Научная статья
УДК 343.14
DOI 10.33184/vest-law-bsu-2025.27.17

Жандров Владимир Юрьевич
Московский университет МВД России имени В.Я. Кикотя, Москва, Россия,
vaisvladimir74@gmail.com

ЦИФРОВАЯ ОПЕРАТИВНАЯ ИНФОРМАЦИЯ: НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ И ПРАВОВОЙ РЕЖИМ ИСПОЛЬЗОВАНИЯ В УГОЛОВНОМ ПРЕСЛЕДОВАНИИ

***Аннотация*.** Смещение преступной активности в информационно-телекоммуникационную среду предопределило необходимость адаптации оперативно-разыскной деятельности к новым условиям, в которых техническая грамотность, аналитические способности и умение работать с цифровыми следами становятся важнейшими компетенциями сотрудников ОВД. Складывающиеся условия цифровой трансформации требуют пересмотра как доктринальных, так и прикладных основ оперативно-разыскной деятельности и, прежде всего, работы с представляющей оперативный интерес цифровой информацией. Цель: сформировать систему аргументов признания цифровой оперативной информации самостоятельным объектом правового регулирования и заслуживающей установления специального режима ее документирования. Методы: сравнительно-правовой, доктринального толкования норм оперативно-разыскного и уголовно-процессуального законодательства, изучения судебных решений по уголовным делам, синтеза, формальной и диалектической логики. Результаты: исследование позволило проанализировать международно-правовые требования к обработке цифровых следов преступной деятельности, оценить законодательный опыт западноевропейских государств по обеспечению допустимости цифровых доказательств, выявить противоречия российской судебной практики по признанию процессуально значимой полученной оперативным путем цифровой информации. Делается вывод, что российское оперативно-разыскное законодательство нуждается в формализации цифровой оперативной информации как особого рода сведений, извлекаемых оперативными подразделениями из информационно-телекоммуникационной среды, подвергнутых первичной верификации и способных трансформироваться в процессуально допустимые доказательства. Это снизит риски нарушения законности и позволит сформировать общий подход в правоприменительной практике по документированию цифровых следов преступлений.

Ключевые слова: оперативно-разыскная деятельность, оперативная информация, допустимость доказательств, киберпреступность, цифровизация

Для цитирования: Жандров В.Ю. Цифровая оперативная информация: нормативное регулирование и правовой режим использования в уголовном преследовании / В.Ю. Жандров // – DOI 10.33184/vest-law-bsu-2025.27.17 // Вестник Института права Башкирского государственного университета. – 2025. – № 3. – С. 172–186.

Original article

Zhandrov Vladimir Yuryevich
Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, Moscow, Russian Federation, vaisvladimir74@gmail.com

DIGITAL INTELLIGENCE: REGULATORY FRAMEWORK AND LEGAL REGIME FOR USE IN CRIMINAL PROSECUTION

Abstract. The shift of criminal activity to the information and telecommunications environment has predetermined the need to adapt operational investigative activities to new conditions, in which technical literacy, analytical skills and the ability to work with digital traces are becoming the most important competencies of the District Department of Internal Affairs staff. The conditions of digital transformation require a revision of both the doctrinal and applied foundations of operational investigative activities and, above all, work with digital information of operational interest. Purpose: to form a system of arguments for recognising digital operational information as an independent object of legal regulation and deserving the establishment of a special regime for its documentation. Methods: comparative legal, doctrinal interpretation of the norms of operational investigative and criminal procedural legislation, study the court decisions in criminal cases, synthesis, formal and dialectical logic. Results: the study allowed us to analyse international legal requirements for processing digital traces of criminal activity, evaluate the legislative experience of Western European states in ensuring the admissibility of digital evidence and identify contradictions in Russian judicial practice in recognising digital information obtained operationally as procedurally significant. It is concluded that Russian operational–search legislation needs to formalise digital operational information as a special kind of data extracted by operational units from the information and telecommunications environment, subject to primary verification and capable of being transformed into procedurally admissible evidence. This will reduce the risks of violating the law and will allow us to formulate a common approach in law enforcement practice for documenting digital traces of crimes.

Keywords: operational-search activity, operational information, evidence admissibility, cybercrime, digitalisation

For citation: Zhandrov V.Yu. Digital Intelligence: Regulatory Framework and Legal Regime for Use in Criminal Prosecution. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2025, no. 3, pp. 172–186. (In Russian). DOI 10.33184/vest-law-bsu-2025.27.17.

