Дата поступления рукописи в редакцию: 30.07.2026 г.
Дата принятия рукописи в печать: 25.09.2026 г.

DOI: 10.24412/2782-3849-2026-9-167-171

САХНО Оксана Олеговна,
подполковник полиции, старший преподаватель кафедры криминалистики Федерального государственного казенного образовательного учреждения высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации»,
e-mail: sahno_oksana@inbox.ru

ЧЕРЕПКОВ Роман Анатольевич,
старший преподаватель кафедры судебной экспертизы и криминалистики Центрального филиала федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия имени В.М. Лебедева» (г. Воронеж),
e-mail: romach197978@yandex.ru

ЧЕРНОЖУКОВА Карина Руслановна,
рядовой полиции, курсант юридического факультета Федерального государственного казенного образовательного учреждения высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации»,
e-mail: karina16042005@yandex.ru

К ВОПРОСУ О ПОНЯТИИ, КЛАССИФИКАЦИИ И ЗНАЧЕНИИ ЦИФРОВЫХ СЛЕДОВ В ДЕЯТЕЛЬНОСТИ ПО РАСКРЫТИЮ И РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ

Аннотация. *В статье исследуется вопрос трансформации учения о следах под влиянием процессов цифровизации. Авторами проводится комплексный анализ цифровых следов как относительно новой категории объектов криминалистического исследования, формулируются ключевые признаки цифрового следа, уделено внимание вопросу классификации следов, содержащихся в цифровом пространстве. Раскрывается содержательная характеристика криминалистически значимой информации, извлекаемой из цифровых следов. Обосновывается необходимость актуализации криминалистических методик и алгоритмов работы с цифровыми следами с учетом современного уровня развитиях цифровых технологий.*

Ключевые слова: *цифровой след, цифровое пространство, доказательство, раскрытие преступления, расследование преступления, следственное действие.*

SAKHNO Oksana Olegovna,
police lieutenant colonel, senior lecturer at the Department of Criminalistics of the Federal State Treasury Educational Institution of Higher Education "Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation"

CHEREPKOV Roman Anatolyevich,
Senior Lecturer, Department of Forensic Science and Forensics, Central Branch of the Federal State Budgetary Educational Institution of Higher Education "V.M. Lebedev Russian State University of Justice" (Voronezh)

CHERNOZHUKOVA Karina Ruslanovna,
ordinary police officer, cadet of the law faculty of the Federal State Treasury Educational Institution of Higher Education "Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation"

TO THE QUESTION OF THE CONCEPT, CLASSIFICATION AND SIGNIFICANCE OF DIGITAL TRACES IN CRIME DETECTION AND INVESTIGATION ACTIVITIES

Annotation. *The article explores the transformation of the doctrine of traces under the influence of digitalization processes. The authors conduct a comprehensive analysis of digital traces as a relatively new category of objects of forensic research, formulate the key features of a digital trace, and pay attention to the classification of traces contained in the digital space. The article reveals the content characteristics of criminologically significant information extracted from digital traces. The authors substantiate the need to update forensic methods and algorithms for working with digital traces, taking into account the current level of development of digital technologies.*

Key words: *digital footprint, digital space, evidence, solving a crime, investigating a crime, investigative action.*

Цифровая трансформация, затрагивающая все сферы общественных отношений, привела к проникновению цифровых устройств и информационных технологий в повседневную жизнь современного человека. Эти процессы обуславливают неизбежную трансформацию механизмов преступной деятельности с формированием цифровых следов, имеющих принципиальное отличие от классических материальных и идеальных отображений.

К цифровым следам необходимо относить регистрационные записи автоматизированных систем, метаданные файлов, сведения о сетевых соединениях, переписки в мессенджерах и транзакционные данные платежных сервисов. Безусловно, приведенный перечень не является исчерпывающим, но дает общее представление о специфике формируемых цифровых следов, а также разнообразных их формах представления.

Анализ практики раскрытия и расследования современных преступлений, показывает, что уровень эффективности в работе с цифровыми следами, а также объектами, их содержащими, требует своего повышения. Разработанные ранее алгоритмы поиска, процессуальной фиксации, изъятия и последующей интерпретации следов нуждаются в своей актуализации. На сегодняшний день актуальна разработка и внедрение методически выверенных криминалистических рекомендаций по вовлечению в процесс расследования информации, содержащейся в цифровых следах и имеющей потенциальное доказательственное значение.

