Научная статья
УДК 343.982.3:004(470)

Эдуард Геннадьевич Хомяков
Удмуртский государственный университет, Ижевск, Россия, ed-18@yandex.ru

О СУЩНОСТИ ЦИФРОВЫХ СЛЕДОВ В КРИМИНАЛИСТИКЕ И ИХ ФИКСАЦИИ

Аннотация. В статье освещаются вопросы, связанные с развитием криминалистического учения о цифровых следах. Предлагается определение цифровых следов, в котором они рассматриваются как совокупность данных, остающихся в результате любой активности пользователя в цифровой среде, оценивается их сущность с позиции двойственной (дуалистической) природы. На основании классического криминалистического учения о следообразовании обозначаются объекты, участвующие в образовании цифровых следов, дается их характеристика. Приводится усеченная классификация цифровых следов, анализируется их связь с цифровыми устройствами. Исходя из сущности цифровых следов, рассматриваются вопросы их обнаружения и фиксации с использованием при этом соответствующих технико-криминалистических (аппаратных и программных) средств. Делается вывод о необходимости регламентации процедуры работы с цифровыми следами (цифровыми доказательствами) как на законодательном, так и на подзаконном уровнях, а также дальнейшего осмысления и развития криминалистического учения о цифровых следах.

Ключевые слова: цифровые следы, данные, виды цифровых следов, цифровые устройства, цифровые доказательства, цифровое пространство, механизм образования цифровых следов, изъятие цифровых следов, фиксация цифровых следов, анализ

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

Original article

Eduard G. Khomyakov
Udmurt State University, Izhevsk, Russia, ed-18@yandex.ru

ON THE NATURE OF DIGITAL TRACES IN FORENSICS AND THEIR FIXATION

Abstract. The article highlights issues related to the development of the forensic sci-ence of digital traces. It proposes the definition of digital traces, in which they are considered as a set of data remaining as a result of any user activity in the digital environment, evaluates their essence from the standpoint of a dual (dualistic) nature. Based on the classical forensic doctrine of trace for-mation, the objects involved in the formation of digital traces are designated and their characteristics are given. A truncated classification of digital traces is given, their connection with digital devices is analyzed. Based on the na-ture of digital traces, the issues of their detection and fixation are considered using appropriate technical and forensic (hardware and software) tools. It is concluded that it is necessary to regulate the procedure for working with dig-ital traces (digital evidence) both at the legislative and by-law levels, as well as further understanding and development of the forensic doctrine of digital traces.

Keywords: digital traces, data, types of digital traces, digital devices, digital evidence, digital space, mechanism of formation of digital traces, removal of digital traces, fixation of digital traces, analysis

For citation: Khomyakov E. G. On the nature of digital traces in forensics and their fixation // Society, law, statehood: retrospective and perspective. 2025. No. 1 (21). P. 71–82. (In Russ.)

Введение

Среди отдельных направлений современной криминалистики особый интерес представляет учение о цифровых следах как источниках криминалистически значимой компьютерной информации [1, с. 198; 2, с. 40–57]. В рамках данного учения различными исследователями предпринимаются попытки раскрыть (уточнить) сущность цифровых следов, рассмотреть механизм их образования, обозначить разновидности, подобрать средства и способы обнаружения, фиксации, изъятия и исследования данных следов.

Можно отметить, что в последнее время появилось достаточно много научных работ, демонстрирующих значительное разнообразие взглядов по обозначенным вопросам. Например, И. И. Лузгин считает целесообразным создание «цифрового следоведения, изучающего извлечения цифровой информации из сетей и технологических коммуникационных средств, как полноценной отрасли раздела криминалистической техники» [3, с. 13].

Также не прекращаются дискуссии по выбору наиболее точного и объективного определения термина «цифровой след» применительно к криминалистике. Целая группа криминалистов (А. М. Багмет, В. В. Бычков, Н. Н. Ильин, С. Ю. Скобелин [4, с. 7], В. Б. Вехов, Е. В. Смахтин[1] и др.) считает, что «цифровой след – это любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи», относит их к материальным невидимым следам.

Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский полагают, что «цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи», относят данные следы к материальным [2, с. 44].

Синонимично данному понятию разными авторами предлагались и анализировались термины «виртуальные следы», «электронно-цифровые следы» («электронные цифровые следы»), «бинарные следы», «информационные следы», «компьютерно-технические следы», «виртуально-информационные следы» с обозначением их преимуществ и недостатков [5; 6; 7; 8; 9], однако полемика по данному вопросу продолжается и в настоящее время. Например, по мнению А. Б. Смушкина «электронные цифровые следы представляют собой следы отражения совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве информационно-технологических устройств, их систем и сетей»; они занимают промежуточное место между материальными и идеальными следами; «электронный цифровой след является одним из видов виртуального следа»[2].

