Д. В. Бахтеев[*]

Е. В. Смахтин[**]

КРИМИНАЛИСТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ С ЦИФРОВЫМИ СЛЕДАМИ[1]

В статье рассматривается цифровая информация с точки зрения ее физической и правовой природы; описываются современные подходы к определению данного понятия в законодательстве и юридической науке. Анализируется соотношение цифровой информации и электронного носителя, на котором эта информация размещается. Рассматривается механизм трансформации цифровых следов в уголовно-процессуальные доказательства. Цифровая информация оценивается с точки зрения классификации информационных следов на материальные и идеальные; формулируется вывод о том, что цифровая информация представляет собой третью специфическую разновидность следовой информации, используемой в доказывании по уголовным делам. Приводится система признаков цифровых следов, к которым относятся опосредованность, возможность копирования и независимого существования копий, возможность преобразования в другие формы, существование на различных носителях, необходимость использования технических средств для их восприятия, обезличенность. Рассматривается классификация

[*] *Бахтеев Дмитрий Валерьевич – доцент кафедры криминалистики Уральского государственного юридического университета (Екатеринбург), кандидат юридических наук, e-mail: dmitry.bakhteev@gmail.com.*

[**] *Смахтин Евгений Владимирович – профессор кафедры уголовного права и процесса Тюменского государственного университета (Тюмень), доктор юридических наук, профессор, e-mail: smaxt@yandex.ru.*

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16001 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

цифровых следов с точки зрения формы их носителя, способа и характера доступа к ним, происхождения, места нахождения, формы представления.
Ключевые слова: цифровая информация, цифровые доказательства, электронная информация, электронный носитель информации, цифровые следы, цифровая криминалистика

XXI век для цивилизации вполне можно назвать цифровой эпохой. Трудно переоценить значение цифровых технологий для практически всех сфер деятельности. Экспоненциально возрастает разнообразие форм, средств и методов обработки цифровой информации, увеличивается ее общий объем, что зачастую не только способствует общественно одобряемым операциям с информацией, но и может иметь непосредственное отношение к преступной деятельности. Криминалистика должна адаптироваться к изменяющимся условиям, что требует не просто совершенствования, но и постоянного обновления криминалистических знаний о технических и тактических аспектах операций с цифровой доказательственной информацией в процессе выявления, раскрытия и расследования преступлений.

Термин «цифровая доказательственная информация» нуждается в уточнении. Во многих научных статьях по криминалистике используются термины «цифровая криминалистика»[1] и «цифровые технологии»[2]. Авторы пишут как о недостатках применения цифровых технологий, так и необходимости их более широкого внедрения в уголовное судопроизводство. Можно предположить, что если эти термины получили широкое распространение в криминалистике, то они должны быть законодательно закреплены. Однако в Федеральном законе от 27 июля 2006 г. № 149-ФЗ (ред. от 18 марта 2019 г.) «Об информации, информационных технологиях и о

[1] См., например: *Мещеряков В. А.* Цифровая криминалистика // Библиотека криминалиста. 2014. № 4. С. 231–241.

[2] См., например: *Гриб В. Г., Тюнис И. О.* Криминалистика и цифровые технологии // Российский следователь. 2019. № 4. С. 9–12.

защите информации» (далее – Закон об информации) и других законах и подзаконных нормативных правовых документах, посвященных этим вопросам[1], указанные термины не определены. В федеральном законодательстве речь идет об информационных технологиях, информационных системах и т. п.

В Федеральном законе от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» законодатель также не упоминает цифровые технологии, а оперирует терминами «информация в электронной форме», «электронный документ», «электронная подпись». Немаловажным обстоятельством для уголовного судопроизводства является то, что, согласно этому Закону, электронный документ признается равнозначным документу на бумажном носителе. Следовательно, наряду с документами на бумажных носителях существует легальное понятие электронных документов. Таким образом, фиксируется дифференциация «классических» и современных способов фиксации юридически значимой информации.