Цифровые следы являются относительно новым типом объектов криминалистического исследования. Само понятие следа в криминалистике имеет длительную историю и разработано в рамках трасологии, как одного из разделов криминалистической техники. Следует отметить, что в рамках указанного раздела преимущественно рассматриваются материально-фиксированные отображения, например, следы рук, обуви или орудий взлома. Распространение цифровых устройств потребовало переосмысления категории следа и расширения его содержания за счет информационных объектов, существующих в электронной форме.

Исследование понятия цифрового следа показывает, что авторы едины в понимании цифрового следа как информационного отображения активности субъекта, однако расходятся в степени детализации среды, в которой такое отображение формируется. Так, например, Л.М. Тайтубаева предлагает определять цифровой след как результат деятельности субъекта, осуществляемой в цифровом пространстве с использованием каких-либо устройств [1, с. 530]. Это определение делает акцент на субъектно-деятельностной природе рассматриваемого явления – след возникает вследствие целенаправленного или сопутствующего взаимодействия лица с программно-аппаратной средой.

По мнению Хомякова Э.Г., к цифровым следам следует относить всю совокупность данных, которые остаются в результате активности пользователя в цифровой среде и формируются как в сети Интернет, так и в мобильных устройствах, а также в системах связи и иных информационных технологических средствах. При этом, образованные цифровые следы, как отмечает автор, могут быть использованы для идентификации поведения, действий или взаимодействий субъекта [2, с. 73]. Сформулированное Хомяковым Э.Г. определение охватывает максимально широкий круг источников обнаружения цифровых следов и особо подчеркивает идентификационную функцию цифрового следа, имеющую важное значение для осуществления раскрытия и расследования преступления.

Формулировка дефиниции «цифровой след» позволяет отграничить данную группу от иных следов преступной деятельности, а также показывает их сущность и многообразие форм выражения. Не менее важно также решение классификационных задач в отношении цифровых следов, которое способствует организации качественной и эффективной работы с тем или иным видом указанных следов на всех этапах расследования.

Используя традиционный трасологический подход, следует сделать вывод, что следообразующим объектом в цифровом пространстве является пользователь, либо программный агент, действующий по его инициативе, а следовоспринимающим объектом выступает аппаратно-программный комплекс, фиксирующий соответству-

ющую активность. При этом, механизм формирования цифрового следа определяется характером взаимодействия, так, например, авторизация на сервисе порождает одну разновидность записей, автоматическая фоновая передача геолокационных данных – другую.

Наиболее распространенным основанием классификации цифровых следов в современной литературе является степень осведомленности и волевого участия субъекта в процессе их образования. По названному критерию выделяют активные и пассивные цифровые следы. Активный цифровой след возникает в результате осознанного действия пользователя, направленного на создание информационного объекта или на передачу сведений. В качестве примером таких действий можно выделить публикацию сообщения в социальной сети, отправку электронного письма, заполнение регистрационной формы или загрузку файлов на облачное хранилище. Осуществляя указанные действия, субъект понимает, что действие происходит с его участием в цифровом пространстве, и, как правило, контролирует содержание передаваемой информации.

Пассивный цифровой след формируется иначе. Как отмечает,

М.В. Ганжа, данный вид следа может быть представлен как совокупность данных о пользователе, при этом указанные следы могут быть образованы с его активным участием, но без его ведома. Примером пассивных следов может выступать формирование цифровых следов в сети Интернет, так, с момента открытия сайта будет сохранено каждое действие пользователя на выбранном им ресурсе [3, с. 58]. При пассивном следообразовании субъект может не осознавать, что определенные сведения о нем сохраняются. Как правило, к этой категории относятся файлы cookie, записи IP-адресов в журналах веб-серверов, данные телеметрии операционных систем, сведения о геопозиции, автоматически передаваемые приложениями. Разграничение активных и пассивных следов значимо в криминалистическом отношении, поскольку пассивные следы в виду своей специфики образования, в меньшей степени подвержены намеренному уничтожению или фальсификации со стороны преступника.

Помимо критерия осведомленности субъекта, в доктрине используются и иные основания деления. По месту локализации цифровые следы разграничиваются на следы, хранящиеся непосредственно на устройстве пользователя (локальные), и следы, зафиксированные на удаленных серверах (сетевые). Локальные следы включают историю браузера, кэшированные файлы, журналы событий операционной системы, метаданные документов, временные файлы приложений. Сетевые следы сохраняются провайдерами услуг связи, администраторами интернет-ресурсов, операторами облачных платформ. Практическое значение этого деления определяется различием процессуальных процедур получения доступа к соответствующим данным, тактическими особенностями и организационной формой их обнаружения и фиксации.

