых доказательств, получаемых в рамках ОРМ и следственных действий, с опорой на современные аналитические концепции и инфраструктурные решения.

В отечественной науке внимание к цифровым доказательствам возросло в последние два десятилетия. Работы исследователей посвящены вопросам правового режима цифровой информации, особенностям ее извлечения и фиксации, проблемам квалификации специалистов, допустимости электронных доказательств в гражданском и уголовном процессе.

Так, ряд ученых отмечают, что цифровые следы трансформируются в электронные доказательства, а основными способами их получения являются изъятие носителей и копирование информации, требующие строгого соблюдения процессуальной формы [1, с. 86–87].

Проблема доступа к зашифрованным данным и их использования в качестве дока-

зательств – предмет активного обсуждения. По мнению А.Л. Осипенко и В.Ф. Луговика, необходимость обеспечения конфиденциальности цифровых коммуникаций неизбежно вступает в противоречие с задачами раскрытия преступлений. Авторы подчеркивают, что развитие криминалистических методов и совершенствование правовой регламентации являются необходимыми условиями для минимизации риска утраты доказательственного значения цифровой информации [2, с. 63].

Большой вклад в исследование данной проблематики внес А.Н. Першин. Он обосновал значение анализа документированной информации как методологической основы получения криминалистически значимых сведений [3; 4].

Особое место в развитии теории оперативно-розыскной информации занимает фундаментальная монография С.С. Овчинского «Оперативно-розыскная информация» (2000), в которой впервые в открытой печати представлены результаты комплексных исследований в сфере информационного обеспечения оперативно-розыскной деятельности [5]. Одновременно в научной литературе акцентируется правовая неопределенность понятия «оперативно-розыскная информация» и высказываются предложения о формировании частной теории оперативно-розыскной информации с учетом реалий цифрового общества [6].

Судебная практика России последних лет демонстрирует постепенное формирование подходов к оценке цифровых доказательств. Однако эти решения зачастую носят казуистический характер и не образуют целостной системы. В итоге степень разработанности проблемы можно охарактеризовать как недостаточную: при наличии фундаментальных теоретических положений отсутствует единый комплексный подход, охватывающий весь цикл обращения с цифровыми доказательствами – от извлечения до судебной верификации – при одновременной интеграции аналитических и инфраструктурных требований.

Обращение к мнению экспертов позволило определить основные пути снижения рисков признания цифровой информации недопустимой. Наиболее значимым из них является выполнение четырех групп условий документирования, повышающих степень верификации цифровых следов преступной деятельности.

Технические параметры извлечения и фиксации цифровых данных

Особое значение имеет подтверждение времени и выбор допустимого источника цифровых сведений, а также применение криптографических методов верификации – хеширования, используемого для подтверждения неизменности данных, логирования, заключающегося в ведении подробного журнала всех действий, связанных с их обработкой, скринкаста (записи информации, отображаемой на экране компьютера, включая текстовые и голосовые комментарии) – и определения порядка хранения данных.

Извлечение цифровых данных при проведении ОРМ или следственных действий требует определения и соблюдения технически допустимых способов доступа к ним, обеспечивающих сохранность полученной информации. Сохранность информации – важная процессуальная гарантия допустимости формируемого доказательства.

Для систематизации методов извлечения цифровой информации в криминалистике принято выделять три уровня доступа.

Первый уровень, визуальный, предполагает считывание информации непосредственно с экрана устройства без применения специализированных средств. Он ограничен функционалом операционной системы и приложений, но может использоваться для фиксации открытой переписки в рамках осмотра. Доступным способом извлечения цифровой переписки на данном уровне является снимок с экрана устройства (скриншот) – запечатление (снятие) информации, отображаемой на экране устройства, посредством его клавиатуры или сенсорного экрана. Информация фиксируется без подключения устройства к другим системам и без изменения данных на носителе. Преимущество состоит в простоте и универсальности, недостаток – в ограниченности объема и невозможности получить удаленные или скрытые сообщения.

Суды все чаще рассматривают переписку в WhatsApp[1], Telegram, Signal и других приложениях как возможное доказательство, однако при этом обращают внимание на про-

1 Принадлежит компании Meta, признанной экстремистской и запрещенной в Российской Федерации.

цессуальную форму ее получения и на то, подтверждается ли она другими материалами дела. Фиксация электронных сообщений с помощью скриншотов приобретает особое значение. Верховный Суд РФ в своих разъяснениях указал, что такие доказательства могут признаваться допустимыми, если они оформлены надлежащим образом: на скриншоте отображены адрес интернет-страницы, дата и время его создания, а также подтверждена принадлежность зафиксированной переписки конкретному электронному устройству. Заверение скриншотов нотариусом не требуется – достаточно подписи стороны или ее процессуального представителя[2].

В определении от 7 февраля 2023 г. по делу № 5-КГ22-144-К2 Верховный Суд РФ указал, что скриншоты переписки могут рассматриваться как письменные доказательства в понимании ст. 55 и 71 ГПК РФ, а отсутствие нотариального удостоверения не является основанием для отказа в их приобщении[3]. Решения нижестоящих судов, формально отказавших в их исследовании, были признаны нарушившими право стороны на справедливое судебное разбирательство. Верховный Суд РФ подчеркнул, что достоверность скриншотов подлежит проверке в совокупности с другими доказательствами по делу, а не исключается автоматически из-за отсутствия формального заверения. Эта позиция имеет универсальное значение: она применима не только в гражданском, но и в уголовном процессе, где вопросы допустимости цифровых доказательств должны решаться исходя из их происхождения, процессуального порядка фиксации и соотнесения с иными материалами дела.