Современное общество становится все более информационным, о чем свидетельствуют процессы всеобщей цифровизации, радикально изменившей не только формы коммуникации, но и характер преступной активности. Интернет перестал быть лишь пространством для поиска и передачи информации – он превратился в сложную операционную инфраструктуру, активно используемую для совершения, координации и сокрытия преступлений. По данным МВД России, в январе-декабре 2024 года количество зарегистрированных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (далее – ИКТ) увеличилось на 12,9 %[1].

Правоохранительная деятельность в условиях цифровизации сталкивается с системным вызовом, обусловленным технологическим изменением природы оперативной и доказательственной информации. Расширение цифрового пространства, появление новых форм криминальных коммуникаций и цифровых следов радикально трансформируют как содержание, так и методы функционирования уголовной юстиции.

Информационно-телекоммуникационная среда (далее – ИТКС) формирует не просто новые формы преступности, но и новую операционную плоскость оперативно-разыскной деятельности (далее – ОРД), требующую интеллектуального, правового и технического переосмысления. Разворачивающаяся здесь криминальная деятельность характеризуется высокой латентностью, технической сложностью и трансграничным характером, что делает традиционные методы ОРД по сбору информации недостаточно эффективными [1, с. 22; 2, с. 57].

В условиях цифровизации оперативная информация все чаще приобретает электронную форму и поступает из нетрадиционных источников – Telegram-ботов, даркнета, криптовалютных сервисов, публичных утечек из всевозможных баз данных. В этой связи повышается значение работы с активными (оставляемыми сознательно) и пассивными (автоматически фиксируемыми системами) цифровыми следами – метаданными, логами, IP-адресами, хеш-суммами, сведениями о транзакциях и сессионными идентификаторами. На практике эти сведения, обладая высокой оперативной значимостью, зачастую оказываются

[1] Сведения представлены в рамках расширенного заседания коллегии МВД России 5 марта 2025 года [Электронный ресурс]. URL: www.kremlin.ru/events/president/news/73770 (дата обращения: 13.08.2025).

вне правового режима использования. Их нельзя отнести к доказательствам в процессуальном смысле, поскольку они не оформляются надлежащим образом, но также и не могут быть признаны традиционной оперативной информацией ввиду специфики способов их получения и фиксации. Возникает правовая коллизия: оперативно значимая информация существует, подтверждает преступную активность, но не получает доказательственной силы. Существование данной проблемы подтверждается как в теоретических исследованиях [3, с. 80], так и данными МВД России, согласно которым в 2024 году средняя раскрываемость преступлений, совершенных с применением ИКТ, составила лишь 22,5 %, а по отдельным составам не превысила и 2,2 %.

Одной из причин сложившейся ситуации является устаревший правовой механизм, регулирующий оперативно-разыскную деятельность. Нормы, детализирующие порядок получения, закрепления, хранения и легализации электронной информации отсутствуют. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (далее – Закон «Об ОРД») не регулирует правовой режим оперативно значимой цифровой информации, не предусматривает формы получения, фиксации и верификации сведений из сети Интернет и других открытых электронных источников. Аналогичным образом УПК РФ не определяет понятие, процедуру фиксации и оценки цифровых следов, обнаруженных до возбуждения уголовного дела, что приводит к правовой неопределенности на стыке оперативных и следственных мероприятий. В условиях правового вакуума оперативные сотрудники вынуждены действовать по своему усмотрению, применяя различное программное/аппаратное обеспечение, предназначенное для обработки, хранения и передачи информации, а также обеспечения функционирования информационных систем (OSINT, парсинг, мониторинг даркнета, блокчейн-трекеры и др.) без четкой правовой процедуры и процессуального статуса полученных данных. При этом международная правовая практика давно движется в направлении адаптации к цифровой среде.

Развитие цифровых технологий и глобализация преступной деятельности обусловили необходимость международной гармонизации подходов к обработке цифровых следов преступной деятельности. В условиях, когда значительная часть электронных данных, имеющих значение для уголовного преследования, генерируется за пределами национальной юрисдикции, возникает задача формирования согласованных стандартов их получения, верификации и процессуального использования. При этом особое значение приобретают модели обращения с цифровыми сведениями, находящимися на стыке оперативно-разыскной и процессуальной деятельности, не имеющими формального статуса доказательств, но служащими их источником.