Использование электронных документов в уголовном судопроизводстве в качестве средств обеспечения документооборота предусмотрено ст. 474.1 УПК РФ. Кроме того, в этом Кодексе определен порядок изъятия электронных носителей информации (ст. 81–81.1 УПК РФ), а ст. 164.1 УПК (введена Федеральным законом от 27 декабря 2018 г. № 533-ФЗ) предусмотрены изъятие электронных носителей информации и копирование с них информации. Установлено, что электронные носители информации при производстве любых следственных действий изымаются с участием специалиста.

Хранение информации где бы то ни было осуществляется в зашифрованном, т. е. цифровом, виде. Закодированная таким образом информация (сообщения, данные) передается по информационно-

[1] См., например: Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16).

телекоммуникационным сетям или обрабатывается в информационных системах, исходя из смысла и содержания ст. 2 Закона об информации. На наш взгляд, именно в силу особенностей хранения такой информации она в криминалистике и уголовно-процессуальной науке получила название «цифровой». Следовательно, использование этого термина в науке вполне оправданно, однако с некоторыми оговорками.

Во-первых, поскольку этот термин законодательно не закреплен, необходимо делать уточнения об этом, в том числе в научных исследованиях. Например, В. Н. Чернышев и Е. С. Лоскутова пишут о требованиях, предъявляемых к собиранию и использованию цифровых доказательств[1]. Однако, если исходить из текста уголовно-процессуального законодательства, цифровых доказательств не существует. Опять же, следуя логике законодателя, использующего термин «электронные носители информации», в науке более корректным следует считать термин «электронные (цифровые) доказательства». В этом смысле более точен Ю. В. Гаврилин, который исследует особенности собирания доказательств в виде сведений на электронных носителях[2].

Во-вторых, необходимо «легализовать» в уголовном судопроизводстве цифровые технологии, уточнив, что электронные документы, их копии хранятся на электронных носителях информации в виде цифровых знаков (сигналов) и доступ к ним осуществляется с использованием средств вычислительной техники. В этом смысле интерес для уголовно-процессуальной и криминалистической науки представляет работа А. И. Зазулина, в которой предлагается новая редакция ст. 74 УПК РФ, а также дается авторское

---

[1] *Чернышов В. Н., Лоскутова Е. С.* Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5. С. 199–203.

[2] *Гаврилин Ю. В.* Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России // Труды Академии МВД России. 2018. № 3. С. 106–112.

определение понятия «цифровая информация»[1]. Если законодатель согласится с подобными предложениями, термин «цифровая информация» будет законодательно закреплен, что следует считать положительным фактором в развитии как науки, так и правоприменения.

Обратимся к вопросу о преобразовании цифровой информации в доказательство. Доказательств с позиций информационной концепции – это единство информации и его материального носителя[2]. В. С. Балакшин обоснованно считает, что доказательство – знаково-информационная система[3]. В такую систему условно могут быть включены:

цифровая информация, содержащаяся на любом электронном носителе;

электронный носитель информации;

процессуально регламентированный порядок собирания, проверки и оценки доказательств, размещенных на электронных носителях (ст. 81–81.1, 164.1 УПК РФ и др.).

Процесс формирования доказательства осуществляется уполномоченными лицами. Условно его можно представить в виде последовательного процессуального преобразования цифровой информации (в контексте уголовно-процессуальной поисковой деятельности – цифрового следа), содержащейся на электронных носителях, в электронное доказательство. Доказательство окончательно формируется уполномоченным лицом только после его процессуального оформления. В ходе собирания каждого доказательства уполномоченное лицо проверяет и оценивает его с точки зрения относимости, допустимости и достоверности. Только при

---

[1] *Зазулин А. И.* Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: автореф. дис. … канд. юрид. наук. Екатеринбург, 2018.

[2] См., например: *Орлов Ю. К.* Основы теории доказательств в уголовном процессе. М., 2000. С. 36.