Выработанные в гражданском и арбитражном процессе подходы находят прямое отражение и в уголовном судопроизводстве, где допустимость цифровых доказательств во многом зависит от надлежащего процессуального оформления. Если при производстве следственных действий (осмотра, выемки, обыска) делаются скриншоты переписки с электронных устройств, их допустимость в суде будет обеспечена при условии соблюдения следующих требований: фиксация технических параметров устройства, отражение времени и даты создания изображения, подтверждение отсутствия возможности его последующего изменения. В совокупности с другими материалами дела такие доказательства могут служить основанием для формирования обвинения.

Второй уровень – логический. Он связан с доступом к файловой системе устройства, осуществляемым с использованием специализированного программного обеспечения, что позволяет копировать каталоги и файлы, включая удаленные, но не перезаписанные. Данный подход применяется при подключении устройства к рабочей станции специалиста или при его синхронизации с компьютером. Так, экспорт чатов Telegram Desktop осуществляется с использованием персонального компьютера специалиста и записывается на внешний носитель информации (оптический диск, флеш-накопитель). Другой способ выгрузки – через устройство лица, в отношении которого проводится проверка, – позволяет использовать авторизованные сессии для экспорта переписки, но несет риск автоматического перезаписывания данных на диске при сохранении файлов. На рабочем столе создается папка с извлеченной перепиской, а устройство, с которого получена эта информация, изымается с целью дальнейшего изучения уже в лабораторных условиях. Основной недостаток данного способа: при экспортировании переписки возможна потеря оперативно значимой информации, поскольку при сохранении новых файлов на компьютере автоматически удаляются и перезаписываются прежние данные.

Третий уровень – физический, предполагающий создание точной посекторной копии (дампа) носителя, что обеспечивает возможность восстановления удаленных данных, но требует высокой квалификации специалиста, применения блокираторов записи и оборудования для снятия образов.

2 О некоторых вопросах применения законодательства о компенсации морального вреда : постановление Пленума Верховного Суда РФ от 01.06.2023 № 15, п. 43, 55 // Доступ из справ.-правовой системы «КонсультантПлюс» ; О некоторых вопросах применения законодательства о договоре строительного подряда : постановление Пленума Верховного Суда РФ от 15.11.2022 № 33, п. 66 // Доступ из справ.-правовой системы «КонсультантПлюс».

3 Определение Верховного Суда РФ от 07.02.2023 № 5-КГ22-144-К2 [Электронный ресурс]. URL: https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-07022023-n-5-kg22-144-k2/ (дата обращения: 18.08.2025).

Разграничение вышеназванных уровней универсально и отражено в методических руководствах Министерства юстиции США[4], глобальных рекомендациях Интерпола[5], а также в аналитических обзорах по судебной информатике[6]. Встраивание рассматриваемой классификации в российский алгоритм работы следователя и специалиста позволяет четко разграничивать методы, применяемые без судебного разрешения, и методы, требующие отдельной санкции (например, при удаленном доступе к «облачным» сервисам по правилам ст. 185 и 186 УПК РФ).

Ключевым условием признания цифровых доказательств допустимыми выступает обеспечение сохранности информации в момент начала доступа к электронному носителю. Даже минимальные изменения, включая непреднамеренные, могут исказить структуру данных или привести к перезаписи удаленных файлов, что осложнит их последующее восстановление и вызовет сомнения в достоверности полученных сведений.

В связи с этим в криминалистической практике используются следующие меры: а) применение аппаратных блокираторов записи при подключении носителей (SATA, IDE, USB) через высокоскоростные интерфейсы; б) использование программных блокираторов записи (например, USB Write Blocker, WinFE Write Protect Tool), запускаемых до подключения устройства; в) обязательное отключение устройства от сети Интернет (режим «в самолете», отключение wi-fi, извлечение sim-карты) для исключения возможности удаленного изменения или удаления данных; г) изоляция устройства в экранированных контейнерах («клетка Фарадея») либо применение средств подавления радиосигнала. Эти меры должны фиксироваться документально, поскольку напрямую влияют на последующую оценку доказательств судом (ст. 75 УПК РФ).

При преодолении паролей или иных механизмов аутентификации для получения доступа к цифровым данным также применяются специализированные средства: программные (загрузочные среды Windows Forensic Environment, Kali Linux в режиме forensics, эксплойты уязвимостей checkm8 для iOS, аппаратные уязвимости MTK-чипсетов для Android, специализированные утилиты сброса паролей Elcomsoft System Recovery, KonBoot); аппаратные (подключение через JTAG, chip-off с последующим чтением памяти программатором); комбинированные (использование аппаратных средств для снятия дампа памяти с последующей расшифровкой специализированным программным обеспечением).