В международной правовой практике четко различаются три категории информации с разной степенью значимости для уголовного преследования: (1) непроверенная информация (англ. «knowledge in rawform») – используется для оценки рисков и формирования общего контекста ситуации, (2) разведыва-

тельная информация (англ. intelligence) – оцененная, соотнесенная с другими данными и проверенная в контексте источника и соответствия действительности, служит инициированию расследования и принятия предварительных мер и (3) процессуально значимая информация (англ. evidence)[2] – обретенная в форму доказательств и применяемая в суде при соблюдении строгих правовых и технических требований.

Согласно рекомендациям Управления ООН по наркотикам и преступности (далее – UNODC), сведения, полученные до возбуждения уголовного дела, могут быть допустимы в суде лишь после их надлежащей трансформации. Такая трансформация включает участие сертифицированного специалиста, верификацию источника информации, подтверждение ее целостности и неизменности, включая использование методов хеширования и журналирования всех действий[3]. Это необходимо для соблюдения принципов допустимости цифровых доказательств и исключения манипуляций или потери достоверности данных при их переходе из одной категории в другую.

Подход UNODC строится на признании цифрового следа как динамически изменяющегося феномена, требующего гибкой, но при этом проверяемой модели обращения. Так, в его Рекомендациях по запросу электронных доказательств за 2014 год подчеркивалась необходимость обеспечения целостности, аутентичности и верифицируемости цифровых данных для их включения в уголовно-процессуальное обращение[4]. В Практическом руководстве по запросу электронных доказательств за рубежом (2022)[5]сделан акцент на разграничении оперативной и доказательственной информации и необходимости создания процедурного фильтра между ними. В частности, цифровая информация, полученная из даркнета или мессенджеров, может служить основанием для возбуждения уголовного дела, однако включается в доказательственную базу лишь после прохождения процедурной трансформации, которая основывается на судебном санкционировании и участии квалифицированного специалиста. Такая

---

[2] Criminal Intelligence Manual for Analysts. United Nations Office on Drugs and Crime (UNODC). Vienna: UNODC, 2011 [Электронный ресурс]. URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf (дата обращения: 30.05.2025).

[3] United Nations Office on Drugs and Crime (UNODC). Guidelines for the Investigation and Prosecution of Cybercrime. Vienna: UNODC, 2022 [Электронный ресурс]. URL: https://www.unodc.org/documents/organized-crime/cybercrime/UNODC_Cybercrime_Guidelines_2022.pdf (дата обращения: 30.05.2025).

[4] United Nations Office on Drugs and Crime. Practical Tips for Requesting Electronic Evidence. Vienna: UNODC, 2014 [Электронный ресурс]. URL: https://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf (дата обращения: 30.05.2025).

[5] United Nations Office on Drugs and Crime. Approaches to Electronic Evidence: Practical Guide for Requesting Electronic Evidence Across Borders. Vienna: UNODC, 2022 [Электронный ресурс]. URL: https://www.unodc.org/documents/organized-crime/GPTOC/GPTOC2/_ebook.pdf (дата обращения: 30.05.2025).

модель направлена на обеспечение допустимости и достоверности цифровых доказательств, минимизацию рисков нарушения процессуальных норм и сохранение баланса между оперативностью и законностью.

В свою очередь, Совет Европы, начиная с Будапештской конвенции о киберпреступности (2001), выступает за признание цифровых следов как объектов особого правового режима[6]. Конвенция и ее Второй дополнительный протокол (2022) закрепляют основные принципы срочной фиксации (англ. preservation), изъятия, трансграничного доступа и защиты цифровой информации. Кроме того, в рамках Cloud Evidence Group (2016) были сформулированы базовые стандарты обращения с цифровыми следами, включая соблюдение процедуры получения доказательств, непрерывную цепочку хранения (англ. chain of custody**)**, прозрачность процессов и обязательный судебный контроль[7]. Указанные документы создают правовую основу для унификации подходов к допустимости цифровых доказательств и обеспечению их надежности в международном сотрудничестве по борьбе с киберпреступностью.

Одним из наиболее институционализированных примеров разграничения разведывательных данных и доказательственной информации служит североамериканская правовая модель. В США применяется механизм «исключения доказательств» (exclusionary rule), согласно которой информация, полученная с нарушением порядка ее сбора, признается недопустимой. Согласно Stored Communications Act (1986)[8]и CLOUD Act (2018)[9] любой доступ к цифровой информации требует получения ордера, санкционированного судом. Эта позиция подтверждена решениями Верховного суда США по делам Carpenter v. United States (2018)[10] и Riley v. California (2014)[11]. Прецеденты определили, что

---

[6] Council of Europe. Convention on Cybercrime (Budapest, 23.XI.2001) [Электронный ресурс]. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата обращения: 30.05.2025).

