Список литературы

1. Вилкова Т. Ю., Масленникова Л. Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу // Вестник Пермского университета. Юридические науки. 2019. Вып. 46. С. 728–751.

2. Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5 (150). URL: https://cyberleninka.ru/article/n/ugolovnoe-sudoproizvodstvo-i-tsifrovye-tehnologii-problemy-sovmestimosti (дата обращения: 16.09.2022).

3. Ищенко П. П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex Russica. 2019. № 12 (157). URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-tsifrovizatsii-dosudebnogo-proizvodstva-po-ugolovnym-delam (дата обращения: 16.09.2022).

4. Качалова О. В. Уголовно-процессуальные проблемы информатизации современного уголовного судопроизводства // Российское правосудие. 2019. № 2. С. 95–98.

А. А. Черноперов,
старший преподаватель,
Санкт-Петербургская академия
Следственного комитета Российской Федерации

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЛЕДОВ В ДОКАЗЫВАНИИ

Аннотация. Статья посвящена определению нового понятия «цифровой след» в криминалистике. Автором с практической точки зрения оценивается значение поиска, выявления, фиксации, изъятия и исследования следов, возникающих при взаимодействии цифровых систем, обосновывается необходимость введения нового термина и приводится одна из формулировок термина «цифровой след». В статье приведены анализ значения использования цифровых следов в доказывании по уголовным делам, способы определения владельца информации и носителей информации, а также способы объективации процесса доказывания через визуализацию цифровых данных.

Ключевые слова: цифровая криминалистика, цифровой след, цифровая информация, электронный носитель информации, владелец информации, объективация доказывания, визуализация

THE USE OF DIGITAL TRACES IN THE INVESTIGATION

Abstract. The article is devoted to the definition of a new concept of “digital footprint” in criminology. From a practical point of view, the author evaluates the importance of searching, identifying, fixing, removing and investigating traces arising from the interaction of digital systems, justifies the need to introduce a new term and provides one of the formulations of the term “digital footprint”. The article provides an analysis of the importance of using digital traces in proving criminal cases, ways to

determine the owner of information and information carriers, as well as ways to objectify the proof process through the visualization of digital data.

Keywords: Digital forensics, Digital footprint, Digital information, Electronic media, Owner of information, Objectification of evidence, Visualization

В соответствии с данными статистики, которые приводит в своей статье Председатель Следственного комитета Российской Федерации А. И. Бастрыкин, «…в 2019 году выявлено 8 812 таких преступлений, в 2020–11493 (+30,4 %), в 2021–12112 (+5,4 %). При этом качество проводимых Следственным комитетом расследований находится на стабильно высоком уровне, а общий объем раскрытых и расследованных преступлений в сфере ИКТ растет пропорционально повышению числа зарегистрированных правонарушений» [1. С. 4]. При расследовании указанной категории преступлений правоприменители сталкиваются с отсутствием единого определения новых явлений, происходящих в сфере информационно-коммуникационных технологий, необходимостью разработки новых методик производства следственных действий при расследовании преступлений указанной категории.

Сразу же необходимо оговориться, что, как и в любой другой недавно возникшей и активно развивающейся отрасли, в информационных технологиях происходит формирование терминологического аппарата и можно встретить разные определения одних и тех же явлений и процессов. Например, понятие «цифровой след» в криминалистике и информационной безопасности имеет абсолютно разные, не связанные значения.

В информационной безопасности значение этого термина узкое и связано только со злонамеренными действиями во время компьютерных инцидентов. В криминалистике же значение этого термина намного шире и включает в себя (об этом мы поговорим позже) все виды взаимодействия. То же можно сказать и о значении терминов в программировании, разработке сценариев и алгоритмов. Поэтому, чтобы избежать неопределенности и ошибочных выводов, договоримся, что в рамках данной статьи будет использоваться только криминалистическим значением терминов.