[3] *Балакшин В. С.* Оценка допустимости доказательств в российском уголовном процессе: моногр. М., 2016. С. 109.

соблюдении указанных критериев полученное доказательство может быть признано таковым.

Исходя из сущности уголовного судопроизводства, одного признания существования цифровых следов недостаточно, необходимы также технологии преобразования таких следов в уголовно-процессуальные доказательства.

Актуальной задачей криминалистики как науки является уточнение порядка работы с цифровыми следами в процессе собирания доказательств. К работе со следами криминалисты, как правило, относят их обнаружение, фиксацию, изъятие и исследование. Применительно к цифровым следам особую значимость представляют также вопросы их хранения и копирования.

П. С. Пастухов подчеркивает роль специальных знаний в информационно-технологическом обеспечении уголовно-процессуального доказывания. Он определил особенности получения доказательственной информации, ее превращения в уголовно-процессуальные доказательства с участием специалистов экспертно-криминалистических подразделений[1], фактически предвосхитив изменения, которые были введены Федеральным законом от 27 декабря 2018 г. № 533-ФЗ (ст. 164.1 УПК РФ).

Подробно вопросы, связанные с использованием цифровых технологий в уголовном судопроизводстве, рассмотрены Л. А. Воскобитовой, по мнению которой, нужен взвешенный подход к внедрению цифровых технологий в уголовное судопроизводство[2]. Основные опасения автора связаны с тем, что цифровая информация может подвергаться изменению, модификации, копированию, монтажу и пр.

Одним из первых шагов законодателя на пути к внедрению цифровых технологий в уголовное судопроизводство можно считать введение ст. 164.1

---

[1] *Пастухов П. С.* Роль и значение специальных знаний в информационно-технологическом обеспечении уголовно-процессуального доказывания // Вестник Пермского университета. Юридические науки. 2014. Вып. 1. С. 298–303.

[2] *Воскобитова Л. А.* Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex russica. 2019. № 5. С. 91–104.

УПК РФ, согласно которой специалист участвует в случаях изъятия электронных носителей информации. Однако в настоящее время обеспечить участие специалиста во всех случаях изъятия электронных носителей информации практически невозможно, прежде всего в силу отсутствия достаточного количества специалистов в области IT-технологий. Вряд ли можно признать удачными повсеместно встречающиеся на практике случаи привлечения в качестве специалистов работников и менеджеров магазинов, торгующих электронными носителями информации.

Считаем, что в ходе производства любого следственного действия лицо, его производящее, должно отчетливо представлять, с какой разновидностью цифровых следов оно столкнулось. Соответственно, одним из основных вопросов, требующих научного обсуждения и решения, является вопрос о сущности и классификации цифровых следов.

В криминалистике существуют разные подходы к дифференциации следов как носителей информации. Условно разделим следы на материальные и идеальные. К материальным следам отнесены любые объекты материальной действительности, способные взаимодействовать на физическом или химическом уровне (пули, гильзы, следы рук, обуви, крови и т. д.). Восприятие такой информации, как правило, осуществляется непосредственно, она в основном носит точный и проверяемый характер. Идеальные следы – это мысли, воспоминания, ощущения и т. п., т. е. отражение объективной действительности в сознании человека, проявляющееся, как правило, вербально, в речи (при допросе, проверке показаний на месте и т. д.). Информация, закодированная в таких следах, воспринимается всегда опосредованно и подвержена ошибкам и искажениям. Р. С. Белкин отмечал, что «механизм возникновения идеальных изменений и сами эти изменения, как мысленные образы в сознании людей – участников или посторонних наблюдателей события, являются объектом исследования криминалистики лишь отчасти, поскольку криминалистика черпает основные данные об этих

процессах из психологии (общей и судебной), физиологии и других наук о человеке»[1].