[7] Council of Europe. Cloud Evidence Group Report. Strasbourg, 2016 [Электронный ресурс]. URL: https://rm.coe.int/cloud-evidence-group-report/16806f9334 (дата обращения: 30.05.2025); Council of Europe. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS № 189), 2022 [Электронный ресурс]. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (дата обращения: 30.05.2025).

[8] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§2701–2713) [Электронный ресурс]. URL: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121 (дата обращения: 11.08.2025).

[9] Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.PublicLaw 115–141. –USA, 2018 [Электронный ресурс]. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943 (дата обращения: 30.05.2025).

[10] Carpenter v. United States, 585 U.S. (2018) [Электронный ресурс]. URL: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (дата обращения: 30.05.2025).

[11] Riley v. California, 573 U.S. 373 (2014) [Электронный ресурс]. URL: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf (дата обращения: 30.05.2025).

сбор геолокационных и иных метаданных без ордера нарушает Четвертую поправку к Конституции США[12]. Таким образом, только информация, полученная с соблюдением процедурной формы, признается допустимой в суде.

В странах Европейского союза допустимость цифровых доказательств основывается на принципах обеспечения подлинности и непрерывности хранения данных, обязательного получения судебной санкции и привлечения независимого эксперта к процессу сбора цифровых следов, что соответствует правовым стандартам, закрепленным Советом Европы[13]. Например, в Германии вопросы сбора и допустимости цифровых следов определяются положениями Уголовно-процессуального кодекса (StPO), в частности, §§100a–g[14], которые определяют порядок получения телекоммуникационной и электронной информации в рамках уголовного процесса.

В Великобритании допустимость и достоверность цифровых доказательств регулируются техническими стандартами, изложенными в руководстве ACPO[15] и государственной Стратегии по цифровой криминалистике[16].

Кроме того, в западноевропейских странах действуют форензик-протоколы, предусматривающие обязательное соблюдение стандартных процедур: создание точных цифровых копий, использование сертифицированных инструментов анализа, логирование всех действий и ведение подробных технических отчетов (англ. forensic reports)[17].

Особое внимание уделяется защите оригинала цифрового объекта и воспроизводимости всех этапов анализа, что соответствует международным требованиям и рекомендациям, изложенным в стандарте ISO/IEC 27037:2012[18].

---

[12] United States Constitution. Fourth Amendment [Электронный ресурс]. URL: https://www.archives.gov/founding-docs/amendments-11-27 (дата обращения: 30.05.2025).

[13] Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Электронный ресурс]. URL: https://rm.coe.int/16806fddc6 (дата обращения: 30.05.2025).

[14] Strafprozessordnung (StPO) §§100a–g [Электронный ресурс]. URL: https://www.gesetze-im-internet.de/stpo/__100a.html (дата обращения: 30.05.2025).

[15] Association of Chief Police Officers (ACPO). Good Practice Guide for Digital Evidence [Электронный ресурс]. URL: https://www.7safe.com/assets/content/guidance/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (дата обращения: 30.05.2025).

[16] UK Government. Digital Forensics Strategy. 2020 [Электронный ресурс]. URL: https://www.gov.uk/government/publications/digital-forensics-strategy (дата обращения: 30.05.2025).

[17] Association of Chief Police Officers (ACPO). Good Practice Guide for Digital Evidence. Version 5.0. London, 2012 [Электронный ресурс]. URL: https://www.7safe.com/assets/content/guidance/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (дата обращения: 30.05.2025).

[18] International Organization for Standardization (ISO). ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence [Электронный ресурс]. URL: https://www.iso.org/standard/44381.html (дата обращения: 30.05.2025).

Данный документ представляет собой свод руководящих принципов по идентификации, сбору, получению и сохранению цифровых доказательств. Он устанавливает единые требования к обращению с цифровыми объектами в целях обеспечения их аутентичности, целостности, воспроизводимости и допустимости в судебных и административных процедурах. В соответствии с рассматриваемым стандартом особое внимание следует уделять принципу минимального вмешательства в оригинал цифрового объекта, ведению непрерывной и достоверной цепочки хранения, использованию сертифицированных средств анализа, а также разграничению ролей участников процесса: от лица, первым получившего доступ к цифровому носителю, до эксперта, производящего анализ.