Итак, что же такое «цифровой след»? «След» является ключевым понятием криминалистики. Первые попытки поиска преступников предпринимались нашими предками как раз через поиск следов. Первыми «криминалистами» были охотники-звероловы, которые из поколения в поколение передавали навыки поиска следов животных и определения по ним давности образования следов, направления движения, размеров зверя и другой информации, важной для удачной охоты. Именно следопыты искали воров и убийц по их следам. Корень «след» содержат такие слова как «следователь», «исследовать» и другие.

В науке криминалистики след является системообразующим понятием, на основе которого строится ее понятийный аппарат и терминология.

Чем дальше развивается наука, тем больше видов следов появляется в криминалистике. Если в конце XIX в. интерес для криминалистов представлял только рисунок папиллярных узоров в следе руки, то в конце XX в. этот след изучался уже не только как рисунок, но и как носитель уникальной информации на молекулярном уровне.

С позиций теории отражения подготовка, совершение и сокрытие любого преступления, в том числе и компьютерного, как и любое другое событие в материальном

мире, всегда вызывает изменения в окружающей среде. Такие изменения и являются следами. Следы возникают всегда, когда происходит взаимодействие двух и более объектов. Что касается взаимодействия физического, то следы такого взаимодействия очевидны и бесследно оно не проходит. При этом объект, который оставляет следы (отражаемый), например, монтировка, использованная для взлома, называют следообразующим. Второй же объект (отражающий), несет на себе как информацию об отражаемом объекте (размеры, форма окончания), так и информацию о способе взаимодействия (удары или давление). Второй объект называют следовоспринимающим.

Следует помнить, что отражаемый объект выступает в то же время и отражающим (частицы краски от косяка на монтировке, кровь потерпевшего на ноже и так далее).

В информационной среде взаимодействие происходит между двумя и более устройствами, результатом которого является изменение информации, хранящейся на каждом из них. Причем, у следов взаимодействия в информационной среде также есть материальная форма, которая выражается в физических устройствах, на которой постоянно или временно хранится изменяемая информация.

Следы, образовавшиеся в результате взаимодействия электронных устройств, наравне со следами взаимодействия преступника с элементами устройства и вещной обстановки места происшествия относятся к объективным следам и должны быть выявлены, изъяты, подвергнуты экспертному исследованию и использованы в доказывании наряду с субъективными доказательствами (показания потерпевшего, свидетелей, иных лиц).

При этом особенности формирования и сохранения следов в электронной среде выделяют их из всей массы криминалистически значимых следов, что потребовало их выделения в отдельный класс – цифровых следов.

Одним из авторов и редактором первого в нашей стране учебника по цифровой криминалистике В. Б. Веховым дается следующее определение указанной группы следов. «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 (прим.1 к ст. 272 УК РФ). Эти следы являются материальными невидимыми следами» [3. С. 97].

Поиск цифровых следов, так же, как и следов материального взаимодействия, строится на основе процесса моделирования. В качестве примера можно привести модель рабочего дня среднестатистического горожанина.

Если мысленно прожить свой обычный день, выделяя моменты, когда наши действия инициируют появление цифровых следов, то получится весьма внушительный объем. Даже если у вас не установлена система «Умный дом» или ее элементы (та же интерактивная колонка), информационные технологии всегда сопровождают вас. Например, смартфон (телефонная книга, журналы вызовов, протоколы соединений, логи систем геопозиционирования).

Итак, проснувшись по будильнику (положение с «включено» изменилось на «выключено», включили телевизор (как минимум – изменятся настройки громкости, номер канала, а если это смарт-ТВ, то останется много больше следов), даже микроволновая печь и кофеварка могут иметь цифровое управление и в их памяти также останется след о вас).

За пределами квартиры вы с большой вероятностью попадете в объектив камер отдельных систем видеонаблюдения (от камеры в лифте и на подъезде до видеорегистраторов в автомобилях) или комплексных систем, таких как «Безопасный город».

Оплатив проезд в общественном транспорте или платную парковку банковской картой или приложением на смартфоне, вы также вы также вносите изменения в информационные системы. Пройдя через турникет по пути на работу или учебу, вы снова оставляете след.

С использованием служебной офисной техники ситуация аналогична (компьютеры, карты памяти, сети).

Путь с работы, посещение торговых центров, иных организаций – это все будет сопровождено появлением новых цифровых следов.