Как отмечалось, роль в этой системе цифровой информации до сих пор окончательно не определена, хотя ряд авторов уже высказали позицию по вопросу о ее сущности и месте в классификации следов[2]. С одной стороны, она обладает свойствами материальных следов, поскольку представляет собой характеристику носителя информации, к примеру уровень намагниченности участка поверхности жесткого диска или электрический заряд в транзисторах твердотельных накопителях (флеш-карты, SSD). С другой стороны, цифровая информация не может восприниматься субъектом познания (например, следователем) непосредственно, для ее обнаружения и исследования требуются технические устройства, равно как для осуществления операций с идеальной информацией необходима ее передача от человека, который ей владеет. Но к идеальным следам цифровую информацию также отнести нельзя.

С точки зрения доказательственной значимости (причем при рассмотрении не только уголовных, но и гражданских, арбитражных и административных дел) цифровая информация относится не к результату вычислительных операций, производимых компьютерной техникой, а к последствиям действий пользователей или администраторов. По аналогии с другими категориями доказательств такая информация может обеспечивать решение задач судопроизводства, однако для работы с ней классических юридических знаний может быть недостаточно.

Некоторые авторы, говоря о доказательственной значимости электронной (цифровой) информации, предлагают сохранять за ее копиями статус

---

[1] *Белкин Р. С.* Курс криминалистики: учеб. пособие для вузов: в 3 т. 3-е изд., доп. М., 2001. Т. 2. С. 25.

[2] *Шелегов Ю. В.*, *Шелегов В. Г.* К вопросу о классификации электронных (цифровых) доказательств // Криминалистика: вчера, сегодня, завтра. 2019. № 2. С. 63–67.

доказательств, определяя ряд условий для этого[1]. Не оспаривая этих суждений, отметим, что помимо обязательного участия специалиста при копировании электронной информации необходимо законодательно обеспечить и другие гарантии, препятствующие преобразованию электронной информации при копировании. Одним словом, копия должна полностью соответствовать оригиналу, а только участие специалиста, тем более формальное, таких гарантий не дает.

Кроме того, УПК, повторим, не предусматривает отдельного вида так называемых электронных, или цифровых, доказательств, оперируя термином «электронные носители информации» или «информация на электронных носителях». С точки зрения современной системы доказательств электронные носители относятся к вещественным доказательствам либо к иным документам. Вопрос о том, следует ли изменить ст. 74 УПК РФ и ввести новый вид доказательств – электронные (цифровые) доказательства, вызывает много споров и предполагает фундаментальное научное исследование, а потому в рамках настоящей статьи не рассматривается.

В зарубежных источниках акцент сделан именно на цифровой сущности рассматриваемых доказательств; электронная природа носителя учитывается, однако интерес вызывает в первую очередь сама цифровая информация, а не ее носитель[2]. При этом используемые термины могут либо отражать технико-криминалистическую сторону исследуемых объектов, их следовую сущность *(digital traces, digital footprints)*, либо отсылать к их доказательственному значению *(digital evidence)*. Однако при составлении нормативных документов

---

[1] *Овсянников Д. В.* Копирование электронной информации как средство уголовно-процессуального доказывания: автореф. дис. … канд. юрид. наук. Екатеринбург, 2018.

[2] См., например: *Sadiku M., Tembely M., Musa S.* Digital Forensics // International Journal of Advanced Research in Computer Science and Software Engineering. 2017. No. 7. P. 274–276. DOI: 10.23956/ijarcsse/V7I4/01404; *Casey E.* Maturation of digital forensics // Digital Investigation. 2019. No. 29. DOI: A1-A2.10.1016/j.diin.2019.05.002.

в большинстве государств используется термин «электронные доказательства»[1]. Полагаем, что такой подход является правильным.