Документ дает конкретные рекомендации по подготовке, обучению и проверке квалификации специалистов, вовлеченных в обработку цифровых доказательств. В нем подчеркивается необходимость документирования всех действий, включая фиксацию времени, места, методов и инструментов, примененных на каждом этапе. Стандарт также вводит понятие «обоснованной целостности» (англ. reasonable integrity), предполагающее возможность независимого воспроизведения всех процедур третьей стороной.

В целях обеспечения объективности и проверяемости ISO/IEC 27037:2012 требует составления технических отчетов, которые могут быть представлены в суде в качестве доказательств правильности проведенных действий. Документ ориентирован не только на правоохранительные органы, но и на организации, занимающиеся инцидент-реакцией и корпоративными расследованиями. Указанные положения делают стандарт универсальной основой для построения национальных форензик-протоколов. В комплексе с ним применяется стандарт ISO/IEC 27050[19], касающийся электронного представления и анализа цифровой информации в правовом контексте. Оба документа закрепляют обязательность идентификации источника, подтвержденной цепочки хранения, технической неизменности объекта и участия квалифицированных специалистов при его обработке. Эти стандарты признаются во многих странах как ориентир для выработки регламентов, обеспечивающих надлежащую процедуру обращения с цифровыми доказательствами.

Значение международного опыта для российской правовой системы заключается не столько в возможности прямого заимствования, сколько в выработке модели, адаптированной к национальным реалиям. В условиях, когда УПК РФ и Закон об ОРД не содержат понятия цифрового следа и не определяют процедуру его легализации, зарубежные практики предоставляют ценные ориентиры: институционализация статуса цифровой информации, пошаговая трансформация ее в доказательственную, судебный контроль, соблюдение процедурной преемственности, техническая достоверность и защита прав субъектов.

---

[19] International Organization for Standardization (ISO). ISO/IEC 27050. Information technology. Security techniques. Electronic discovery [Электронный ресурс]. URL: https://www.iso.org/standard/44382.html (дата обращения: 30.05.2025).

Отправной точкой разработки отечественной модели обращения с цифровой информацией должно стать ее признание в качестве самостоятельного объекта нормативного регулирования и разработки, соответственно, правового режима ее использования. Это должно стать стратегической задачей для российской системы, где цифровая оперативная информация пока используется преимущественно в обход нормативных процедур и без должной гарантии достоверности.

Современные условия цифровизации преступной среды требуют переосмысления существующего понятийного аппарата ОРД. Классические подходы, выработанные в рамках аналогового оборота информации, теряют применимость в отношении сетевых, анонимных и распределенных цифровых форм преступности. На этом фоне все чаще встает вопрос о необходимости выделения нормативного оформления «цифровой оперативной информации» (далее – ЦОИ) как особого рода сведений, извлекаемых оперативными подразделениями из информационно-телекоммуникационной среды до возбуждения уголовного дела. Она должна быть закреплена в Законе об ОРД как самостоятельный вид информации, получаемой в цифровой среде, зафиксированной техническими средствами, подвергнутой первичной верификации и способной в последующем трансформироваться в процессуально допустимое доказательство. В противном случае, без законодательного признания такого переходного статуса оперативная практика обречена на правовую недееспособность, а следственная – на доказательственные риски.

В отсутствии правового режима ЦОИ российская правоприменительная практика сталкивается с противоречием: с одной стороны, цифровая информация необходима для эффективного расследования, с другой – она не вписывается в рамки существующего правового инструментария. Это подрывает как эффективность следствия, так и устойчивость судебных решений, основанных на такой информации.

Проблема надлежащей фиксации цифровых следов особенно актуальная для этапа доследственной проверки. Сведения, полученные в ИТКС, активно используются следственными органами как источник инициативной информации о криминальном событии – на основании ст.ст. 140–145 УПК РФ они могут служить основанием для возбуждения уголовного дела при оформлении их в рапорте, заключении специалиста либо приобщении к сообщению о преступлении. Это особенно характерно для оперативных подразделений полиции, в чьи функциональные задачи, в первую очередь, входит именно выявление преступлений. Тем не менее, отсутствие процессуальной формы и стандартов оценки достоверности цифровой информации создает риск признания ее недопустимой в качестве доказательства.