Следующим основанием классификации выступает содержание информации. Так, цифровые следы могут быть разделены на идентификационные, коммуникационные, навигационные и транзакционные. Идентификационные следы позволяют установить личность пользователя или индивидуализировать устройство: учетные записи, цифровые сертификаты, MAC-адреса сетевых интерфейсов, IMEI мобильных терминалов. Коммуникационные следы отражают факт и содержание обмена информацией между субъектами – переписку в мессенджерах, записи телефонных соединений, электронную корреспонденцию. Навигационные следы фиксируют перемещение пользователя в физическом пространстве (данные GPS, информация о подключении к базовым станциям сотовой связи) и в виртуальной среде (история посещенных веб-страниц, журналы DNS-запросов). Транзакционные следы отображают совершение финансовых или юридически значимых операций: платежи через электронные системы, переводы криптовалюты, действия в информационных системах государственных органов. Учет содержащейся в цифровых следах информации поможет верно определить источник и порядок работы с ним, для успешного извлечения и последующей интерпретации цифровых следов.

Дополнительным классификационным признаком служит характер носителя. Цифровые следы обнаруживаются в энергозависимой (оперативная память, кэш процессора) и энергонезависимой (жесткие диски, твердотельные накопители, флеш-карты) памяти. Криминалистическое значение классификации по данному основанию состоит в том, что следы в энергозависимой памяти могут быть утрачены при отключении питания устройства. Понимание специфики и характера носителя цифровых следов требует от субъектов расследования принятия взвешенного и обоснованного решения о необходимости применения специализированных средств их извлечения и алгоритмах действий с цифровыми следами на определенном устройстве.

Криминалистическая значимость информации, извлекаемой из цифровых следов, определяется ее способностью устанавливать обстоятельства, подлежащие доказыванию по уголовному делу. Цифровые следы содержат сведения о действиях лица, времени и месте их соверше-

ния, используемых средствах, контактах с иными субъектами. Эти сведения приобретают процессуальное значение при условии их надлежащего обнаружения, закрепления и оценки в соответствии с требованиями уголовно-процессуального законодательства.

Отметим, что понятие криминалистически значимой информации, содержащейся в цифровой среде, требует своего уточнения. В.А. Скрипко определяет ее как закодированную информацию, представленную в цифровом виде и находящуюся в компьютерной среде, а также относящуюся к расследуемому событию [4, с. 194]. Приведенное определение указывает на два важных признака: форму существования (цифровой код в компьютерной среде) и относимость к расследуемому событию. Второй признак особенно важен, поскольку объем информации, хранимой на современных устройствах, исчисляется гигабайтами и терабайтами, и лишь незначительная часть этих сведений имеет отношение к предмету доказывания. Отбор релевантных данных составляет самостоятельную криминалистическую задачу, решение которой зависит от квалификации субъекта расследования, привлеченного специалиста и корректности постановки вопросов при назначении экспертизы.

Содержательную характеристику такой информации А.В. Ким раскрывает следующим образом – эта информация, являясь носителем следов преступления, содержит криминалистически значимые сведения об обстоятельствах преступной деятельности. (например, логи систем, метаданные файлов, сетевые журналы, видеозаписи) [5, с. 82]. Вышеуказанная формулировки подчеркивает, что криминалистически значимая информация неоднородна по своему составу и позволяют охарактеризовать механизм произошедшего преступления по различным параметрам. Так, логи систем фиксируют хронологию событий в программной среде и позволяют восстановить последовательность действий пользователя. Метаданные файлов содержат сведения о дате создания, модификации, авторстве документа, использованном программном обеспечении. Сетевые журналы отражают параметры соединений, IP-адреса, объем переданных данных, протоколы взаимодействия. Видеозаписи, сохраненные в цифровом формате, позволяют идентифицировать лиц и фиксировать обстоятельства произошедшего события в их динамике.

Роль цифровых следов в доказывании определяется прежде всего их информативностью. Один изъятый смартфон может содержать переписку, подтверждающую наличие предварительного сговора, геолокационные данные, фиксирующие присутствие лица на месте преступления в определенный момент, фотографии и видеозаписи, отображающие обстановку и участников события, финансовые транзакции, свидетельствующие о корыстном мотиве. Столь высокая концентрация разнородных сведений в пределах одного носителя объясняет возрастающее внимание правоприменителей к цифровым источникам доказательственной информации.