В структуре криминалистики формируются системные отрасли (подотрасли), посвященные изучению цифровых следов. Так, научное обоснование частной криминалистической теории компьютерной информации и средствах ее обработки предложил В. Б. Вехов[2]. М. А. Романенко ратует за термин «судебная дигитология», под которой им понимается отрасль криминалистической техники, а ее предметом являются «знания о сборе, закреплении (фиксации) и исследовании электронно-цифровых устройств, программ и явлений, в основе функционирования которых лежат вычислительные процессы, имеющие объективное выражение, с целью выявления фактов и обстоятельств, значимых для дела. При этом объектами судебной дигитологии выступают те устройства (персональные компьютеры, их комплектующие, периферийное оборудование (принтеры, сканеры и т. д.), цифровые фотоаппараты, сотовые телефоны и др.), действие которых будет основано на вычислительных процессах»[3]. Перспективы использования предлагаемого термина сомнительны, однако необходимость изучения указанных следов совершенно очевидна.

Рассмотрим отдельные содержательные характеристики цифровой информации в контексте ее потенциального преобразования в уголовно-процессуальное доказательство.

1. Опосредованность. Существование цифровой информации невозможно без материального носителя.

---

[1] *Mason S.* World electronic signature legislation Digital Evidence and Electronic Signature // Law Review. 2018. Vol. 15. DOI: http://dx.doi.org/10.14296/deeslr.v15i0.4917.

[2] *Вехов В. Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. … д-ра юрид. наук. Волгоград, 2008. С. 457–477.

[3] *Романенко М. А.* Новый подход к содержанию криминалистической системы криминалистической техники // Вестник Пермского университета. 2008. № 2. С. 118.

2. Возможность копирования без утраты объема и содержания копируемой информации. Копия отдельного файла полностью ему идентична и может существовать (изменяться) безотносительно оригинала.

3. Одновременное существование нескольких копий. Один и тот же фрагмент цифровой информации может быть зафиксирован на разных, зачастую удаленных друг от друга, носителях, которые могут быть и не быть синхронизированы. Доступ к такой информации могут одновременно иметь различные субъекты.

4. Возможность преобразования в другие формы. Содержание мультимедийного компьютерного файла может быть преобразовано в аналоговую форму, скриншот или текстовый документ, которые можно распечатать, и т. д.

5. Возможность существования на различных носителях.

6. Необходимость применения специальных технических средств для восприятия цифровой информации.

7. Обезличенность. В большинстве случаев установление автора или владельца цифровой информации может представлять существенную проблему для правоохранительных органов.

Цифровые следы как форма существования цифровой информации могут быть классифицированы по различным основаниям.

Первым основанием классификации цифровых следов выступает *форма носителя*. Выделяют цифровые следы, расположенные на оптических носителях (CD, DVD, blu-ray диски и пр.), полупроводниковых носителях (флеш-накопители, SSD и магнитные носители (жесткие диски).

Другим основанием деления цифровых следов является *способ доступа* к ним – локальный или удаленный. В первом случае доступ осуществляется непосредственно через устройство, содержащее носитель, на котором находятся цифровые следы. При этом возможен весь комплекс криминалистических операций по обнаружению, фиксации, изъятию и исследованию следов. При расположении искомой информации на удаленном

носителе доступ к следам возможен только при использовании подключения к телекоммуникационным сетям. При этом исключается изъятие следов в традиционном криминалистическом понимании, однако они могут быть скопированы на носитель.

По *характеру доступа* цифровые следы могут быть доступными (например, электронные документы), скрытыми (скрытые файлы, информация, скрытая с помощью методов стеганографии) и зашифрованными. В последнем случае сам факт наличия информации очевиден субъекту расследования, однако доступ к ее содержанию заблокирован, как правило, с помощью паролей или иных средств идентификации или аутентификации ее создателя или владельца.

По *характеру происхождения* цифровые следы дифференцируются на оставленные человеком непосредственно (электронные документы, записи в социальных сетях и т. п.) и опосредованно (данные телеметрии, файлы регистрации, атрибуты создаваемых файлов и т. п.). Следы первой группы могут быть исследованы в ходе производства следственных действий (например, в ходе осмотра места происшествия), следы же второй группы требует использования специальных знаний (как правило, производства компьютерно-технических исследований).