Российская судебная практика демонстрирует противоречивость в подходах к допустимости цифровых следов. Одни суды признают допустимым исследование локально доступной информации на изъятых устройствах (скриншотов переписок, данных мониторинга сайтов, лог-файлов) без отдельного разрешения, но при наличии протокола осмотра, заключения специалиста и

хеш-сумм[20]. В то же время, отдельные региональные суды занимают более жесткую позицию, исключая доказательства, полученные без санкции суда, если речь идет о сетевых или операторских данных[21]. Следует отметить, что Конституционный Суд Российской Федерации[22], как и Верховный Суд Российской Феде-

[20] Об отказе в жалобе адвоката Решетина М. В. на приговор Увельского районного суда Челябинской области на нарушение положения ч. 5 ст. 186.1 УПК РФ и ч. 6, 7 ст. 186 УПК РФ : апелляционное определение Челябинского областного суда от 30 мая 2016 г. № 10-2537/2016 // Доступ из электронной базы судебных актов, решений и нормативных документов SudAct.ru [Электронный ресурс]. URL: https://sudact.ru (дата обращения: 18.08.2025); Об отказе в удовлетворении ходатайства следователя по особо важным делам о разрешении производства осмотра мобильных телефонов, изъятых в ходе производства обыска в жилище : апелляционное постановление Приморского краевого суда от 2 февраля 2015 г. № 22-455/15 [Электронный ресурс]. URL: http://docs.pravo.ru/document/view/68631850/ (дата обращения: 18.08.2025); Новиков А.В. Использование переписки в мессенджерах в качестве доказательств: анализ судебной практики // Адвокатская газета. – 2022. – № 6. [Электронный ресурс]. URL: https://www.advgazeta.ru/mneniya/ispolzovanie-perepiski-v-messendzherakh-v-kachestve-dokazatelstv-analiz-sudebnoy-praktiki/ (дата обращения: 18.08.2025).

[21] Об отмене постановления в части отказа удовлетворить жалобу на осмотр SMS-сообщений без судебного решения : кассационное определение Омского областного суда от 24 мая 2012 г. № 22-2225/12 // Доступ из электронной базы судебных актов, решений и нормативных документов SudAct.ru [Электронный ресурс]. URL: https://sudact.ru (дата обращения 18.08.2025); О признании недопустимыми протоколов осмотра телефонов, составленных следователем без судебного разрешения : приговор Курганского городского суда Курганской области от 25 июня 2014 г. по делу № 1-230/2014 [Электронный ресурс] // Судебный департамент при Верховном Суде РФ : сайт. URL: https://kurgansky--krg.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=34637754&delo_id=1540006&new=0&text_number=1 (дата обращения: 18.08.2025); О признании недопустимыми доказательств, получение детализации телефонных соединений через «личный кабинет» без судебного решения : приговор Каргапольского районного суда Курганской области от 31 октября 2017 г. по делу № 1-51/2017 // Доступ из электронной базы судебных актов, решений и нормативных документов SudAct.ru [Электронный ресурс]. URL: https://sudact.ru (дата обращения: 18.08.2025).

[22] 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 июня 2023 г. № 1773-О // Доступ с сайта юридической информационной системы «Легалакт» [Электронный ресурс]. URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-27062023-n-1773-o/ (дата обращения: 17.08.2025); 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»; 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 // Доступ с сайта юридической информационной системы «Легалакт» [Электронный ресурс]. URL: https://legalacts.ru/kodeks/UPK-RF/chast-2/razdel-viii/glava-24/statja-176/#101325 (дата обращения: 17.08.2025).

рации[23] допускают возможность осмотра и исследования переписки, хранящейся локально на изъятом устройстве, без отдельного судебного разрешения, при условии соблюдения процессуальной формы и гарантий сохранности. Такое расхождение подтверждает правовую уязвимость цифровых сведений, получаемых на досудебных стадиях, и отсутствие единообразных стандартов их допустимости.

Отсутствие единообразия в судебной практике по этому вопросу лишь подтверждает правовую уязвимость цифровых сведений, полученных в досудебный период.

Особую проблему составляет риск ретроактивной легализации цифровых следов, когда информация о цифровых следах, полученная вне процессуальных процедур (например, в ходе оперативных мероприятий), впоследствии подменяется следственными действиями – повторной выемкой, фиксацией, привлечением специалиста. Это нарушает принцип допустимости доказательств и противоречит запрету использовать те, которые получены незаконным путем, который закреплен в международной практике и подтвержден правовыми позициями Европейского суда по правам человека[24].