В. Б. Вехов, описывая сущность электронно-цифрового следа в своей диссертационной работе 2008 года, указывал, что под данным термином понимается «любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов» [10, с. 22–23]; в настоящее время схожее определение дается им в отношении цифрового следа.

А. В. Нестеров и К. К. Сейтенов предлагают обратить внимание на «электронные следы-данные, виртуальные следы-данные и/или цифровые следы-данные» [11, с. 98].

В этой связи представляется весьма актуальным дальнейшее изучение сущности

[1] Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. М. : Издательство Юрайт, 2024. С. 97.

[2] Смушкин А. Б. Цифровизация криминалистической деятельности : учебное пособие / А. Б. Смушкин; под ред. В. Б. Вехова. М. : КНОРУС, 2024. С. 93.

цифровых следов, связанных с событием преступления, с акцентированием внимания на их фиксации и сохранении.

Методы

В исследовании применялись как традиционные общенаучные формально-логические методы – анализ и синтез, сравнение, аналогия и индукция, так и специальные – метод интеграции данных в информационных системах, метод информационного подхода. В целях обобщения и упорядочения цифровых следов в качестве исследуемых объектов, их разделения по определенным признакам использовался метод классификации. Исследование основано на изучении теоретических материалов по цифровизации криминалистической и судебно-экспертной деятельности, а также практики работы отечественных и зарубежных правоохранительных органов с цифровыми данными.

Результаты

Соглашаясь с точкой зрения ученых-криминалистов о сложной природе цифровых следов и неоднозначного понимания их сущности, считаем возможным следующее их определение. Цифровые следы – это совокупность данных, остающихся в результате любой активности пользователя (субъекта) в цифровой среде (цифровом пространстве), включая Интернет, мобильные устройства, системы связи и иные информационные технологические средства; эти данные, генерируемые пользователями или их цифровыми устройствами во время взаимодействия с программными продуктами, информационными системами и сервисами, могут использоваться для идентификации поведения, действий или взаимодействий субъекта.

В этой связи вызывает интерес точка зрения А. Г. Себякина, который, отдавая предпочтение термину «электронно-цифровой след», считает, что «не совсем корректно определять след как информацию» в связи с тем, что «информация является субъективным отражением объективных данных», кроме того, «информативность следа является одним из его свойств <…> Соответственно, информативность не может являться свойством информации, а является свойством объективных данных» [12, с. 45–46].

При этом данные можно рассматривать как «интерпретируемое представление информации в формализованном виде, удобном для передачи, интерпретации или обработки», а цифровое пространство как «пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур»[1].

Цифровые устройства – компьютеры, серверы, смартфоны, планшеты, цифровые камеры и видеорегистраторы, цифровые носители данных (жесткие диски, USB- и SSD-накопители и др.) и т. д. – это устройства, которые обрабатывают данные в дискретной, то есть цифровой форме. Они преобразуют всю информацию в двоичный код (нулевые и единичные сигналы) для ее хранения, обработки и передачи. Цифровые устройства являются разновидностью электронных устройств, которые также могут быть аналоговыми.

Цифровые следы могут быть активными – сознательно оставляемыми пользователем или пассивными – автоматически генерируемыми соответствующими цифровыми устройствами (смартфонами, планшетами, ноутбуками, цифровыми фото- и видеокамерами, цифровыми гаджетами для дома и т. д.).

Активные цифровые следы – это данные, которые пользователь сознательно создает и размещает в цифровом пространстве на различных информационных ресурсах, например, публикации в социальных сетях, комментарии, электронные письма и т. д.

Пассивные цифровые следы – это данные, которые генерируются автоматически в

[1] Толковый словарь терминов и понятий по вопросам цифровой трансформации. URL: https://library.bsuir.by/ru/tolkovyy-slovar-terminov-i-ponyatiy-po-voprosam-tsifrovoy-transformatsii; URL: https://elib.bsu.by/bitstream/ (дата обращения: 18.10.2024).

ходе взаимодействия с цифровыми устройствами или онлайн-сервисами, такие как IP-адреса, метаданные о времени и месте входа, история посещенных сайтов и использованных приложений.