Досуг сегодня также связан с использованием цифровых технологий. Посмотрев фильм, просмотрев новости или поиграв в компьютерные игры, вы снова оставляете следы. Умный браслет даже за качеством вашего сна следит!

Как уже говорилось выше, криминалистическое значение имеет вся совокупность следов. В то же время, важно помнить о принципе достаточности. При расследовании преступления необходимо на основе модели произошедшего определять каждый раз, какой объем носителей информации и устройств необходимо исследовать, чтобы собрать достаточное количество информационных следов для установления важных по делу обстоятельств.

В этом процессе важно избежать двух крайностей: с одной стороны – не утонуть в море второстепенной или вовсе ненужной информации, с другой – не упустить важные детали.

Далее кратко проанализируем способы поиска цифровых следов, применяемых сегодня в следственной практике и способах их объективации, легитимации и использования в доказывании по уголовным делам, в том числе, при рассмотрении уголовного дела судом с участием присяжных заседателей.

Учитывая огромное количество возможных цифровых следов необходимо их, прежде всего, классифицировать. В качестве одного из критериев классификации может быть использовано определение того, связан ли этот след непосредственно с объектом преступного посягательства (защищаемая информация) или с орудием совершения преступления (подготовленное специальным образом устройство, которое обеспечило злоумышленнику доступ в защищаемую систему), или такие следы возникли в связи с совершенным преступлением, но ни к орудию преступления, ни к объекту преступного посягательства отношения не имеющие (журнал WI-FI-роутера, который зарегистрировал сотовый телефон преступника в непосредственной близости к месту преступления).

К первой категории мы можем отнести статистическую информацию о деятельности предприятия, направленную ранее в подразделения Инспекции по налогам и сборам. Сюда же относятся данные с камер видеонаблюдения, в зону обзора которых попало место происшествия и пути подхода/отхода преступника.

Во вторую категорию входит вся информация, созданная в результате активных действий лица, совершившего преступление, в ходе подготовки к его совершению (получение несанкционированного доступа в систему), непосредственно во время

совершения преступления (изменение, копирование и удаление данных), а также сразу после совершения, с целью сокрыть следы преступления (очистка системных журналов, удаление следов присутствия в системе и другое).

В третью группу входят следы, связанные с объектом посягательства (фальсифицированные данные бухгалтерского и иных учетов, измененные персональные данные, взломанные защитные программные средства и другие).

В любом случае, поиск цифровых следов начинается с построения следователем (желательно с участием специалиста в области компьютерной информации) мысленной модели произошедшего, которая должна включать все три стадии преступного поведения (подготовка, совершение, сокрытие следов).

С учетом построенной модели проводятся следственные действия, начиная с неотложных, направленных на исключение возможности утраты имеющихся следов. При производстве всех следственных действий, связанных с изъятием носителей информации должен присутствовать специалист в области компьютерной техники.

Фиксация обнаруженных цифровых следов должна производиться в максимально короткий срок, так как данные могут быть изменены, модифицированы. В протоколах следственных действий обязательно указывается время копирования информации, а также системное время устройства, с которого производится изъятие.

В протоколе следственного действия кроме того указываются следующие сведения: устройство, в котором обнаружены виртуальные следы; собственник устройства (если установлен); владелец информации (может отличаться от собственника, если такой установлен), наличие у устройства возможности подключения к сети Интернет или иным телекоммуникационным и локальным сетям и следы такого подключения.

Отдельно должна быть описана операционная система, под управлением которого находится устройство (семейства Windows, Linux, MAC-OC, Android). Должны быть указаны признаки неправомерности использования программного обеспечения, к которым могут относиться наличие программных средств обхода активации, отсутствие фирменных наклеек на корпусе устройства, использование операционной системы MAC-OC на устройствах, произведенных не Apple.

Изъятие обнаруженного цифрового следа и одновременно его фиксация проводятся при обязательном участии специалиста в области компьютерной техники. Наиболее предпочтительным является изготовление специалистом полного образа (виртуальной копии, изготавливаемой с помощью специального программного обеспечения или даже специальных аппаратных средств) осматриваемого носителя информации и производство манипуляций в дальнейшем уде с полученным образом.