Применение специализированных загрузочных сред и эксплойтов может повлечь изменение содержимого системных файлов и даже блокировать доступ к части пользовательских данных (например, к сохраненным паролям браузеров). Поэтому в случае их применения рекомендуется работать на изолированных от сети рабочих станциях, использовать только сертифицированное программное обеспечение и оборудование, вести непрерывную видеозапись процесса. Эти меры позволяют воспроизвести действия специалиста при судебной проверке, подтвердить техническую корректность полученных данных и обеспечить допустимость цифровых доказательств в судебном процессе.

Привлечение специалиста

Согласно Закону «Об ОРД» и УПК РФ извлечь цифровую информацию может оперативный сотрудник или следователь. Однако технически сложные действия разрешается выполнять привлекаемым специалистом (ст. 6, 7, 8 Закона «Об ОРД», ч. 6 ст. 164, ч. 1 ст. 164.1 УПК РФ).

Недосказанность Закона «Об ОРД» в части статуса и требований к специалисту компенсируются положениями, выработанными правоохранительной теорией и практикой. Специалистом принято считать лицо, обладающее научными, техническими либо ины-

4 U.S. Department of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Washington: NIJ, 2004 [Электронный ресурс]. URL: https://www.ojp.gov/pdffiles1/nij/199408.pdf (дата обращения: 16.08.2025).

5 INTERPOL. Global Guidelines for Digital Forensics Laboratories. Lyon: INTERPOL, 2020 [Электронный ресурс]. URL: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics (дата обращения: 16.08.2025).

6 Percipient. Overview: The Three Types of Forensic Collections (Physical vs. Logical vs. Targeted). 2019 [Электронный ресурс]. URL: https://percipient.co/overview-the-three-types-of-forensic-collections-physical-vs-logical-vs-targeted (дата обращения: 16.08.2025).

ми специальными знаниями, умениями и навыками, допущенное к участию в проведении ОРМ [7, с. 290; 8, с. 32], выступающее субъектом криминалистического обеспечения ОРД и, что особенно процедурно важно, имеющее правовой статус лица, оказывающего содействие органам, осуществляющим ОРД (ст. 17 Закона «Об ОРД») [9, с. 99].

В системе МВД России в качестве специалистов привлекаются сотрудники экспертно-криминалистических подразделений. Соответствующая организационная модель была создана приказом МВД России от 25 ноября 2019 г. № 878[7], предусматривающим включение экспертно-криминалистических подразделений в контур межведомственного обмена, создание специализированных подразделений и упорядочения технико-криминалистического обеспечения расследования IT-преступлений. Вне системы МВД России в качестве специалистов привлекаются государственные судебные эксперты (правовой статус установлен Федеральным законом от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»), сотрудники IT-подразделений правоохранительных органов, а также сертифицированные специалисты по информационной безопасности.

Основные формы участия специалистов при осуществлении ОРД: консультации, проведение исследований, техническая помощь, непосредственное участие при проведении ОРМ [10, с. 68]. При производстве следственных и иных процессуальных действий специалисты привлекаются по правилам ст. 58 УПК РФ.

Ключевое условие выбора специалиста – наличие у кандидата знаний и навыков работы с цифровыми носителями, в том числе с применением сертифицированных аппаратно-программных средств, что гарантирует правильность фиксации данных и исключает претензии по поводу их изменения. В контексте документирования и формирования цифровых доказательств это особенно важно, поскольку соблюдение методики извлечения данных напрямую зависит от квалификации исполнителя и использования им специализированных средств. Например, при снятии физического образа носителя специалист обязан применять аппаратные или программные блокираторы записи, сертифицированные в установленном порядке, что исключает внесение изменений в данные и предотвращает автоматическую перезапись удаленной информации.

Специалист также выполняет комплекс подготовительных мероприятий: отключает устройство от сетей передачи данных, фиксирует технические характеристики носителя (модель, серийный номер, интерфейс подключения), проверяет целостность корпуса и пломб, рассчитывает контрольные хэш-суммы до и после извлечения. Эти сведения отражаются в протоколе (акте) ОРМ[8] либо процессуального действия (ст. 166–167 УПК РФ) и являются ключевыми для подтверждения неизменности цифровых доказательств (ст. 75, 89 УПК РФ).

Независимо от формы мероприятия привлечение квалифицированного специалиста позволяет не только минимизировать риск утраты или изменения информации, но и обеспечить надлежащую фиксацию всех примененных программно-аппаратных средств (наименование, версия, лицензионный статус), что повышает доверие суда к достоверности полученных данных и способствует признанию их допустимыми доказательствами.

Обеспечение возможности проведения независимой экспертной проверки собранных цифровых данных

Независимая экспертная проверка цифровых данных также выступает значимым условием их допустимости и достоверности.

7 Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий» : приказ МВД России от 25.11.2019 № 878 // Доступ из справ.-правовой системы «КонсультантПлюс».

8 Об утверждении Инструкции о порядке проведения сотрудниками органов внутренних дел Российской Федерации гласного оперативно-розыскного мероприятия обследование помещений, зданий, сооружений, участков местности и транспортных средств и Перечня должностных лиц органов внутренних дел Российской Федерации, уполномоченных издавать распоряжения о проведении гласного оперативно-розыскного мероприятия, обследование помещений, зданий, сооружений, участков местности и транспортных средств : приказ МВД России от 01.04.2014 № 199 (ред. от 13.10.2023) [Электронный ресурс] // Офиц. интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 17.08.2025).