Можно также отметить, что для криминалистического описания следов, оставляемых пользователями в цифровой среде (цифровом пространстве), в английском языке в зависимости от контекста принято использовать термины «digital traces» или «digital footprints»; термин «digital evidence» в большей степени отражает их доказательственное (процессуальное) значение [13, с. 66].

Природу цифровых следов, безусловно, следует рассматривать с двух сторон (позиций); в этом проявляется их двойственная (дуалистическая) природа.

Материальный аспект цифровых следов проявляется в том, что для их существования требуется физическая среда – носители данных, процессоры, сети передачи данных. Информация может храниться на жестких дисках, картах памяти, передаваться по проводам, иными способами, и эти физические носители обеспечивают существование цифровых данных; то есть оборот цифровых данных требует реальных физических ресурсов.

Кроме того, цифровые данные, представленные в виде битов и байтов, основаны на физических процессах. В цифровых устройствах биты – это конкретные физические состояния: уровень напряжения или тока в цепи, магнитные состояния на жестком диске, фотонные потоки в оптоволокне и т. д. Эти состояния можно зафиксировать и количественно оценить через физические измерения.

Идеальными цифровые следы можно считать в связи с тем, что они представляют собой информацию: числа, текст, изображения, лог-файлы, метаданные и др. Эта информация сама по себе не имеет материальной формы; цифровые данные можно рассматривать как идеальные, поскольку они являются абстракцией: набором символов или чисел, которые имеют смысл только в контексте их интерпретации. Например, последовательность 100101 может быть интерпретирована как число, текст, изображение или команда в зависимости от контекста. Этот аспект данных ближе к идеальной сущности, так как сама по себе информация не имеет физической формы, а представляет нечто концептуальное.

Различные цифровые данные, такие как текстовые, аудио-, фото- и видеофайлы, а также другие формы информации, воспринимаются людьми как абстрактные сущности, которые можно передавать через различные носители без изменения их содержания.

Это сочетание материальных и идеальных аспектов делает цифровые следы сложными для однозначной классификации, и их природа зависит от того, как и в каком контексте они рассматриваются.

В классической криминалистике, согласно криминалистическому учению о следообразовании, след является результатом взаимодействия двух объектов – следообразующего и следовоспринимающего[1].

Следообразующим объектом для цифрового следа можно считать материальный (физический) или виртуальный объект, действие которого порождает цифровой след в информационном пространстве. Такими объектами могут быть цифровые устройства с установленными на них программными средствами (программным обеспечением) в обязательной взаимосвязи с субъектом (человеком), применяющим их в своей жизни, в том числе в преступной деятельности. Следообразующий объект генерирует данные, которые могут быть использованы для его идентификации, отслеживания его действий, анализа поведения. Именно в этой связи проявляется криминалистический аспект цифровых следов.

При рассмотрении особенностей действий (функционирования) следообразую-

[1] Применительно к цифровым следам целесообразно в отдельной работе рассмотреть использование терминов «следообразующая среда» и «следовоспринимающая среда».

щего объекта можно оценить виды и типы цифровых следов, которые образуются в процессе следообразования.

Человек в ходе работы на различных цифровых устройствах формирует цифровые следы, например, в истории браузера и в логах[1] приложений; обозначает свою активность, используя ресурсы сети Интернет, создавая публикации, комментарии, лайки на веб-сайтах и в социальных сетях, производя поисковые запросы и т. д.; оставляет свои локационные данные (информацию о местоположении и перемещениях).

Цифровые устройства генерируют данные об используемых приложениях, сетевых соединениях, времени работы и других параметрах; «умные устройства», объединенные в сеть (система Интернет вещей (IoT)) – камеры, датчики, умные часы, бытовая и иная техника, – оставляют цифровые следы в виде данных о взаимодействии с сетью или другими устройствами. При этом серверы и сетевое оборудование фиксируют сетевые соединения, логи доступа, ошибки и другие события.

Программные средства (операционные системы, социальные сети, менеджеры, браузеры) фиксируют логи действий пользователя, историю входов в систему и выхода из нее, данные о запущенных программах, взаимодействие пользователей (их публикации, лайки, комментарии), данные о сообщениях, времени отправки, метаданные о контактах, посещенные веб-сайты, сохраненные файлы cookie, историю поисковых запросов и также образуют цифровые следы.

Сети функционируют, используя IP-адреса, DNS-запросы, сетевые пакеты: каждый раз, когда устройство подключается к сети Интернет, оно использует IP-адрес, который можно отследить; DNS-запросы содержат данные о том, какие доменные имена запрашивались при обращении к интернет-ресурсам; логи сетевого трафика и пакетов создают следы о взаимодействии с другими устройствами и веб-сайтами.