Среди практических механизмов, применяемых для легализации цифровой информации, можно выделить несколько вариативных сценариев. Первый – повторная фиксация информации через процессуальные действия: осмотр сайтов, переписки, цифровых носителей. Второй – оформление заключения специалиста по ранее полученной информации. Третий – приобщение цифровых следов к рапорту оперативного сотрудника как приложение к сообщению о преступлении. Четвертый – фиксация цифровой информации в рамках провер-

---

[23] Об оставлении без изменения приговора … (о допустимости осмотра и исследования информации с телефона, изъятого в соответствие со ст. 176 УПК РФ*)* : кассационное определение Верховного Суда РФ от 30 сентября 2014 г. по делу № 2-18/08 // Доступ из электронной базы судебных актов, решений и нормативных документов SudAct.ru. [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); По апелляционным жалобам на приговор Новосибирского областного суда от 2 октября 2018 года : апелляционное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 1 августа 2019 г. № 67-АПУ19-8 по делу № 2-003/2018 // Доступ из электронной базы судебных актов, решений и нормативных документов SudAct.ru [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).

[24] Council of Europe. Practice Direction on the “Fruit of the Poisonous Tree” Doctrine [Электронный ресурс]. URL: https://rm.coe.int/practice-direction-fruit-of-the-poisonous-tree/16808e9b19 (дата обращения: 30.05.2025); United Nations Office on Drugs and Crime (UNODC). Good practices for the investigation and prosecution of cases involving electronic evidence [Электронный ресурс]. URL: https://www.unodc.org/documents/organized-crime/UNODC_Electronic_Evidence.pdf (дата обращения: 30.05.2025).

ки сообщений по ст. 144 УПК РФ. Эти подходы позволяют формально легализовать цифровую информацию как оперативную, но не решают проблемы отсутствия ее нормативного статуса и процедурной преемственности.

Традиционно в научной и правоприменительной литературе оперативная информация определяется как совокупность сведений, представляющих интерес для предупреждения, выявления, пресечения и раскрытия преступлений, а также розыска лиц, скрывающихся от следствия или отбывания наказания. Так, по определению Д.В. Гребельского, – это первичные и выводные данные о лицах, преступных фактах, состоянии сил и условий ОРД [4, с. 62]. Н.А. Губанова подчеркивает, что оперативная информация представляет собой данные, специфичные по цели, методу получения и режиму применения, подлежащие проверке и доступные только уполномоченным субъектам ОРД [5, с. 71]. Позицию о семиотических и логико-прагматических аспектах информации также развивают Б.Я. Советов, С.С. Овчинский [6] и др. Таким образом, по своему значению «оперативная информация» в российской терминологии сопоставима с «intelligence» – категорией разведывательной информации в международной классификации. В свою очередь, «цифровая оперативная информация» может быть определена как сведения (сообщения, данные), полученные в рамках оперативно-разыскной деятельности из цифровой среды (включая сеть Интернет, даркнет, мессенджеры, блокчейн-структуры), зафиксированные в электронной форме, обладающие оперативной значимостью и потенциальной пригодностью для использования в уголовном процессе после прохождения процедуры легализации.

Формализация цифровой оперативной информации позволит отграничить ее от иной информации уровня оперативной осведомленности, представляющей собой предварительные, часто непроверенные сведения. Скриншоты, логи, блокчейн-отчеты и другие сведения могут обладать значительной фактической ценностью, однако вне надлежащей процедуры фиксации оказываются лишены юридической силы. Отказ от юридического разграничения этих категорий информации приводит к ситуации, при которой цифровые следы могут использоваться на этапе разработки, но не включаются в дело как допустимые доказательства [1, с. 72]. В подобной логике рассуждений цифровую оперативную информацию следует рассматривать как промежуточную категорию, находящуюся между имеющей оперативное значение информацией и электронными доказательствами. В отличие от первой, она технически надлежащим образом зафиксирована и обладает потенциальной доказательственностью, т.е. способностью трансформироваться в надлежащее доказательство. В то же время ЦОИ отличается от вещественных доказательств, так как не имеет материального воплощения, существует исключительно в виде цифрового сигнала или массива данных и требует специальных технологий анализа. Ее статус должен быть связан с определенной процедурой сбора и сопровождаться обязательными требованиями к верификации.

Включение цифровой оперативной информации в структуру нормативного регулирования позволит упорядочить действия оперативных подразделений, создать правовую форму для систематического использования цифровых данных и устранить правовую неопределенность, препятствующую легитимному применению таких сведений в уголовном процессе. В противном случае, процессуальная недопустимость цифровых следов часто вызвана не их ненадежностью, а отсутствием закрепленных процедур обращения с ними [1, с. 72].