После того как цифровой след обнаружен, его, как и другие следы преступления, необходимо подробно описать в протоколе соответствующего следственного действия и изъять. Описание цифрового следа подразумевает знание основ функционирования операционной системы и программного обеспечения, при использовании которого обнаруженный цифровой след возник. Данные сведения может сообщить следователю специалист, участвующий в следственном действии или привлекаемый к участию в уголовном деле.

Изъятие предварительно зафиксированных цифровых следов производится двумя способами: с изъятием устройства – носителя информации (например, компьютера) и с копированием цифровых следов на иные носители.

Важным вопросом является установление владельца изымаемой информации и владельца носителя информации, на котором она была обнаружена. На практике часты ситуации, когда информация хранится пользователями на арендуемом оборудовании, для архивирования данных используются внешние data-центры и так далее. Кроме того, на устройстве подозреваемого может быть обнаружена похищенная или незаконно распространяемая информация, автором и владельцем которой он не является. В целях решения ряда вопросов необходимо связать информацию, носитель информации и владельца информации и носителя данной информации.

Существует несколько способов, которыми можно решить обозначенную задачу:

– владелец устройства и информации участвует в следственном действии и явно указывает (в протоколе следственного действия или отдельном заявлении), что изъятое принадлежит ему, и он готов предоставить подтверждающие это документы;

– в ходе следственного действия или других следственных действий обнаружены документы, в которых прямо поименован конкретный владелец устройства и информации;

– в самих изымаемых данных, а также на устройстве, с которого или с которым они изымаются, имеются сведения, указывающие прямым или косвенным образом на владельца (хранящиеся или ранее удаленные файлы изображений и видеозаписей владельца, идентификатор носителя, на который сохранена информация обнаружен в памяти устройства, принадлежащего конкретному человеку и так далее);

– экспертным путем (автороведческая, трасологическая, генетическая экспертизы и заключения специалистов).

Современные реалии уголовного судопроизводства диктуют необходимость придавать процессу обнаружения, исследования и изъятия доказательств и им самим максимально наглядную форму. В уголовном деле должны содержаться сведения в форме, доступной для восприятия лицами, не обладающими техническим образованием и в форме, доступной для восприятия обывателями с минимальным запасом знаний (присяжные заседатели). Таким образом, мы подошли к следующему разделу лекции – легитимация и объективация доказательств. С данными понятиями вы уже встречались в курсе уголовно-процессуального права (уголовного процесса), однако есть необходимость кратко остановиться на них применительно к процессу использования цифровых следов в раскрытии и расследовании преступлений.

Представление доказательств в суде с участием присяжных имеет определенные отличия от процедуры рассмотрения дела профессиональным судьей. Помимо общих требований, предъявляемых законом к доказательствам: относимости, допустимости и достоверности, – доказательства должны представляться присяжным в максимально понятной для них форме и в объеме, достаточном для формирования необходимого представления о деле и вынесения вердикта. Государственный обвинитель путем представления доказательств должен убедить коллегию в правильности своих выводов, склонить присяжных на свою сторону, сделать их своими единомышленниками.

Для успешного выполнения этой работы, учитывая специфику состава суда и психологические особенности восприятия присяжными заседателями обстоятельств исследуемого события, прокурор должен уметь владеть психологическими

приемами убедительной речи, позволяющими установить с присяжными тесный контакт, вызвать интерес и доверие к себе и своему выступлению.

Для присяжных заседателей представляемые прокурором доказательства должны быть очевидными для восприятия, понятными по содержанию и «прозрачными» по источнику их происхождения.

Указанные рекомендации можно воплотить в жизнь, применяя технические средства в суде (визуальный ряд, слайды, схемы, заслушивание показаний свидетелей, потерпевших, обвиняемых с применением аудио-, видеозаписи и другое).