Она предполагает организацию такого порядка сбора, фиксации и хранения цифровых сведений, при котором третьи лица – судебные эксперты или специалисты – смогут объективно воспроизвести совершенные действия и подтвердить полученные результаты. В противном случае цифровые материалы теряют доказательственную ценность, так как исключается возможность их верификации в условиях состязательного процесса.

В отечественной литературе подчеркивается, что электронные доказательства являются особо уязвимым объектом исследования: даже простейшие действия с носителем (например, включение компьютера) могут повлечь изменения в содержании документа или его реквизитах. Эти обстоятельства требуют от суда и экспертов строгого соблюдения процессуальных гарантий сохранности таких данных. В частности, необходимо назначение экспертизы на ранней стадии процесса, выбор квалифицированных специалистов и использование процедур, исключающих искажение информации. Как отмечает М.А. Митрофанова, именно надлежащее обращение с электронными доказательствами и фиксация всех условий их исследования позволяют обеспечить возможность последующей независимой проверки и тем самым гарантировать допустимость результатов экспертизы [11].

Особого внимания требует вопрос методического обеспечения судебной экспертизы цифровых данных. В современной литературе подчеркивается, что процесс выбора и применения методов исследования должен быть формализован и поддаваться проверке. Так, А.А. Шелупанов и А.Р. Смолина обосновывают необходимость выстраивания четкой последовательности действий на подготовительной стадии экспертизы: от анализа постановления о назначении экспертизы и материалов дела до осмотра объектов и планирования дальнейших шагов. Такой регламент позволяет эксперту заблаговременно определить пригодность представленных материалов, оценить необходимость использования специальных средств и заявить ходатайства о применении частично разрушающих методов, если без них невозможно провести исследование [12].

Идея автоматизации выбора методик и построения их формализованных моделей получила развитие. Исследователи предлагают использовать классификацию методик по задачам и объектам экспертизы и представлять их в виде структурированных моделей, позволяющих фиксировать последовательность действий с учетом ограничений времени, ресурсов и применимости методов. Такой подход обеспечивает прозрачность экспертных действий и делает их воспроизводимыми в случае назначения повторной или дополнительной экспертизы [13]. Следовательно, надлежащее методическое обеспечение, как в части регламентации подготовительных действий, так и в части формализации выбора методов исследования, выступает гарантией проверяемости и воспроизводимости судебной компьютерно-технической экспертизы, а значит, необходимым условием для признания цифровых данных допустимыми доказательствами.

Применение формализованных методик компьютерно-технической экспертизы обеспечивает воспроизводимость и проверяемость экспертных действий, что имеет ключевое значение для соблюдения процессуальных гарантий допустимости доказательств. Использование структурированного алгоритма и документирование всех стадий исследования позволяет суду и сторонам убедиться в достоверности заключения и при необходимости инициировать его независимую проверку. Практика экспертных организаций показывает, что такие подходы не только реализуемы, но и повышают качество и эффективность экспертной деятельности, что усиливает доверие суда к представленным цифровым доказательствам [14].

Таким образом, независимая экспертная проверка цифровых данных возможна лишь при соблюдении комплекса процессуальных условий, обеспечивающих сохранность и воспроизводимость данных. К их числу относятся закрепление первоначального состояния носителей, контроль целостности информации, соблюдение «цепочки сохранности», применение сертифицированных средств и формализованных методик исследования. Выполнение указанных требований обеспечивает суд и участников процесса возможностью объективной проверки достоверности цифровых доказательств и служит гарантией их допустимости.

Соблюдение правового режима доступа к цифровой информации

Современный этап развития цифровых технологий и активное использование электронных коммуникаций привели к кардинальному изменению форм и способов фиксации информации, обладающей доказательственным значением в уголовном судопроизводстве. Особую актуальность имеет переписка через мессенджеры и иные интернет-сервисы, поскольку нередко она содержит сведения, прямо указывающие на обстоятельства совершения преступлений, планы их подготовки, участников и другие значимые факты. В связи с этим все чаще в рамках проведения обследования помещений, строений, участков местности либо в ходе обыска и выемки сотрудники оперативных подразделений обнаруживают и получают доступ к электронным устройствам – стационарным компьютерам, ноутбукам, планшетным компьютерам, принадлежащим задержанным. После получения физического и программного доступа к устройству встает вопрос о порядке извлечения данных, в первую очередь переписки в мессенджерах (WhatsApp[9], Telegram, Signal и др.), а также о правомерности данных действий в контексте оперативно-розыскного и уголовно-процессуального законодательства.

Конституционный Суд РФ исходит из того, что при добровольной огласке одним из участников коммуникации сведения перестают быть тайной для третьего лица (государственного органа), что меняет режим доступа. В таком случае получение и использование этих сведений не нарушает тайну переписки иных лиц, если соблюдены процессуальные требования[10]. Другие выводы Конституционного Суда РФ: а) «онлайновое» извлечение/дозагрузка с серверов (включая сведения о соединениях, контент из облака) – сфера судебной санкции (ст. 185–186.1 УПК РФ); б) изучение локально доступной информации на изъятом устройстве – в общем случае по правилам осмотра/экспертизы, без отдельного судебного решения, но с соблюдением гарантий фиксации и сохранности (протокол, участие специалиста и пр.)[11].

Соблюдение законности при доступе к цифровой оперативной информации зависит от способа ее получения.