С процессуальной точки зрения информация из цифровых следов может быть вовлечена в доказывание в различных формах. Электронный носитель, содержащий криминалистически значимую информацию, может быть признан вещественным доказательством в порядке, установленном уголовно-процессуальным законодательством, и в последующем приобщен к материалам дела. Извлеченные из устройства сведения, зафиксированные в протоколе осмотра или в заключении эксперта, также могут быть источником доказательственной информации и приобретают такой статус, являясь составными частями протоколов следственных действий, а также заключений и показаний эксперта. Выбор той или иной формы представления зависит от характера носителя информации, способа извлечения информации и ее значения в каждом конкретном случае.

Рассмотрим значение информации, источниками которой выступают цифровые следы на различных этапах расследования. Так, анализ цифровых следов, обнаруженных на этапе возбуждения уголовного дела, позволит оперативно установить наличие признаков состава преступления и принять обоснованное процессуальное решение по итогам проверки поступившего заявления или сообщения. В ходе предварительного расследования такая информация способствует выдвижению и проверке следственных версий, установлению личности подозреваемого, определению круга соучастников, выявлению способа совершения преступления, мотивов действий преступника и наступивших последствий. При формировании обвинительного заключения цифровые доказательства подкрепляют совокупность всех собранных по делу доказательств, а в ряде случаев составляют основу обвинения – прежде всего по делам о преступлениях в сфере компьютерной информации, мошенничестве с использованием электронных средств платежа, незаконном обороте информации ограниченного доступа.

Следует отметить, что оценка криминалистического значения цифровых следов сопряжена с рядом сложностей. Специфика получаемой информации, а также значительный объем извлекаемых данных требуют обязательного участия лиц, обладающих специальными знаниями и применения ими специализированного программного обеспечения для интерпретации и анализа цифровых следов. Трансграничный характер

цифровой среды, а также возможность хранения интересующей информации на серверах за пределами юрисдикции Российской Федерации, существенно осложняют получение доказательственной информации субъектом расследования. Стремительное развитие цифровых технологий, быстрое устаревание технических средств и разнообразие форматов хранения информации в цифровой среде, могут создать риск утраты доступа к ранее зафиксированным сведениям или невозможность их изъятия по прошествии времени. Все вышесказанное позволяет сделать вывод о том, что с учетом современного состояния информационных технологий немаловажное значение имеет качественное и своевременное повышение уровня владения навыками работы с цифровыми следами, образованными в цифровом пространстве каждого сотрудника правоохранительных органов.

Классические принципы работы с материально-фиксированными отражениями, разработанные ранее, требует адаптации применительно к условиям цифровой реальности, где след формируется в виде последовательностей двоичного кода и характеризуется чрезвычайной уязвимостью и возможностью модификации. Конечной целью изучения цифровых следов и их криминалистического значения является активное совершенствование криминалистических рекомендаций, направленных на повышение качества предварительного расследования преступлений, на этапах подготовки, совершения и сокрытия которых могут быть обнаружены цифровые следы.

Список литературы:

[1] Тайтубаева Л. М. Механизм образования цифровых следов и способы их обнаружения // Право и государство: теория и практика. – 2023. – № 12 (228). – С. 530–532.

[2] Хомяков Э.Г. О сущности цифровых следов в криминалистике и их фиксации // Общество, право, государственность: ретроспектива и перспектива. – 2025. – № 1 (21). – С. 71–82.

[3] Ганжа М.В. Проблемы унификации и использования понятия «электронно-цифровой след» с учетом специфики реализации на практике // Вестник Уральского юридического института МВД России. – 2024. – № 2 (42). – С. 55–60.

[4] Скрипко В.А. О классификации криминалистически значимой компьютерной информации // Вестник Института права Башкирского государственного университета. – 2025. – Т. 8. – № 2 (26). – С. 187–197.

[5] Ким А. В. Компьютерная информация: понятие, содержание, форма // Судебная экспертиза и исследования. – 2026. – № 1. – С. 79–86.

References:

[1] Titubaeva L. M. Mechanism of formation of digital traces and methods of their detection // Law and state: theory and practice. – 2023. – № 12 (228). - S. 530-532.

[2] Khomyakov E.G. On the essence of digital traces in forensics and their fixation // Society, law, statehood: retrospective and perspective. – 2025. – № 1 (21). - S. 71-82.

[3] Ganzha M.V. Problems of unification and use of the concept of "electronic-digital footprint," taking into account the specifics of implementation in practice // Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. – 2024. – № 2 (42). - S. 55-60.

[4] Skripko V.A. On the classification of criminally significant computer information // Bulletin of the Institute of Law of Bashkir State University. – 2025. - VOL. 8. – № 2 (26). - S. 187-197.

[5] Kim A. V. Computer information: concept, content, form // Forensic examination and research. – 2026. – № 1. - S. 79-86.