Каждый следообразующий объект уникален, и его цифровой след может использоваться для установления связи между этим объектом и его функционированием в цифровом пространстве.

Следовоспринимающими объектами в данном случае становятся различные объекты цифрового пространства, охваченные преступной деятельностью.

С учетом обозначенного механизма цифрового следообразования можно выделить несколько типов цифровых следов, представляющих интерес для следствия, которые можно фиксировать при осмотре или экспертном исследовании, например, компьютерного устройства:

1. Файловые следы. Это наиболее распространенный тип цифровых следов, к которому можно отнести: удаленные, скрытые, измененные и временные файлы, историю браузера.

2. Сетевые следы, характеризующие сетевые взаимодействия и соединения устройства с внешними серверами. К ним относят: логи подключений – записи всех попыток подключения устройства к сети; сетевой трафик – данные о передаче информации между устройством и внешними ресурсами; IP-адреса – уникальные идентификаторы сетевых устройств, DNS-запросы – запросы, которые отправляются устройством к DNS-серверу с целью преобразования доменного имени в IP-адрес, необходимый для установления соединения с веб-сервером или другим сетевым ресурсом.

3. Следы операционной системы, к которым относят: журналы событий (англ. event logs) – записи (логи, лог-файлы), которые содержат хронологическую информацию о действиях и событиях, происходящих в системе, программе или сети (входы в систему, изменения в файлах и другие действия); данные о запуске программ – информация о том, какие программы были запущены на устройстве и в какое время; системные ошибки, которые могут указывать на попыт-

[1] Лог (лог-файл) – это записи событий и сообщений, создаваемые компьютерной программой или системой во время ее работы.

ки взлома или несанкционированного доступа к системе.

4. Метаданные, к которым относят: временные метки (англ. timestamps) – данные о времени создания и последнего изменения файлов; геолокацию – информацию о местоположении устройства при создании или изменении файлов.

Исходя из сущности цифровых следов должны решаться вопросы их обнаружения, фиксации, изъятия и исследования. Задача обнаружения цифровых следов связана с поиском цифровых (электронных) носителей информации – как материальных, так и виртуальных.

Материальные цифровые носители информации могут либо входить в состав цифровых устройств, либо храниться отдельно от них. В качестве подобных носителей информации могут выступать магнитные носители (дискеты, жесткие диски), оптические диски (CD, DVD, Blu-ray), полупроводниковые носители (флеш-накопители, карты памяти, твердотельные накопители).

Виртуальные цифровые носители информации – это не физические объекты, а цифровые среды, где данные существуют в электронном виде и могут быть доступны через сеть Интернет или другие сети. Примером подобных носителей выступают облачные хранилища (Яндекс Диск, Google Диск, Dropbox, TeraBox и др.), виртуальные машины или серверы, сетевые базы данных (сетевые хранилища), логические разделы данных, существующие только в виртуальной среде.

Изъятие цифровых (электронных) носителей информации должно производиться с соблюдением требований Уголовно-процессуального кодекса Российской Федерации (ч. 4.1 ст. 164; ст. 164.1; ч. 8 ст. 166), в том числе с участием специалиста. При этом не все сотрудники следственных и оперативных подразделений понимают, «какой именно специализации и компетенции в области информационно-компьютерных технологий специалист им требуется», «каким требованиям должен соответствовать специалист, какими методиками обладать, какие технические средства использовать, чтобы обеспечить исчерпывающие меры к обнаружению и фиксации доказательств и исключить их утрату» [14, с. 182].

Без сомнения, в качестве подобного специалиста можно привлекать судебного эксперта, имеющего право самостоятельного производства судебной компьютерной экспертизы и обеспеченного соответствующими технико-криминалистическими средствами. Однако в настоящее время это практически неисполнимо, «прежде всего в силу отсутствия достаточного количества специалистов в области IT-технологий» [13, с. 64] и необходимого инструментария в их распоряжении.

Фиксация цифровых следов на месте обнаружения материальных цифровых носителей информации, которые являются в большинстве своем элементами цифровых устройств, может производиться путем копирования информации, которую они содержат. При этом исследование откопированной информации и определение той, которая имеет отношение к событию конкретного преступления (выявление цифровых следов), должно производиться в рамках производства компьютерной (компьютерно-технической) экспертизы.

В качестве копировщиков могут использоваться специальные устройства – аппаратные и программные блокираторы записи (Write Blockers), которые предотвращают изменение данных на жестком диске при его подключении к компьютеру для анализа и копирования данных. Копирование может производиться и на материальные носители информации (жесткие и оптические диски, твердотельные накопители) при их наличии у следователя и специалиста.

