УДК 343.98

Кушнарев Александр Сергеевич
Уральский государственный юридический университет имени В.Ф. Яковлева
Институт прокуратуры
Россия, Екатеринбург
KUSHNAREV-02@LIST.RU
Kushnarev Alexander
Ural State Law University named after V.F. Yakovlev
Institute of Procuracy
Russia, Ekaterinburg

ЦИФРОВЫЕ СЛЕДЫ В КРИМИНАЛИСТИКЕ, ИХ ИСПОЛЬЗОВАНИЕ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация: автором в настоящей работе исследуется теоретическая проблема формулирования определения нового типа следа, образующегося в компьютерном пространстве. Приведены различные подходы к определению данного термина, рассмотрены сущностные характеристики таких дефиниций как «цифровой след», «виртуальный след», «компьютерный след». Изучена классификация цифровых следов. Рассмотрены сферы применения цифровых следов.

Ключевые слова: криминалистика, трасология, цифровой след, виртуальный след, цифровые технологии.

DIGITAL TRACES IN CRIMINALISTICS, THEIR USE IN CRIME INVESTIGATION

Annotation: in this paper the author studies the theoretical problem of formulating a definition of a new type of trace formed in computer space. Different approaches to the definition of this term are given, essential characteristics of such definitions as

"digital trace", "virtual trace", "computer trace" are considered. The classification of digital traces is studied. The spheres of application of digital traces are considered.
Key words: forensics, traceology, digital trace, virtual trace, digital technologies.

«Прежде чем спорить, давайте договоримся о терминах» - сей постулат французского мыслителя Вольтера представляется наиболее уместным для темы настоящей работы, ибо определение понятия «цифровой след» как прямо не закреплено в законодательстве, так и достаточно четко не определено в науке, различные трактовки дефиниции лишь подтверждают многоаспектность данного понятия.

Для начала отметим, что основу учений о следах в криминалистике составляет раздел трасологии. При этом учеными формулируются различные определения криминалистической трасологии. Так, Г.Л. Грановский пишет, что криминалистическая трасология представляет собой область криминалистического знания о следах, отражающих признаки внешнего строения следообразующих объектов, о механизме следообразования, а также о средствах, методах и приемах их обнаружения, фиксации, изъятия, сохранения и исследования в целях установления обстоятельств, имеющих значение для уголовного судопроизводства [5, с. 43]. В.Я. Карлов под криминалистической трасологией понимает отрасль криминалистической техники, изучающая закономерности образования материальных следов и разрабатывающая научно-технические средства, приемы и методы обнаружения, фиксации, изъятия и исследования следов с целью использования их для раскрытия и расследования преступлений [7].

Таким образом, можно заключить, что криминалистическая трасология представляет собой учение о следах, составляющее раздел криминалистической техники, в рамках которого разрабатываются теоретические основы следообразования в механизме совершения преступления, а также приемы и

методы обнаружения, фиксации, изъятия и исследования следов для раскрытия преступлений.

Для более подробного изучения темы настоящей работы представляется необходимым перейти к раскрытию первичной ячейки всего раздела трасологии, а именно понятия «след». Категория «след» является базовой в трасологии. Несмотря на основополагающий характер, данное понятие не находит единообразного толкования в науке и практике, что создает определенные предпосылки для использования соответствующей категории в различных смыслах. Как известно, каждое преступное посягательство, будучи «событием объективной действительности, вызывает разнообразные изменения в окружающей обстановке» [6]. Иными словами, взаимодействуя с окружающим миром, лицо, которым совершается противоправное посягательство, вносит в нее определенные изменения, тем самым оставляя следы.

С точки зрения науки криминалистики под следами преступления понимаются источники информации о событиях прошлого, деятельность относительно выявления, фиксации, исследования, оценки и использования следов-источников информации составляет путь расследования [13]. Г.Л. Грановский под понятием «след» понимает любое материальное отображение свойств вещей и явлений, позволяющее судить об их свойствах и использовать их отражение для решения идентификационных, диагностических, классификационных и интеграционных задач. При этом помимо материальных следов мы можем говорить и о запечатленных в памяти человека образах, неразрывно связанных с событием преступления, несущих в себе информацию о нем, так называемые – идеальные следы [16, с. 380].

Однако трасология изучает лишь определенные следы, которые могли бы объединяться общими закономерностями и предполагать некие общей методики для своего исследования (термин «следы» в узком смысле).