1. Прямой доступ к открытым данным. Если переписка отображается на экране и необходимые сообщения уже загружены в оперативную память устройства, их фиксация допустима в рамках ОРМ обследование помещений, зданий, сооружений, участков местности и транспортных средств (ст. 6, 8 Закона «Об ОРД»). В таких случаях допускается фотографирование, видеосъемка либо составление акта ОРМ, поскольку речь идет о визуальном уровне доступа и дополнительного судебного разрешения к имеющейся санкции руководителя органа, правомочного на осуществление ОРД, не требуется. Аналогично строится работа и при обыске (ст. 182 УПК РФ), когда осматривается обнаруженное устройство. В этом случае запись информации (фотографирование, видеосъемка, составление протокола с дословным воспроизведением текста сообщений) не приводит к установлению нового соединения с сервером, не затрагивает тайну переписки сверх объема уже доступных данных и потому не требует получения дополнительного судебного разрешения.

2. Удаленный доступ к данным. Любые действия, направленные на получение сообщений, отсутствующих во временном хранилище данных (прокрутка чата для загрузки прежних сообщений, скачивание вложений (фото, видео, документов), переход в архивные чаты) фактически представляют собой удаленный доступ к информации. Такие действия связаны с установлением нового соединения с сервером, выходят за пределы визуального уровня и квалифицируются как вмешатель-

9 Принадлежит компании Meta, признанной экстремистской и запрещенной в Российской Федерации.

10 Об отказе в принятии к рассмотрению жалобы гражданки Дьячковой Ольги Геннадьевны на нарушение ее конституционных прав пунктами 6 и 14 части первой и частью четвертой статьи 6, пунктом 3 статьи 7, частью второй статьи 8 Федерального закона «Об оперативно-розыскной деятельности», частью второй статьи 7, пунктом 4 части второй статьи 38, статьями 125, 140 и 146 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 16.11.2006 № 454-О // Доступ из справ.-правовой системы «КонсультантПлюс».

11 Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 25.01.2018 № 189-О [Электронный ресурс]. URL: https://legalacts.ru/kodeks/UPK-RF/chast-2/razdel-viii/glava-24/statja-176/#101325 (дата обращения: 17.08.2025).

ство в сферу частной коммуникации, что требует судебной санкции (ст. 23 Конституции РФ, ст. 8 Закона «Об ОРД», ст. 186 УПК РФ).

Такие же правила действуют при извлечении данных из «облачных» сервисов (резервных копий в iCloud, Google Drive, «облачных» архивов мессенджеров), для чего также необходима санкция суда. Подобный доступ предполагает установление соединения с серверами и затрагивает тайну переписки, что накладывает дополнительные процессуальные ограничения. Это касается и режима использования модуля «Облачные сервисы» в «Мобильном криминалисте», обеспечивающего логический и физический доступ к резервным копиям в iCloud, Google Drive, WhatsApp[12], Telegram. Для работы с такой информацией требуется ввод учетных данных, прохождение двухфакторной аутентификации и судебное разрешение. Все действия протоколируются с обязательным участием представителей общественности либо понятых, вносятся в акт обследования/протокол обыска, сопровождаются фото- и видеосъемкой, а также подробным описанием порядка получения информации. Следует учитывать, что при входе в аккаунт с нового устройства доступ к истории переписки можно получить лишь спустя некоторое время (до 24 часов), что важно для процессуального планирования.

Для минимизации процессуальных рисков рекомендуется:

– незамедлительно зафиксировать состояние переписки на момент ее обнаружения с помощью фото- и видеосъемки, включая отображение даты, времени и идентификатора чата;

– убедиться, что в момент фиксации устройство отключено от сетей передачи данных (wi-fi, мобильный интернет, Bluetooth) либо помещено в экранированный контейнер («клетка Фарадея») для исключения автоматической синхронизации или изменения содержимого чата;

– сохранить текущий объем данных в неизменном виде, не производя дозагрузку истории до получения соответствующего судебного разрешения;

– отразить в протоколе либо в акте ОРМ не только содержание переписки, но и технические параметры устройства (модель, операционная система, версия мессенджера), а также факт отсутствия соединения с сетью во время фиксации.

Такая детализация позволит в дальнейшем подтвердить, что полученная информация соответствует состоянию переписки в момент изъятия устройства и не была изменена в результате неконтролируемой синхронизации или целенаправленных действий сотрудников. Одновременно это обеспечит допустимость сведений, полученных в рамках ОРМ, как ориентировочной информации для последующих следственных действий.

3. Доступ с преодолением защиты («взлом»). Поскольку обход защиты часто предполагает вмешательство в программную или аппаратную среду устройства, получение доступа к защищенным данным предполагает вторжение в конституционно охраняемую сферу частной жизни и потому должен выполняться в рамках реализуемого с санкции суда ОРМ (ст. 8, 9 Закона «Об ОРД»), а при производстве следственного действия – при наличии судебного решения (ст. 165, 186 УПК РФ). Исключения возможны лишь в неотложных случаях, когда промедление может привести к утрате критически важной информации, и с обязательным последующим получением судебного разрешения. При преодолении защиты устройств следует зафиксировать в протоколе основания для обхода защиты.