Для поиска цифровых следов, содержащих информацию о событии преступления, возможно использование и специализированного программного обеспечения, например, EnCase, FTK (Forensic Toolkit), Autopsy, Wireshark или их отечественных аналогов [15].

Необходимо отметить, что следователи, как правило, не обладают квалификацией

специалистов (экспертов) в области цифровой криминалистики и их основная задача при обнаружении цифровых устройств – обеспечить их сохранность и изоляцию от внешних воздействий до передачи судебному эксперту для производства экспертного исследования (экспертизы). Это приводит к необходимости разработки методик и стандартов, которые позволяют минимизировать риск утраты или искажения цифровых данных на этапе первичного осмотра.

Так, если цифровое устройство выключено, то следователь не должен его включать, а должен описать его внешний вид, место обнаружения, положение и подключенные периферийные устройства (при их наличии). Действия следователя при обнаружении включенного цифрового устройства, например, компьютера, требуют особой осторожности, так как любое вмешательство может изменить цифровые следы или привести к их утрате. Поэтому при обнаружении включенного компьютера следователь должен сделать фотоснимки его экрана, фиксирующие все открытые программы (запущенные приложения), активные окна, документы, текстовые сообщения и другую информацию, например, сетевые подключения, часы.

Также необходимо зафиксировать текущее состояние устройства в письменном виде. Оно может включать: текущие дату и время (указанные на экране устройства), идентификаторы открытых приложений и файлов, наличие подключений к сети, подключенные внешние устройства (например, USB-накопители или внешние жесткие диски).

Следователь не должен пытаться самостоятельно закрывать программы, перемещать файлы или пытаться разобраться в содержимом компьютера. Важно помнить, что даже перемещение курсора или взаимодействие с операционной системой может изменить журналы событий, временные метки файлов или активировать автосохранение файлов.

После фиксации текущего состояния компьютера, произведенного вышеуказанными способами, необходимо произвести его изоляцию от сетевого подключения (проводного и беспроводного), чтобы предотвратить удаленный доступ к нему или автоматическое удаление данных. Для этого следует отключить кабель Ethernet (при его подключении), Wi-Fi через физическую кнопку на устройстве (если такая есть) или с помощью сетевых настроек, если следователь обладает минимальными техническими знаниями. В качестве альтернативного варианта – поместить цифровое устройство в экранирующий чехол (сумку Фарадея – Faraday Bag), что полностью заблокирует его доступ к беспроводной сети.

При участии специалиста возможна фиксация цифровых следов на работающем цифровом устройстве. Это прежде всего анализ и фиксация оперативной памяти (ОЗУ, RAM). Использование специальных инструментов для захвата содержимого оперативной памяти, например, программ FTK Imager или Belkasoft RAM Capturer, позволяет снять копию данных из оперативной памяти, то есть зафиксировать все текущие процессы, сетевые соединения и временные данные, которые будут утрачены при выключении устройства.

Далее для сохранения всех данных на цифровом устройстве необходимо создание образа (копии) жесткого диска, для чего могут использоваться копировщики – блокираторы записи. Это позволяет избежать случайной порчи данных и дает возможность работать с копией при дальнейшем ее анализе (исследовании).

Для фиксации сетевых соединений специалист также может использовать специальные инструменты, например, программу-анализатор трафика для компьютерных сетей Wireshark; она способна фиксировать сетевой трафик и производить анализ активных подключений цифрового устройства. Цифровые сетевые следы могут включать IP-адреса, порты, данные пакетов, сессии и другую информацию, которая позволяет отследить действия пользователей или устройств в сети.

Сетевые следы могут помочь в установлении факта подключения устройства

к сети, географического местоположения устройства через анализ IP-адресов, активности пользователя в сети, включая доступ к веб-ресурсам и отправку данных.

Также при дальнейшем исследовании цифрового устройства необходимо произвести снятие (запись) логов операционной системы и временных файлов.

Системные журналы (логи) операционной системы могут содержать критическую информацию о последних действиях пользователя, попытках доступа, ошибках и других событиях. Объем логов сильно зависит от активности системы, уровня детализации логирования и времени, в течение которого логи собираются. В некоторых случаях, особенно на серверах, объем логов может исчисляться гигабайтами. Например, на активно используемом компьютере лог событий может занимать от нескольких мегабайт до десятков гигабайт в зависимости от числа приложений, настроек системы и ее интенсивного использования. К основным типам системных журналов (логов) относят журнал событий (Event logs), журнал безопасности (Security logs), журнал приложений (Application logs), журнал сетевых подключений (Network logs).