Подобного рода «институализация» ЦОИ позволит снизить риски нарушения законности, которые в настоящее время остаются высокими. В первую очередь, это угроза расширительной интерпретации прав оперативных органов на сбор цифровых данных без достаточных оснований и судебного контроля. Возможность получения информации из мессенджеров, даркнета и социальных сетей без ведома пользователя требует баланса между эффективностью преследования и сохранением конституционных гарантий тайны личной жизни, переписки и информации (ст. 23–24 Конституции Российской Федерации). Особую опасность представляет собой практика обращения с цифровой информацией вне рамок уголовного процесса – без ее надлежащей фиксации, хеширования и верификации. Такая информация, оставаясь вне правового поля, формирует так называемый «теневой оборот» цифровых сведений, не обладающих юридическим статусом. Это ведет к подмене установленной уголовно-процессуальной процедуры неформальными оперативными действиями, нарушая принципы допустимости и проверяемости доказательств. В результате подрывается доверие к правосудию и создаются условия для произвольного вмешательства в частную жизнь граждан, не обеспеченного судебным контролем и правовыми гарантиями.

Таким образом, надлежащее обращение с цифровой информацией в современных условиях становится ключевым элементом оперативно-разыскной и процессуальной деятельности. Установление правового режима фиксации и последующего использования ЦОИ устранит риск произвольного использования цифровых следов, обеспечит защиту прав сторон, повысит предсказуемость судебных решений и укрепит легитимность доказательной базы по делам, связанным с цифровой преступностью. Признание ее нормативного статуса позволит легализовать эффективные методы анализа цифровой среды, обеспечить трансформацию фактической информации в правовую форму и сохранить баланс между интересами государства и гражданина. Нормативное оформление ЦОИ как промежуточной категории формирования электронных доказательств представляется необходимым шагом на пути к созданию целостной модели работы с цифровыми следами в российской системе ОРД и уголовного судопроизводства.

Список источников

1. Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы : монография / С.П. Щерба, Е.А. Архипова, Е.В. Быкова ; под ред. С.П. Щербы. – Москва : Проспект, 2022. – 168 с.

2. Жандров В.Ю. Решение задач оперативно-розыскной деятельности посредством получения сведений в информационно-телекоммуникационной среде / В.Ю. Жандров // Вестник Московского университета МВД России. – 2024. – № 4. – С. 56–65.

3. Васюков В.Ф. К вопросу о получении оперативно значимой информации из открытых источников информации сети «Интернет» / В.Ф. Васюков, А.Ю. Афанасьев // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2024. – № 1 (65). – С. 79–86.

4. Гребельский Д.В. Теоретические основы и организационно-правовые проблемы деятельности органов внутренних дел. – Москва : Академия МВД СССР, 1977. – С. 60–69.

5. Губанова Н.А. Понятие оперативно-розыскной информации / Н.А. Губанова // Научный портал МВД России. – 2014. – № 4 (28). – С. 70–72.

6. Овчинский С.С. Оперативно-розыскная информация / С.С. Овчинский. – Москва : Инфра-М, 2000. – 365 с.

References

1. Shcherba S.P. (ed.). Collection of Electronic Evidence in Criminal Cases in Russia and Abroad: Experience and Problems. Moscow, Prospect, 2022. 168 p. (In Russian).

2. Zhandrov V.Yu. Solving the Tasks of Operational-Investigative Activities by Obtaining Information in the Information and Telecommunications Environment. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2024, no. 4, pp. 56–65. (In Russian).

3. Vasyukov V.F., Afanasyev A.Yu. On the Issue of Obtaining Operationally Significant Information from Open Sources of Information on the Internet. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* 2024, no. 1 (65), pp. 79–86. (In Russian).

4. Grebelsky D.V. Theoretical Foundations and Organisational and Legal Problems of the Internal Affairs Bodies Activities. Moscow, Academy of the Ministry of Internal Affairs of the USSR, 1977, pp. 60–69. (In Russian).

5. Gubanova N.A. Concept of Operational Search Information. *Scientific Portal of the Russian Ministry of the Interior,* 2014, no. 4 (28), pp. 70–72. (In Russian).

6. Ovchinsky S.S. Operational Search Information. Moscow, Infra-M, 2000. 367 p. (In Russian).

Информация об авторе

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

Information about the Author

Zhandrov Vladimir Yuryevich *– Candidate of Sciences (Law), Associate Professor, Associate Professor of the Chair of Operational Investigative Activities and Special Techniques*

Статья поступила в редакцию 12.09.2025; одобрена после рецензирования 18.09.2025; принята к публикации 23.09.2025.
The article was submitted 12.09.2025; approved after reviewing 18.09.2025; accepted for publication 23.09.2025.