Опыт поддержания обвинения по такой категории дел показывает, что у присяжных заседателей куда больший интерес вызывает использование в суде, при осуществлении процесса доказывания, элементов наглядности. И, наоборот, при малейшем сомнении в качестве проведенного предварительного расследования или в случае непонимания изложенных им обстоятельств, присяжные выносят оправдательный вердикт. Как правило, сложности доказывания возникают по многоэпизодным и групповым уголовным делам, а также делам экономической направленности, когда от присяжных требуется наличие не только жизненного опыта и здравого смысла при принятии решений, но и специальных познаний в различных сферах человеческой деятельности. Нехватка и сложность понимания поступающей к присяжным от сторон процесса значимой информации вызывают у них внутреннее смятение и неуверенность в правоте обвинения.

Одним из способов объективации доказательств, полученных на основе цифровых следов, является их визуализация. Визуализация данных – это наглядное представление массивов различной информации.

Существует несколько типов визуализации, отличающихся по степени сложности, целевому назначению, функциям. Перечислим основные из них:

– обычное визуальное представление количественной информации в схематической форме. К этой группе можно отнести всем известные круговые и линейные диаграммы, гистограммы и спектрограммы, таблицы и различные точечные графики.

– данные при визуализации могут быть преобразованы в форму, усиливающую восприятие и анализ этой информации. Например, карта и полярный график, временная линия и график с параллельными осями, диаграмма Эйлера;

– концептуальная визуализация позволяет разрабатывать сложные концепции, идеи и планы с помощью концептуальных карт, диаграмм Ганта, графов с минимальным путем и других подобных видов диаграмм;

– стратегическая визуализация переводит в визуальную форму различные данные об аспектах работы организаций. Это всевозможные диаграммы производительности, жизненного цикла и графики структур организаций;

– графически организовать структурную информацию с помощью пирамид, деревьев и карт данных поможет метафорическая визуализация, например, схема Санкт-Петербургского метро;

– комбинированная визуализация подразумевает объединение нескольких сложных графиков в одну схему [2. С. 9].

Подводя итог проведенному исследованию, можно уверенно сказать, что современная криминалистика находится в стадии формирования учения о цифровых следах, нарабатывается понятийный аппарат, устанавливаются междисциплинарные связи.

Исследователи единодушны во мнении о необходимости введения новых терминов, уточнения определений ранее использовавшихся, устранения неоднозначного понимания в рамках разных дисциплин одних и тех же понятий.

Практическая же криминалистика уже сейчас работает с цифровыми носителями информации. Криминалисты трудятся над поиском наилучших способов выявления и фиксации цифровых следов, их исследования, объективации и использования в доказывании.

Список литературы

1. Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий, 2022. URL: //skspba.ru/course/index.php?categoryid=15.

2. Фалилеев В. А. Демонстрационный характер формирования доказательств, представляемых суду присяжных // Законность. 2017. № 8. с. 8–11.

3. Цифровая криминалистика: учебник для вузов / Вехов В. Б. [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. – Москва: Издательство Юрайт, 2022. – 417 с. – (Высшее образование). – ISBN 978–5–534–14600–4. – Текст: электронный //Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/497080.

4. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; ответственный редактор С. В. Зуев. – Москва: Издательство Юрайт, 2022. – 193 с. – (Высшее образование). – ISBN 978–5–534–13286–1. – Текст: электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/497476 (дата обращения: 19.08.2022).

5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

А. Ю. Чупрова,
доктор юридических наук, профессор,
Всероссийский государственный университет юстиции

ПРОБЛЕМЫ ОТВЕТСТВЕННОСТИ ЗА РАСПРОСТРАНЕНИЕ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ ЛИЧНЫХ ВИДЕОМАТЕРИАЛОВ ИНТИМНОГО ХАРАКТЕРА

Аннотация. Целью работы является исследование проблем уголовной ответственности за оборот личных материалов, содержащих действия сексуального характера, распространенных в виртуальном пространстве помимо воли лица. В статье проводится анализ объективных признаков и предмета рассматриваемой группы деяний, вопросов правовой оценки обращения подобных видеоматериалов в сети Интернет, раскрываются правовые подходы к их квалификации. В результате проведенного исследования были сделаны выводы о целесообразности внесения