Логи могут помочь определить точное время инцидента, например, взлома системы или попытки несанкционированного доступа. По журналам аутентификации можно отследить, кто и когда пытался получить доступ к системе, откуда была произведена попытка входа (IP-адрес) и была ли она успешной. Логи событий, такие как запуск или завершение служб (приложений операционной системы), могут показать, какие действия выполнялись на компьютере, а также выявить подозрительные процессы.

Временные файлы (temporary files, temp files) – это файлы, которые создаются операционной системой или программами для временного хранения данных в процессе их работы и располагаются в специальных системных каталогах. Они нужны для выполнения определенных задач, ускорения работы программ, а также обеспечения стабильности работы системы; они обычно удаляются автоматически после завершения программы, но иногда могут оставаться на устройстве (например, при сбое программы).

Следует помнить о том, что для возможности дальнейшего использования цифровых следов в уголовном судопроизводстве они должны быть зафиксированы с использованием специальных инструментов (сертифицированного программного и аппаратного обеспечения), методик и процедур, исключающих изменение исходных данных, сохраняющих при этом их целостность и подлинность.

Правоохранительные органы за рубежом при работе с цифровыми доказательствами чаще всего используют в этих целях специализированные руководства и стандарты, наиболее соответствующие специфике их деятельности. Это прежде всего международные стандарты цифровой криминалистики: ISO/IEC 27037:2012[1], ISO/IEC 27041:2015, ISO/IEC 27042:2015.

К ним также можно отнести методические рекомендации от правоохранительных агентств, например, руководства и протоколы Федерального бюро расследований, Европола и Интерпола. Эти организации имеют свои собственные внутренние стандарты и руководства по цифровой криминалистике, которые часто более детализированы в плане процедур и процедурных требований и нацелены на решение правоохранительных задач.

В Великобритании с 2012 года используется ACPO (Association of Chief Police Officers) Good Practice Guide for Digital Evidence[2]. Ру-

[1] В Российской Федерации на основе ISO/IEC 27037:2012 подготовлен ГОСТ Р ИСО/МЭК 27037-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

[1] ACPO Good Practice Guide for Digital Evidence. URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (дата обращения: 18.10.2024).

ководство описывает подходы и принципы обращения с цифровыми доказательствами, которые являются стандартными для полиции Великобритании и широко используются в других странах. Данный документ предоставляет практические рекомендации по правильному изъятию и фиксации цифровых доказательств, достоверности и допустимости цифровых доказательств в суде, минимизации риска нарушения целостности цифровых данных при их изъятии и анализе. Цифровые следы в указанном руководстве не упоминаются, но их можно рассматривать в контексте цифровых доказательств.

В США Национальным институтом стандартов и технологий разработано руководство по криминалистическому анализу цифровых данных (Guide to Integrating Forensic Techniques into Incident Response) – NIST 800-86[1]. Данный документ предлагает методы и процедуры, позволяющие собирать, анализировать и сохранять цифровые доказательства в ходе реагирования на киберинциденты. В нем описаны этапы работы с цифровыми доказательствами (их сбор, анализ, сохранение (документирование)), типичные программные и аппаратные средства для сбора и анализа цифровых доказательств.

Руководство NIST 800-86 оперирует понятием «цифровые доказательства», которые могут быть представлены файлами, логами, сетевыми данными и прочими цифровыми артефактами, оставляемыми в результате действий пользователей или систем. Понятие «цифровые следы» не является в США официально признанным термином в рамках таких документов, поэтому оно не применяется, хотя подразумевается в контексте анализа цифровых доказательств. Цифровые следы можно считать частью тех данных, которые NIST 800-86 рассматривает как цифровые доказательства.

NIST 800-86 носит рекомендательный характер, правоохранительные органы могут его использовать, но этот документ не является основным или обязательным для них. Данное руководство разработано для более широкой аудитории, включая ИТ-специалистов, аналитиков по кибербезопасности и тех, кто занимается реагированием на киберинциденты в организациях.

Кроме того, зарубежные правоохранительные органы руководствуются законодательством и судебной практикой своих стран, исходя из чего у них могут быть установлены конкретные требования к процессу сбора и обработки цифровых следов (цифровых доказательств).