Сложность в трактовке соответствующей категории возникает в связи с тем, что при трасологической идентификации, следы рассматриваются в различных ракурсах и применительно к разным процессам, что обусловило возникновение множества основания классификации следов. Так, по критерию носителя информации выделяют материальные и идеальные следы [14]. Ряд авторов выдвигает гипотезу о существовании «цифровых» [12] следов, или же, как пишут другие специалисты, «компьютерно-технические» следы [2, с. 169]. Некоторые специалисты с учетом необходимости использования инновационных технологий в трасологии на основе анализа методических подходов заявляют о необходимости выделения самостоятельного раздела трасологии – цифровой трасологии [10]. Именно эти следы и станут дальнейшим предметом настоящей работы.

С появлением компьютерных технологий возникли новые виды преступлений и уже начиная с конца XX века криминалистами была затронута проблема формулирования понятия нового типа следа, образующегося в компьютерном пространстве и его места в общепризнанной классификации следов на материальные и идеальные.

Важно отметить, что вместе со стремительным развитием компьютерных технологий появилась и IT-сфера. Тем не менее, криминалистические возможности развиваются пропорционально развитию IT-сферы, посему в криминалистической теории наблюдается тенденция изучения тематики цифровых следов преступной деятельности в следующих направлениях:

- в узком направлении: предупреждение, раскрытие и расследование преступлений в сфере компьютерной информации (гл. 28 УК РФ): неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и др., которые в большинстве случаев являются предикатными для совершения (либо сокрытия) других преступлений

(хищений, распространения экстремистских материалов, фальсификации итогов голосования и др.).

- в широком направлении: противодействие киберпреступности (сфера высоких технологий), т.е. не только указанных выше преступлений, но и преступлений, совершенных с использованием IT-технологий. К ним можно отнести: доведение до самоубийства с использованием сети Интернет или склонение к самоубийству; дистанционные хищения в сфере финансов; призывы к осуществлению террористической, экстремистской деятельности, массовым беспорядкам; оборот наркотиков и оружия, порнографических материалов; организация азартных игр; преступления против половой неприкосновенности несовершеннолетних, фишинг, кража личных данных, информационная блокада, шпионаж, шантаж и прочее [1].

Стремительно развивающееся пространство компьютерных технологий, IT-технологий, появление новых принципов создания вычислительных систем (квантовые технологии) приводит к различным подходам в определении конкретного названия данного типа следов.

Ряд авторов (В.А. Мещеряков, А.Ю. Головин, В.Ю. Агибалов, А.Б. Смушкин) склоняются к использованию термина «виртуальный след», другие предлагают название «информационный след» (В.В. Борисов, Г.М. Шаповалова), третьи оперируют понятием «электронно-цифровой след» (В.Б. Вехов, А.В. Шебалин, В.В. Поляков). Существуют и иные, менее распространённые, названия интересующею дефиниции. Предлагается провести анализ наиболее универсальных и часто используемых понятий.

Родоначальник понятия «виртуальный след» В.А. Мещеряков определял его как «любые изменения состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации

(т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе на электромагнитном поле» [11].

Иного мнения придерживается Б.В. Вехов, который дал определение понятию «электронно-цифровой след». Под данным термином автор понимает «любую криминалистически значимую компьютерную информацию т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [4]. Однако, справедливо было подмечено А.Н. Колычевой, которая в своей работе высказала положительное мнение о данном определении В.Б. Вехова, но посчитала необходимым внести корректировки по причине «синонимического дублирования» (электронно-цифровой след и электронно-цифровая форма) [9]. При этом остается открытым вопрос о необходимости в подразделении электронно-цифровых следов на следы, образующиеся в компьютерных системах, и следы, находящиеся, в информационно-телекоммуникационной сети Интернет, так как сеть Интернет выступает в роли средства передачи информации, поскольку является системой сетей связи и совокупности технических средств, объединяющей компьютерные системы. На мой взгляд, с учетом необходимости данного подразделения термина «электронно-цифровой след», а также в целях избежания дублирования термина и определения, остановиться на понятии «цифровой след». Наиболее удачно, на мой взгляд, сформулировать определение термина «цифровой след» получилось у А.А. Бесонова, который понимает под цифровыми следами информацию, зафиксированную в цифровом формате, содержащуюся в электронно-вычислительных машинах и иных цифровых устройствах, созданных на основе их технологий, в средствах подвижной радиотелефонной связи и на различных носителях цифровой

информации, причинно-связанная с событием преступления, позволяющая установить обстоятельства совершенного преступления и преступника» [3].