«Взлом» потенциально изменяет системные файлы, конфигурацию операционной системы и может привести к утрате или изменению зашифрованных данных, в том числе сохраненных паролей, ключей шифрования и токенов доступа. Для обеспечения правовых гарантий документирования цифровой информации путем преодоления защиты данных необходимо:

– фиксировать в акте/протоколе наименование, версию и разработчика примененных средств, а также алгоритм действий специалиста/эксперта;

– указывать все изменения, внесенные в системные файлы или конфигурацию устройства;

– сохранять контрольные хэш-суммы извлеченных образов до и после совершения действий по разблокировке, чтобы подтвердить неизменность пользовательских данных;

12 Принадлежит компании Meta, признанной экстремистской и запрещенной в Российской Федерации.

– при наличии возможности выполнять полное резервное копирование (физический образ) до начала процедур по обходу защиты.

Также, если устройство уже изъято на законных основаниях (например, при обыске или выемке), следователь вправе назначить судебную компьютерно-техническую экспертизу (ст. 195–196 УПК РФ). В этом случае эксперт действует в пределах процессуального поручения и применяет необходимые технические методы, включая обход защиты, без отдельного судебного решения.

Конституционный Суд РФ подтвердил, что получение информации, уже находящейся в электронной памяти устройства, изъятого и осматриваемого по правилам УПК РФ, не требует отдельного судебного решения. Это может быть осмотр (ст. 176–178 УПК РФ) и/или последующая экспертиза (ст. 195–207 УПК РФ). В одном из своих определений Конституционный Суд РФ указал, что при соблюдении процессуальной формы и гарантий прав участников «специальная санкция суда» не нужна именно на изучение памяти носителя, который уже изъят в установленном порядке[13]. Таким образом, судебная санкция необходима для доступа к информации, но не для ее исследования экспертом после законного изъятия носителя.

Тот же подход сохранен в практике Верховного Суда РФ, который в кассационном определении от 30 сентября 2014 г. № 2-18/08 констатировал, что осмотр мобильного телефона, изъятого у владельца и исследованного по правилам ст. 176 УПК РФ, не требует самостоятельного судебного решения[14]. Эта позиция повторена в 2019 г. в апелляционном определении от 1 августа № 2-003/2018. Верховный Суд РФ вновь подтвердил отсутствие необходимости в отдельной санкции для осмотра технических устройств и содержащейся в них информации, если носители изъяты процессуально корректно[15]. Таким образом, когда следователь действует в рамках осмотра уже изъятого устройства и не устанавливает новое соединение с серверами/сервисами, отдельной санкции, как правило, не требуется.

Заключение

Извлечение и процессуальное закрепление цифровых следов преступной деятельности представляет собой сложный комплекс правовых и технических задач. Особенности архитектуры современных сервисов – распределенное хранение данных, сквозное шифрование, многофакторная аутентификация – предопределяют необходимость применения специальных программно-аппаратных средств и привлечения квалифицированных специалистов.

Вместе с тем отсутствие унифицированных методических процедур, четкой регламентации правового статуса отдельных действий (осмотр, выемка, контроль и запись переговоров), а также единых стандартов фиксации и хранения цифровых данных создает риск признания полученной информации недопустимой. Судебная практика подтверждает, что нарушение процессуальной формы, недостаточная фиксация технических параметров или вмешательство в данные без надлежащих правовых оснований могут привести к утрате информацией доказательственного значения.

Минимизировать риски процедурных нарушений может принятие алгоритма обеспечения допустимости цифровых доказательств, включающего пять основных этапов.

Первый этап, подготовительный, состоит в выборе и надлежащем правовом обеспечении реализации ОРМ, следственных действий, в рамках которого осуществляется получение цифровой информации (контроль и запись переговоров, осмотр, выемка), получении при необходимости судебного решения на его проведение, привлечении специалиста.

Второй этап, технический, заключается в отключении устройства от сетей передачи

13 Об отказе в принятии к рассмотрению жалобы гражданина Брянцева А.Ю. на нарушение его конституционных прав пунктом 7 части второй статьи 29, частями первой и второй статьи 75, частями первой, четвертой и пятой статьи 165 и частью третьей статьи 183 УПК РФ : определение Конституционного Суда РФ от 27.06.2023 № 1773-О [Электронный ресурс]. URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-27062023-n-1773-o/ (дата обращения: 17.08.2025).

14 Кассационное определение Верховного Суда РФ от 30.09.2014 по делу № 2-18/08 [Электронный ресурс]. URL: https://sudact.ru/vsrf/doc/0dPzawB0fmm6/?vsrf-txt=&vsrf-case_doc=2-18%2F08&vsrf-lawchunkinfo=&vsrf-date_from=&vsrf-date_to=&vsrf-judge=&_=1755454649779 (дата обращения: 17.08.2025).

15 Апелляционное определение Судебной коллегии по уголовным делам от 01.08.2019 № 67-АПУ19-8 по делу № 2-003/2018 [Электронный ресурс]. URL: https://sudact.ru/vsrf/doc/0CTvl5sbeaxc/?vsrf-txt=&vsrf-case_doc=2-003%2F2018&vsrf-lawchunkinfo=&vsrf-date_from=&vsrf-date_to=&vsrf-judge=&_=1755457357391 (дата обращения: 17.08.2025).