По *месту нахождения* выделяют цифровые следы, физически находящиеся на компьютерных устройствах преступника (например, исходный код вредоносного программного обеспечения или шаблоны для изготовления подложных документов), потерпевшего (например, функционирующее вредоносное программное обеспечение), сторонних лиц (например, электронная почта на сервере организации, предоставляющей услуги такого рода). Разумеется, цифровые следы могут одновременно располагаться на носителях, относящихся ко всем трем группам. Физическое нахождение следа на электронных носителях информации не исключает и их виртуального нахождения в так называемых облачных сервисах. Поскольку непосредственное изъятие таких следов практически невозможно, они не

рассматриваются в классификации по этому основанию. Однако их копирование в ходе производства следственного действия не исключено.

Следует учитывать, что доказывание связи цифровых следов с конкретным лицом всегда зависит от типа устройства и в некоторых случаях может быть усложнено. Так, подозреваемый может заявить, что доступ к его персональному компьютеру имела группа людей; им также может быть выдвинута версия о том, что его учетная запись в социальной сети была взломана третьими лицами и т. д.

С точки зрения *формы представления* большинство цифровых следов – это текстовая информация, однако в следственно-судебной практике встречаются случаи использования следов в графической или звуковой форме.

Таким образом, цифровые следы не могут быть отнесены к идеальным, а также не в полной мере соответствуют характеристикам материальных следов. Они представляют третью специфическую разновидность следовой информации, используемой в доказывании по уголовным делам. Исходя из этого, несомненна актуальность дальнейшего изучения сущности цифровых следов, а также особенностей работы с ними. Причем необходимо комплексное исследование рассматриваемых следов как уголовно-процессуальными, так и криминалистическими методами.

Список литературы

Балакшин В. С. Оценка допустимости доказательств в российском уголовном процессе: моногр. М., 2016.

Белкин Р. С. Курс криминалистики: учеб. пособие для вузов: в 3 т. 3-е изд., доп. М., 2001. Т. 2.

Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. … д-ра юрид. наук. Волгоград, 2008.

Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5.

Гаврилин Ю. В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России // Труды Академии МВД России. 2018. № 3.

Гриб В. Г., Тюнис И. О. Криминалистика и цифровые технологии // Российский следователь. 2019. № 4.

Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: автореф. дис. … канд. юрид. наук. Екатеринбург, 2018.

Мещеряков В. А. Цифровая криминалистика // Библиотека криминалиста. 2014. № 4.

Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания: автореф. дис. … канд. юрид. наук. Екатеринбург, 2018.

Орлов Ю. К. Основы теории доказательств в уголовном процессе. М., 2000.

Пастухов П. С. Роль и значение специальных знаний в информационно-технологическом обеспечении уголовно-процессуального доказывания // Вестник Пермского университета. Юридические науки. 2014. Вып. 1.

Романенко М. А. Новый подход к содержанию криминалистической системы криминалистической техники // Вестник Пермского университета. 2008. № 2.

Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5.

Шелегов Ю. В., Шелегов В. Г. К вопросу о классификации электронных (цифровых) доказательств // Криминалистика: вчера, сегодня, завтра. 2019. № 2.

Casey E. Maturation of digital forensics // Digital Investigation. 2019. No. 29. DOI: A1-A2.10.1016/j.diin.2019.05.002.

Mason S. World electronic signature legislation Digital Evidence and Electronic Signature // Law Review. 2018. Vol. 15. DOI: http://dx.doi.org/10.14296/deeslr.v15i0.4917.

Sadiku M., Tembely M., Musa S. Digital Forensics // International Journal of Advanced Research in Computer Science and Software Engineering. 2017. No. 7. DOI: 10.23956/ijarcsse/V7I4/01404.