Итак, предлагается выделить наиболее сущностные признаки цифровых следов:

- являются одной из объективных форм существования компьютерной информации;

- невозможность существования без материального носителя, что указывает на его опосредованность другим устройством, предметом и т. д.;

- удобство в копировании, поскольку данное действие можно совершать неограниченное количество раз без ущерба его объему и содержания;

- гибкость, выражающаяся в возможности изменения формы следа (например, скриншот может преобразоваться в распечатанный документ);

- обезличенность, поскольку идентификация автора, пользователя или владельца является трудоемким и не всегда приводящим к положительному результату процессом;

- 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.

На сегодняшний день с учетом большого массива имеющейся информации о цифровых следах мы можем говорить и о их криминалистической классификации. Так, в зависимости от формы носителя выделяют цифровые следы, расположенные на оптических носителях (CD, DVD, blu-ray диски и пр.), полупроводниковых носителях (флеш-накопители, SSD и магнитные носители).

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.

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), исследование же следов второй группы требует использования специальных знаний (как правило, производства компьютерно-технических исследований).

Наконец, по месту их 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.

Велико значение цифровых следов при расследовании преступлений [15]. Так, например, при расследовании преступлений следователь может обратиться к различным сервисам, будь то Google Maps, система навигации Яндекс и др. В хронологии на Google Maps можно посмотреть маршруты, а также места, в которых побывал подозреваемый: эта информация определяется на основе истории местоположений. Ее можно изменить или удалить в хронологии (в том числе за целые периоды). Такая хронология видна только пользователю и доступна как на мобильных устройствах, так и на компьютере. Такая же система постоянной геолокации с возможностью записи всех перемещений доступна пользователям Apple. Разумеется, все данные, сохраненные в истории пользователя, являются конфиденциальными и могут быть использованы для получения дополнительной информации только с согласия пользователя. Но в тех случаях, когда речь идет о получении сведений от свидетеля или потерпевшего и интересы подозреваемого и следователя совпадают, психологическая составляющая, которая являлась основой для формирования событий в памяти допрашиваемого, становится ненужной, поскольку электронно-цифровые следы имеют более веское доказательственное значение: их невозможно подделать, сфальсифицировать или иным образом зафиксировать помимо воли лица, чьи показания могут быть использованы в качестве доказательств по уголовному делу. Автомобильные навигаторы имеют

функцию записи истории перемещений автомобиля, так называемых треков. Данная информация может быть записана в истории в тех случаях, когда эта функция активирована в настройках устройства. Некоторые пользователи фиксируют конечную точку своего маршрута или посещаемые места, для того чтобы в следующий раз не искать их на карте и не вводить координаты заново. Причем если был осуществлен вход в аккаунт, то и на другом устройстве, например в сервисах "Яндекс", происходит авторизация пользователя по логину и паролю, и все настройки становятся доступными, в том числе и треки с фиксированными маршрутами и конечными пунктами.

Неоценимую услугу могут оказать электронно-цифровые следы при проверке алиби. В тех случаях, когда подозреваемый или обвиняемый выдвигает алиби, следователь обязан провести проверку всех обстоятельств, указанных подозреваемым или обвиняемым для решения вопроса по существу, поскольку от этой проверки может зависеть дальнейшее развитие следственной ситуации, которая из благоприятной может быть переведена в неблагоприятную для следствия или дознания. В данном случае лицо, которое заявляет о наличии алиби, также заинтересовано в том, чтобы проверка прошла с благоприятным для него исходом, поэтому добровольно предоставляет всю имеющуюся в его распоряжении информацию о своих перемещениях, зафиксированных на электронных устройствах.

В последнее время широкое распространение получили различные социальные сети, мессенджеры и т.п., которые также фиксируют информацию о времени посещения и о материалах, там размещаемых. Даже простое фотографирование или видеосъемка с помощью смартфона не только дают представление о месте и времени сделанного снимка или видеофайла, но также автоматически привязывают файл к месту фотографирования, что в последующем может оказать неоценимую услугу в раскрытии и расследовании преступлений.