данных, применении блокираторов записи, использовании «клетки Фарадея» при работе с мобильными устройствами. Затем – извлечение данных – фиксирование всех технических параметров и расчет контрольных хэш-сумм с применением сертифицированных программно-аппаратных средств.

Третий этап – документирование. Его назначение состоит в фиксации методики получения информации, используемых технических средств и условий сохранности данных, что обеспечивает воспроизводимость действий и непрерывность «цепочки сохранности». В акте ОРМ или протоколе следственного действия указываются правовое основание производства, состав участников (включая специалиста, с описанием его компетенции), объект и способ доступа (устройство, аккаунт, сервис), а также меры неизменности информации – отключение сетевых интерфейсов, применение блокираторов записи и др. Обязательно фиксируются программные средства: их название, версия, настройки и последовательность применения. К протоколу прилагаются логи, фото- и видеозапись, хэш-суммы файлов до и после обработки.

Документирование должно завершаться перечнем артефактов (файлы, базы данных, дампы, переписки) с указанием их формата, размера и контрольных сумм, а также сведений о «цепочке сохранности» носителей и их передаче между уполномоченными лицами. При работе с мессенджерами или облачными сервисами отражаются идентификаторы чатов, дата и время фиксации, состояние сетевых соединений, а при извлечении удаленных данных – реквизиты судебной санкции.

Таким образом, документирование выступает центральным элементом алгоритма минимизации рисков процедурных нарушений. Оно объединяет технические и юридические средства фиксации, исключает возможность изменения цифровых данных и гарантирует их допустимость в качестве доказательств.

Четвертый этап, хранение и передача цифровой информации, сводится к обеспечению целостности данных при передаче между подразделениями, фиксации всех изменений местонахождения и ответственных лиц.

Пятый этап – подготовка к судебному исследованию. На этом этапе обеспечивается возможность воспроизведения процедуры извлечения данных и независимой проверки их неизменности.

Соблюдение рассмотренных требований формирует документированную цепочку обращения с цифровыми данными, гарантирующую аутентичность и сохранность информации на всех этапах ее движения и позволяющую сохранить ее юридическое значение для последующего включения в уголовное дело без риска признания недопустимой при доказывании. Совокупное применение данных мер и алгоритма устраняет сомнения в достоверности и правомерности получения цифровых доказательств в ходе проведения как оперативно-розыскных мероприятий, так и следственных действий, обеспечивая их надлежащее сохранение для использования в судебном процессе.

До внесения изменений в федеральные законы логично принятие ведомственных инструкций во всех заинтересованных правоохранительных органах. Данные документы должны регламентировать порядок обнаружения, фиксации, передачи и хранения представляющей оперативный интерес цифровой информации, стандартизировать участие специалистов, технические форматы данных и образцы документации. В российской практике разработка таких инструкций может стать мостом между существующей оперативной практикой и будущим нормативным режимом цифровой оперативной информации.

Одновременно с этим важнейшим направлением является формирование судебных стандартов допустимости цифровой информации. Целесообразно инициировать разработку проекта постановления Пленума Верховного Суда РФ по вопросам использования цифровых доказательств, в котором будет закреплен статус цифровой оперативной информации и ее доказательственного значения при условии соблюдения процедурных требований получения и фиксации. Введенный стандарт позволит сформировать устойчивую практику, исключающую произвольное лишение цифровых следов доказательственной силы.

Наконец, ключевым условием устойчивости разрабатываемого режима обращения с цифровой оперативной информацией является его согласование с международными

правовыми стандартами. Работа по гармонизации положений российского законодательства должна заключаться не в механическом заимствовании зарубежных моделей, а в выработке национальной системы, сочетающей универсальные требования к цифровым следам и специфику российской правовой традиции. Формализация цифровой оперативной информации через ее нормирование, регламентацию методов получения, внедрение процессуальных фильтров при соответствии международным стандартам станет важнейшим этапом развития уголовного судопроизводства в эпоху цифровых коммуникаций.

Список источников

1. Дубоносов Е.С. Проблемы сбора цифровой информации в ходе оперативно-розыскной деятельности / Е.С. Дубоносов, Я.С. Титаренко // Актуальные проблемы защиты прав и свобод граждан: историко-теоретические и правовые аспекты : материалы Всероссийской научно-практической конференции, Тула, 28 февраля 2023 г. – Тула : Всероссийский государственный университет юстиции (РПА Минюста России), 2023. – С. 82–88.
2. Осипенко А.Л. Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений / А.Л. Осипенко, В.Ф. Луговик // Общество и право. – 2021. – № 2 (76). – С. 60–68.
3. Першин А.Н. Анализ как метод познания документированной информации / А.Н. Першин // Научный вестник Омской академии МВД России. – 2014. – № 3 (54). – С. 54–58.
4. Першин А.Н. Электронный документ и электронное сообщение: понятие и особенности поиска в электронной среде / А.Н. Першин // Научный вестник Омской академии МВД России. – 2015. – № 3 (58). – С. 34–38.
5. Овчинский С.С. Оперативно-розыскная информация / С.С. Овчинский. – Москва : Инфра-М, 2000. – 367 с.
6. Остапенко П.И. К вопросу о понятии оперативно-розыскной информации / П.И. Остапенко // Юридический вестник Кубанского государственного университета. – 2017. – № 4 (33). – С. 17–18.
7. Шумилов А.Ю. Оперативно-розыскная энциклопедия / А.Ю. Шумилов. – Москва, 2004. – 363 с.
8. Луговик В.Ф. Оперативно-разыскной кодекс Российской Федерации: авторский проект / В.Ф. Луговик. – Омск : Омская юридическая академия, 2014. – 38 с.
9. Горшкова В.С. Специалист как субъект криминалистического обеспечения оперативно-розыскной деятельности органов внутренних дел / В.С. Горшкова // Алтайский юридический вестник. – 2024. – № 2 (46). – С. 95–101.
10. Сенатов А.В. Некоторые аспекты использования оперативными подразделениями помощи специалистов при осуществлении оперативно-розыскной деятельности / А.В. Сенатов, А.А. Чайковский // Вестник Казанского юридического института МВД России. – 2016. – № 4 (26). – С. 68–71.
11. Митрофанова М.А. Особенности экспертизы электронных доказательств в арбитражном процессе / М.А. Митрофанова // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. – 2011. – Т. 11, № 2. – С. 117–119.