Необходимо отметить, что в документах Федерального бюро расследования и других правоохранительных органов США термин «цифровые доказательства» («digital evidence») используется для обозначения всех видов информации, получаемой с цифровых устройств или в результате интернет-деятельности. В Великобритании в контексте практических руководств по сбору и анализу доказательств термин «цифровые доказательства» заменил термин «электронные доказательства» («electronic evidence»); он является более актуальным и предпочитаемым в официальных документах, стандартах и правоприменительной практике.

Российские исследователи, в свою очередь, отмечают, что Уголовно-процессуальный кодекс Российской Федерации «не предусматривает отдельного вида так называемых электронных или цифровых доказательств, оперируя термином «электронные носители информации» или «информация на электронных носителях»» [13, с. 65], при этом «отсутствие законодательного определения понятия «цифровое доказательство» не позволяет единообразно и четко определить сущность рассматриваемого понятия, а также перечень объектов, относящихся к нему, что в конечном итоге затрудняет практику применения цифровых следов в доказывании по уголовным делам» [16, с. 37].

Заключение

Цифровые следы становятся неотъемлемой частью современных криминалистиче-

[2] NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response. URL: https://csrc.nist.gov/pubs/sp/800/86/final (дата обращения: 18.10.2024).

ских исследований, что требует дальнейшего развития технико-криминалистических средств, приемов и методов их обнаружения, фиксации, изъятия и исследования в рамках соответствующего криминалистического учения. Необходимо продолжить формирование понятийно-терминологического аппарата в рамках цифровизации криминалистической и судебно-экспертной деятельности, а также регламентировать порядок работы с цифровыми следами (цифровыми доказательствами) прежде всего на уровне уголовно-процессуального закона, при этом обозначить критерии их достоверности и допустимости, а также на уровне подзаконных актов, например, разработать соответствующие регламенты (требования, правила) в федеральных органах исполнительной власти (Министерство внутренних дел, Федеральная служба безопасности, Следственный комитет Российской Федерации), предусматривающие среди прочего их техническую защиту и сохранение. В рамках оценки значимости криминалистической информации, содержащейся в цифровых следах, необходимо определение конкретного круга задач, решение которых возможно с использованием данных следов в рамках выявления, раскрытия, расследования и предупреждения отдельных видов преступлений. В целом криминалистическое учение о цифровых следах требует дальнейшего осмысления и развития.

СПИСОК ИСТОЧНИКОВ

1. Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193–202.

2. Теория информационно-компьютерного обеспечения криминалистической деятельности : монография / под ред. Е. Р. Россинской. М. : Проспект, 2022. 256 с.

3. Лузгин И. И. Цифровое следоведение как отрасль криминалистической техники // Вопросы криминологии, криминалистики и судебной экспертизы. 2023. № 2 (54). С. 11–17.

4. Цифровые следы преступлений : монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин; Следственный комитет Российской Федерации; Московская академия Следственного комитета Российской Федерации. М. : Общество с ограниченной ответственностью «Проспект», 2021. 168 с.

5. Жижилева А. А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы // Вопросы российской юстиции. 2019. № 3. С. 913–918.

6. Переверзева Е. С., Комов А. В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 172–178.

7. Перов В. А. Электронный след: понятие, виды, способы обнаружения и фиксации // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: материалы Всероссийской научно-практической конференции. М. : Московская академия Следственного комитета Российской Федерации, 2021. С. 103–106.

8. Логвинец Е. А., Каторгина Н. П. К вопросу о сущности и природе цифровых следов в криминалистике // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности : сборник научных статей по материалам международной научно-практической конференции / Академия управления МВД России. Часть 1. М. : Академия управления Министерства внутренних дел Российской Федерации, 2023. С. 267–275.

9. Соколова А. В. Трансформация понятийно-категориального аппарата криминалистики в условиях цифровизации // Санкт-Петербургский международный криминалистический форум : материалы международной научно-практической конференции. Санкт-Петербург : Санкт-Петербургский университет МВД России, 2024. С. 726–728.

10. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. ... док. юрид. наук. Волгоград : Волгоградская академия МВД России, 2008. 45 с.

11. Нестеров А. В., Сейтенов К. К. Общенаучная категория следа: судебно-экспертный аспект // Теория и практика судебной экспертизы. 2020. Т. 15. № 4. С. 98–105.

12. Себякин А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации : дис. ... канд. юрид. наук. М. : Московская академия Следственного комитета, 2021. 271 с.

13. Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 61–68.

14. Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 178–185.

15. Фролова Т. О. Применение программных средств и автоматизированных систем при исследовании объектов различных родов/видов судебной экспертизы: перспективы их развития // Политехнический молодежный журнал. 2023. № 5 (82). С. 1–10.