Дополнительные сведения также можно получать из мобильных приложений, в частности из банковских сервисов. Банковские транзакции с указанием времени перевода и переводимых сумм, а также магазинов, в которых производилась оплата, помогут восстановить ассоциативные связи в памяти допрашиваемого с событиями, датами и др.

В последнее время тенденция динамики увеличения количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий постоянно прогрессирует [8, с. 110]. Видится, что совершенствование данной отрасли в условиях активного развития возможностей сети Интернет, новейших технологий, криминалистической техники, новых способов совершения преступлений, будет способствовать не только развитию отдельных теоретических положений криминалистической науки, но положительно отразится на практическом использовании данных знаний при раскрытии и расследований преступлений.

В будущем использование цифровых следов преступлений, вероятно, станет еще более распространенным и важным, поскольку технологии продолжают развиваться и становятся все более интегрированными в нашу повседневную жизнь. Это означает, что цифровые следы преступлений будут становиться все более важным аспектом уголовных расследований, и криминалисты должны быть готовы эффективно использовать их в качестве доказательств. Поэтому понимая и принимая преимущества и недостатки данного явления, криминалисты могут эффективно использовать цифровые следы в качестве улик в уголовных расследованиях и быть в курсе последних достижений в области технологий и преступности.

Для того чтобы эффективно использовать цифровые следы преступлений в качестве доказательств, важно, чтобы криминалисты и правоохранительные органы работали сообща. Криминалисты могут предоставить необходимые знания и опыт о природе и использовании цифровых следов в уголовных

расследованиях, в то время как правоохранительные органы могут предоставить необходимые ресурсы для сбора, хранения, анализа и обработки цифровых следов.

Важно признать, что цифровые следы преступления не являются заменой традиционным формам доказательств. Скорее, они являются дополнительным инструментом, который может предоставить ценную информацию и помочь в расследованиях. Наиболее эффективным способом расследования является комбинация традиционных и цифровых доказательств, для получения полной картины преступления и построения убедительной доказательной базы.

Список литературы:

1. Бахтеев Д.В. Криминалистическая классификация цифровой доказательственной информации // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сб. статей Междунар. науч.-практ. конф. М.: Академия управления МВД России, 2018. С. 44–49.

2. Бессонов А.А. Информация о типичных следах преступления как элемент его криминалистической характеристики // Гуманитарные исследования. 2014. № 4 (52). С. 169-174.

3. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О. Е. Кутафина. 2019. №3 (55). URL: https://cyberleninka.ru/article/n/o-nekotoryh-vozmozhnostyah-sovremennoy-kriminalistiki-v-rabote-s-elektronnymi-sledami (дата обращения: 06.04.2024).

4. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. С. 401.

5. Грановский Г.Л. Основы трасологии. М.: Мир, 2017. 43 с.

6. Дягилева М.В. Значение криминалистических следов в уголовном процессе // Universum: экономика и юриспруденция. 2022. № 4 (91). С. 10-12.

7. Карлов В.Я. Криминалистика: тезаурус-словарь и схемы: учебное пособие. М.: Альфа-Пресс, 2011. 272 с.

8. Кирсанова С.О., Калинина А.А. Виртуальные следы: понятие, сущность, проблемы // Вопросы студенческой науки. № 3(19). Март, 2018. С. 110.

9. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. - Москва, 2019.-С. 10.

10. Майлис Н.П. Нетрадиционные виды следов, используемые в раскрытии и расследовании преступлений // Эксперт-Криминалист. 2018. N 3. С. 35-36.

11. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков // Издательство Воронежского государственного университета. 2002. № 3. 104 с.

12. Рахимов А.И. Идеальные следы преступления и их классификация // Гуманитарные, социально-экономические и общественные науки. 2022. № 3. С. 150-152.

13. Россинская Е.Р. Настольная книга судьи: судебная экспертиза. М.: Проспект, 2020. 464 с.

14. Рясов А.А., Гонтарь С.Н. К вопросу о классификации трасологических следов // Мир науки, культуры, образования. 2014. № 5 (48). С. 306-308.

15. Сажаев А.М., Мишуточкин А.Л. Значение электронно-цифровых следов в тактике допроса свидетелей и потерпевших // Расследование преступлений: проблемы и пути их решения. 2022. № 3.

16. Торбин Ю.Г. Учение о следах преступления в работах учёных криминалистов и процессуалистов XIX и XX веков // Военное право. 2017. № 1 (41). С. 379-391.