References

1. Dubonosov E.S., Titarenko Ya.S. Problems of Collecting Digital Information During Operative Search Activities. *Actual Problems of Protecting the Rights and Freedoms of Citizens: Historical, Theoretical and Legal Aspects. Materials of the All-Russian Scientific and Practical Conference, Tula, February 28, 2023*. Tula, All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) Publ., 2023, pp. 82–88. (In Russian).
2. Osipenko A.L., Lugovik V.F. Problems of Access of Law Enforcement Agencies to Hidden Computer Information When Solving Crimes. *Society and Law*, 2021, no. 2 (76), pp. 60–68. (In Russian).
3. Pershin A.N. Analysis as the Method of Learning Documented Information. *Scientific Bulletin of the Omsk Academy of the Ministry of the Interior of Russia*, 2014, no. 3 (54), pp. 54–58. (In Russian).
4. Pershin A.N. Electronic Document and Electronic Message: Notion and Peculiarities of Search in Electronic Environment. *Scientific Bulletin of the Omsk Academy of the Ministry of the Interior of Russia,* 2015, no. 3 (58), pp. 34–38. (In Russian).
5. Ovchinsky S.S. Operative and Search Information. Moscow, Infra-M Publ., 2000. 367 p.
6. Ostapenko P. I. On the Concept of Operative and Search Information. *Legal Bulletin of the Kuban State University*, 2017, no. 4 (33), pp. 17–18. (In Russian).
7. Shumilov A.Yu. Operative and Search Encyclopedia. Moscow, 2004. 363 p.
8. Lugovik V.F. Operative and Search Code of the Russian Federation: Author's draft. Omsk Law Academy Publ., 2014. 38 p.
9. Gorshkova V.S. Specialist as a Subject of Criminalistic Support for Operational Investigative Activities of Internal Affairs Bodies. *Altai Law Journal,* 2024, no. 2 (46), pp. 95–101. (In Russian).
10. Senatov A.V., Tchaikovsky A.A. Some Aspects of the Use of Specialists' Assistance by Operational Units in the Implementation of Operative and Search Activities. *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 2016, no. 4 (26), pp. 68–71. (In Russian).
11. Mitrofanova M.A. Features of Examination of Electronic Evidence in Arbitration Proceedings. *Izvestiya of Saratov University. Economics. Management. Law*, 2011, vol. 11, no. 2, pp. 117–119. (In Russian).

12. Шелупанов А.А. Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы / А.А. Шелупанов, А.Р. Смолина // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2016. – Т. 19, № 1. – С. 31–34.

13. Шелупанов А.А. Теоретические аспекты автоматизации формирования частных методик производства компьютерно-технической экспертизы / А.А. Шелупанов, А.Р. Смолина // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2016. – Т. 19, № 2. – С. 67–70.

14. Шелупанов А.А. Формальные основы системы поддержки формирования частных методик производства компьютерно-технической экспертизы / А.А. Шелупанов, А.Р. Смолина // Информационно-управляющие системы. – 2017. – № 3 (88). – С. 99–104.

12. Shelupanov A.A., Smolina A.R. The Methodology of Preparatory Stage of Computer Forensics. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki,* 2016, vol. 19, no. 1, pp. 31–34. (In Russian).

13. Shelupanov A.A., Smolina A.R. Theoretical Aspects of Particular Methodologies Design Support System for Computer Forensics Provision. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki,* 2016, vol. 19, no. 2, pp. 67–70. (In Russian).

14. Shelupanov A.A., Smolina A.R. Formal Foundation of Particular Methodology Design Support System for Computing Expertise. *Information and Control Systems,* 2017, no. 3 (88), pp. 99–104. (In Russian).

Информация об авторе

Жандров Владимир Юрьевич – кандидат юридических наук, доцент кафедры оперативно-разыскной деятельности и специальной техники.

Information about the Author

Zhandrov Vladimir Yuryevich – Candidate of Sciences (Law), Associate Professor of the Department of Operative Investigative Activities and Special Equipment.

Статья поступила в редакцию 07.12.2025; одобрена после рецензирования 15.01.2026; принята к публикации 15.01.2026.
The article was submitted 07.12.2025; approved after reviewing 15.01.2026; accepted for publication 15.01.2026.