16. Абдразяпов Р. Р. Отдельные вопросы использования цифровых следов в доказывании по уголовным делам // Общество, право, государственность: ретроспектива и перспектива. 2024. № 1 (17). С. 34–40.

REFERENCES

1. Rossinskaya E. R. Theory of information and computer support for forensic activities: concept, system, basic patterns // Bulletin of East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. No. 2 (89). P. 193–202. (In Russ.)

2. Theory of information and computer support for forensic activities: monograph / edited by E. R. Rossinskaya. M. : Prospect, 2022. 256 p. (In Russ.)

3. Luzgin I. I. Digital investigation as a branch of forensic technology // Issues of criminology, forensic science and forensic examination. 2023. No. 2 (54). P. 11–17. (In Russ.)

4. Digital traces of crimes: monograph / A. M. Bagmet, V. V. Bychkov, S. Yu. Skobelin, N. N. Ilyin; Investigative Committee of the Russian Federation; Moscow Academy of the Investigative Committee of the Russian Federation. M. : Limited Liability Company «Prospect», 2021. 168 p. (In Russ.)

5. Zhizhileva A. A. On some theoretical aspects of the use of the concepts of digital, electronic, virtual traces in forensic science // Issues of Russian Justice. 2019. No. 3. P. 913–918. (In Russ.)

6. Pereverzeva E. S., Komov A. V. Virtual and digital traces: a new approach to understanding // Bulletin of St. Petersburg University of the Ministry of Internal Affairs of Russia. 2021. No. 1 (89). P. 172–178. (In Russ.)

7. Perov V. A. Electronic trace: concept, types, methods of detection and recording // Counteracting cybercrimes and crimes in the field of high technologies : materials of the All-Russian scientific and practical conference. M. : Moscow Academy of the Investigative Committee of the Russian Federation, 2021. P. 103–106. (In Russ.)

8. Logvinets E. A., Katorgina N. P. On the essence and nature of digital traces in forensic science // State scientific and technical policy in the field of forensic support of law enforcement activities : a collection of scientific articles based on the materials of the international scientific and practical conference / Academy of Management of the Ministry of Internal Affairs of Russia. Volume Part 1. M. : Academy of Management of the Ministry of Internal Affairs of the Russian Federation, 2023. P. 267–275. (In Russ.)

9. Sokolova A. V. Transformation of the conceptual and categorical apparatus of forensic science in the context of digitalization // St. Petersburg International Forensic Forum : Proceedings of the International Scientific and Practical Conference. St. Petersburg : St. Petersburg University of the Ministry of Internal Affairs of Russia, 2024. P. 726–728. (In Russ.)

10. Vekhov V. B. Forensic science doctrine of computer information and means of its processing : abstract. diss. ... Doctor of Law. Volgograd : Volgograd Academy of the Ministry of Internal Affairs of Russia, 2008. 45 p. (In Russ.)

11. Nesterov A. V., Seitenov K. K. General scientific category of trace: forensic aspect // Theory and practice of forensic examination. 2020. Vol. 15. No. 4. P. 98–105. (In Russ.)

12. Sebyakin A. G. Tactics of using knowledge in the field of computer technology in order to obtain forensically significant information : dis. ... Cand. of Law. M. : Moscow Academy of the Investigative Committee, 2021. 271 p. (In Russ.)

13. Bakhteyev D. V., Smakhtin E. V. Forensic features of the production of procedural actions with digital traces // Russian Law Journal. 2019. No. 6 (129). P. 61–68. (In Russ.)

14. Semikalenova A. I., Ryadovsky I. A. Use of special knowledge in detecting and recording digital traces: analysis of modern practice // Actual problems of Russian law. 2019. No. 6 (103). P. 178–185. (In Russ.)

15. Frolova T. O. Application of software and automated systems in the study of objects of various types/ kinds of forensic examination: prospects for their development // Polytechnical youth journal. 2023. No. 5 (82). P. 1–10. (In Russ.)

16. Abdrazyapov R. R. Certain issues of using digital traces in evidence in criminal cases // Society, law, statehood: retrospective and perspective. 2024. No. 1 (17). P. 34–40. (In Russ.)

Информация об авторе:
Хомяков Э. Г. – кандидат юридических наук.

Information about the author:
Khomyakov E. G. – Candidate of Law.

Статья поступила в редакцию 22.10.2024; одобрена после рецензирования 02.11.2024; принята к публикации 21.03.2025.

The article was submitted 22.10.2024; approved after reviewing 02.11.2024; accepted for publication 21.03.2025.